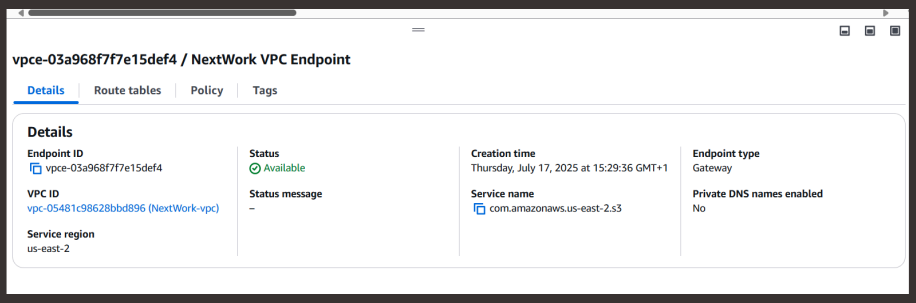
nextwork.org

VPC Endpoints

Joba Amunigun
https://www.linkedin.com/in/dvoice



Joba Amunigun
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

What is Amazon VPC and why is it useful? Amazon VPC (Virtual Private Cloud) is a secure and customizable virtual network that I can build inside AWS. It gives me full control over my cloud network setup—IP ranges, subnets, routing, and security. It's useful because it allows me to: Isolate and secure my resources, like EC2 instances and databases, in a private environment. Control how data flows, both inside the network and to the internet. Design real-world infrastructure that mimics what companies use in production. Build smarter architecture that scales, protects data, and connects services with precision. In short, Amazon VPC is the backbone of any serious cloud environment, and understanding it helps me build infrastructure that's both secure and production-ready.

How I used Amazon VPC in this project

I used Amazon VPC today to set up VPC Endpoints ,specifically S3 Gateway. This provides the VPC direct access to another AWS services

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

One thing i didn't expect was to see my own access to the S3 Bucket getting blocked . Once i saved my Bucket new policy to block all access/traffic except traffic from my endpoint.

Joba Amunigun
NextWork Student

This project took me...

This project took me about 3 hours, including setup, testing, and exploring how VPC endpoints interact with S3. I also spent extra time understanding endpoint policies and fine-tuning access control — it was worth it to see everything working smoothly.

Joba Amunigun
NextWork Student

In the first part of my project...

Step 1 - Architecture set up

In this step , I will be setting up the foundation of this project . I.e. Creating a VPC ,Launching an EC2 instance ,Setting up an S3 bucket. So that i can set up an end point architecture and test that set up in the last step of the project

Step 2 - Connect to EC2 instance

In this step, I am connecting directly to my EC2 Instance - Connecting to the EC2 Instance will help me access Amazon S3 and learn 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 my AWS Environment - We can think of access keys like "login details" for EC2 Instances/Applications (non humans) to interact with the AWS Services

Step 4 - Interact with S3 bucket

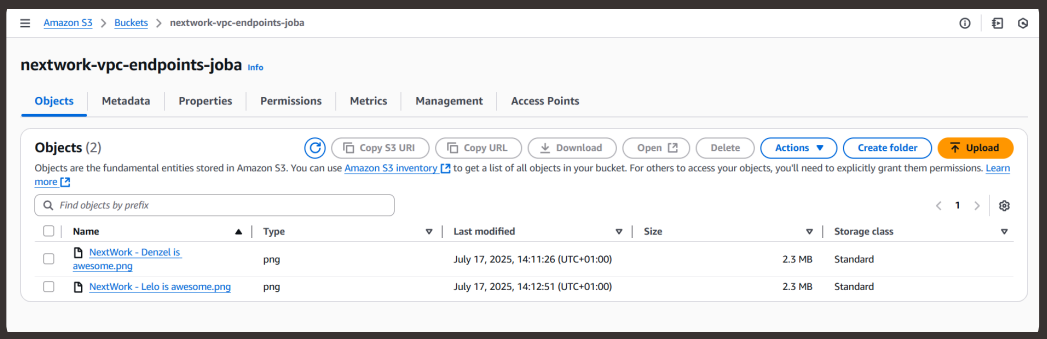
In this step, I will be applying my ACCESS KEY credentials to my EC2 Instance and then using AWS CLI and my EC2 Instance to access Amazon S3

Joba Amunigun
NextWork Student

Architecture set up

I started my project by launching three key resources - VPC ,EC2 Instance and S3 Bucket.

