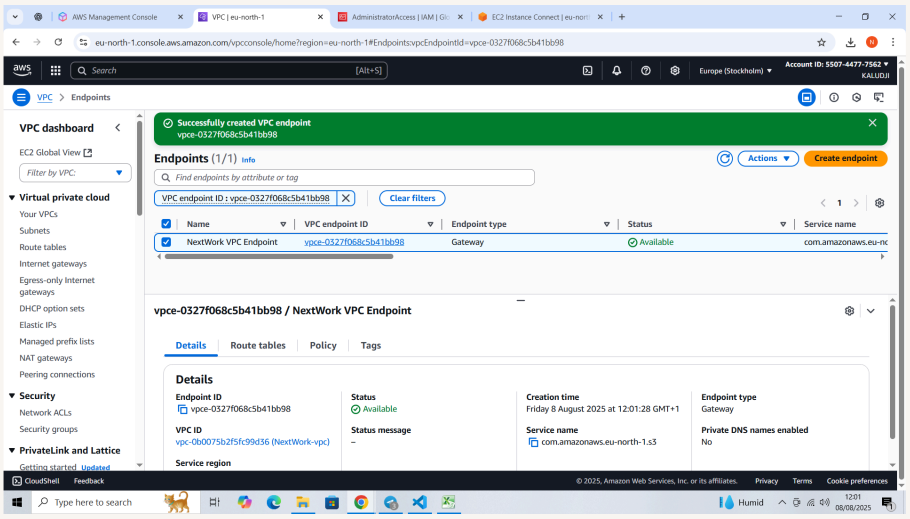
nextwork.org

VPC Endpoints

Nchindo Boris



Nchindo Boris
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a service that lets you create a custom, isolated virtual network within the AWS cloud.

How I used Amazon VPC in this project

I used Amazon VPC in this project to create a VPC Endpoint in order to access my S3 Bucket securely and not through the public internet

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

I did not expect this project to be this easy to do

This project took me...

This project took me 45 minutes to complete

In the first part of my project...

Step 1 - Architecture set up

In this step, I am going to: - Create a VPC from scratch! - Launch an EC2 instance, which I will connect to using EC2 Instance Connect later. - Set up an S3 bucket.

Step 2 - Connect to EC2 instance

In this step, I am going to Connect directly to your EC2 instance.

Step 3 - Set up access keys

In this step, I am going to Give your EC2 instance access to your AWS environment.

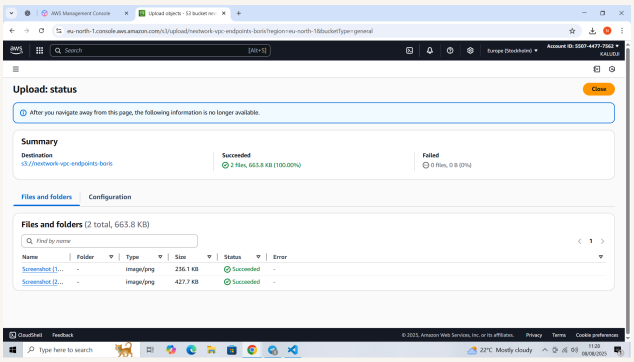
Step 4 - Interact with S3 bucket

In this step, I am going to: - Head back to your EC2 instance. - Get your EC2 instance to access your S3 bucket.

Architecture set up

I started my project by launching a VPC and an EC2 Instance

I also set up an S3 bucket and uploaded 2 files into it



Access keys

Credentials

To set up my EC2 instance to interact with my AWS environment, I configured; - Access key ID - Secret key - Default region - Default output format

Access keys are a set of security credentials that allow access to your AWS account

The secret access key is like the password that pairs with your access key ID (your username).

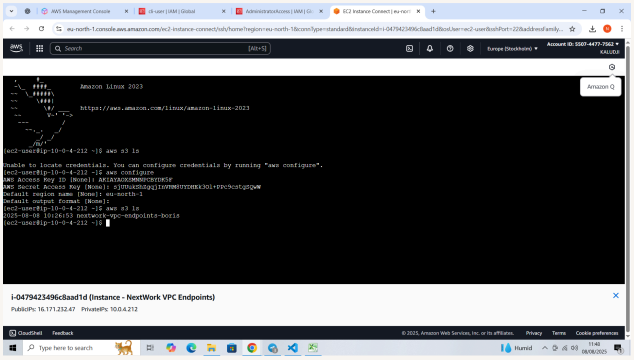
Best practice

The best practice is to avoid long-term access keys whenever possible and instead use IAM Roles (with Temporary Credentials)

