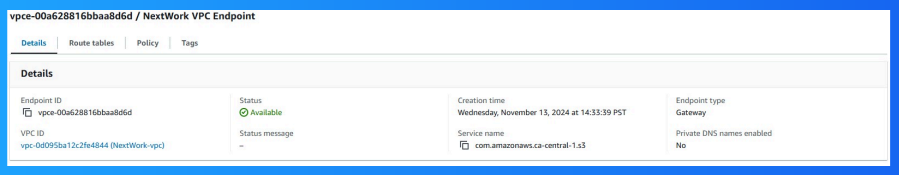
NextWork.org

# VPC Endpoints

Nikhil Bhan



N

**Nikhil Bhan**
NextWork Student



# Introducing Today's Project!

## What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) allows users to create a private and isolated network in their AWS account. They can manage and organize resources as well as configure permissions and access to those resources.

## How I used Amazon VPC in this project

In this project I used Amazon VPC to launch a VPC and a S3 Bucket. I created a VPC Endpoint to prevent traffic from going through the Internet to reach S3; during this process I set up policies on the bucket and the endpoint to control access.

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

I wasn't expecting to learn how to configure policies in VPC Endpoints and S3 Buckets to create secure connections in my AWS environment.

## This project took me...

This project took me 2 hours to complete. I took another 30 minutes to write my documentation as well.

N
**Nikhil Bhan**
NextWork Student
NextWork.org

# In the first part of my project...

## Step 1 - Architecture set up

In this step I'll create a VPC and launch an EC2 instance in it. I'll use EC2 Instance Connect to connect with my instance. I'm going to create an S3 Bucket as well.

## Step 2 - Connect to EC2 instance

In this step I'm going to connect directly to my EC2 instance on the AWS Management Console.

## Step 3 - Set up access keys

In this step I'll give my EC2 instance access to my AWS environment.

## Step 4 - Interact with S3 bucket

In this step I'm going to use my EC2 instance to access my S3 bucket.

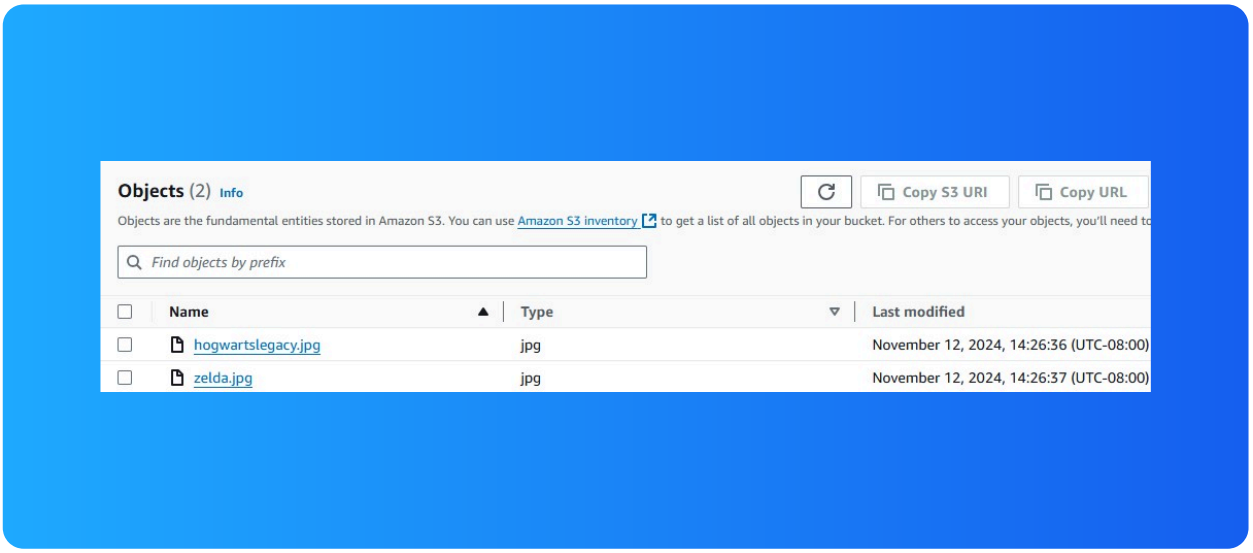
**Nikhil Bhan**
NextWork Student



# Architecture set up

I started my project by launching a VPC in my AWS account. I also created an EC2 instance with 1 Available Zone, 1 public subnet and a security group.

