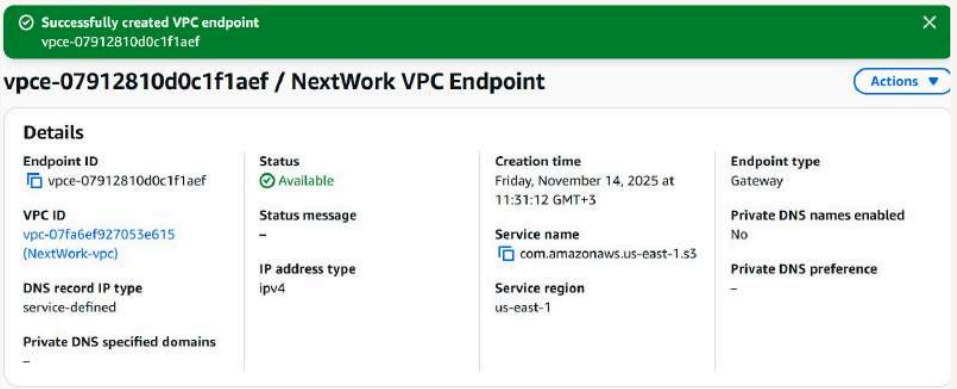
nextwork.org

VPC Endpoints

GA Mohamed Galole



GA
Mohamed Galole
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a private, isolated virtual network within AWS where you can launch and control your cloud resources. It is useful because it lets you manage networking, security, and traffic flow.

How I used Amazon VPC in this project

I used Amazon VPC in today’s project to build a secure network environment, create a public subnet, and launch my EC2 instance inside it. I also set up a VPC Endpoint so the instance could access my S3 bucket privately.

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

One thing I didn't expect in this project was how easily a strict bucket policy could lock me out of my own S3 bucket. It showed me how powerful and sensitive resource-based permissions are when working with VPC Endpoints and private access.

Mohamed Galole
NextWork Student

This project took me...

This project took me two hours to complete.

GA
Mohamed Galole
NextWork Student
nextwork.org

In the first part of my project...

Step 1 - Architecture set up

In this step, I will create new VPC then launch an EC2 instance inside the VPC. I will later connect to this EC2 instance using EC2 Instance Connect. I will create an S3 bucket, which will be used later to test secure access through a VPC endpoint.

Step 2 - Connect to EC2 instance

In this step, I will connect to my EC2 using EC2 Instance Connect and try to access my S3 bucket through the public internet. I'm doing this because it establishes a baseline to confirm that the EC2 instance can reach S3 before adding VPC endpoint

Step 3 - Set up access keys

In this step, I will create access keys for my IAM user so that my EC2 instance can access my AWS environment using the AWS CLI. I'm doing this because access keys allow programmatic access to AWS services

Step 4 - Interact with S3 bucket

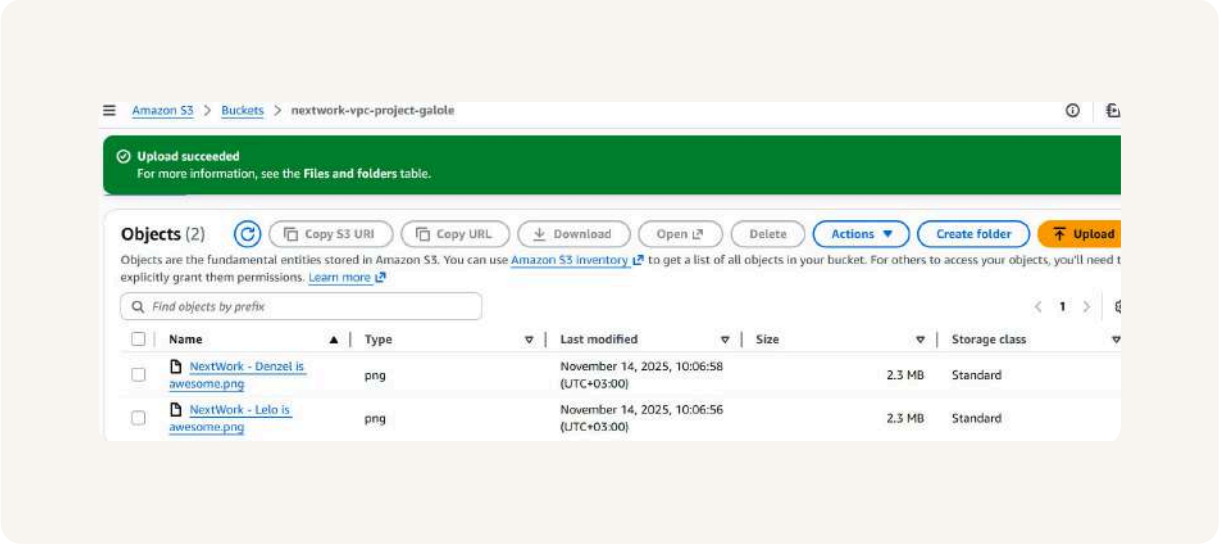
In this step, I will configure my EC2 instance to access my S3 bucket using the access keys I created. I'm doing this because it allows me to test connectivity and ensure that my instance can interact with S3 before setting up the VPC Endpoint.