Connecting to my S3 bucket

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

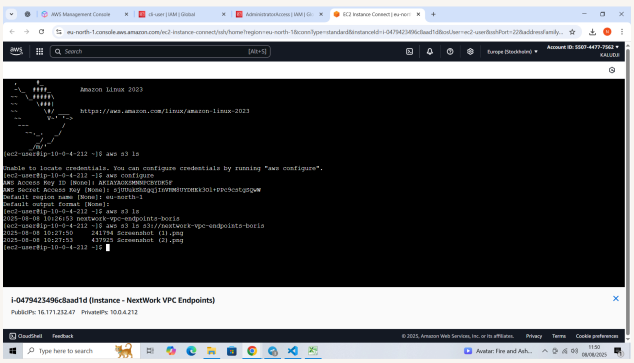
The terminal responded with 2025-08-08 10:26:53 nextwork-vpc-endpoints-boris. This indicated that the access keys I set up have connected me with my AWS S3 Bucket.



Nchindo Boris
NextWork Student

Connecting to my S3 bucket

I also tested the command aws s3 ls s3://nextwork-vpc-endpoints-boris . which returned the list of objects in my s3 bucket.

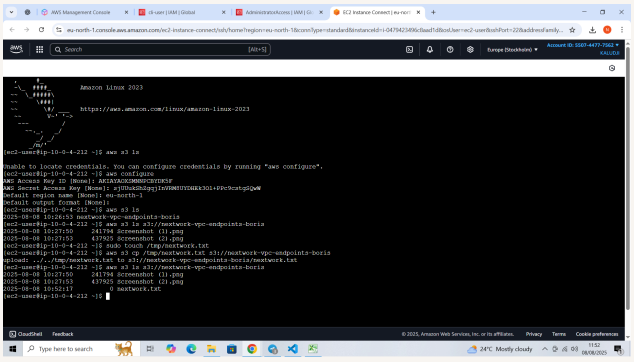


Uploading objects to S3

To upload a new file to my bucket, I first ran the command sudo touch /tmp/nextwork.txt. This command creates create a blank .txt file in your EC2 instance..

The second command I ran was aws s3 cp /tmp/nextwork.txt s3://nextwork-vpc-endpoints-boris. This command will upload the empty file into your bucket.

The third command I ran was aws s3 ls s3://nextwork-vpc-endpoints-boris. which validated that there is an empty file nextwork.txtwith no data, it has 0 bytes.



Nchindo Boris
NextWork Student

In the second part of my project...

Step 5 - Set up a Gateway

In this step, I am going to Set up a way for your VPC and S3 to communicate direclty.

Step 6 - Bucket policies

In this step, I am going to Limit your S3 bucket access's to only traffic from your endpoint.

Step 7 - Update route tables

In this step, I am going to: - Test your VPC endpoint set up. - Troubleshoot a connectivity issue.

Step 8 - Validate endpoint conection

n this step, I am going to: - Test your VPC endpoint set up (again). - Restrict your VPC's acccess to your AWS environment.

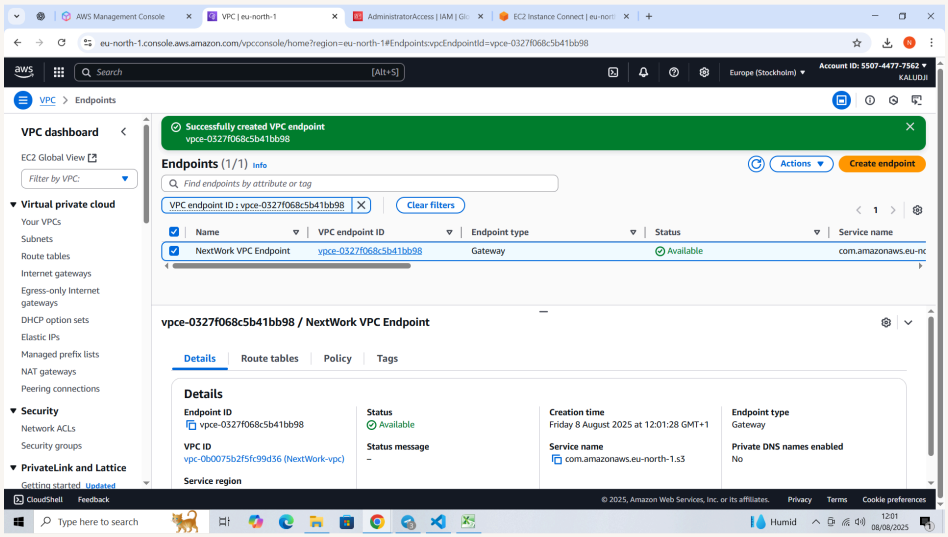
Nchindo Boris
NextWork Student

Setting up a Gateway

I set up an S3 Gateway, which is a type of endpoint which work by simply adding a route to your 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 in AWS is a service that allows private connections between your VPC and other AWS services without needing the traffic to go over the internet.