I also set up an S3 bucket, where I uploaded 2 image files to be stored.



N
**Nikhil Bhan**
NextWork Student


# Access keys

## Credentials

To set up my EC2 instance to interact with my AWS environment, I configured the Access Key ID, Secret Access Key and the Default Output Format which I kept empty. I also needed to specify the name of the Region, which is ca-central-1 (Canada).

Access keys are credentials that are used to provide applications access to AWS resources. The access keys are like the username and these can be set up manually in the AWS Management Console in the IAM service.

Secret Access Keys are like passwords; these keys are credentials that are used in combination with Access Key IDs. Both credentials are required to allow applications and servers access to AWS resources.

## Best practice

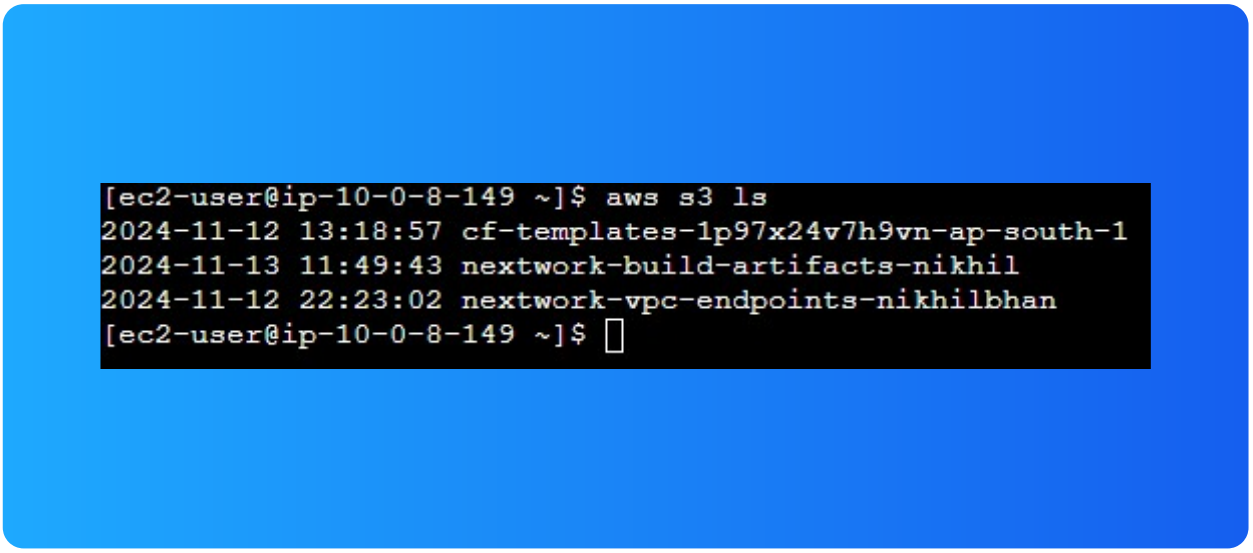
Although I'm using access keys in this project, a best practice alternative is to use a role which can be created in AWS Identity Access and Management (IAM). I can attach permissions to the role and then assign it to my EC2 instance.

N
**Nikhil Bhan**
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 that are in my AWS environment.

The terminal responded with a list of S3 buckets in my AWS environment. This indicated that the access keys I set up were configured correctly and the EC2 instance was able to use them to successfully connect to S3.



