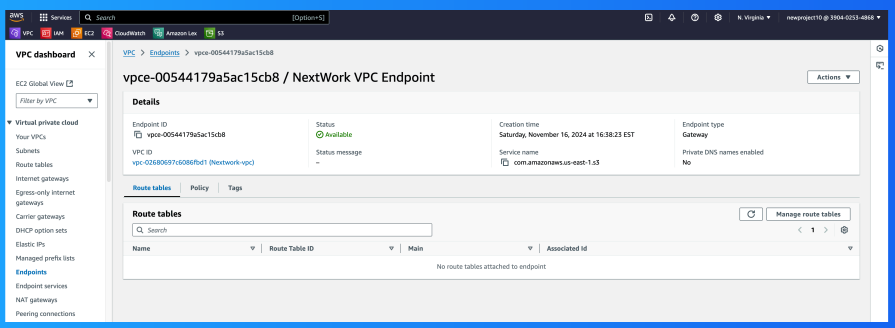
NextWork.org

VPC Endpoints

AL alexten3517@gmail.com



AL
alexten3517@gmail.com
NextWork Student
NextWork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon is a networking service and gives us ability to isolate our resources from the public internet, set up secure connections between our resources.

How I used Amazon VPC in this project

We used Amazon VPC today set up a VPC endpoint, specifically an S3 Gateway. This provides our VPC with direct, private access to another AWS service.

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

One thing I did not expect on this project was to see how resourceful it was to use our CLI commands to really showcase how our access was denied and accepted using these commands.

This project took me...

I spent about 1.5 hours learning and putting this project together while utilizing Chat gpt to really show me how some our the AWS services work under the hood.

AL
alexten3517@gmail.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 foundation of this project ,we are launching a VPC, EC2 instance and and a S3 bucket so that we can setup an endpoint architechture and test that setup in the last step of this project.

Step 2 - Connect to EC2 instance

In this step, we are connecting directly to our EC2 instance using EC2 instant connect, Connecting to instance will help us accessing S3 and running commands later in this project.

Step 3 - Set up access keys

In this step we will setup an access key so that our EC2 instance will have access to our AWS enviorment.We can think of access keys almost like log in details for EC2 instance/applications to interact with our AWS services.

Step 4 - Interact with S3 bucket

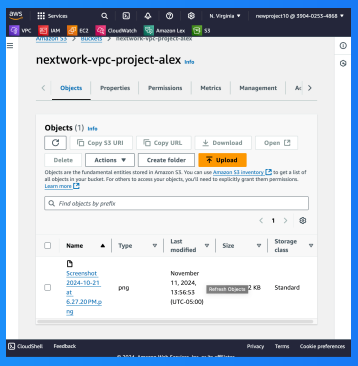
In this step we are applying our access keys credentials to our EC2 instance and then we are using AWS CLI and our EC2 instance to access amazon S3.

AL
alexten3517@gmail.com
NextWork Student

Architecture set up

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

In this step we were able to upload a file to our S3 bucket so we can then utilize our EC2 instance to then verify our connection to our VPC Endpoint.



Access keys

Credentials

To set up my EC2 instance to interact with my AWS environment I configured the AWS access key ID, that matches that key ID, the default region type and then the default output format.

Access keys are credentials that an EC2 instance/other server/application would need in order to get access to our AWS enviorment e.g. creating resources, reading whats inside our AWS account.