Mohamed Galole
NextWork Student

Architecture set up

I started my project by creating a new VPC with one public subnet, an Internet Gateway, and the necessary route table for internet access. I launched an EC2 instance inside the public subnet and created a security group to control its traffic.

I created an S3 bucket and uploaded two objects in it.



GA
Mohamed Galole
NextWork Student
nextwork.org

Access keys

Credentials

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

Access keys are a pair of credentials (an Access Key ID and a Secret Access Key) that allow programmatic access to AWS services. They are used by the AWS CLI, SDKs, or applications to authenticate and make API calls to your AWS account.

A Secret Access Keys are the confidential part of an AWS access key pair, used together with the Access Key ID to authenticate and authorize programmatic requests to AWS services. It acts like a password, so it must be kept secure and never shared.

Best practice

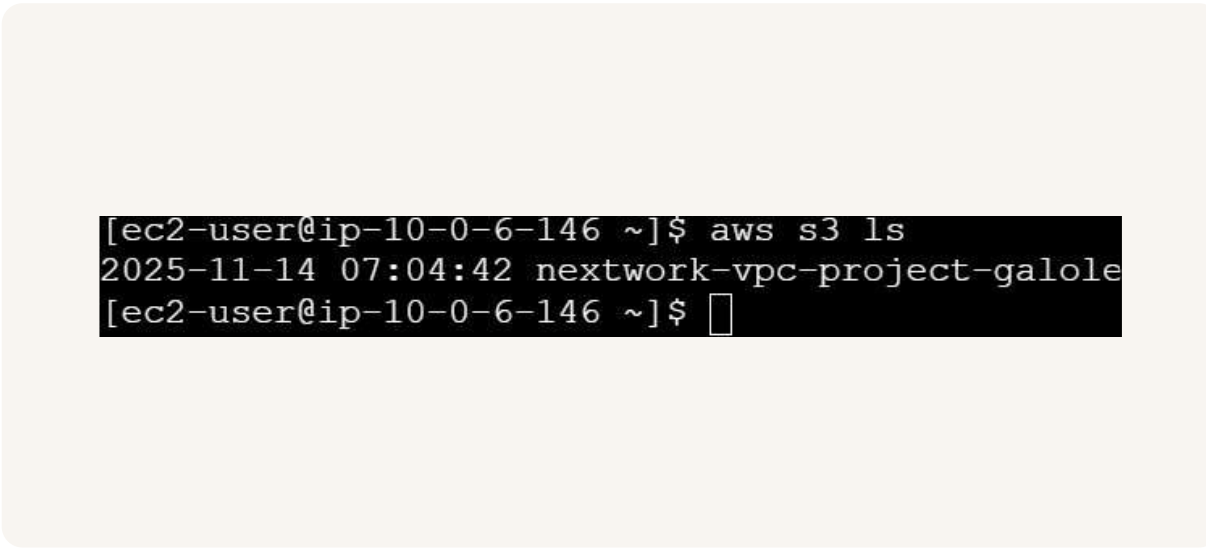
Although I’m using access keys in this project, a best-practice alternative is to use IAM roles. Roles provide temporary, automatically rotated credentials and remove the need to store or expose access keys on your EC2 instance.

GA
Mohamed Galole
NextWork Student

Connecting to my S3 bucket

The command I ran was aws s3 ls. This command is used to list all S3 buckets that my IAM credentials have permission to access. It helps verify that my EC2 instance can reach S3 over the public internet before I configure the VPC Endpoint.