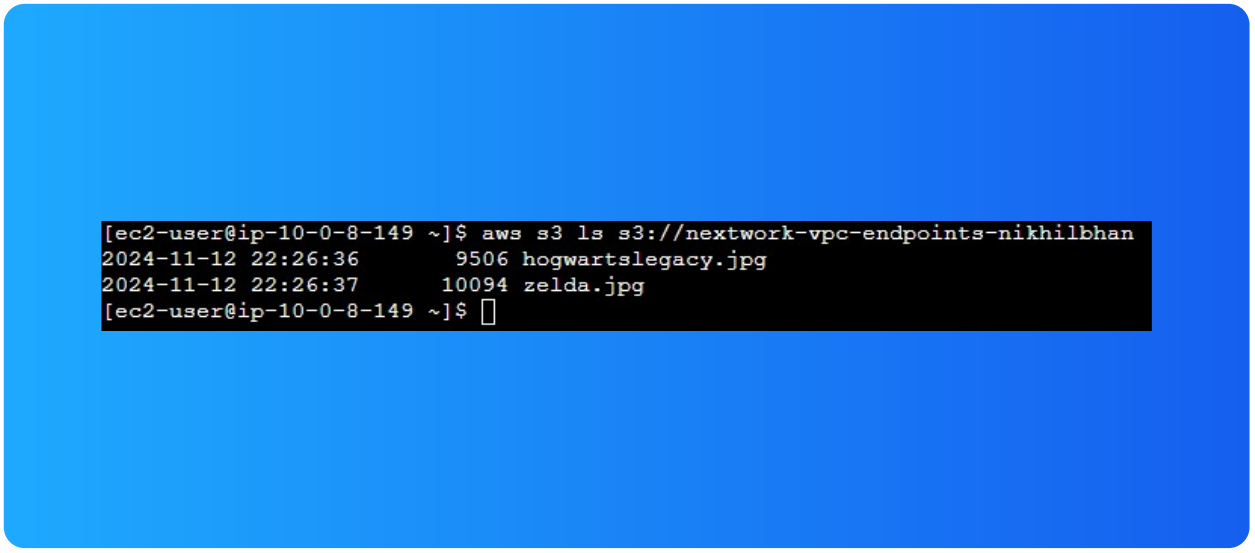
N

**Nikhil Bhan**
NextWork Student



# Connecting to my S3 bucket

I also tested the command aws s3 ls s3://nextwork-vpc-endpoints-nikhilbhan, which returned a list of the objects that were being stored in the S3 Bucket I created.



N

**Nikhil Bhan**
NextWork Student

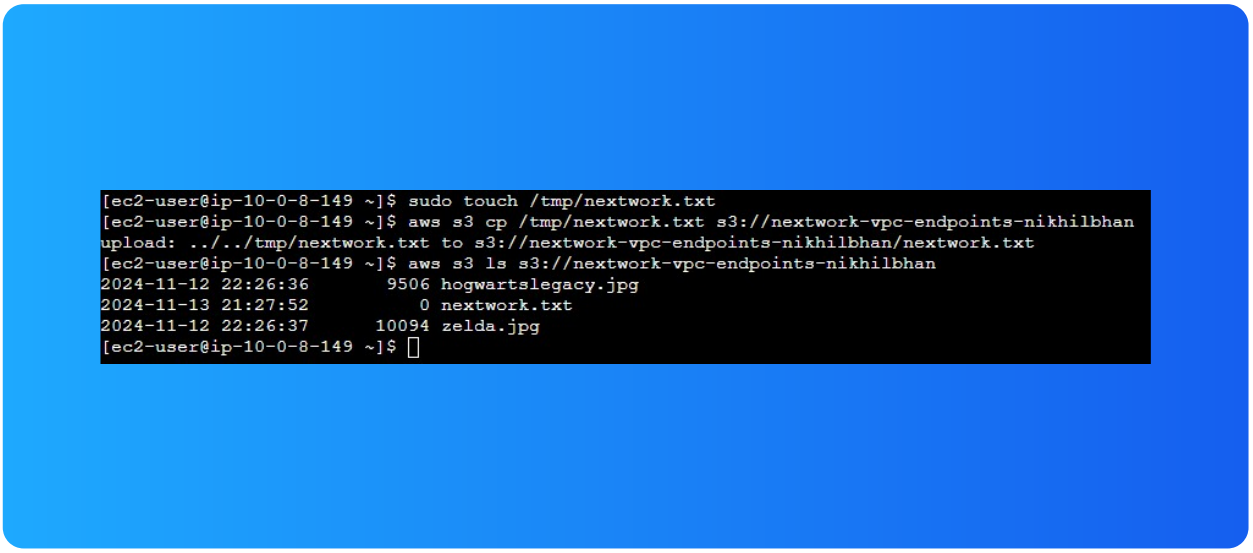


# Uploading objects to S3

To upload a new file to my bucket, I first ran the command sudo touch /tmp/nextwork.txt. This command creates an empty .txt document in the TMP directory (temporary) on my EC2 instance.

The second command I ran was aws s3 cp /tmp/nextwork.txt s3://nextwork-vpc-endpoints-nikhilbhan. This command will copy the nextwork.txt file on my EC2 instance and upload it to the S3 Bucket.

The third command I ran was aws s3 ls s3://nextwork-vpc-endpoints-nikhilbhan, which validated that the nextwork.txt file was successfully uploaded to the S3 bucket.



