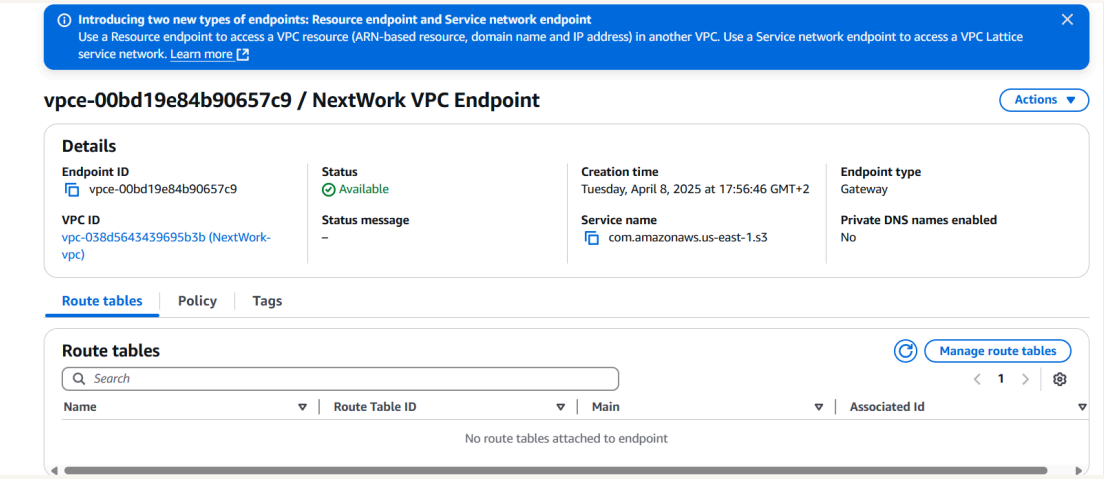
nextwork.org

VPC Endpoints

LW lwazi995@outlook.com



LW
lwazi995@outlook.com
NextWork Student
NextWork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is allows you to create a private network within AWS. It gives you control over IP ranges,subnets and security. Making it ideal for hosting secure applications and resources in a cloud environment.

How I used Amazon VPC in this project

In todays project we used VPC within our EC2 instance to allow access or deny access using our endpoints policy and implementing it through our S3 Gateway and buckets. This provides our VPC direct, private access.

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

I didn't expect the the error message I got when from the S3 bucket that denied access and only allowed it to a certain VPC.

This project took me...

The project in particular took me about 3 and half hours to complete.

LW
lwazi995@outlook.com
NextWork Student
NextWork.org

In the first part of my project...

Step 1 - Architecture set up

In this step we are setting up the foundations of this project (i.e. Launching VPC EC2 instant and S3 bucket) so that we can set up an Endpoint architecture and test it and test that set up in the last step of this project.

Step 2 - Connect to EC2 instance

In this step we are connecting directly to our EC2 using our EC2 connect this will help us access S3 and run commands later in the project.

Step 3 - Set up access keys

In this step I am going to give the EC2 instance access to your AWS environment. We can think of access keys almost like login details for EC2, Applications and non-humans to interact with our AWS services.

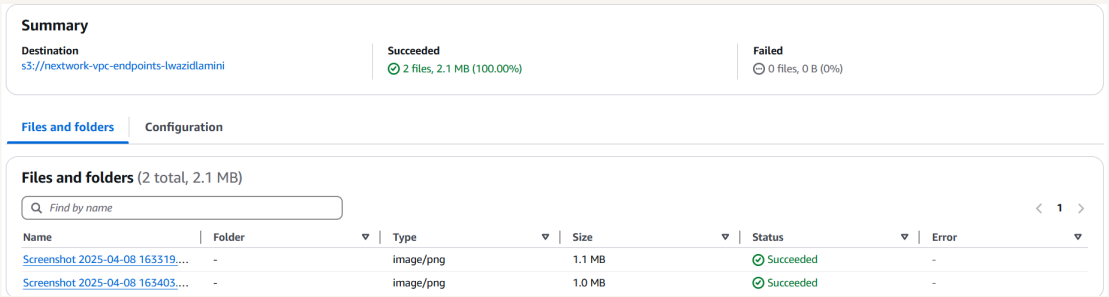
Step 4 - Interact with S3 bucket

In this step we are applying our access key credentials to our EC2 instance, and then using AWS CLI and our EC2 instance to access Amazon S3.

