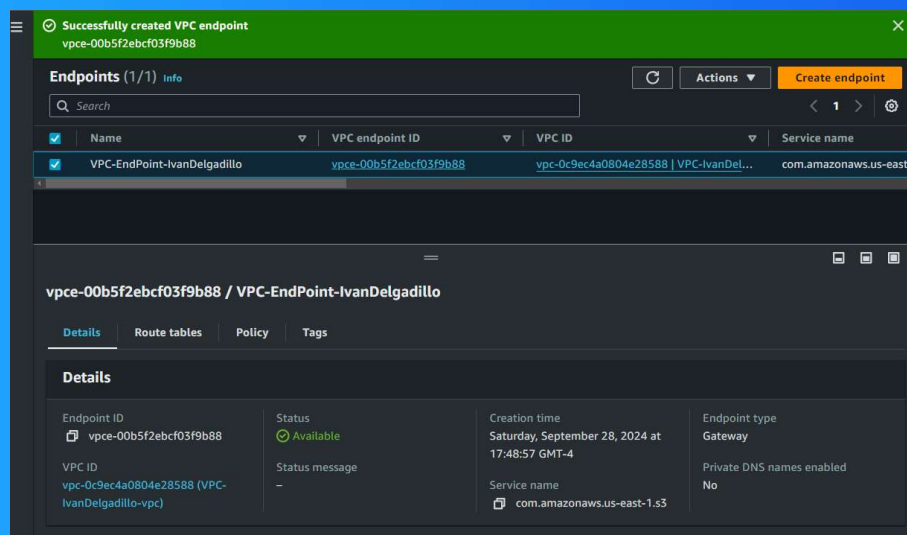




VPC Endpoints



Ivan Delgadillo Fernandez





Ivan Delgadillo Fernandez
NextWork Student

[NextWork.org](https://nextwork.org)

Introducing Today's Project!

What is Amazon VPC?

Amazon Virtual Private Cloud (Amazon VPC) gives you full control over your virtual networking environment, including resource placement, connectivity, and security.

How I used Amazon VPC in this project

I use VPC endpoint to access an S3 bucket.

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

I didn't expect configure policy editor

This project took me...

120 minutes



Ivan Delgadillo Fernandez
NextWork Student

[NextWork.org](https://nextwork.org)

In the first part of my project...

Step 1 - Architecture set up

Create a VPC from scratch! Launch an EC2 instance, which you'll connect to using EC2 Instance Connect later. Set up an S3 bucket.

Step 2 - Connect to EC2 instance

Connect directly to your EC2 instance.

Step 3 - Set up access keys

I will go create a access keys to access in the S3 bucket

Step 4 - Interact with S3 bucket

I'm going to connect to your S3 bucket using access keys



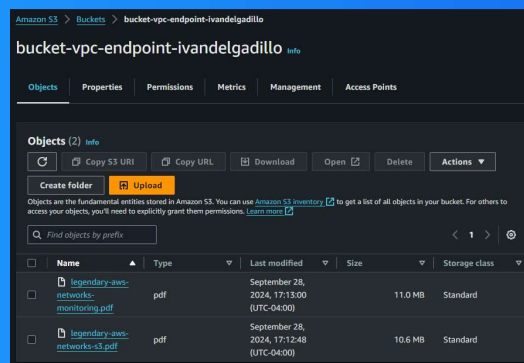
Ivan Delgadillo Fernandez
NextWork Student

[NextWork.org](https://nextwork.org)

Architecture set up

I launched a Public instance

I also setup S3 bucket





Ivan Delgadillo Fernandez
NextWork Student

[NextWork.org](https://nextwork.org)

Access keys

Credentials

To set up my EC2 instance to interact with my AWS environment, I configured Access Keys

Access keys are credentials for your applications and other servers to log into AWS and talk to your AWS services/resources

The Access Key ID and Secret Access Key are our AWS credentials for programmatic access to AWS services using APIs

Best practice

It is best practice to not have access keys assigned to your root user, to remove or delete old access keys, to rotate access keys regularly



Ivan Delgadillo Fernandez
NextWork Student

[NextWork.org](https://nextwork.org)