N
**Nikhil Bhan**
NextWork Student


# In the second part of my project...

## Step 5 - Set up a Gateway

In this step I'm going to configure my AWS environment so that my EC2 instance can connect directly to Amazon S3 instead of going throught the Internet, which would not be secure.

## Step 6 - Bucket policies

In this step I'll secure my S3 bucket by limiting access to only traffic coming from the endpoint I created.

## Step 7 - Update route tables

In this step I'm going to test the setup of my VPC Endpoint by accessing the S3 bucket and troubleshoot any issues that may occur.

## Step 8 - Validate endpoint conection

In this step I'm going to test the VPC endpoint again by using the EC2 instance to access the S3 bucket.

Nikhil Bhan
NextWork Student

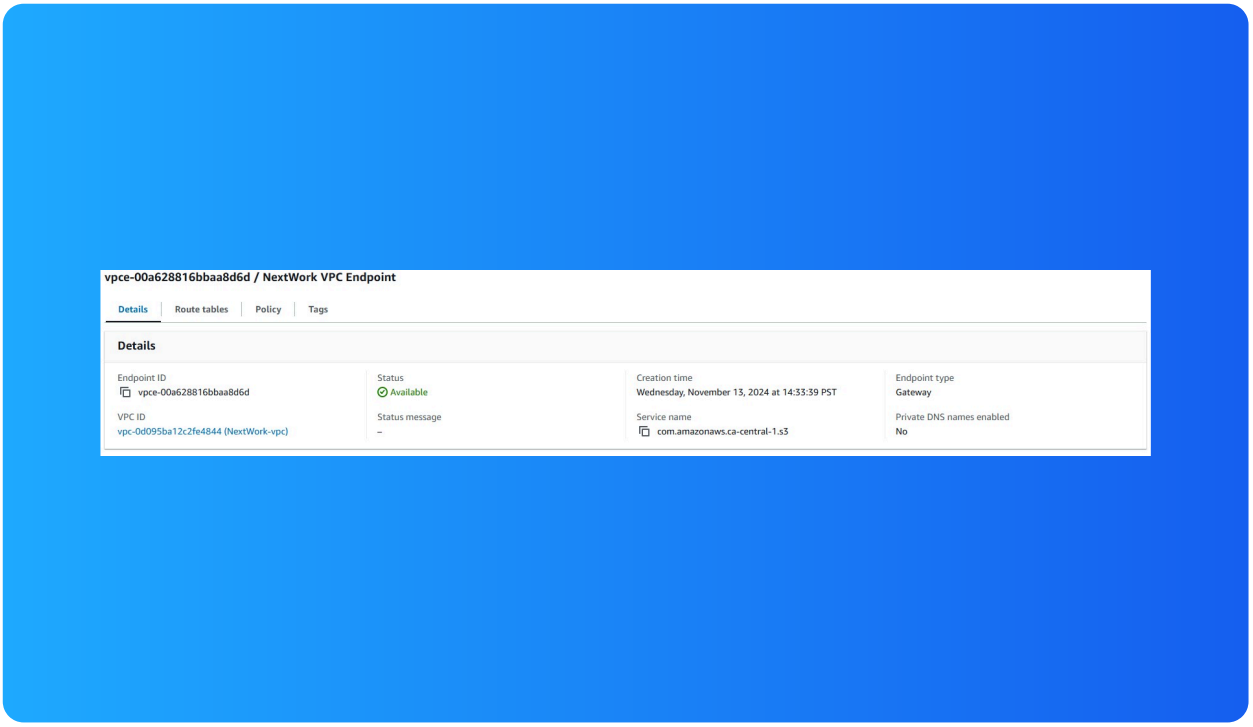


# Setting up a Gateway

I set up an S3 Gateway, which is a type of endpoint that's used primarily for Amazon S3. The gateway adds a route to my VPC route table that directs traffic in my network to get sent to S3 instead of going through the Internet to reach it.

## What are endpoints?

An endpoint is a service in AWS that allows a private connection between a VPC and other AWS services; this prevents traffic from going through the Internet to reach AWS services, which may not be secure.



N

**Nikhil Bhan**
NextWork Student



# Bucket policies

A bucket policy is a type of IAM policy and it's used to set access permissions to an S3 Bucket. By doing this the user can allow who can access the bucket and what actions would be permitted.