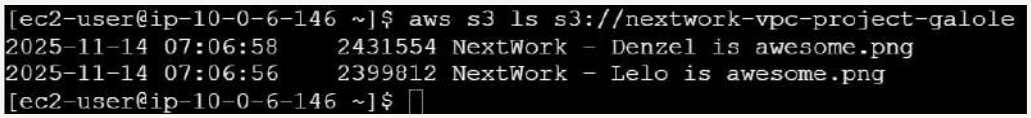
The terminal responded with nextwork-vpc-project-galole, the bucket I created. This indicated that the access keys I set up were working correctly and that my EC2 instance could successfully access and list my S3 bucket.



GA
Mohamed Galole
NextWork Student

Connecting to my S3 bucket

I also tested the command aws s3 ls s3://nextwork-vpc-project-galole which returned the list of objects inside the bucket. This confirmed that my EC2 instance had proper access to the specific S3 bucket.



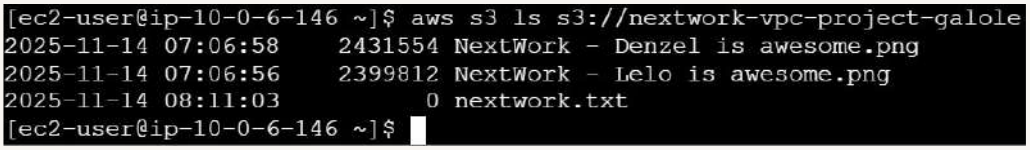
Mohamed Galole
NextWork Student

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 in the /tmp directory, which I can then upload to my S3 bucket.

The second command I ran was aws s3 cp /tmp/nextwork.txt s3://nextwork-vpc-project-galole This command wil upload the local file nextwork.txt to my S3 bucket, making it available in the cloud.

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



GA
Mohamed Galole
NextWork Student

In the second part of my project...

Step 5 - Set up a Gateway

In this step, I will set up a VPC Endpoint so my VPC can communicate directly with my S3 bucket without using the public internet. I'm doing this because it provides a secure, private connection between my EC2 instance and S3, improving security.

Step 6 - Bucket policies

My next step is to restrict my S3 bucket so that it only accepts traffic coming from my VPC Endpoint. This means that even if someone tries to access the bucket over the public internet, they won't be able to only resources inside my VPC.

Step 7 - Update route tables

In this step, I will test my VPC Endpoint by trying to access the S3 bucket from my EC2 instance and troubleshoot any connectivity issues that arise. I'm doing this because it ensures that the endpoint is correctly configured.

Step 8 - Validate endpoint conection

In this step, I will test my VPC Endpoint again to confirm that my EC2 instance can access the S3 bucket privately and then restrict the VPC’s access to my AWS environment by tightening IAM roles and bucket policies.

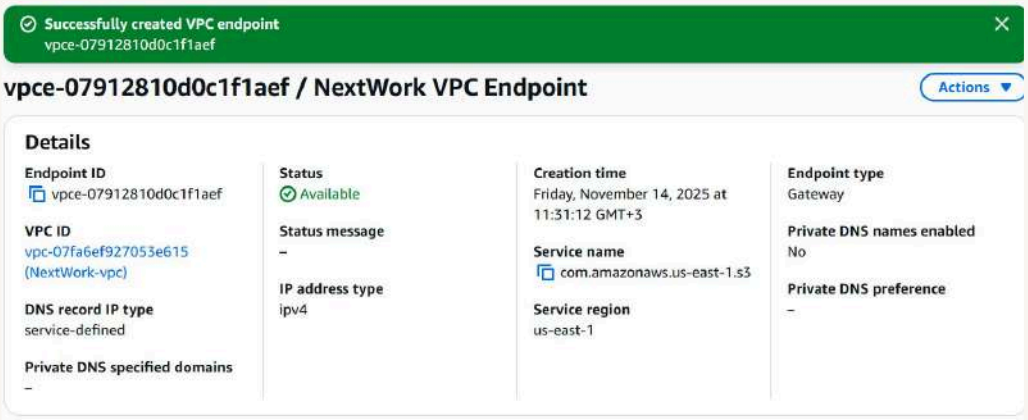
GA
Mohamed Galole
NextWork Student

Setting up a Gateway

I set up an S3 Gateway, which is a type of VPC Endpoint that provides a target in your VPC route table to connect to supported AWS services like S3 or DynamoDB.

