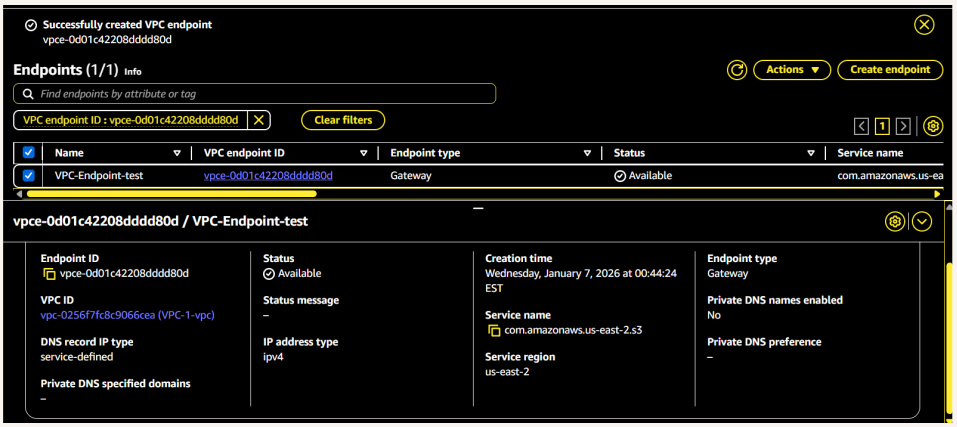
nextwork.org

VPC Endpoints

Michael K.



Michael K.
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) is alogicallyisolatedvirtualnetworkwithinAWSwhere i can launch and manage AWSresources(suchasEC2instances,RDSdatabases, and load balancers) using myowndefinedIPaddressrange,subnets,route tables, and network gateways.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to access Amazon S3 privately and securely without having to go through the Internet.

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

One thing I didn't expect in this project was the time i spent to understand how Endpoints work.

This project took me...

This project took me 4 hours.

Michael K.
NextWork Student

In the first part of my project...

Step 1 - Architecture set up

In this step, I will create a VPC from scratch, launch an EC2 instance, which i'll connect to using EC2 Instance connect later. Lastly, set up an S3 bucket.

Step 2 - Connect to EC2 instance

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

Step 3 - Set up access keys

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

Step 4 - Interact with S3 bucket

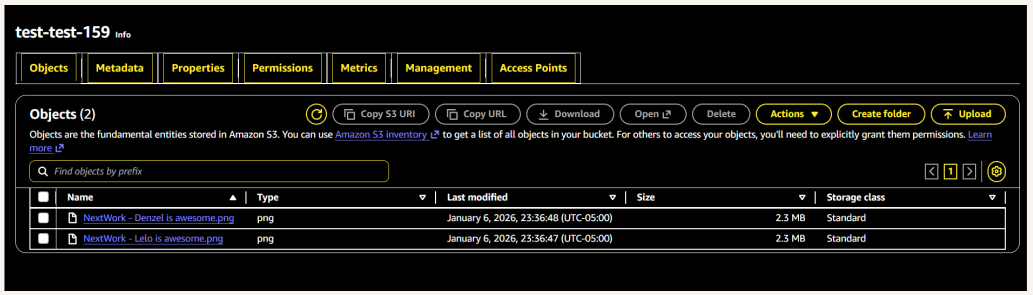
In this step, I will head back to my EC2 instance and get my EC2 instance to access my S3 bucket.

Michael K.
NextWork Student

Architecture set up

I started my project by launching a VPC, it's resources and an Instance in the VPC for the test.

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



Michael K.
NextWork Student

Access keys

Credentials

To set up my EC2 instance to interact with my AWS environment, I configured Access Key ID, Secret Access Key, the Region and the JSON output.

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

A Secret access keys is like the password that pairs with my access key ID (your username). I need both to access AWS services.

Best practice

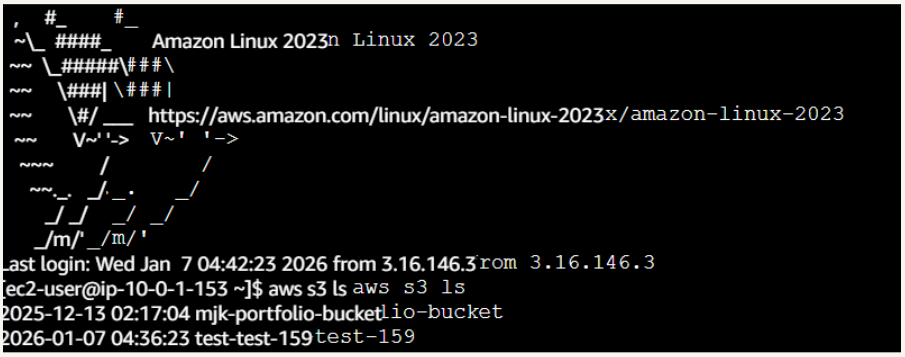
Although I'm using access keys in this project, a best practice alternative is to use an IAM role with the right permissions and attach it to the instance.

