



nextwork.org

VPC Endpoints

LW

lwazi995@outlook.com

Introducing two new types of endpoints: Resource endpoint and Service network endpoint
Use a Resource endpoint to access a VPC resource (ARN-based resource, domain name and IP address) in another VPC. Use a Service network endpoint to access a VPC Lattice service network. Learn more [? \[2\]](#)

vpce-00bd19e84b90657c9 / NextWork VPC Endpoint

Actions ▾

Details		Creation time		Endpoint type
Endpoint ID	vpce-00bd19e84b90657c9	Status	Available	Gateway
VPC ID	vpc-038d5643439695b3b (NextWork-vpc)	Status message	-	Private DNS names enabled
		Service name	com.amazonaws.us-east-1.s3	No

Route tables | Policy | Tags

Route tables

[Manage route tables](#)

Name	Route Table ID	Main	Associated Id
No route tables attached to endpoint			

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is allows you to create a private network within AWS. It gives you control over IP ranges, subnets and security. Making it ideal for hosting secure applications and resources in a cloud environment.

How I used Amazon VPC in this project

In todays project we used VPC within our EC2 instance to allow access or deny access using our endpoints policy and implementing it through our S3 Gateway and buckets. This provides our VPC direct, private access.

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

I didn't expect the error message I got when from the S3 bucket that denied access and only allowed it to a certain VPC.

This project took me...

The project in particular took me about 3 and half hours to complete.

In the first part of my project...

Step 1 - Architecture set up

In this step we are setting up the foundations of this project (i.e. Launching VPC EC2 instant and S3 bucket) so that we can set up an Endpoint architecture and test it and test that set up in the last step of this project.

Step 2 - Connect to EC2 instance

In this step we are connecting directly to our EC2 using our EC2 connect this will help us access S3 and run commands later in the project.

Step 3 - Set up access keys

In this step I am going to give the EC2 instance access to your AWS environment. We can think of access keys almost like login details for EC2, Applications and non-humans to interact with our AWS services.

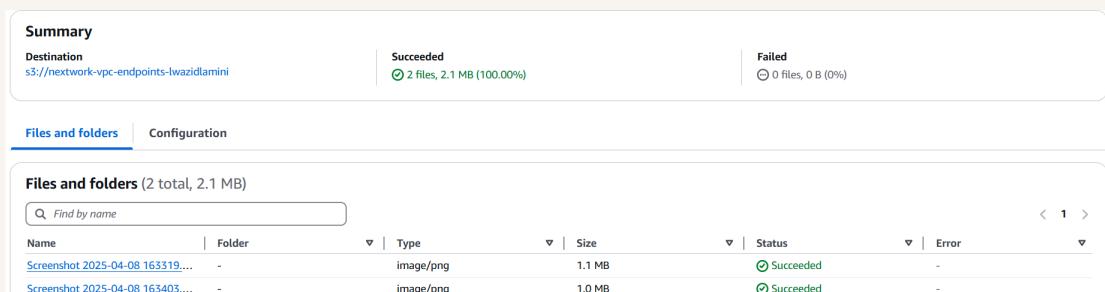
Step 4 - Interact with S3 bucket

In this step we are applying our access key credentials to our EC2 instance, and then using AWS CLI and our EC2 instance to access Amazon S3.

Architecture set up

I started my project by launching 3 key services a VPC,EC2 instance and S3 bucket.

I also set up my S3 bucket and added two files to the bucket from my local computer.



The screenshot shows the AWS Lambda function configuration page. At the top, there's a summary section with the destination URL `s3://nextwork-vpc-endpoints-lwazidlamini`. Below it, a table shows the upload status:

Succeeded	Failed
2 files, 2.1 MB (100.00%)	0 files, 0 B (0%)

Below the summary is a navigation bar with **Files and folders** (which is underlined) and **Configuration**.

The main area displays a table titled "Files and folders (2 total, 2.1 MB)". The table has columns: Name, Folder, Type, Size, Status, and Error. There are two rows of data:

Name	Folder	Type	Size	Status	Error
Screenshot 2025-04-08 163319...	-	image/png	1.1 MB	Succeeded	-
Screenshot 2025-04-08 163403...	-	image/png	1.0 MB	Succeeded	-

Access keys

Credentials

To set up my EC2 instance to interact with my AWS environment, I configured AWS Access key ID, The Secret Access key that matches the Access key ID, The Default region type and the Default Output Format.

Access keys are part of a credential! Your credentials are made up of a username and password; think of the access key ID as the username.

Secret access keys are like passwords in the context of access keys/credentials for our EC2 instance to get credentials to our AWS environment

Best practice

Although I'm using access keys in this project, Although I'm using access keys in this project IAM admin roles instead this means the neccessary permissions will be attached to an IAM role, then the role will be associated with the relevant resources

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 nextwork-vpc-endpoints-lwazidlamini This indicated that the access keys I set up were set up correctly and gives my EC2 Access to my AWS Account and environment.

```
Default region name [us-east-1]:  
Default output format [JSON]:  
[ec2-user@ip-10-0-0-188 ~]$ aws s3 ls  
2025-04-08 14:31:53 nextwork-vpc-endpoints-lwazidlamini  
[ec2-user@ip-10-0-0-188 ~]$ █
```

Connecting to my S3 bucket

I also tested the command aws s3 ls s3://nextwork-vpc-endpoints-lwazidlamini which returned with the files inside the S3 bucket.

```
[ec2-user@ip-10-0-0-188 ~]$ aws s3 ls s3://nextwork-vpc-endpoints-lwazidlamini
2025-04-08 14:35:16    1118785 Screenshot 2025-04-08 163319.png
2025-04-08 14:35:17    1096241 Screenshot 2025-04-08 163403.png
[ec2-user@ip-10-0-0-188 ~]$ █
```

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 option to upload files into my my S3 bucket.