I also set up an Amazon S3 bucket named nextwork-vpc-endpoints-joba as part of this step. After creating the bucket, I uploaded two test files into it to simulate real-world data storage and validate access from my private EC2 instance using the VPC Gateway Endpoint.




Joba Amunigun
NextWork Student

Access keys

Credentials

To set up my EC2 instance to interact with my AWS environment, I configured AWS Access Key ID , AWS Secret Access Key , Default region name and Default output format

Access keys are a part of a credential (made up of a username and password) for your applications and other servers to log into AWS and talk to your AWS services/resources.

Secret access key is like the password that pairs with your access key ID (your username). You need both to access AWS services. Secret is a key word here - anyone who has it can access your AWS account, so we need to keep this away from anyone else!

Best practice

Although I'm using access keys in this project, a best practice alternative is to use IAM admin roles instead! This means that the necessary permission will be attached to an IAM role and then the role will be associated with the relevant resources

Joba Amunigun
NextWork Student

Connecting to my S3 bucket

The command I ran was "aws s3 ls". This command is used to to LIST all the S3 BUCKETS in the AWS account.

The terminal responded with a list of my accounts S3 buckets .This indicated that the access keys was set up correctly and can give my EC2 Instance access to my AWS account and environment

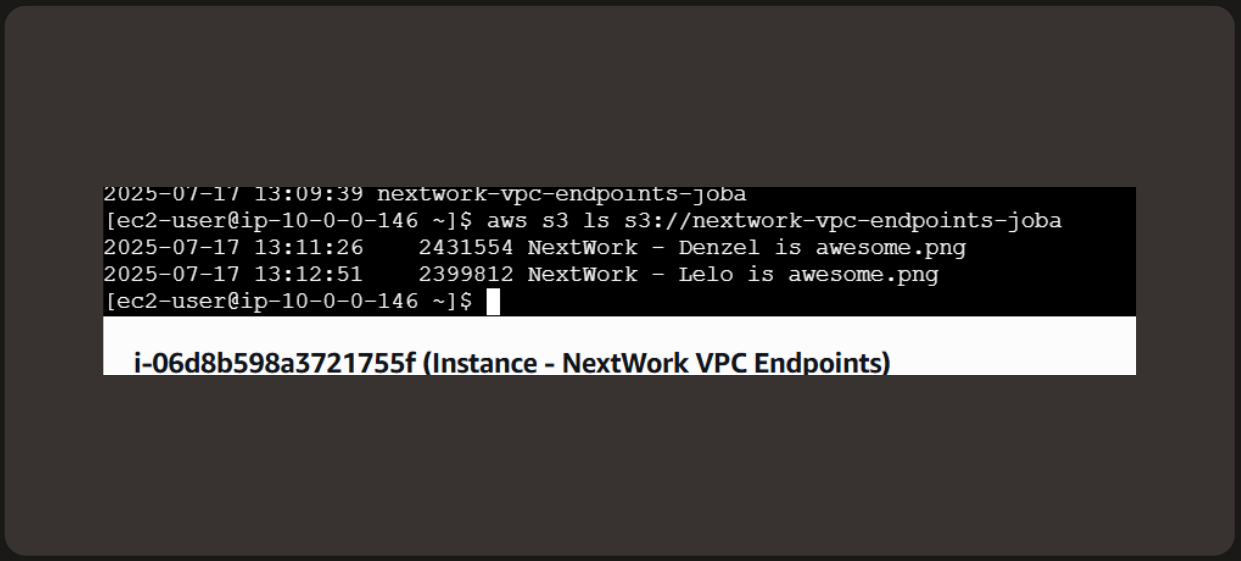
```
usage: aws [options] s3 <subcommand> [parameters]
aws: error: too few arguments
[ec2-user@ip-10-0-0-146 ~]$ aws s3 ls

Unable to locate credentials. You can configure credentials by running "aws configure".
[ec2-user@ip-10-0-0-146 ~]$ aws configure
AWS Access Key ID [None]: AKIAVX5RHRPESR6J3UWK
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-2
Default output format [None]:
[ec2-user@ip-10-0-0-146 ~]$ aws s3 ls
2025-07-17 13:09:39 nextwork-vpc-endpoints-joba
[ec2-user@ip-10-0-0-146 ~]$
```