What are endpoints?

An endpoint is a network interface that allows private connections between your VPC and AWS services without using the public internet. It enables resources in your VPC, like EC2 instances, to securely access services such as S3 or DynamoDB directly.



GA
Mohamed Galole
NextWork Student

Bucket policies

A bucket policy is a JSON-based access control document attached to an S3 bucket that defines who can access the bucket and what actions they can perform. It allows you to set permissions at the bucket level.

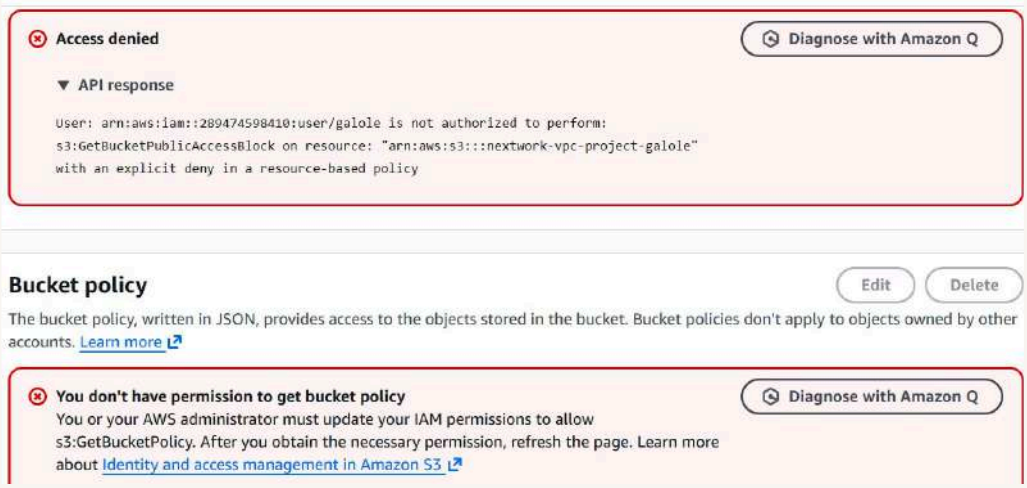
My bucket policy restricts access to the S3 bucket so that only traffic coming from my VPC Endpoint is allowed. This ensures that no one can access the bucket over the public internet, keeping the data secure and accessible only from my VPC.

GA
Mohamed Galole
NextWork Student

Bucket policies

Right after saving my bucket policy, my S3 bucket page showed 'denied access' . This was because the policy I applied restricted access too tightly, and my IAM user didn’t have permission to perform s3:GetBucketPolicy or other necessary actions.

I updated my route table to ensure that traffic from my VPC to S3 is directed through the VPC Endpoint. This is necessary because, without the correct route, requests to S3 would still try to go over the public internet instead of private connection

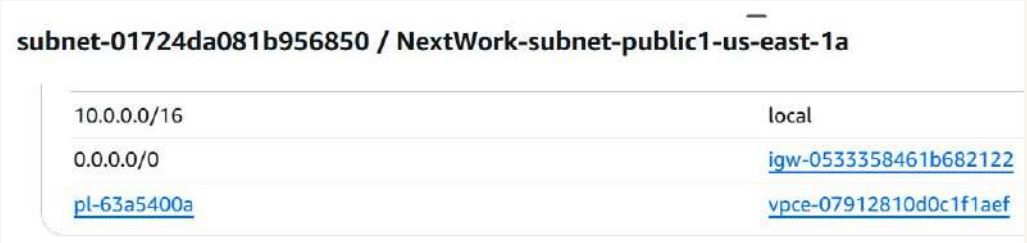


GA
Mohamed Galole
NextWork Student

Route table updates

To update my route table, I added a route that directs all traffic for the S3 service to the VPC Endpoint. This ensures that any requests from my VPC to S3 go through the private endpoint instead of the public internet

After updating my public subnet's route table, my terminal could return list of objects I uploaded to the bucket.



Mohamed Galole
NextWork Student

Endpoint policies

An endpoint policy is a JSON-based document attached to a VPC Endpoint that controls what actions and resources can be accessed through that endpoint.

I updated my endpoint's policy by restricting it so that the VPC Endpoint could only access my specific S3 bucket instead of all S3 buckets in my account. I could see the effect of this right away because any attempt to access other S3 buckets failed

The place to learn & showcase your skills

Check out nextwork.org for more projects