The second command I ran was aws s3 cp /tmp/nextwork.txt s3://nextwork-vpc-endpoints-lwazidlamini. This command will add the file network.txt into my S3 bucket using my EC2 instant command line.

The third command I ran was aws s3 ls s3://nextwork-vpc-endpoints-lwazidlamini which validated that the file has been loaded to the S3 bucket using the EC2 instant command line.

```
ec2-user@ip-10-0-0-188 ~]$ aws s3 ls s3://nextwork-vpc-endpoints-lwazidlamini
025-04-08 14:35:16    1118785 Screenshot 2025-04-08 163319.png
025-04-08 14:35:17    1096241 Screenshot 2025-04-08 163403.png
025-04-08 15:35:54      0 nextwork.txt
ec2-user@ip-10-0-0-188 ~]$ █
```

In the second part of my project...

Step 5 - Set up a Gateway

In this step I am going to be setting up a VPC endpoint so that communication between our VPC and other services (especially S3) is direct and secure

Step 6 - Bucket policies

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

Step 7 - Update route tables

In this step we are testing our endpoint connection between our bucket and EC2 instance

Step 8 - Validate endpoint connection

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

Setting up a Gateway

I set up an S3 Gateway, which is a type of end point specifically designed for Amazon S3 Gateway by updating the route table of associate subnets, so that S3 bound traffic goes through the Gateway instead of the internet.

What are endpoints?

An endpoint is VPC component that allows our VPC to have direct connection to AWS environment, so that traffic doesn't have to go through the public internet!

The screenshot shows the AWS VPC Endpoint configuration page. At the top, there is a blue banner with the message: "Introducing two new types of endpoints: Resource endpoint and Service network endpoint. Use a Resource endpoint to access a VPC resource (ARN-based resource, domain name and IP address) in another VPC. Use a Service network endpoint to access a VPC Lattice service network. Learn more" with a link icon.

The main section displays the endpoint details:

Details	Status	Creation time	Endpoint type
Endpoint ID: vpce-00bd19e84b90657c9	Status: Available	Creation time: Tuesday, April 8, 2025 at 17:56:46 GMT+2	Endpoint type: Gateway
VPC ID: vpc-038d5643439695b3b (NextWork-vpc)	Status message: -	Service name: com.amazonaws.us-east-1.s3	Private DNS names enabled: No

Below the details, there are tabs for "Route tables", "Policy", and "Tags". The "Route tables" tab is selected, showing a table with one row:

Name	Route Table ID	Main	Associated Id
No route tables attached to endpoint			

At the top right of the main content area, there is an "Actions" dropdown menu with options: "Edit endpoint", "Delete endpoint", and "Manage route tables".

Bucket policies

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

My bucket policy will deny traffic from all sources accept traffic coming from my VPC endpoint.

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Deny",  
6       "Principal": "*",  
7       "Action": "s3:*",  
8       "Resource": [  
9         "arn:aws:s3:::nextwork-vpc-endpoints-lwazidlamini",  
10        "arn:aws:s3:::nextwork-vpc-endpoints-lwazidlamini/*"  
11      ],  
12      "Condition": {  
13        "StringNotEquals": {  
14          "aws:sourceVpce": "vpce-00bd19e84b90657c9"  
15        }  
16      }  
17    }  
18  ]  
19 }  
20
```

Bucket policies

Right after saving my bucket policy, my S3 bucket page showed 'denied access' warnings. This was because it has a deny policy that restricts access unless its from a specific VPC.

'I also had to update my route table because my S3 bucket was giving access denied after I set the command aws s3 ls s3://nextwork-vpc-endpoints-yourname my route table didn't provide a route in my public subnets to my VPCs

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

✖ 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](#)

▶ API response

🔍 Diagnose with Amazon Q

Route table updates

To update my route table, I went to my endpoints and created a new route table allowing access to my VPC public subnet.

After updating my public subnet's route table, my terminal could return all the files located in my S3 bucket through a the same aws s3 ls command.

Routes (3)	
<input type="text"/> Filter routes	
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-0f62ea5cffd0ed059
pl-63a5400a	vpce-00bd19e84b90657c9

Endpoint policies

An endpoint policy is restriction of the traffic that only certain range and resources have access to the endpoint.

I updated my endpoint policy by adding the deny command to my endpoint JSON policy to restrict unauthorized access because my EC2 was denied access once I set the policy and run another command.

```
[ec2-user@ip-10-0-0-188 ~]$ aws s3 ls s3://nextwork-vpc-endpoints-lwazidlamini
An error occurred (AccessDenied) when calling the ListObjectsV2 operation: User: arn:aws:iam::522154353718:user/IwaziDlaminiIAMUser is not authorized to perform: s3:ListBucket on resource: "arn:aws:s3:::nextwork-vpc-endpoints-lwazidlamini" with an explicit deny in a VPC endpoint policy
[ec2-user@ip-10-0-0-188 ~]$
```



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for
more projects