Architecture set up

I started my project by launching 3 key services a VPC,EC2 instance and S3 bucket.

I also set up my S3 bucket and added two files to the bucket from my local computer.



LW
lwazi995@outlook.com
NextWork Student

Access keys

Credentials

To set up my EC2 instance to interact with my AWS environment, I configured AWS Access key ID, The Secret Access key that matches the Access key ID, The Default region type and the Default Output Format.

Access keys are part of a credential! Your credentials are made up of a username and password; think of the access key ID as the username.

Secret access keys are like passwords in the context of access keys/credentials for our EC2 instance to get credentials to our AWS environment

Best practice

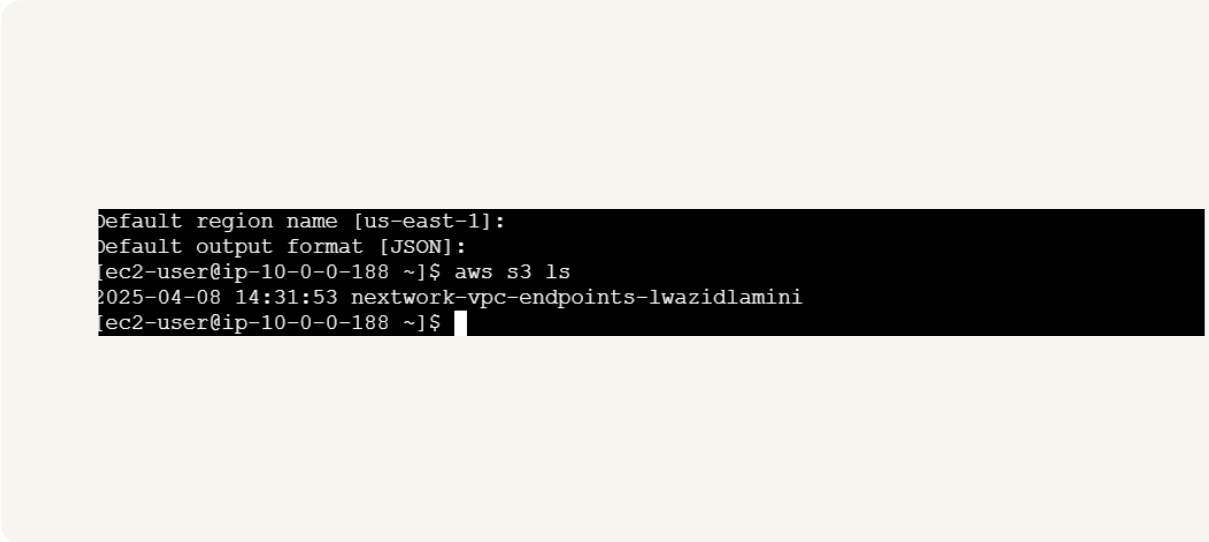
Although I'm using access keys in this project,Although I'm using access keys in this project IAM admin roles instead this means the neccessary permissions will be attached to an IAM role, then the role will be associated with the relevant resources

LW
lwazi995@outlook.com
NextWork Student

Connecting to my S3 bucket

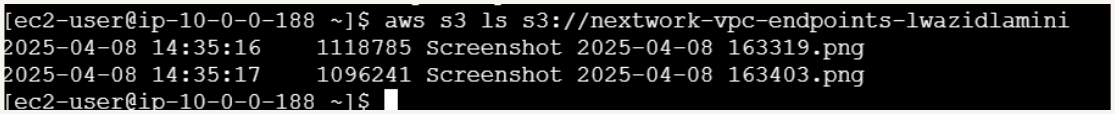
The command I ran was aws s3 ls. This command is used to list all buckets in an AWS account.

The terminal responded with The terminal responded with nextwork-vpc-endpoints-lwazidlamini This indicated that the access keys I set up were set up correctly and gives my EC2 Access to my AWS Account and environment.



Connecting to my S3 bucket

I also tested the command aws s3 ls s3://nextwork-vpc-endpoints-lwazidlamini which returned with the files inside the S3 bucket.



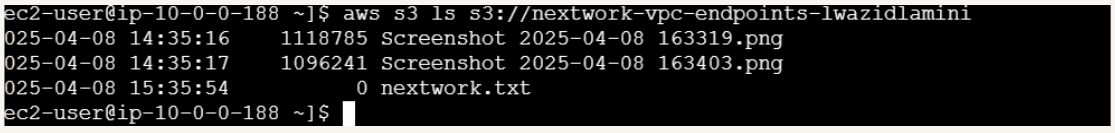
LW
lwazi995@outlook.com
NextWork Student

Uploading objects to S3

To upload a new file to my bucket, I first ran the command sudo touch /tmp/nextwork.txt This command creates an option to upload files into my my S3 bucket.

The second command I ran was aws s3 cp /tmp/nextwork.txt s3://nextwork-vpc-endpoints-lwazidlamini. This command will add the file network.txt into my S3 bucket using my EC2 instant command line.

The third command I ran was aws s3 ls s3://nextwork-vpc-endpoints-lwazidlamini which validated that the file has been loaded to the S3 bucket using the EC2 instant command line.



LW
lwazi995@outlook.com
NextWork Student

In the second part of my project...

Step 5 - Set up a Gateway

In this step I am going to be setting up a VPC endpoint so that commuication between our VPC and other services (especially S3) is direct and secure

Step 6 - Bucket policies

In this step I am testing the endpoint connection by blocking off all traffic to our S3 bucket, except for traffic coming from our end point.

Step 7 - Update route tables

In this step we are testing our endpoint connection between our bucket and EC2 instance

Step 8 - Validate endpoint conection

In this step I am going to validate our VPC endpoint set up one more time. I am also going to use endpoint policies to restrict access our EC2 access to our AWS environment.

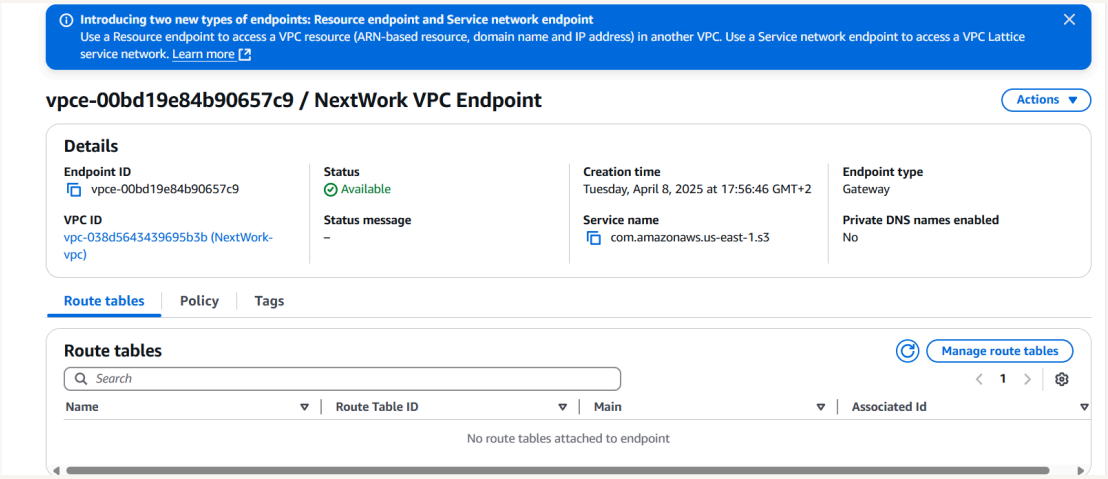
LW
lwazi995@outlook.com
NextWork Student

Setting up a Gateway

I set up an S3 Gateway, which is a type of end point specifically designed for Amazon S3 Gateway by updating the route table of associate subnets, so that S3 bound traffic goes through the Gateway instead of the internet.