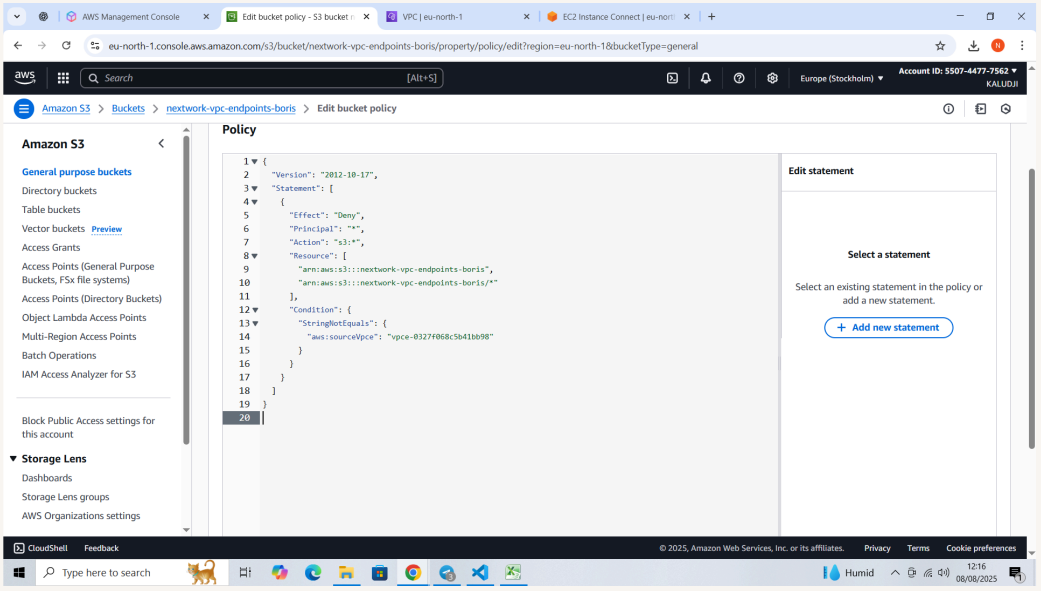


Nchindo Boris
NextWork Student

Bucket policies

A bucket policy is a type of IAM policy designed for setting access permissions to an S3 bucket

My bucket policy will This policy denies all actions (s3:*) on your S3 bucket and its objects to everyone (Principal: "*")... unless the access is from the VPC endpoint with the ID defined in aws:sourceVpce.