My bucket policy denies all actions on the S3 bucket and the objects to everyone. Only the VPC Endpoint defined by the VPC ID in the policy will be allowed to access the S3 bucket.

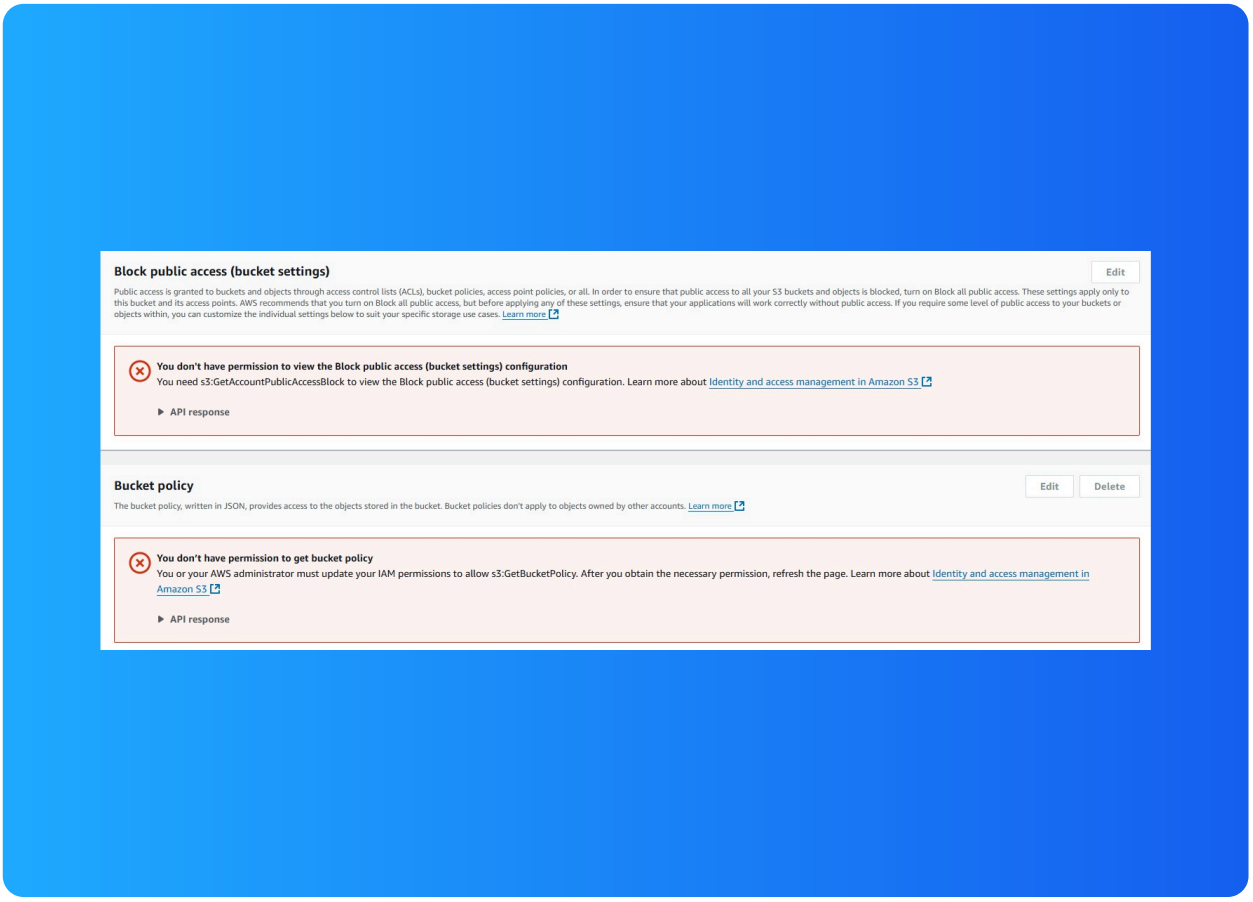
**Nikhil Bhan**
NextWork Student



# Bucket policies

Right after saving my bucket policy, my S3 bucket page showed 'Denied Access' warnings. This was because my policy denies all actions on the bucket, even from the AWS Management Console. Only my VPC Endpoint can access the bucket and objects.

I also had to update my route table because it controls where traffic goes in my network and if there's no direct route to S3 then the EC2 instance will try to send traffic through the Internet.



