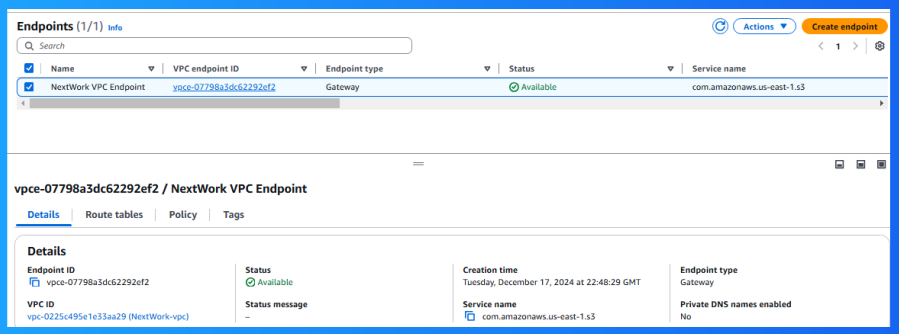
NextWork.org

VPC Endpoints

Gloria



G
Gloria
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) is a secure, isolated network in AWS where you can launch resources like EC2 instances. It’s useful because it gives control over networking, such as IP ranges, subnets and security.

How I used Amazon VPC in this project

I used Amazon VPC in today's project to create a secure network environment.I set up a VPC endpoint to allow my EC2 instance to access an S3 bucket privately, ensuring traffic stayed within the AWS network instead of going through the public internet

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

One thing I didn't expect in this project was how VPC endpoints significantly improve security by allowing private access to AWS services like S3. It eliminates the need for internet access, reducing exposure to external threats.

This project took me...

This project took me 45 minutes to complete, including setting up the VPC, creating the S3 bucket, configuring the VPC endpoint, and testing secure access to the S3 bucket from my EC2 instance.

G
Gloria
NextWork Student

In the first part of my project...

Step 1 - Architecture set up

In this step, I will create a VPC as the network environment, launch an EC2 instance inside it, and set up an S3 bucket. This forms the foundation of the project, allowing me to connect resources in the VPC to S3 securely and test VPC endpoints.

Step 2 - Connect to EC2 instance

In this step, I am connecting directly to my EC2 instance to test accessing S3 through the public internet. This will help me understand how traffic flows without a VPC endpoint and highlight the need for a more secure, private connection to S3.

Step 3 - Set up access keys

In this step, I am creating access keys to provide my EC2 instance with credentials to securely access AWS services. This allows the instance to authenticate and interact with resources like S3 using the AWS CLI.

Step 4 - Interact with S3 bucket

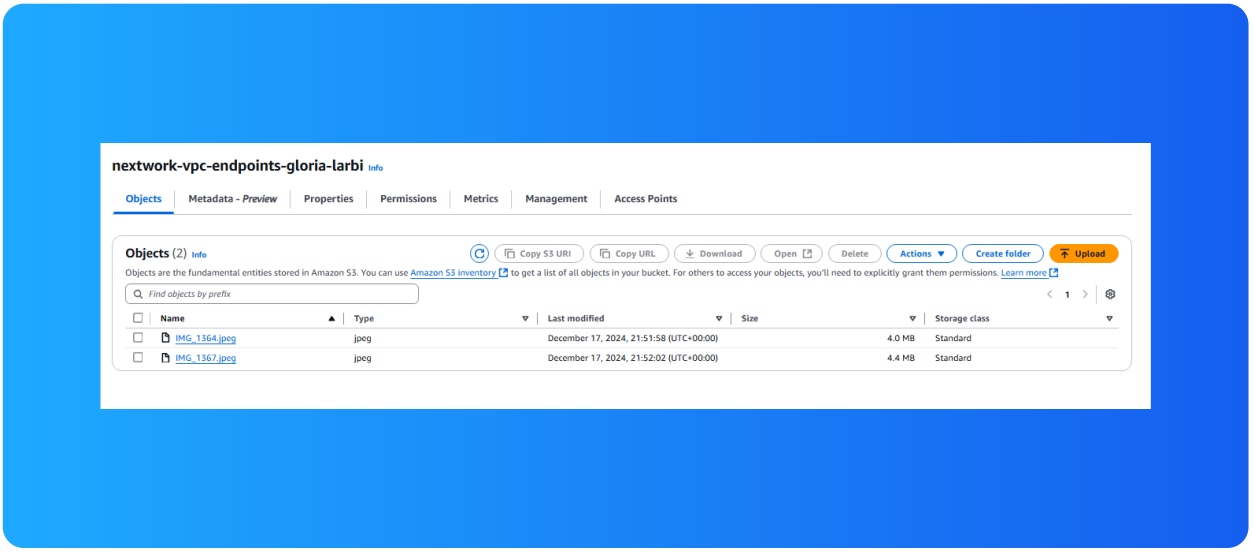
In this step, I will connect to my EC2 instance and access my S3 bucket using the AWS CLI.This will test if the instance can interact with the bucket using access keys, verifying connectivity and my ability to manage S3 resources from the instance.

Gloria
NextWork Student

Architecture set up

I started my project by launching a VPC named NextWork with a public subnet and no private subnets. I then launched an EC2 instance named Instance-NextWork VPC Endpoints in the public subnet, enabled a public IP, and created a security group for SSH

I also set up an S3 bucket named nextwork-vpc-endpoints-gloria-larbi and uploaded two files into it. This bucket will act as a cloud storage space that I can access from my EC2 instance to verify connectivity and interact with the files stored in S3.



Access keys

Credentials

To set up my EC2 instance to interact with my AWS environment, I configured the Access Key ID, the Secret Access Key, the Default Region Name, and the Default Output Format. These settings allow the AWS CLI to securely access and manage AWS services.

Access keys are credentials that allow secure programmatic access to AWS services. They consist of an Access Key ID and a Secret Access Key and are used to authenticate and authorize requests made through tools like the AWS CLI.

Secret access keys are unique codes that work like a password, paired with an Access Key ID, to authenticate and securely access AWS services. They must be kept private to prevent unauthorized access to your AWS account.

Best practice

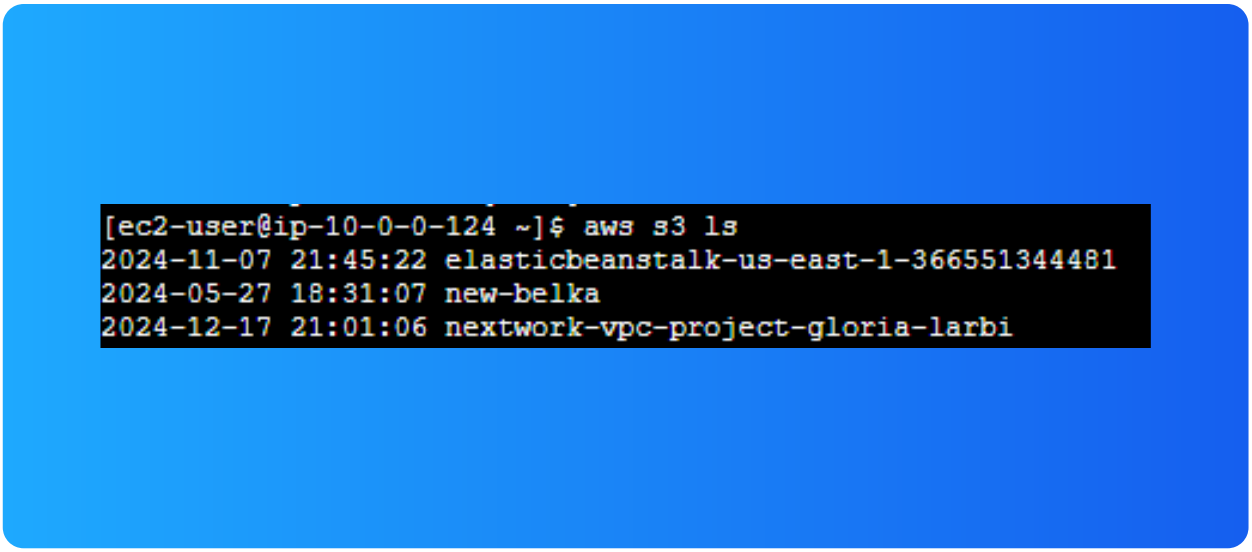
Although I'm using access keys in this project, a best practice alternative is to use IAM roles. IAM roles provide temporary credentials to instances, improving security by eliminating the need to store or manage long-term access keys.