Joba Amunigun
NextWork Student

Connecting to my S3 bucket

I also tested the command "aws s3 ls s3://nextwork-vpc-endpoints-yourname" which returned a list of all of the OBJECTS (Uploaded files) that are inside my bucket



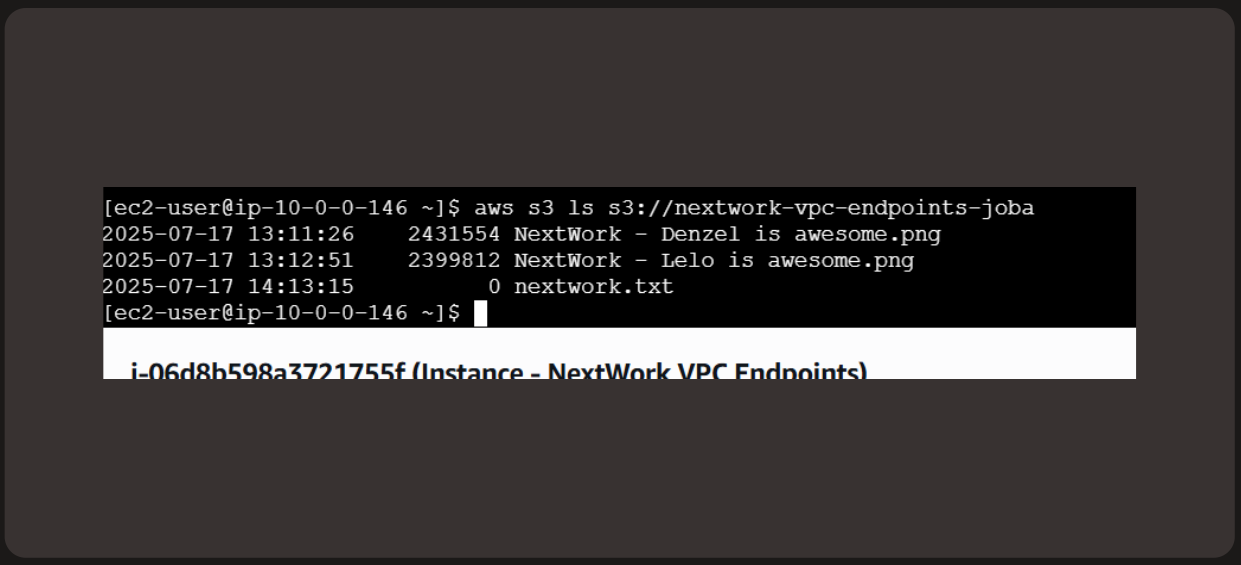
Joba Amunigun
NextWork Student

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 file named "nextwork.txt" and save it locally in the EC2 Instance.

The second command I ran was "aws s3 cp /tmp/nextwork.txt s3://nextwork-vpc-endpoints-joba" . 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-yourname" again .which validated that a new file was created and uploaded into my S3 Bucket.




Joba Amunigun
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 will be testing my Endpoint connection by blocking off ALL traffic to my S3 Bucket ,execpt for traffic coming from my endpoint.

Step 7 - Update route tables

In this step , i will be testing my VPC endpoint set up - Making sure that S3 bucket's access is only limited to the endpoint, and confirming that my EC2 instance doesn't have access to my bucket. Troubleshoot a connectivity issue.

Step 8 - Validate endpoint conection

In this step , I will be VALIDATING my VPC Endpoint setup one more time. I am also going to use end points policies to restrict EC2 access to my AWS Environment .