N
**Nikhil Bhan**
NextWork Student



# Route table updates

To update my route table, I added the public subnet to the VPC endpoint's route table. By doing this the VPC route table would be able to send traffic directly to S3 through the NextWork VPC Endpoint that I created.

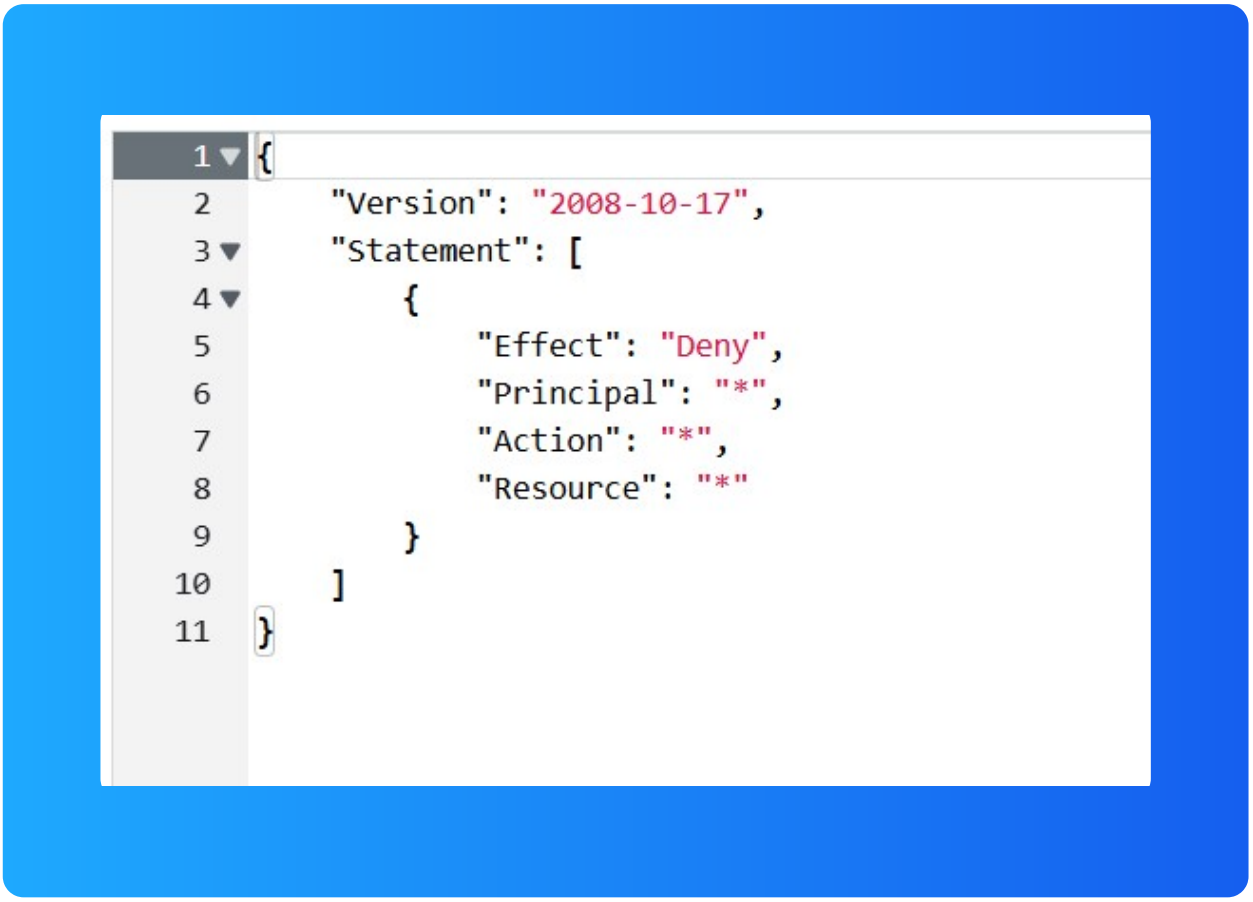
After updating my public subnet's route table, my terminal could return the list of objects in the S3 bucket.

N
**Nikhil Bhan**
NextWork Student


# Endpoint policies

An endpoint policy is a type of policy that specifies what resources and actions are allowed by an endpoint.

I updated my endpoint's policy by changing the policy's Effect statement from "Allow" to "Deny". I could see the effect of this right away, because I tried to use my EC2 instance to access the S3 bucket, but I was denied access.



# Everyone should be in a job they love.

Check out nextwork.org for more projects