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

Best practice

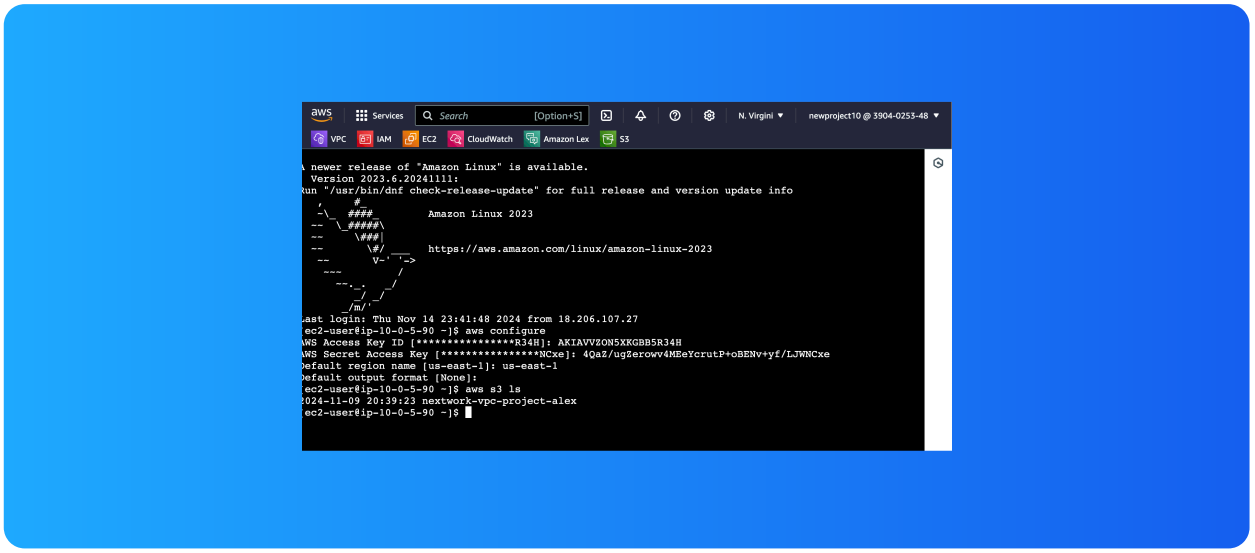
Although I'm using access keys in this project, a best practice alternative is to use IAM admin roles instead. This means the necessary permission will be attached to an IAM role, and then the role will be associated with the relevant resources.

AL
alexten3517@gmail.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 the AWS account.

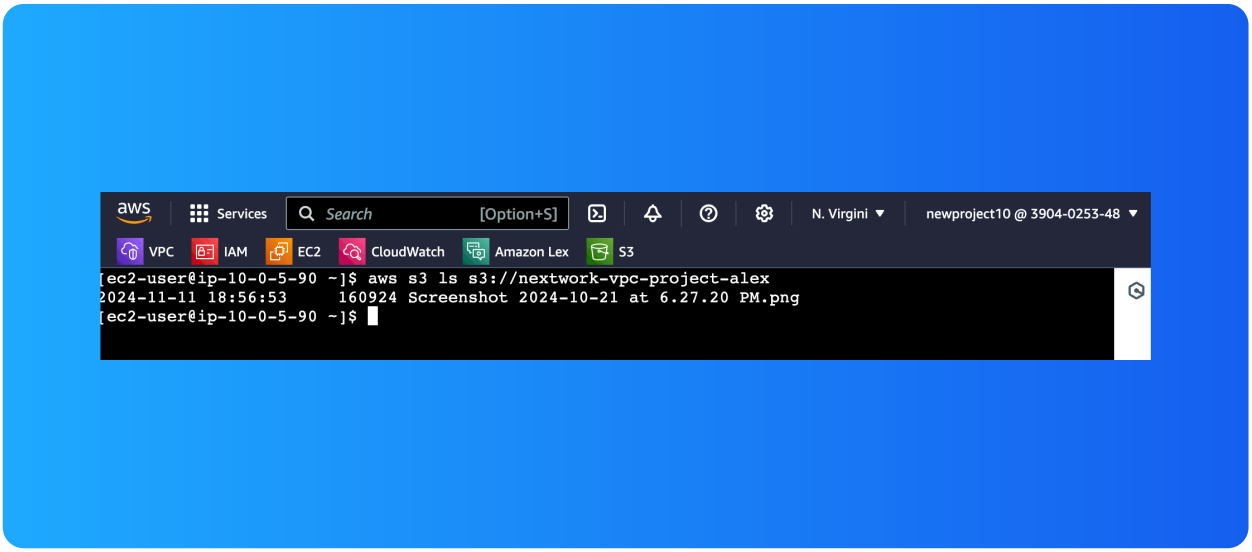
The terminal responded with a list of our S3 buckets. This indicated that the access keys were set up correctly and can give my EC2 instance access to my AWS account and enviroment.



AL
alexten3517@gmail.com
NextWork Student

Connecting to my S3 bucket

I also tested the command aws s3 ls s3://nextwork-vpc-project-alex which returned a list of all of the objects inside the S3 bucket.



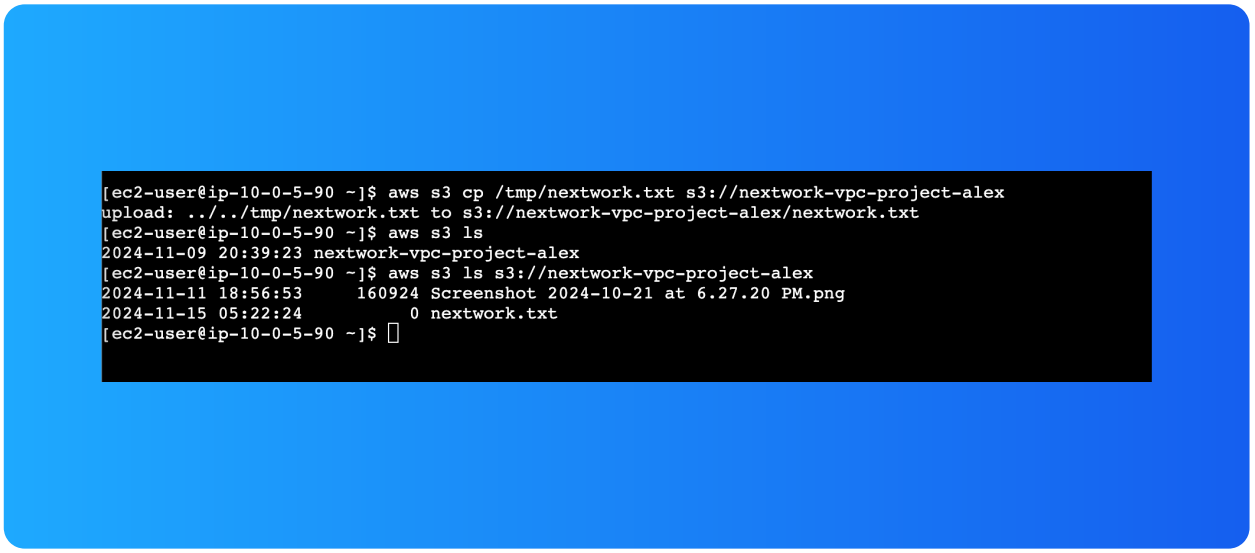
AL
alexten3517@gmail.com
NextWork Student

Uploading objects to S3

To upload a new file to my bucket, I first ran the command sudo touch. This command creates a creates and empty file named nextwork.txt and saves it locally in the EC2 instance.

The second command I ran was AWS s3 cp / tmp/nextwork/project/alex. This command will copy the file I created i.e. nextwork.txt and upload that to my s3 bucket.

The third command I ran was aws s3 ls s3://nextwork-vpc-project.alex which validated that a new file was created and uploaded into our s3 bucket.



AL
alexten3517@gmail.com
NextWork Student
NextWork.org

In the second part of my project...

Step 5 - Set up a Gateway

In this step, we are setting up a VPC endpoint so that communication between our VPC and other services (especially s3) is direct and secure.

Step 6 - Bucket policies

In this step we are testing by blocking off all traffic to our s3 bucket except for traiffic coming frou our endpoint.

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 we are going to validate our VPC setup one more time. We are also going to use endpoint policies to restrict our EC2 instances access to our AWS enviroment.