What are endpoints?

An endpoint is VPC component that allows our VPC to have direct connection to AWS environment, so that traffic doesn't have to go through the public internet!



LW
lwazi995@outlook.com
NextWork Student

Bucket policies

A bucket policy is type of policy that has granular control over who has access to an S3 bucket, and what are the actions they can perform.

My bucket policy will deny traffic from all sources accept traffic coming from my VPC endpoint.

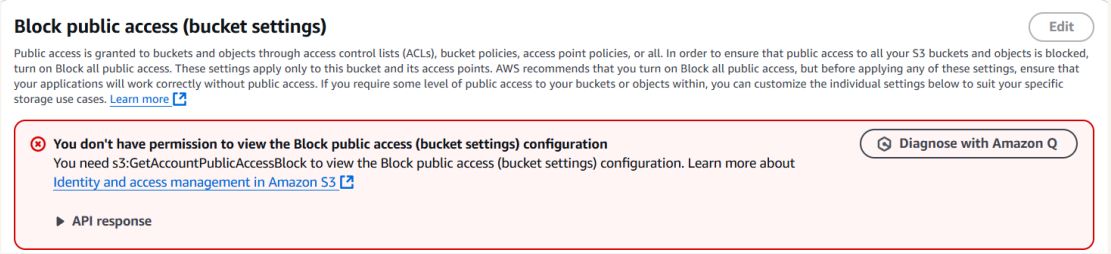
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::nextwork-vpc-endpoints-lwazidlamini",
        "arn:aws:s3:::nextwork-vpc-endpoints-lwazidlamini/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpce": "vpce-00bd19e84b90657c9"
        }
      }
    }
  ]
}
```

LW
lwazi995@outlook.com
NextWork Student

Bucket policies

Right after saving my bucket policy, my S3 bucket page showed 'denied access' warnings. This was because it has a deny policy that restricts access unless its from a specific VPC.

'I also had to update my route table because my S3 bucket was giving access denied after I set the command aws s3 ls s3://nextwork-vpc-endpoints-yourname my route table didn't provide a route in my public subnets to my VPCs

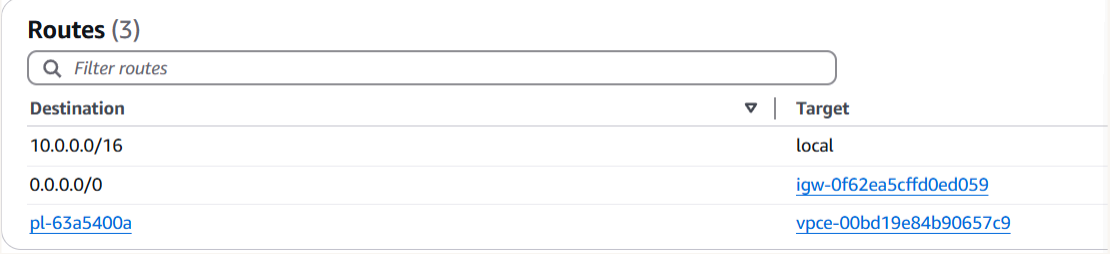


LW
lwazi995@outlook.com
NextWork Student

Route table updates

To update my route table, I went to my endpoints and created a new route table allowing access to my VPC public subnet.

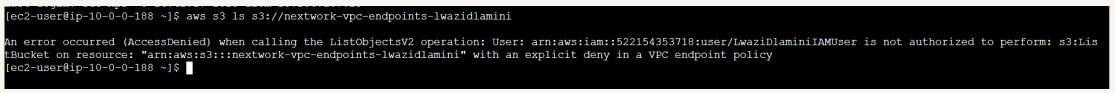
After updating my public subnet's route table, my terminal could return all the files located in my S3 bucket through a the same aws s3 ls command.



Endpoint policies

An endpoint policy is restriction of the traffic that only certain range and resources have access to the endpoint.

I updated my endpoint policy by adding the deny command to my endpoint JSON policy to restrict unauthorized access because my EC2 was denied access once I set the policy and run another command.



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for more projects