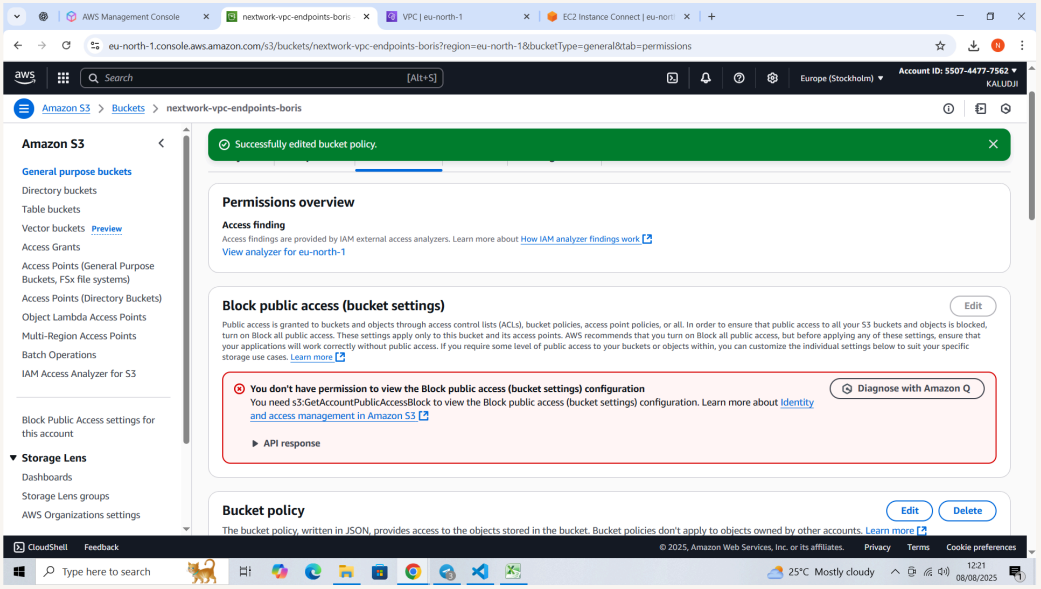


Nchindo Boris
NextWork Student

Bucket policies

Right after saving my bucket policy, my S3 bucket page showed 'denied access' warnings. This was because Your policy denies all actions unless they come from your VPC endpoint. This means any attempt to access your bucket from other sources is blocke

I also had to update my route table because the EC2 instance is trying to get to your S3 bucket through the public internet instead and so a route that directs traffic bound for S3 to your VPC endpoint is required to be added on the route table

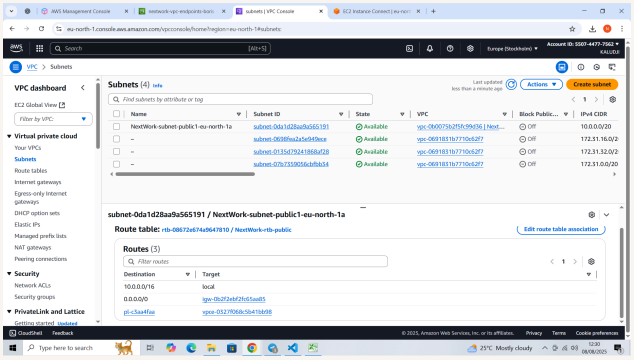


Nchindo Boris
NextWork Student

Route table updates

To update my route table, I; Select Endpoints Select the checkbox next to your endpoint, and select Route tables Select Manage route tables Select the checkbox next to your public route table. Select Modify route tables. Refresh the Subnets page

After updating my public subnet's route table, my terminal could return the content of my S3 bucket

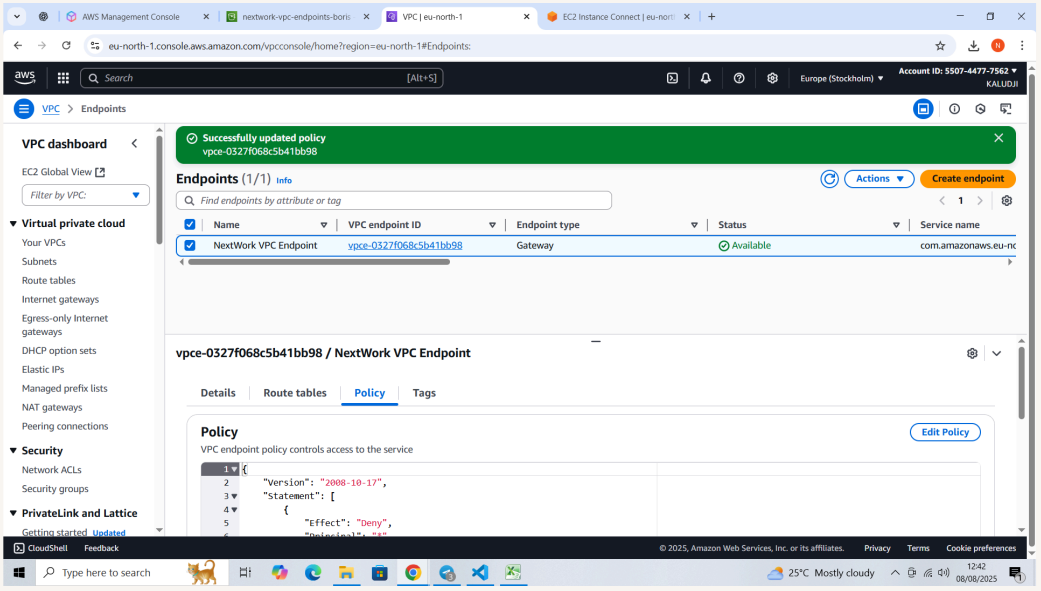


Nchindo Boris
NextWork Student

Endpoint policies

'An endpoint policy is a JSON policy document attached to a VPC Endpoint that controls and restricts access to the AWS service through that endpoint.

I updated my endpoint's policy by Select Edit policy. Change the line "Effect": "Allow" to "Effect": "Deny"!. I could see the effect of this right away, because access to my S3 bucket is denied on the CLI. .



The place to learn & showcase your skills

Check out nextwork.org for more projects