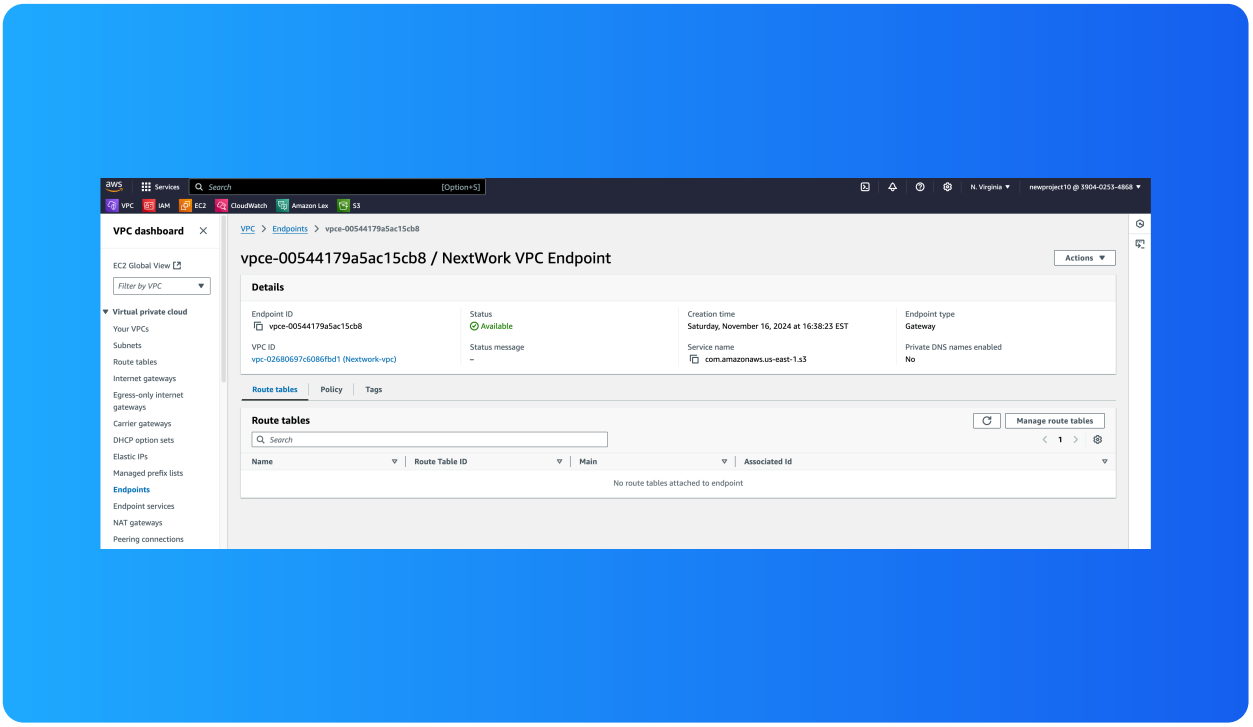
AL
alexten3517@gmail.com
NextWork Student

Setting up a Gateway

A gateway is a network device or service that allows devices on one network to communicate with devices on another network.

What are endpoints?

An endpoint is connection we create which allows us to communicate with services that live outside our VPC. It allows us to utilize a private gateway to keep our communications private from the internet.



Bucket policies

A bucket policy are the permissions written in json format which will block all incoming public traffic. It controls who has access to the S3 bucket and what actions they can perform.

My bucket policy will deny traffic from ALL sources -except for traffic coming from my VPC endpoint.