Michael K.
NextWork Student

Connecting to my S3 bucket

The command I ran was <<aws s3 ls>>.

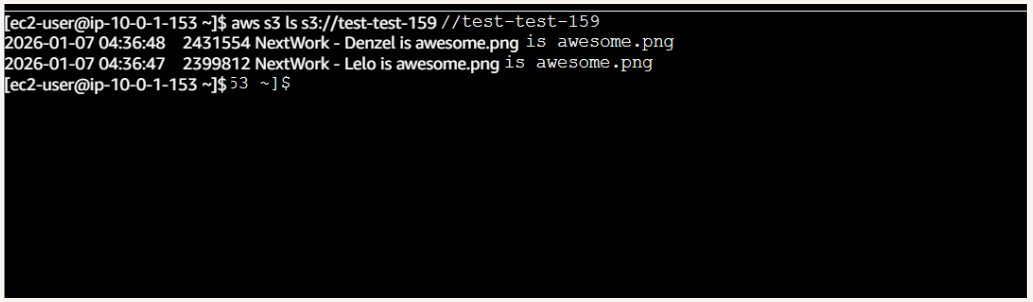
The terminal responded by listing the buckets found in my account after i re-typed the previous command. This indicated that the access keys I set up worked.



Michael K.
NextWork Student

Connecting to my S3 bucket

I also tested the command <<aws s3 ls s3://test-test-159>> which returned the objects in my bucket.



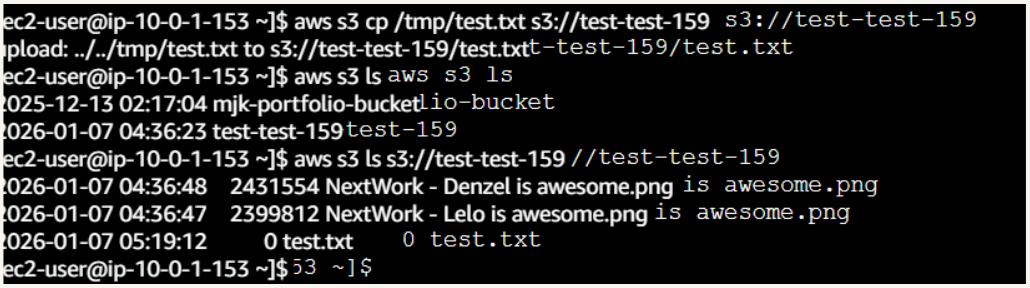
Michael K.
NextWork Student

Uploading objects to S3

To upload a new file to my bucket, I first ran the command <<sudo touch /temp/test.txt>>. This command creates the file in my instance.

The second command I ran was <<aws s3 cp /temp/test.txt s3://test-test-159>> This command will upload the file in my s3 bucket "test-test-159"

The third command I ran was <<aws s3 ls s3://test-test-159>> which validated that the file was now in my bucket.



Michael K.
NextWork Student

In the second part of my project...

Step 5 - Set up a Gateway

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

Step 6 - Bucket policies

In this step i'll limit my S3 bucket access's to only traffic from my endpoint.

Step 7 - Update route tables

In this step, I will Test your VPC endpoint set up and troubleshoot any connectivity issue if it pops up.

Step 8 - Validate endpoint conection

In this step, I will test my VPC endpoint set up (again) and restrict my VPC's acccess to my AWS environment.

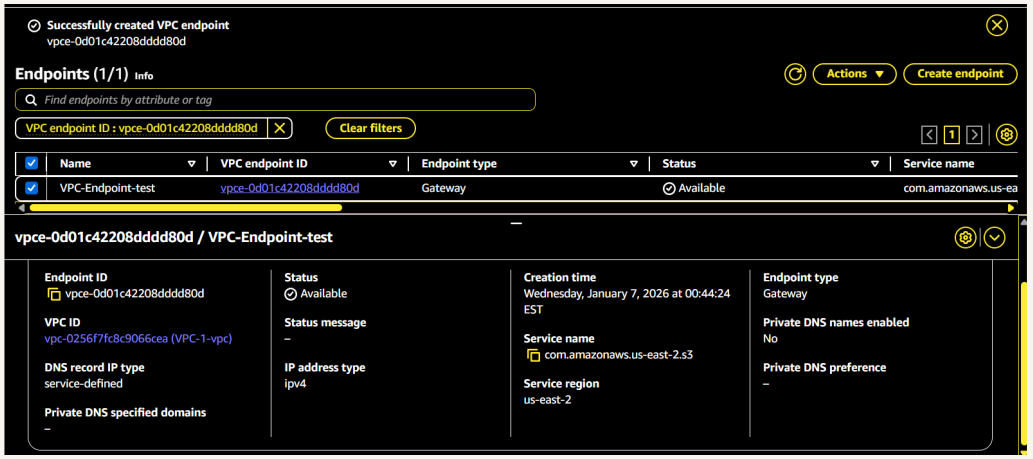
Michael K.
NextWork Student

Setting up a Gateway

I set up an S3 Gateway, which is a type of endpoint used specifically for Amazon S3 and DynamoDB (DynamoDB is an AWS database service). Gateways work by simply adding a route to my VPC route table that directs traffic bound for S3 or DynamoDB 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.



