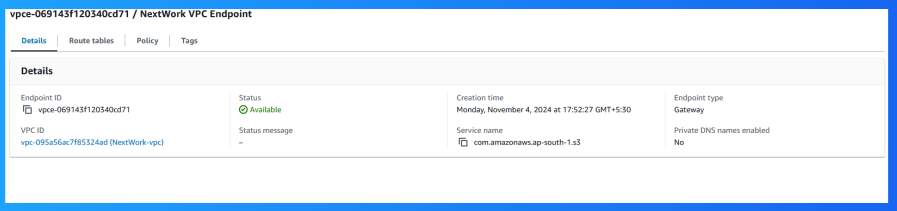
NextWork.org

VPC Endpoints

Saish Nar



Saish Nar
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is an application that holds and stores Isolated Cloud Resources. VPC also means Virtual Private Cloud. This is useful application to provide an additional layer of security for workloads and data.

How I used Amazon VPC in this project

Amazon VPC was used to demonstrate the ability to set up direct, private access to S3 from your VPC.

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

The one thing that I did not expect was the ability to quickly configured VPC endpoints using policies.

This project took me...

This project took me two hours to complete.

Saish Nar
NextWork Student

In the first part of my project...

Step 1 - Architecture set up

In this step, I am setting up the foundations of this project - i.e. launching a VPC, EC2 instance and S3 bucket so that I can set up an endpoint architecture and test that setup in the last step of this project.

Step 2 - Connect to EC2 instance

In this step, I am connecting directly to my EC2 instance using EC2 instance Connect. Connecting to my EC2 instance will help me to accessing S3 and running commands later in this project.

Step 3 - Set up access keys

In this step, I will set up an access key so that my EC2 instance will have access to AWS environment. I can think of access keys almost like "login details" for EC2 instances/applications (non humans) to interract with my AWS services.

Step 4 - Interact with S3 bucket

In step, I am applying my access key credentials to my EC2 instance, and then I am using AWS CLI and my EC2 instance to access Amazon S3.

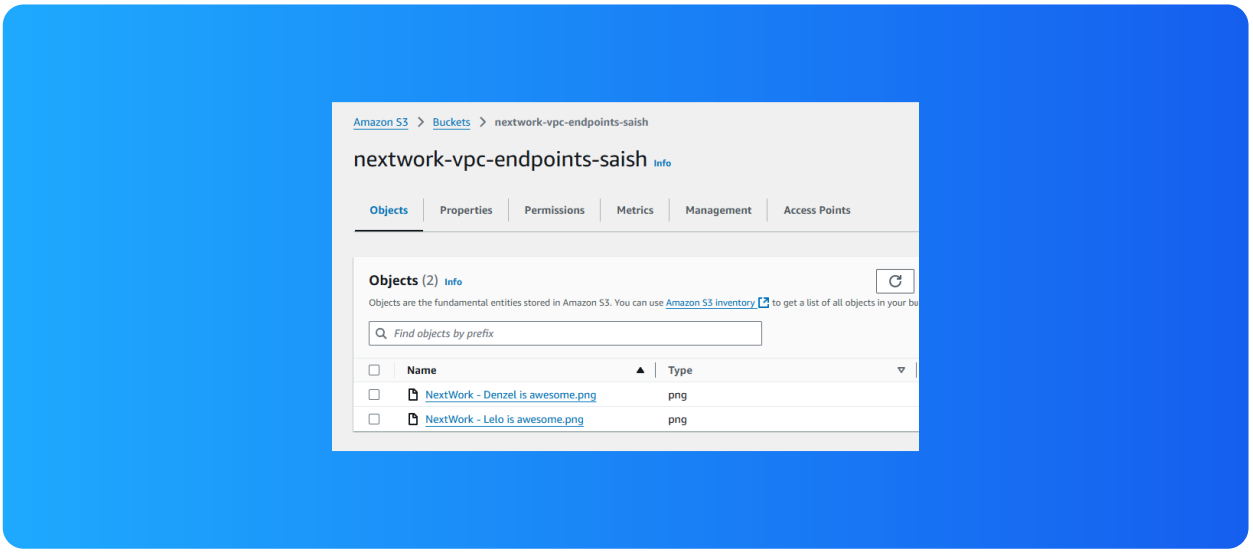
Saish Nar
NextWork Student

NextWork.org

Architecture set up

I started my project by launching three key resources - a VPC, EC2 instance and S3 bucket.