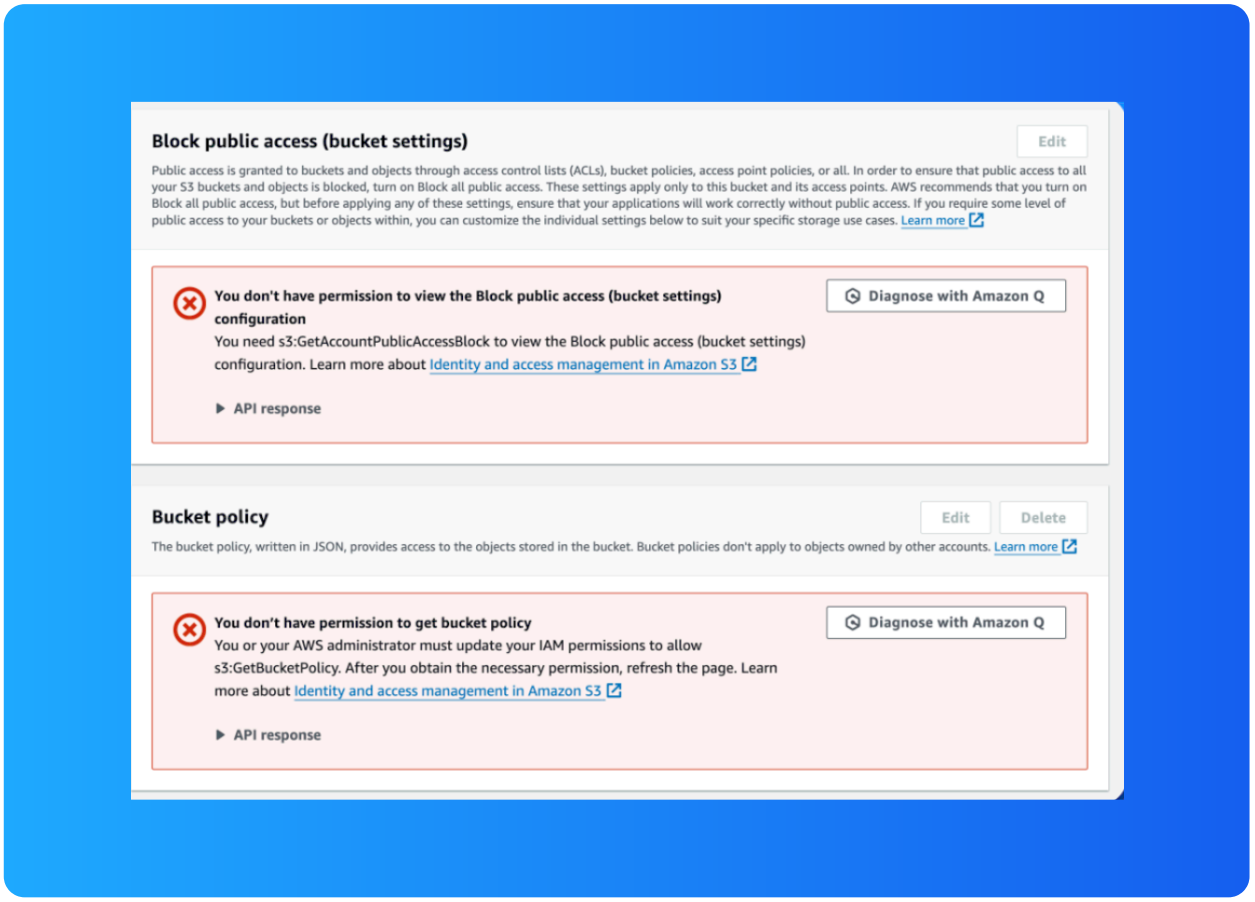
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::nextwork-vpc-project-alex",
        "arn:aws:s3:::nextwork-vpc-project-alex/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpce": "vpce-00544179a5ac15cb8"
        }
      }
    }
  ]
}
```

AL
alexten3517@gmail.com
NextWork Student

Bucket policies

Right after saving my bucket policy, my S3 bucket page showed 'denied access' warnings. This was because all access was blocked. Blocked because policyies must be set up in able to allow access to it.

I also had to update my route table because my route table by default didnt provide a route for traffic in my public subnet to the VPC endpoint.

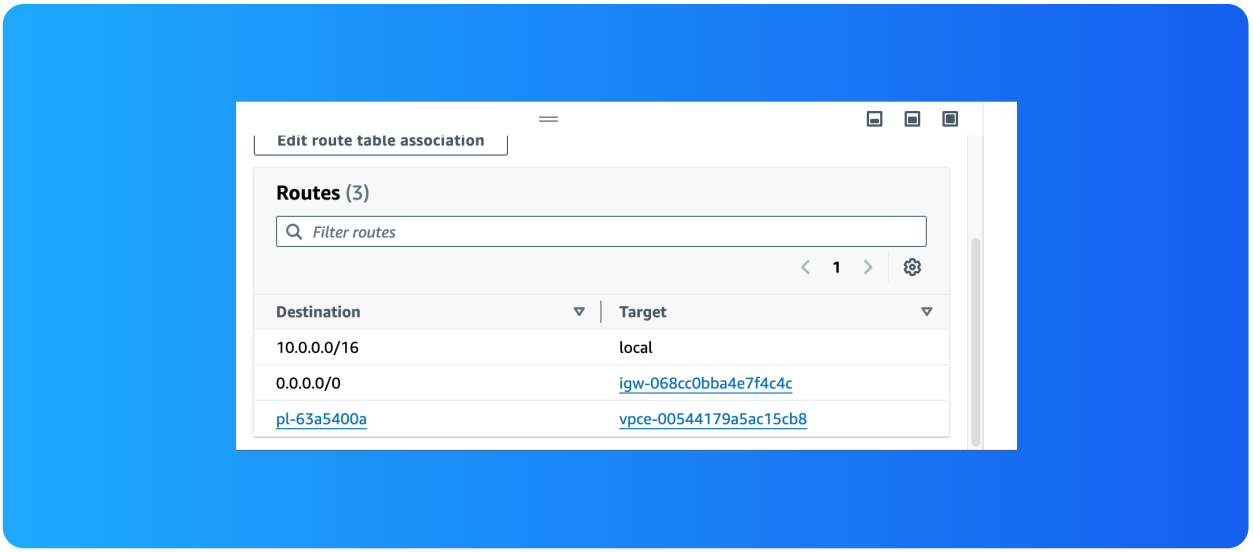


AL
alexten3517@gmail.com
NextWork Student

Route table updates