Michael K.
NextWork Student

Bucket policies

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

My bucket policy will deny 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 your VPC endpoint can get any access to your S3 bucket!

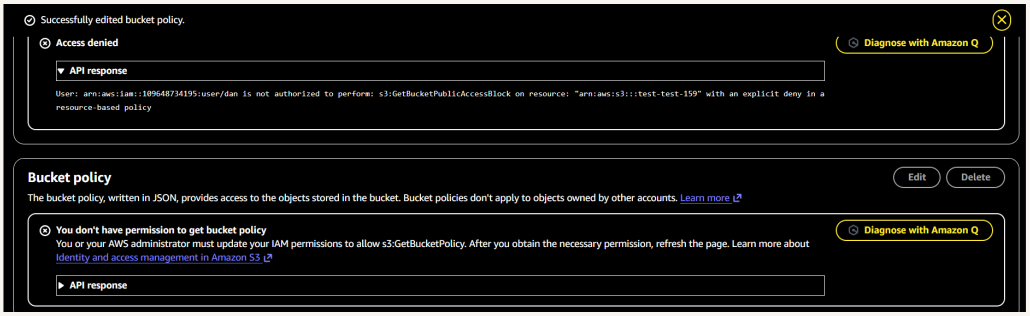
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::test-test-159",
        "arn:aws:s3:::test-test-159/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpce": "vpce-0d01c42208dddd80d"
        }
      }
    }
  ]
}
```

Michael K.
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 my VPC endpoint. This means any attempt to access my bucket from other sources, including the AWS Management Console, is blocked!

I also had to update my route table because i needed to add the gateway that will allow traffic to enter s3.

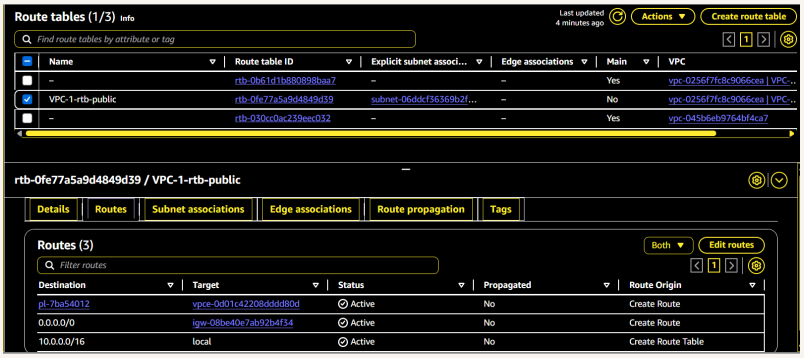


Michael K.
NextWork Student

Route table updates

To update my route table, I added the route table in the Endpoints route table section.

After updating my public subnet's route table, my terminal could return the list of objects in my bucket after runing <<aws s3 ls s3://test-test-159>>

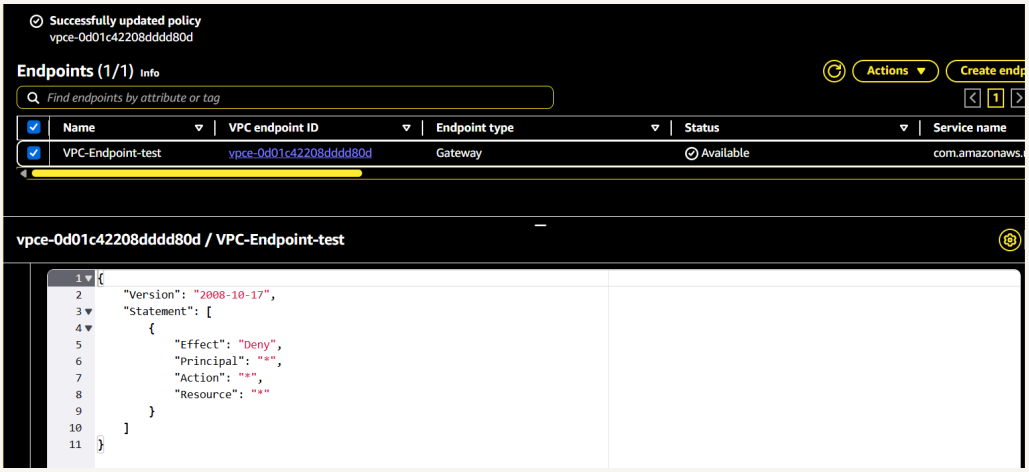


Michael K.
NextWork Student

Endpoint policies

An endpoint policy is one which determines and control access to s3 through the control of the Gateway.

I updated my endpoint's policy by changing the "Effect" to <<Deny>>. I could see the effect of this right away, because the gateway was blocked and i couldnt access s3 anymore.



The place to learn & showcase your skills

Check out nextwork.org for more projects