I also set up an S3 bucket with two files inside.



Saish Nar
NextWork Student

Access keys

Credentials

To set up my EC2 instance to interact with my AWS environment, I configured the AWS access key ID, secret access key (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 my AWS environment e.g. creating ressources, reading what's inside my AWS account etc.

Secret access keys are like password in the context of access keys/credentials for my EC2 instance to get access to my AWS services/environments.

Best practice

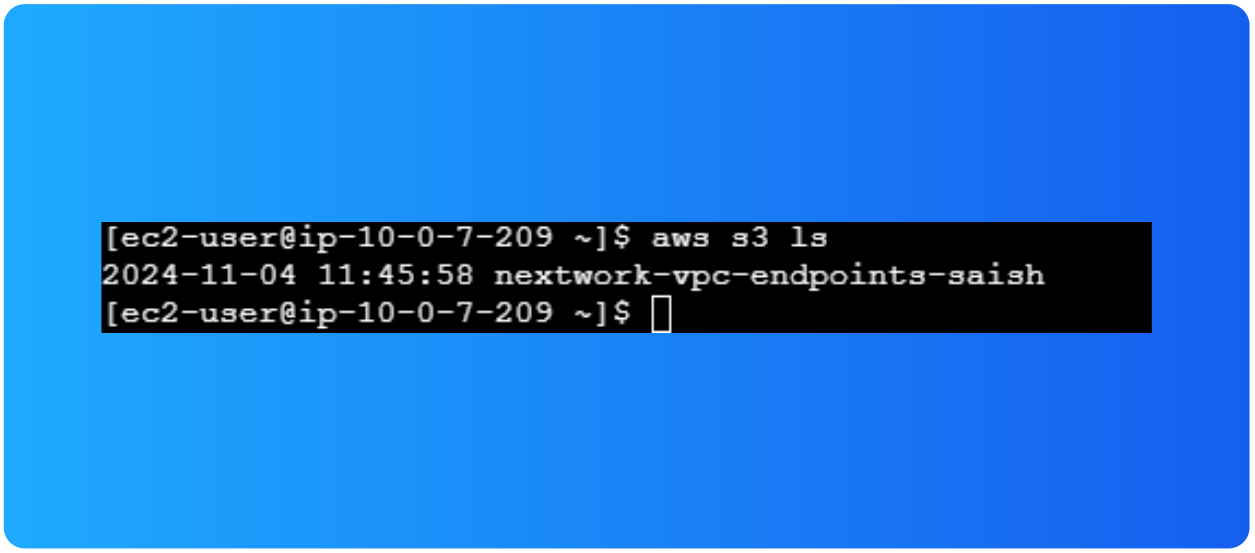
Although I'm using access keys in this project, a best practice alternative is to use IAM admin roles instead. This means any necessary permissions will be attached to an IAM role. Then, the role will be associated with the relevant resources.

Saish Nar
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 a list of my account's S3 buckets. This indicated that my access keys were set up correctly and can give my EC2 instance access to my AWS account and environment.