Connecting to my S3 bucket

The command I ran was "aws s3 ls" This command is used to listed a S3 buckets

The terminal responded with name of bucket and This indicated that the access keys I set up was successful

```
aws | Services | Search | Dashboard | Notifications | Help | Settings | N. Vi ▼
VPC | Billing and Cost Management | EC2 | IAM
[ec2-user@ip-10-0-5-13 ~]$
[ec2-user@ip-10-0-5-13 ~]$
[ec2-user@ip-10-0-5-13 ~]$ aws s3 ls
2024-09-28 21:12:14 bucket-vpc-endpoint-ivandelgadillo
[ec2-user@ip-10-0-5-13 ~]$
[ec2-user@ip-10-0-5-13 ~]$
```

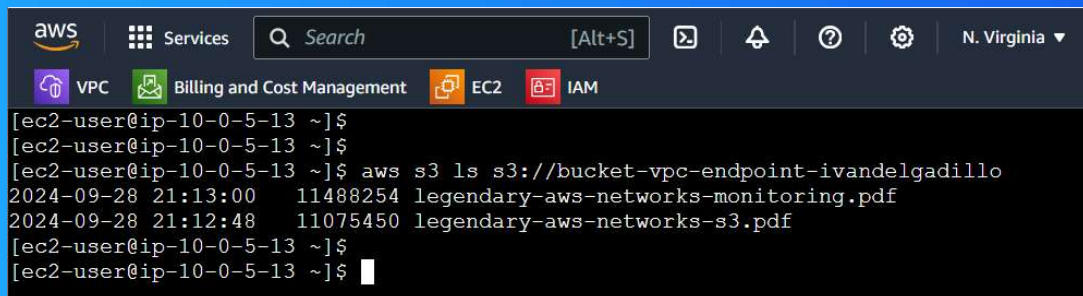


Ivan Delgadillo Fernandez
NextWork Student

NextWork.org

Connecting to my S3 bucket

I also tested the command "aws s3 ls s3://" which returned the list of files on S3 bucket



```
aws
Services Search [Alt+S]
VPC Billing and Cost Management EC2 IAM
[ec2-user@ip-10-0-5-13 ~]$
[ec2-user@ip-10-0-5-13 ~]$
[ec2-user@ip-10-0-5-13 ~]$ aws s3 ls s3://bucket-vpc-endpoint-ivandelgadillo
2024-09-28 21:13:00 11488254 legendary-aws-networks-monitoring.pdf
2024-09-28 21:12:48 11075450 legendary-aws-networks-s3.pdf
[ec2-user@ip-10-0-5-13 ~]$
[ec2-user@ip-10-0-5-13 ~]$
```



Ivan Delgadillo Fernandez
NextWork Student

NextWork.org

Uploading objects to S3

to upload a new file to my bucket, I first ran the command "sudo touch /tmp/ivandelgadillo.txt" This command creates a file

The second command I ran was "aws s3 cp /tmp... s3://" This command will upload the file to S3 bucket

The third command I ran was "aws s3 ls s3://..." which validated that file was uploaded.

```
aws
Services
Search [Alt+S]
VPC Billing and Cost Management EC2 IAM
[ec2-user@ip-10-0-5-13 ~]$
[ec2-user@ip-10-0-5-13 ~]$
[ec2-user@ip-10-0-5-13 ~]$ sudo touch /tmp/ivandelgadillo.txt
[ec2-user@ip-10-0-5-13 ~]$
[ec2-user@ip-10-0-5-13 ~]$ aws s3 cp /tmp/ivandelgadillo.txt s3://bucket-vpc-endpoint-ivandelgadillo
upload: ../../tmp/ivandelgadillo.txt to s3://bucket-vpc-endpoint-ivandelgadillo/ivandelgadillo.txt
[ec2-user@ip-10-0-5-13 ~]$
[ec2-user@ip-10-0-5-13 ~]$
[ec2-user@ip-10-0-5-13 ~]$ aws s3 ls s3://bucket-vpc-endpoint-ivandelgadillo
2024-09-28 21:32:15          0 ivandelgadillo.txt
2024-09-28 21:13:00    11488254 legendary-aws-networks-monitoring.pdf
2024-09-28 21:12:48    11075450 legendary-aws-networks-s3.pdf
[ec2-user@ip-10-0-5-13 ~]$
[ec2-user@ip-10-0-5-13 ~]$
```




Ivan Delgadillo Fernandez
NextWork Student

[NextWork.org](https://nextwork.org)

In the second part of my project...