To update my route table I visited the endpoints page of my VPC console and modified the route table from there to associate our VPC's public subnet.

After updating my public subnet's route table, my terminal (aws s3 ls s3://nextwork-vpc-project-alex) could return all the objects inside the S3 bucket which means my EC2 instance could connect to my S3 bucket. Access no longer denied.

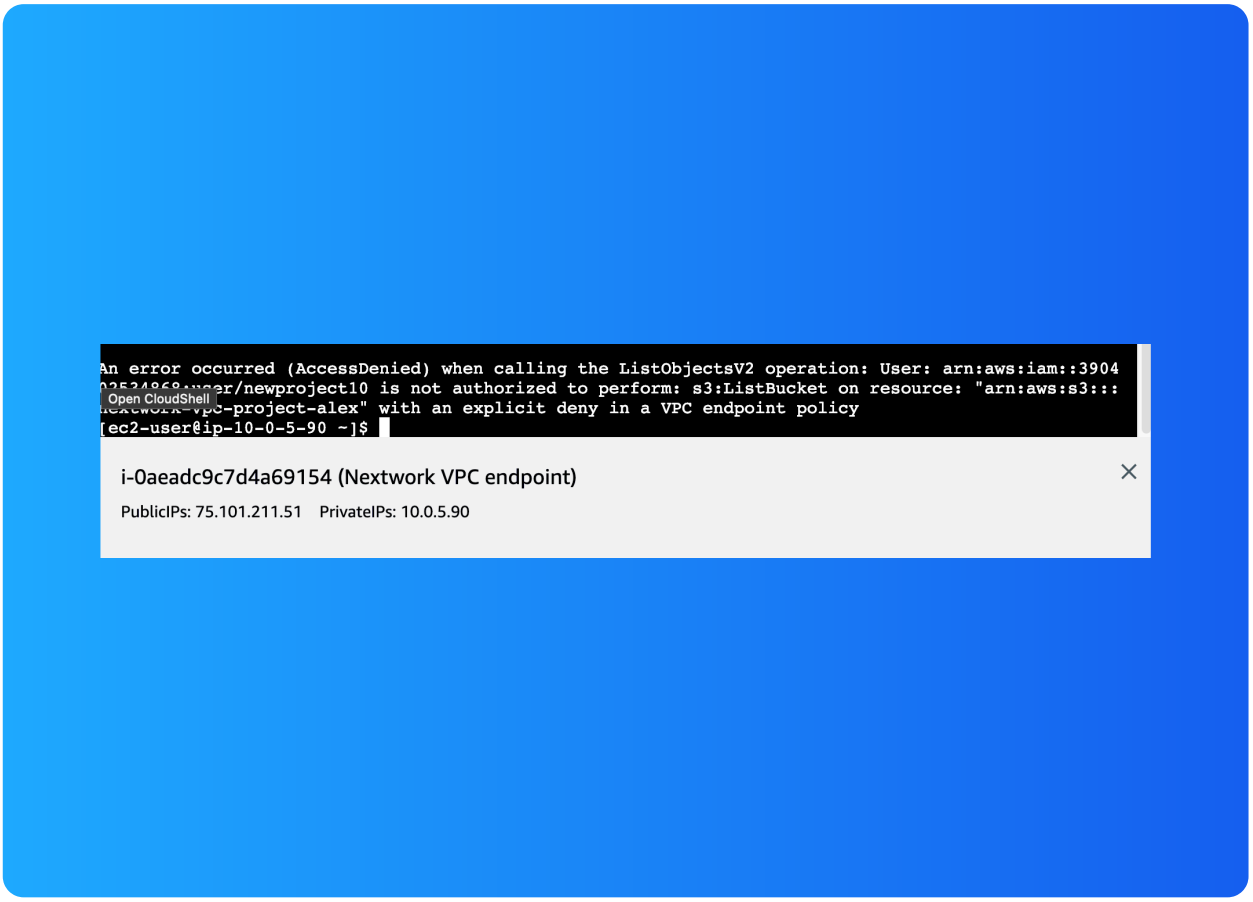


AL
alexten3517@gmail.com
NextWork Student

Endpoint policies

An endpoint policy is a type of policy designed for specifying the range of resources and actioins permitted by an endpoint.

I updated my endpoint's policy by changing to effect from allow to deny. I could see the effect of this right away, because my EC2 instance was again denied access to S3 when I tried to run another 'AWS S3' command.



Everyone should be in a job they love.

Check out nextwork.org for more projects