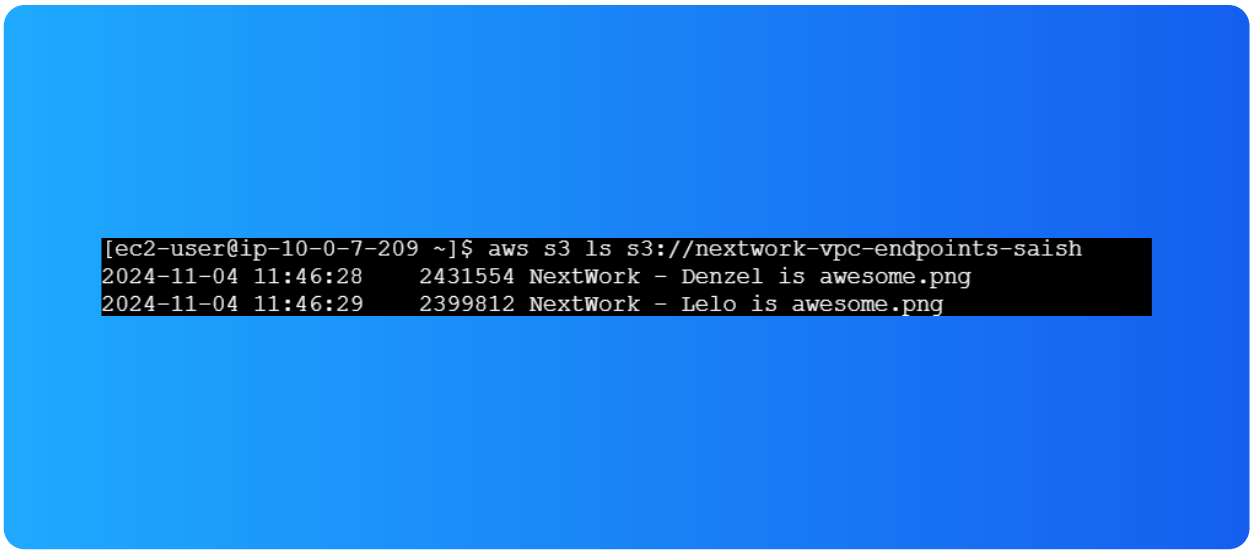


Saish Nar
NextWork Student

NextWork.org

Connecting to my S3 bucket

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



Saish Nar
NextWork Student

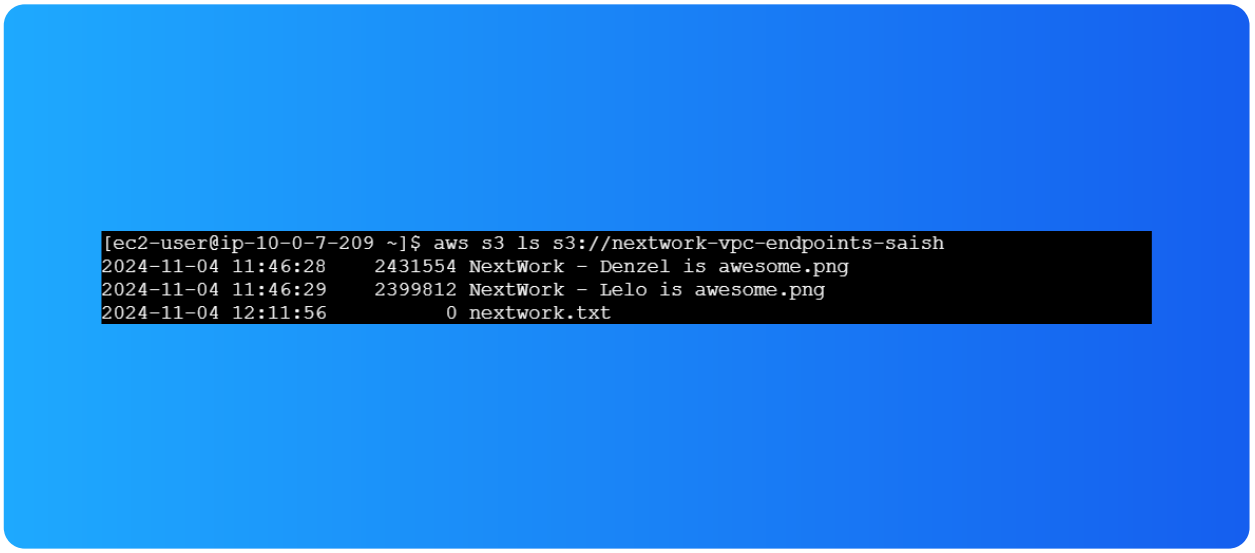
NextWork.org

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 empty file named nextwork.txt and saves it locallly in the EC2 instance.