Step 5 - Set up a Gateway

Set up a way for your VPC and S3 to communicate directly

Step 6 - Bucket policies

Limit your S3 bucket access's to only traffic from your endpoint

Step 7 - Update route tables

Test your VPC endpoint set up. Troubleshoot a connectivity issue

Step 8 - Validate endpoint connection

Test VPC endpoint set up (again). Restrict your VPC's access to your AWS environment



Ivan Delgadillo Fernandez
NextWork Student

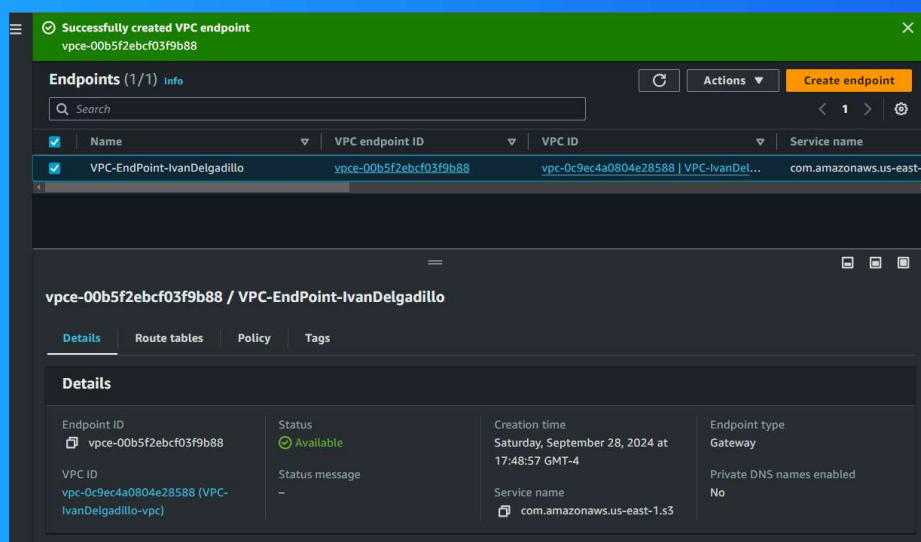
[NextWork.org](https://nextwork.org)

Setting up a Gateway

A Gateway is a type of endpoint used specifically for Amazon S3 and DynamoDB (DynamoDB is an AWS database service). Gateways work by simply adding a route to your VPC route table that directs traffic bound for S3 or DynamoDB to head straight for the

What are endpoints?

An endpoint is connection privately





Bucket policies

A bucket policy is a type of IAM policy designed for setting access permissions to an S3 bucket. Using bucket policies, you get to decide who can access the bucket and what actions they can perform with it.