Gloria
NextWork Student

Connecting to my S3 bucket

The command I ran was `aws s3 ls`. This command is used to list all the S3 buckets in my AWS account, showing their names and creation dates. It can help verify if my EC2 instance can connect to S3 through the public internet.

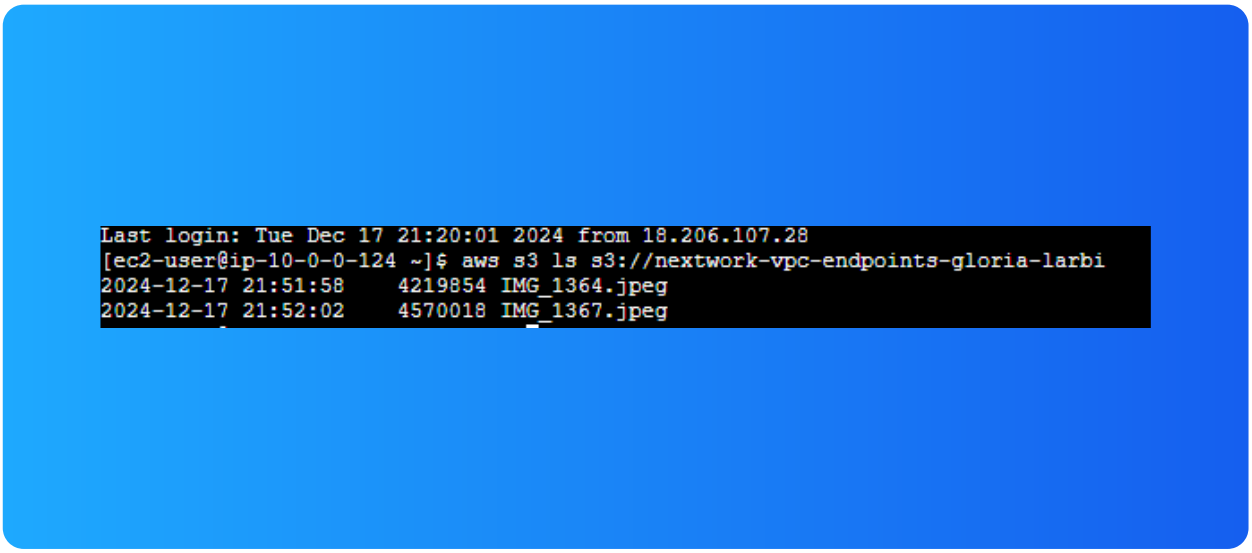
The terminal responded with the list of S3 buckets in my AWS account. This indicated that the access keys I set up were working correctly, and my EC2 instance was able to connect to AWS and access S3 using the AWS CLI.



G
Gloria
NextWork Student

Connecting to my S3 bucket

I also tested the command aws s3 ls s3://nextwork-vpc-endpoints-gloria-larbi, which returned list of objects inside my S3 bucket, file names, sizes, and upload timestamps. This confirmed that my EC2 instance could access and interact with S3 bucket.