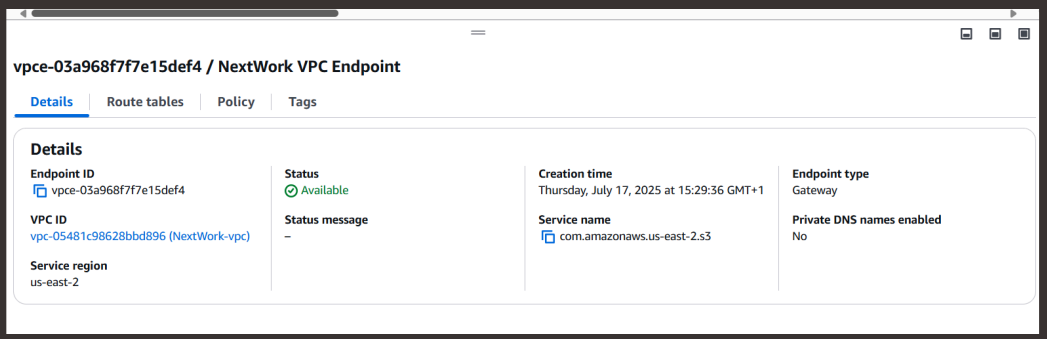
Joba Amunigun
NextWork Student

Setting up a Gateway

I set up an S3 Gateway, which 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 Gateway instead of the internet.

What are endpoints?

An endpoint is 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. - making sure your data stays within the AWS network for security.

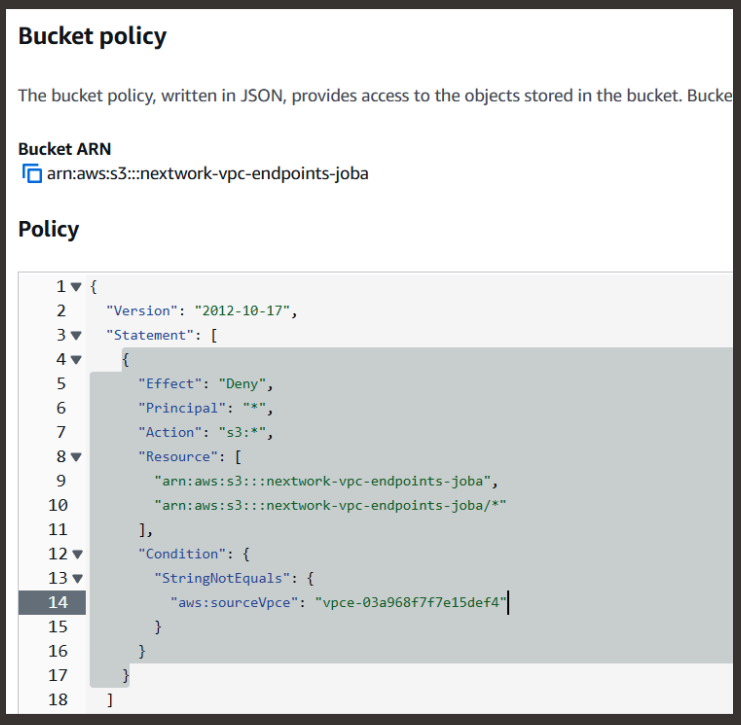


Joba Amunigun
NextWork Student

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 deny traffic from ALL sources execpt for traffic coming from my VPC endpoint.

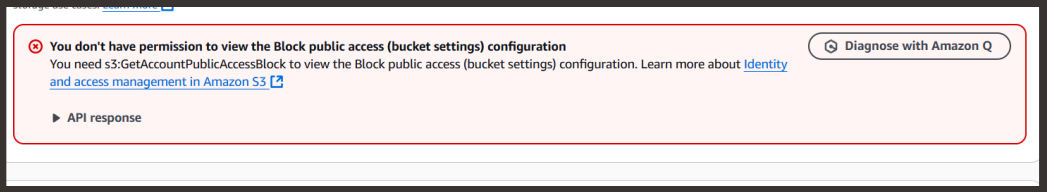



Joba Amunigun
NextWork Student

Bucket policies

Right after saving my bucket policy, my S3 bucket page showed 'denied access' warnings. This was because the bucket policy set denies all actions unless they come from your VPC endpoint. This means any attempt to access the bucket from other sources, including the AWS Management Console, will be blocked! . This is why permission to ("Block public access (bucket settings)" ,"Object Ownership","Access control list (ACL)", "Cross-origin resource sharing (CORS)") is denied.