The second command I ran was 'aws s3 cp /tmp/nextwork.txt s3://nextwork-vpc-endpoints-saish'. 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-endpoints-saish'. which validated that a new file was created and uploaded into my S3 bucket.



Saish Nar
NextWork Student

In the second part of my project...

Step 5 - Set up a Gateway

In this step, I am setting up a VPC endpoint so that communication between my VPC and other services (especially S3) is direct and secure.

Step 6 - Bucket policies

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

Step 7 - Update route tables

In this step, I am testing my endpoint connection between my bucket and EC2 instance.

Step 8 - Validate endpoint conection

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

Saish Nar
NextWork Student

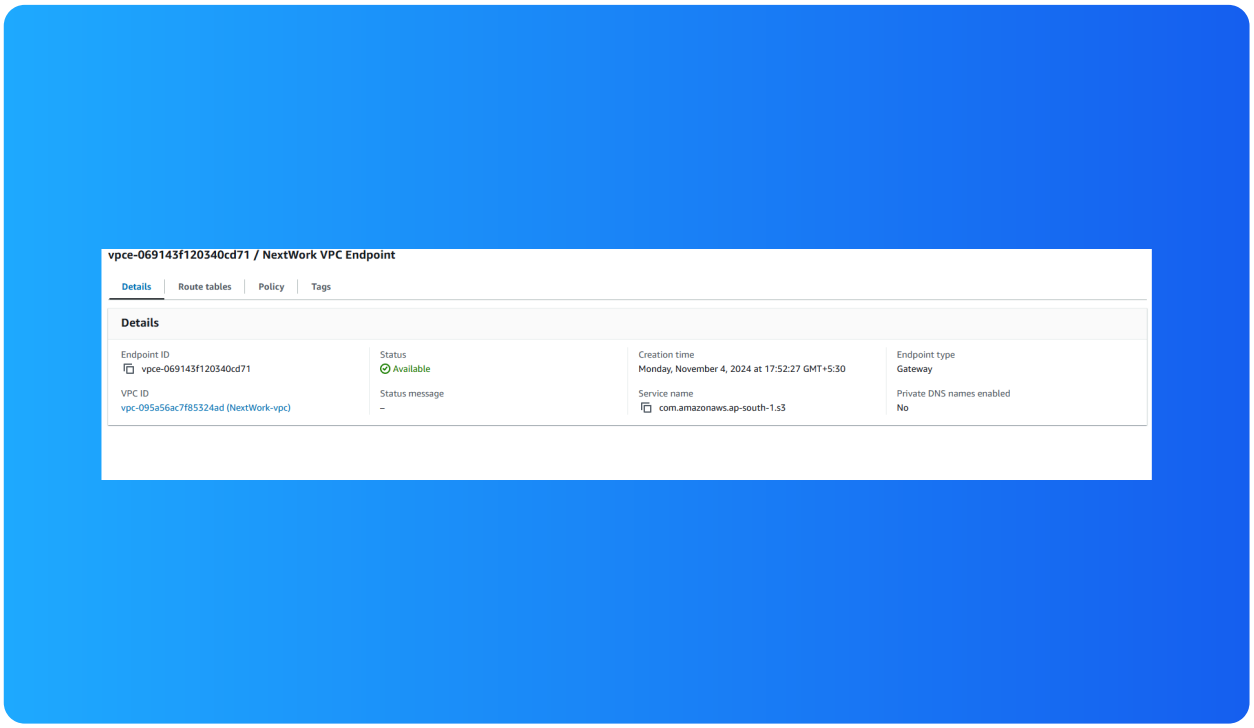
NextWork.org

Setting up a Gateway

I set up an S3 Gateway, which is a type of endpoint specifically designed for Amazon S3 Gateway work by updating the route table of associated subnets, So that S3 bound traffic goes through the Gateway instead of the internet.

What are endpoints?

An endpoint is VPC component that allows my VPC to have a direct connection to AWS services, so that traffic doesn't have to go through the public internet.