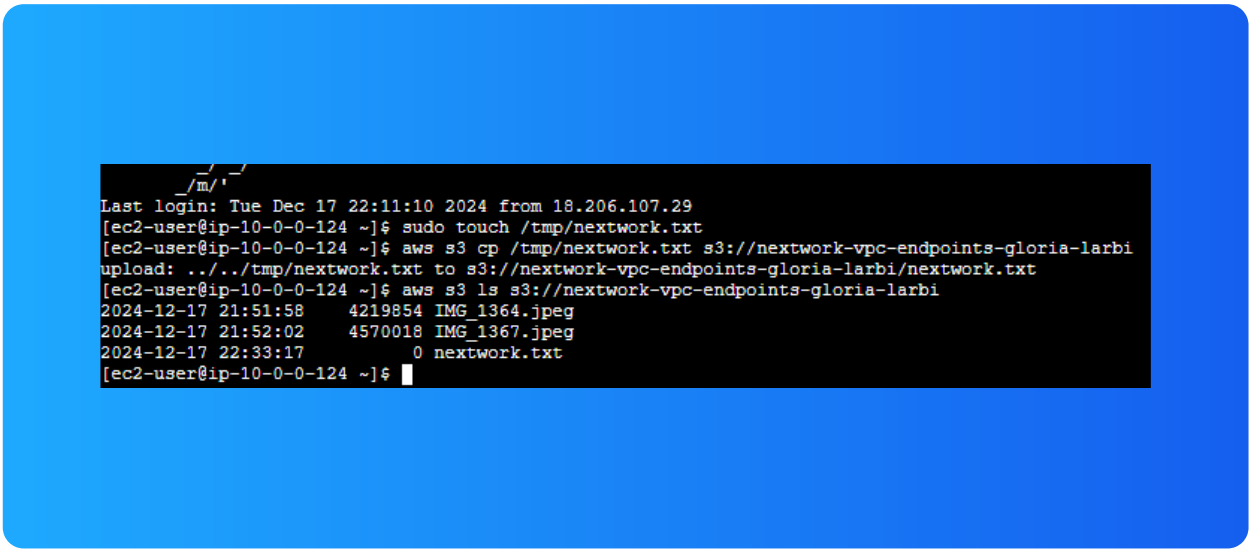
Gloria
NextWork Student

Uploading objects to S3

To upload a new file to my bucket, I first ran the command `sudo touch /tmp/test.txt`. This command creates an empty file named `test.txt` in the `/tmp` directory on my EC2 instance, which I can then upload to my S3 bucket.

The second command I ran was `aws s3 cp /tmp/test.txt s3://nextwork-vpc-endpoints-gloria-larbi`. This command will upload the `test.txt` file from my EC2 instance to my S3 bucket, allowing me to store it in the cloud.

The third command I ran was `aws s3 ls s3://nextwork-vpc-endpoints-gloria-larbi`, which validated that the file `test.txt` was successfully uploaded by displaying the file name, size, and upload timestamp inside my S3 bucket.



G
Gloria
NextWork Student

In the second part of my project...

Step 5 - Set up a Gateway

In this step, I will create a VPC endpoint to allow my VPC to communicate directly with S3 without using the public internet. This improves security by keeping the traffic private within the AWS network, reducing exposure to external threats.

Step 6 - Bucket policies

In this step,I am creating a secure bucket policy to restrict access to my S3 bucket so that only traffic coming through my VPC endpoint can access it. This will validate that my VPC endpoint is working and the bucket is not accessible on internet.

Step 7 - Update route tables

In this step, I am testing whether my EC2 instance can still access my S3 bucket after restricting access to only the VPC endpoint. This will confirm if the endpoint is set up correctly or help me troubleshoot any connectivity issues.

Step 8 - Validate endpoint conection

In this step, I am testing my VPC endpoint setup again by accessing my S3 bucket to confirm that traffic is routed through the endpoint. I will also restrict my VPC's access to ensure that it securely interacts with AWS services only.

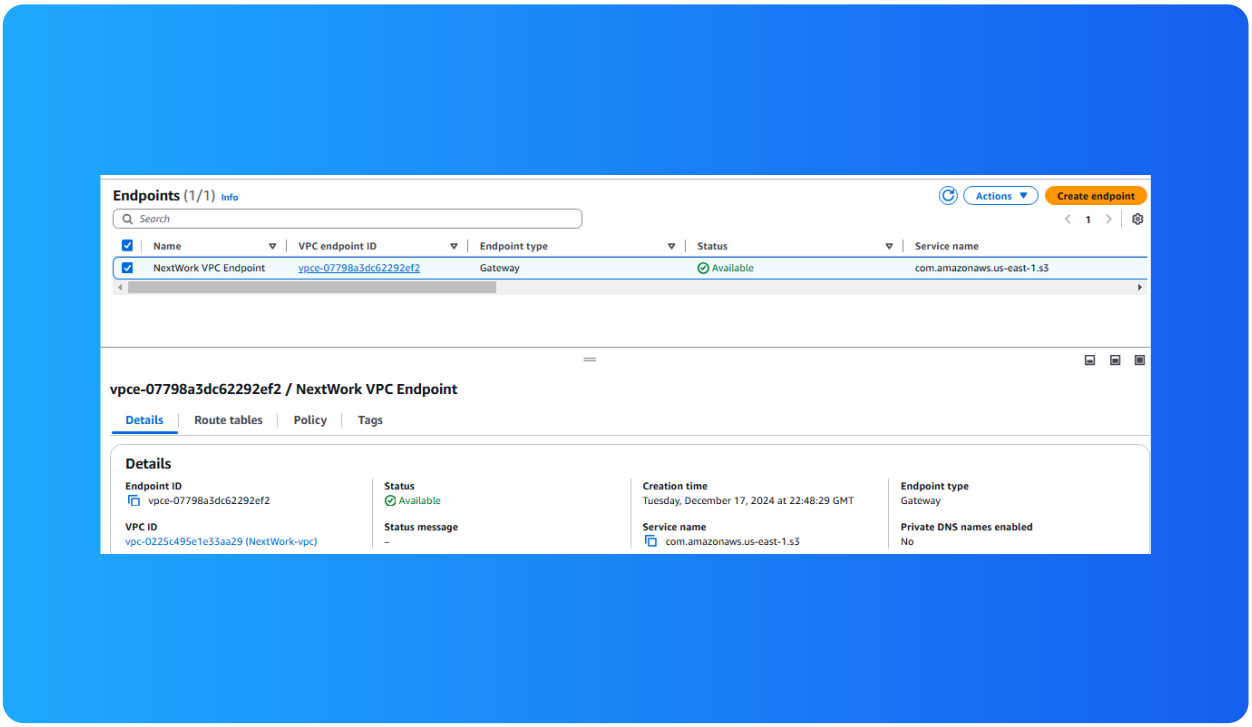
Gloria
NextWork Student

Setting up a Gateway

I set up an S3 Gateway, which is a type of VPC endpoint that allows my VPC to access Amazon S3 securely.It acts as a private gateway, routing traffic to S3 without going through the public internet, improving security and reducing data transfer cost.

What are endpoints?

An endpoint is a private connection that allows resources in a VPC to securely communicate with AWS services, like S3, without sending traffic over the public internet. This improves security, reduces latency, and helps lower data transfer costs.



G
Gloria
NextWork Student

Bucket policies

A bucket policy is a set of permissions attached to an S3 bucket that controls access to the bucket and its objects. It specifies who can access the bucket, what actions they can perform, and under what conditions, ensuring secure and managed access.

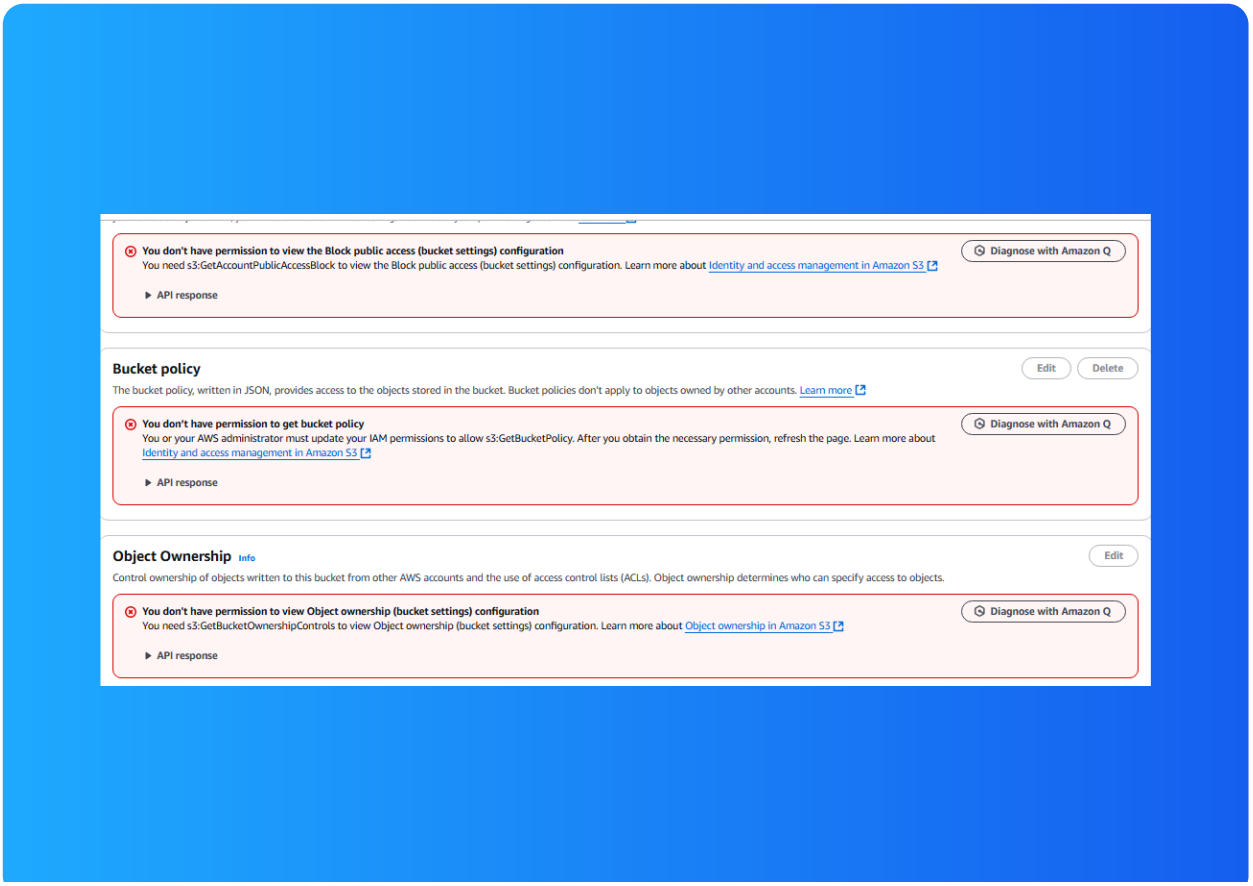
My bucket policy will deny all access to the S3 bucket unless the request comes from the specified VPC endpoint (vpce-07798a3dc62292ef2). This ensures that only traffic routed through the VPC endpoint can access the bucket, blocking public access

Gloria
NextWork Student

Bucket policies

Right after saving my bucket policy, my S3 bucket page showed 'denied access' warnings. This was because the bucket policy explicitly denies all access except from the specified VPC endpoint, and my current access did not meet that policy.

I also had to update my route table because the VPC endpoint needed a route for traffic to flow directly to Amazon S3. Without this update, the EC2 instance wouldn't know how to access S3 through the endpoint, and the connection would fail.

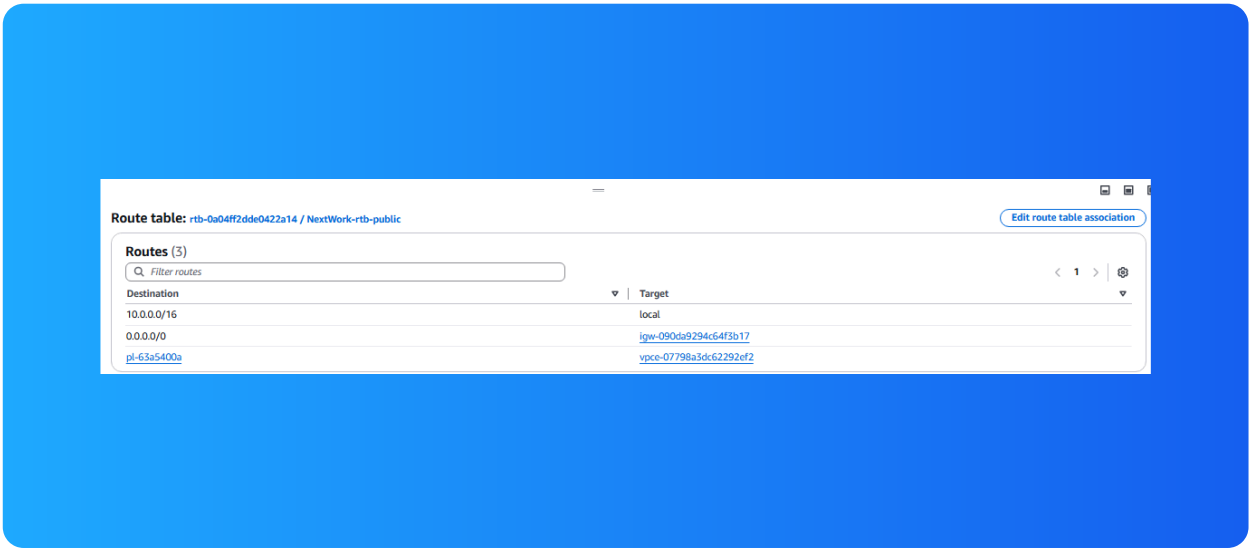


Gloria
NextWork Student

Route table updates

To update my route table, I associated my public subnet's route table with the VPC endpoint.This ensures that traffic bound for S3 is routed directly through the endpoint instead of the public internet, enabling secure and private access to my bucket

After updating my public subnet's route table, my terminal could return the list of objects in my S3 bucket. This confirmed that traffic from my EC2 instance was successfully routed through the VPC endpoint to access the S3 bucket securely.