My bucket policy will permit allow to endpoint

Policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Deny",  
6       "Principal": "*",  
7       "Action": "s3:*",  
8       "Resource": [  
9         "arn:aws:s3:::bucket-vpc-endpoint-ivandelgadillo",  
10        "arn:aws:s3:::bucket-vpc-endpoint-ivandelgadillo/*"  
11      ],  
12      "Condition": {  
13        "StringNotEquals": {  
14          "aws:sourceVpce": "vpce-00b5f2ebcf03f9b88"  
15        }  
16      }  
17    }  
18  ]  
19 }  
20 }
```



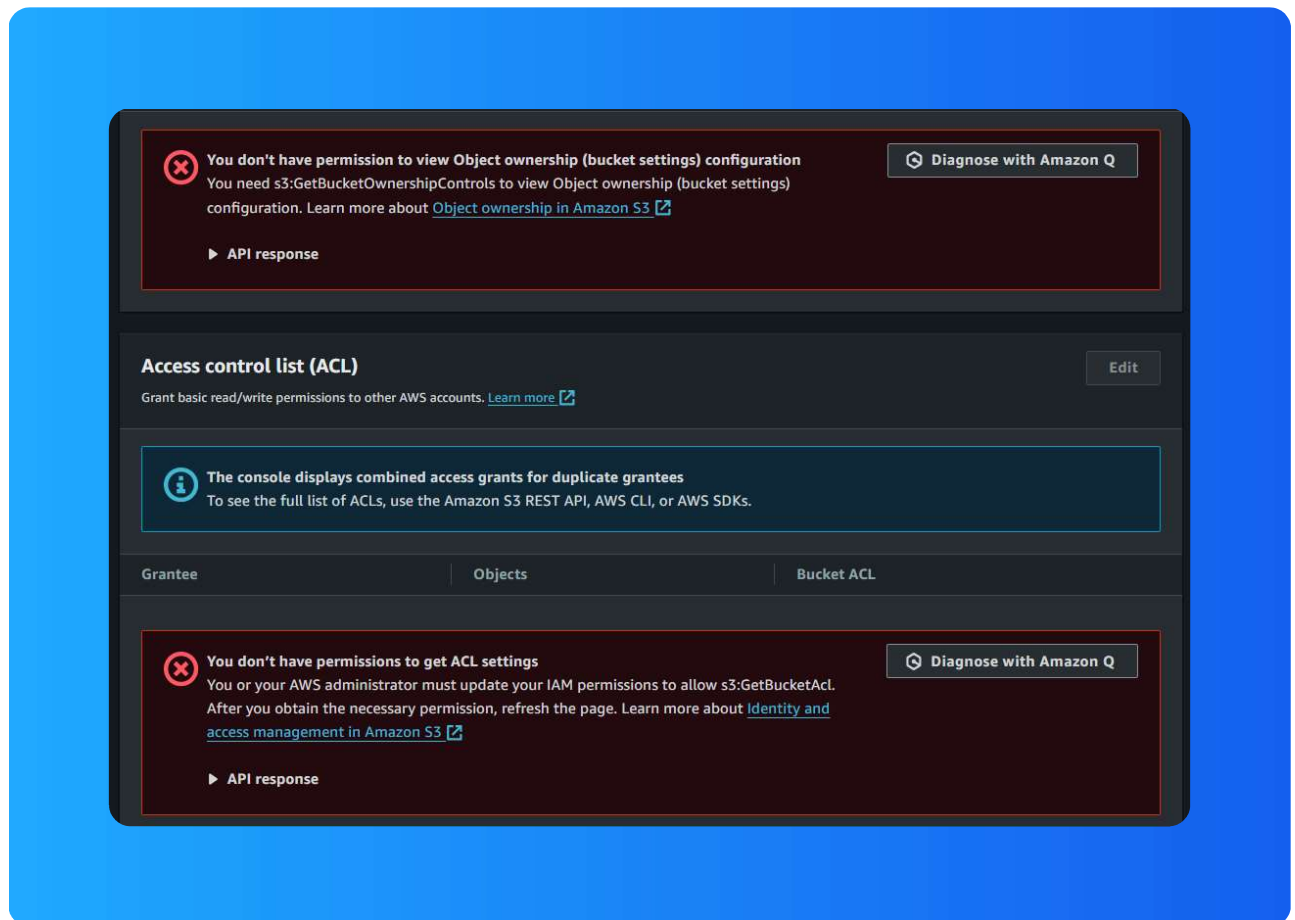
Ivan Delgadillo Fernandez
NextWork Student

NextWork.org

Bucket policies

Right after saving my bucket policy, my S3 bucket page showed 'denied access' warnings. This was because the policy denies all actions unless they come from your VPC endpoint.

I also had to update my route table because the route was not at the VPC endpoint





Ivan Delgadillo Fernandez
NextWork Student

[NextWork.org](https://nextwork.org)

Route table updates

To update my route table, I modify routes tables on VPC endpoint

After updating my public subnet's route table, my terminal could return the access successfully.

subnet-09e9f20f403f3ef1b / VPC-IvanDelgadillo-subnet-public1-us-east-1a

Details Flow logs **Route table** Network ACL CIDR reservations Sharing Tags

Route table: rtb-0787ab1f4df15f648 / VPC-IvanDelgadillo-rtb-public [Edit route table association](#)

Routes (3)

< 1 > ⚙

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-05be28c7e19113231
pl-63a5400a	vpce-00b5f2ebcf03f9b88



Ivan Delgadillo Fernandez
NextWork Student

NextWork.org

Endpoint policies

An endpoint policy is control to allow or deny access.

I updated my endpoint's policy by "Effect: Deny" I could see the effect of this right away, because it is more granular





Everyone should be in a job they love.

Check out nextwork.org for
more projects