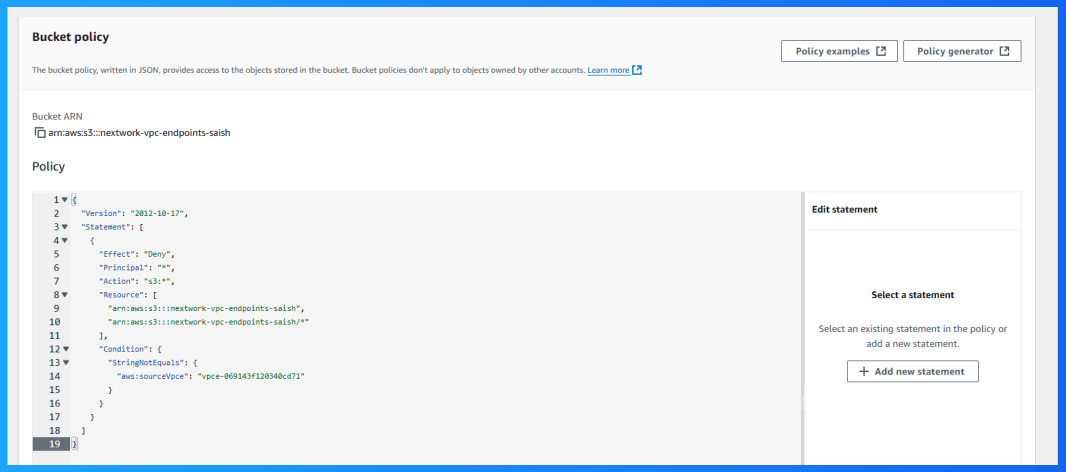


Saish Nar
NextWork Student

Bucket policies

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

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

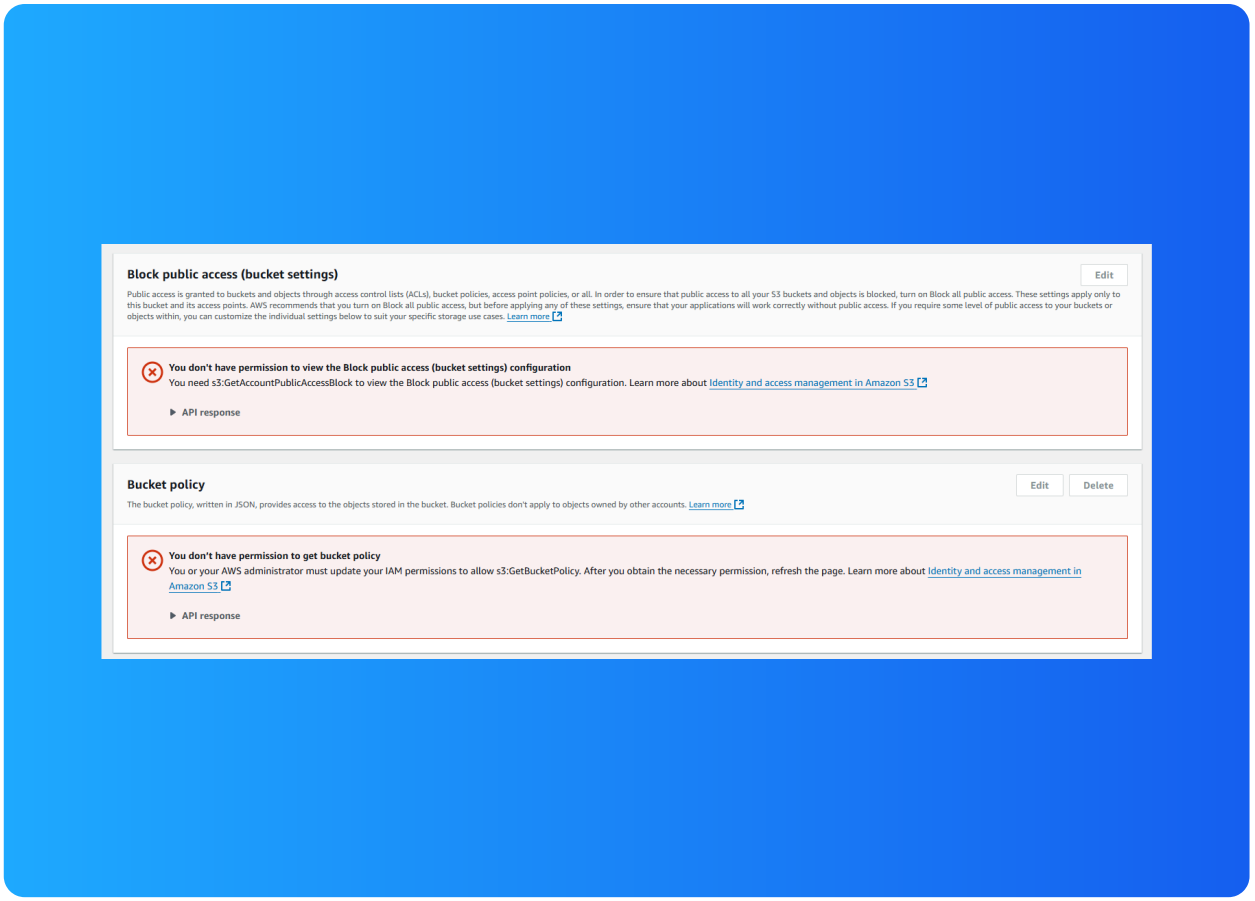


Saish Nar
NextWork Student

Bucket policies

Right after saving my bucket policy, my S3 bucket page showed 'denied access' warnings. This was because my bucket policy is denying all traffic that doesn't come from my endpoint. i.e. the policy denies traffic from the AWS Management Console.

I also had to update my route table because my route table, by default, didn't provide a route for traffic in my public subnet to the VPC endpoint.



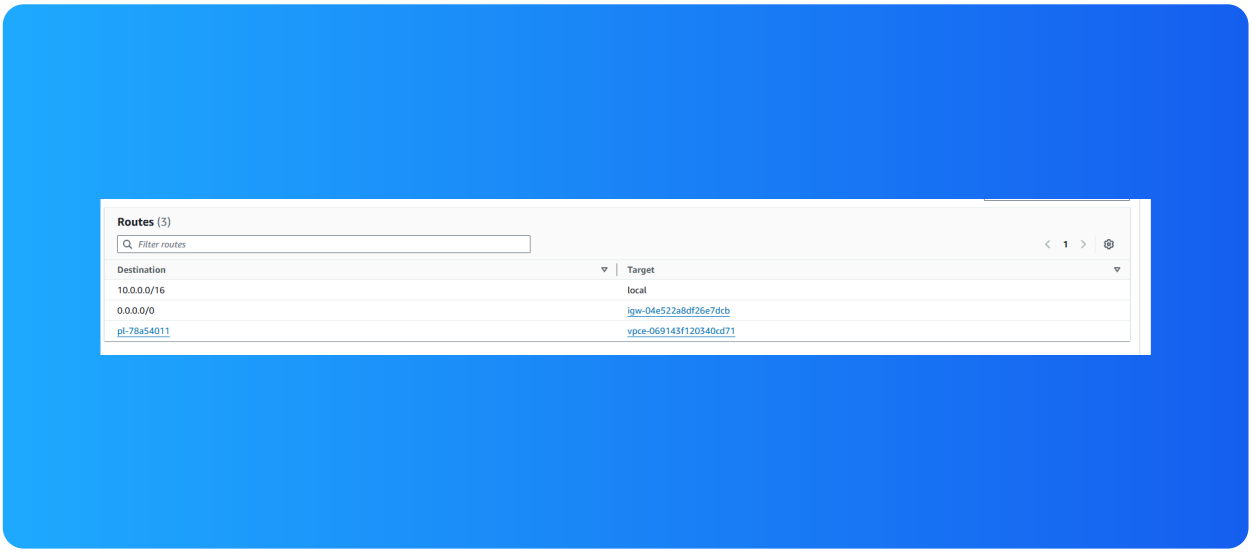
Saish Nar
NextWork Student

NextWork.org

Route table updates

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

After updating my public subnet's route table, my EC2 instance could connect with my S3 bucket. Access was no longer denied.



Saish Nar
NextWork Student

NextWork.org

Endpoint policies

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

I updated my endpoint's policy by changing the 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