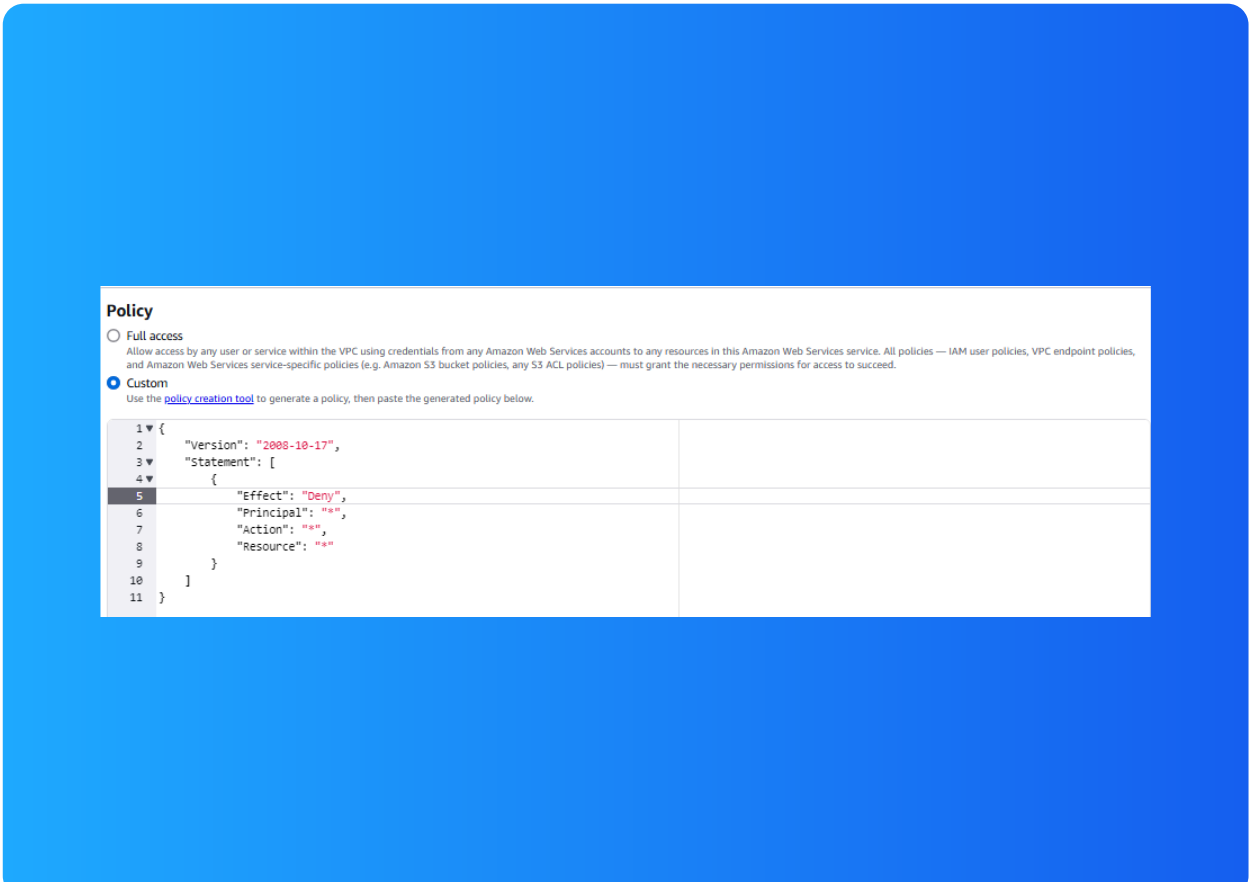


Gloria
NextWork Student

Endpoint policies

An endpoint policy is a set of permissions attached to a VPC endpoint that controls access to certain AWS services.It defines who can use the endpoint, what actions are allowed, and under what conditions, ensuring secure and controlled communication.

I updated my endpoint's policy by changing the line Effect: Allow to Effect: Deny. I could see the effect of this right away, because when I ran the aws s3 ls command, access to my S3 bucket was blocked, confirming the endpoint now denies all access.



Everyone should be in a job they love.

Check out nextwork.org for more projects