I also had to update my route table because my route table doesn't have a route that directs traffic bound for S3 to your VPC endpoint. Hence, traffic from my EC2 instance is actually trying to get to my S3 bucket through the public internet instead. -(The route table is the GPS / traffic controller directing traffic from your EC2 instances.)


You don't have permission to view the Block public access (bucket settings) configuration
You need s3:GetAccountPublicAccessBlock to view the Block public access (bucket settings) configuration. Learn more about Identity and access management in Amazon S3
Diagnose with Amazon Q
API response

Joba Amunigun
NextWork Student

Route table updates

To update my route table, I visisted the Endpoint page of my VPC console and I modified the route table from there to associate my VPC Public Subnet.

After updating my public subnet's route table, my terminal (EC2 Instance) could access my S3 Bucket. Access was no longer denied

```
ec2-user@ip-10-0-0-146 ~]$ aws s3 ls s3://nextwork-vpc-endpoints-joba
025-07-17 13:11:26    2431554 NextWork - Denzel is awesome.png
025-07-17 13:12:51    2399812 NextWork - Lelo is awesome.png
025-07-17 14:13:15          0 nextwork.txt
ec2-user@ip-10-0-0-146 ~]$
```

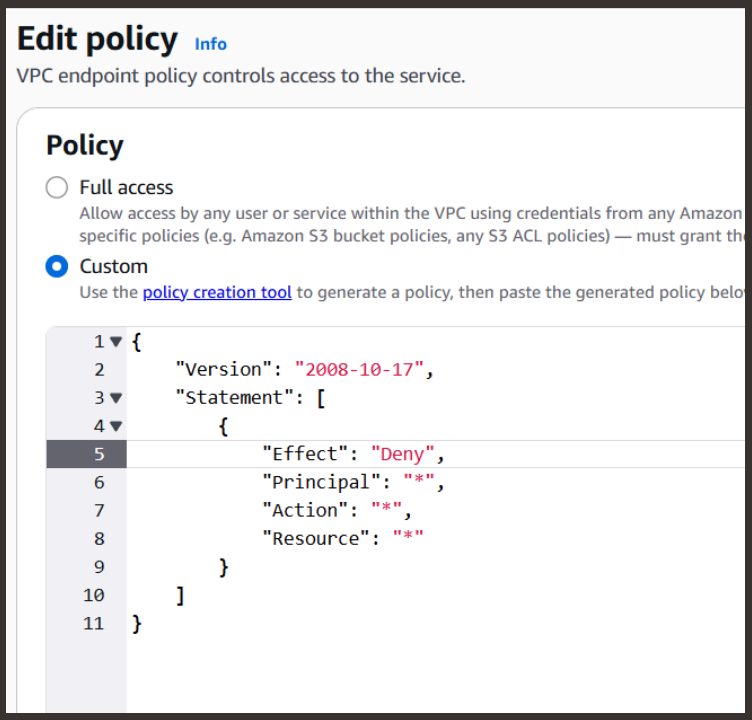

Joba Amunigun
NextWork Student

Endpoint policies

An endpoint policy is a JSON-based resource policy attached to a VPC endpoint that controls which AWS services and actions can be accessed through that endpoint. It acts as a permissions filter at the network level, allowing you to define what services your resources can talk to over the endpoint, and who is allowed to do so. This is especially useful for tightening access—ensuring only specific buckets, services, or actions are allowed from your private resources without exposing them to the public internet.

'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 once again denied access to my S3 Bucket when i tried another AWS S3 command i.e "aws s3 ls s3://nextwork-vpc-endpoints-joba" ,

Joba Amunigun
NextWork Student



nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects