



nextwork.org

VPC Endpoints



ucbethuel

The screenshot shows the AWS VPC Endpoints console. At the top, there is a header with tabs for 'Name', 'VPC endpoint ID', 'Endpoint type', 'Status', and 'Service'. Below the header, a table lists one endpoint:

Name	VPC endpoint ID	Endpoint type	Status	Service
NextWork VPC Endpoint	vpce-0a878d77171777277	Gateway	Available	com.amazonaws.com

Below the table, the endpoint details are shown:

vpce-0a878d77171777277 / NextWork VPC Endpoint

Details (selected) | Route tables | Policy | Tags

Details

Endpoint ID vpce-0a878d77171777277	Status Available	Creation time Monday, September 8, 2025 at 18:13:14 GMT+1	Endpoint type Gateway
VPC ID vpc-023784503586e175c (NextWork-0-vpc)	Status message -	Service name com.amazonaws.eu-west-1.s3	Private DNS names enabled No
Service region eu-west-1			

OR

ucbethuel

NextWork Student

nextwork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is Virtual Private Cloud and it is useful because it helps us create private network and connect our resources together.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC Endpoint to connect to amazon s3 resource internally without going through the public route.

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

null

This project took me...

This project took me 1 hour 32 mins.

OR

ucbethuel
NextWork Student

nextwork.org

In the first part of my project...

Step 1 - Architecture set up

In this step, I will create my PC from scratch, launch my S3 and EC2 instance.

Step 2 - Connect to EC2 instance

In this step, I will be connecting to directly my ec2 instance.

Step 3 - Set up access keys

In this step, I will give my ec2 instance access to aws environment using access key.

Step 4 - Interact with S3 bucket

In this step, I will ec2 instance access to my s3 aws resource.

OR

ucbethuel
NextWork Student

nextwork.org

Architecture set up

I started my project by launching an ec2 instance.

I also set up aws s3 resource

Objects (2)			
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you must grant them permission to do so.			
<input type="text"/> Find objects by prefix		<input type="button" value="C"/>	<input type="button" value="Copy S3 URI"/> <input type="button" value="Copy URL"/> <input type="button" value="Download"/> <input type="button" value="Open"/>
Name	Type	Last modified	Size
<input type="checkbox"/>  Screenshot 2025-09-04 170526.png	png	September 8, 2025, 16:16:49 (UTC+01:00)	
<input type="checkbox"/>  Screenshot 2025-09-04 172857.png	png	September 8, 2025, 16:16:50 (UTC+01:00)	

 OR

ucbethuel
NextWork Student

nextwork.org

Access keys

Credentials

To set up my EC2 instance to interact with my AWS environment, I configured my aws environment by providing the details regarding 1. Access Id 2. Secret key 3. region code 4. output format.

Access keys are credentials which is needed for us to get access to aws services via CLI.

Secret access keys are like password for logging in to our aws via CLI.

Best practice

Although I'm using access keys in this project, a best practice alternative is to use AWS CloudShell, AWS CLI V2.

OR

ucbethuel
NextWork Student

nextwork.org

Connecting to my S3 bucket

The command I ran was "aws s3 ls" This command is used to list available s3 resources linked to my account.

The terminal responded with list of available buckets. This indicated that the access keys I set up was succesfully.

```
Default output format [None]:  
[ec2-user@ip-10-0-0-48 ~]$ aws s3 ls  
2025-09-08 15:15:45 nextwork-vpc-project-ucbethuel  
[ec2-user@ip-10-0-0-48 ~]$ █
```

OR

ucbethuel
NextWork Student

nextwork.org

Connecting to my S3 bucket

I also tested the command aws s3 ls s3://nextwork-vpc-project-ucbethuel which returned list of object in my bucket.

```
25-09-08 15:15:45 nextwork-vpc-project-ucbethuel
c2-user@ip-10-0-0-48 ~]$ aws s3 ls s3://nextwork-vpc-project-ucbethuel
25-09-08 15:16:49      215396 Screenshot 2025-09-04 170526.png
25-09-08 15:16:50      55295 Screenshot 2025-09-04 172857.png
c2-user@ip-10-0-0-48 ~]$ |
```

OR

ucbethuel
NextWork Student

nextwork.org

Uploading objects to S3

The first command I ran was aws s3 ls. This command is used to list s3 services connected to my account.

The second command I ran was "aws s3 cp /tmp/test.txt s3://nextwork-vpc-project-ucbethuel" This command will copy file form a source (i.e /tmp/test.txt) to a destination (i.e s3://nextwork-vpc-project-ucbethuel)

The third command I ran was s3://nextwork-vpc-project-ucbethuel which validated that the test.txt file was copied.

```
n: $'\E[200~sudo': command not found
-user@ip-10-0-0-48 ~]$ sudo touch /tmp/test.txt
-user@ip-10-0-0-48 ~]$ touch /tmp/test2.txt
-user@ip-10-0-0-48 ~]$ aws s3 cp /tmp/test.txt s3://nextwork-vpc-project-ucbethuel
ad: ../../tmp/test.txt to s3://nextwork-vpc-project-ucbethuel/test.txt
-user@ip-10-0-0-48 ~]$ aws s3 ls s3://nextwork-vpc-project-ucbethuel
-09-08 15:16:49      215396 Screenshot 2025-09-04 170526.png
-09-08 15:16:50      55295 Screenshot 2025-09-04 172857.png
-09-08 15:32:24      0 test.txt
-user@ip-10-0-0-48 ~]$
```

OR

ucbethuel
NextWork Student

nextwork.org

In the second part of my project...

Step 5 - Set up a Gateway

In this step, I will set up VPC endpoint so that my VPC can connect directly without using public routes.

Step 6 - Bucket policies

I will be validating first if our VPC endpoint actually work and in order to validate, i have to block all traffic except the ones coming within aws.

Step 7 - Update route tables

In this step, I will be testing my Bucket to see if i can still use public route or just my VPC endpoint alone.

Step 8 - Validate endpoint connection

In this step, I will test my bucket one more time.

OR

ucbethuel
NextWork Student

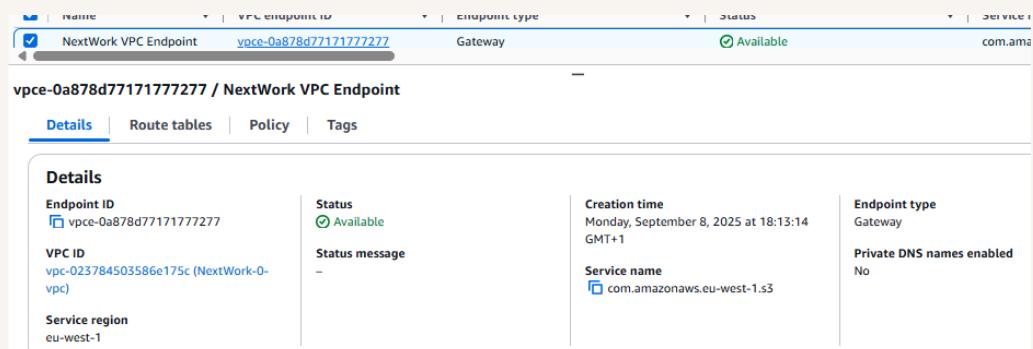
nextwork.org

Setting up a Gateway

I set up an S3 Gateway, which allows us to connect to s3 without going through the public route.

What are endpoints?

An endpoint is an internal route which connect amazon global services to our VPC.



Bucket policies

A bucket policy are rules that guide the a mangement of a buckets.

My bucket policy will deny all a endpoint access except the one 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-project-ucbethuel",
10         "arn:aws:s3::::nextwork-vpc-project-ucbethuel/*"
11       ],
12▼       "Condition": {
13▼         "StringNotEquals": {
14            "aws:sourceVpce": "vpce-0a878d77171777277"
15          }
16        }
17      }
18    ]
19  }
20 |
```

OR

ucbethuel
NextWork Student

nextwork.org

Bucket policies

Right after saving my bucket policy, my S3 bucket page showed 'denied access' warnings. This was because I blocked all kind of endpoint access, except only my VPC endpoint.

I also had to update my route table because traffic coming from my ec2 need to know the nearest place to follow in order to get to aws s3 resource.

The screenshot shows two separate sections of the AWS S3 console. The top section is titled 'Block public access (bucket settings)' and displays a green success message: 'Successfully edited bucket policy.' It includes a 'Edit' button and a 'Diagnose with Amazon Q' button. A red box highlights an error message: '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.' Below this is a '► API response' link. The bottom section is titled 'Bucket policy' and also displays a green success message: 'Successfully edited bucket policy.' It includes 'Edit' and 'Delete' buttons and a 'Diagnose with Amazon Q' button. A red box highlights another error message: 'You don't have permission to get bucket policy. You or your AWS administrator must update your IAM permissions to allow s3:GetBucketPolicy. After you obtain the necessary permission, refresh the page. Learn more about Identity and access management in Amazon S3.' Below this is a '► API response' link.

OR

ucbethuel
NextWork Student

nextwork.org

Route table updates

To update my route table, I added it from my vpc endpoint and choose the subnet associated to ec2 instance.

After updating my public subnet's route table, my terminal could return the list of objects in my s3 buckets.

Route table: rtb-0bc9681075061d384 / NextWork-0-rtb-public	
Routes (3)	
<input type="text"/> Filter routes	
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-02d095a29d19b757d
pl-6da54004	vpce-0a878d77171777277

OR

ucbethuel
NextWork Student

nextwork.org

Endpoint policies

An endpoint policy is a rule that guide if an endpoint can access a resource like s3 or not.

I updated my endpoint's policy by chenging Effect key value to "Dany", and I could see the effect of this right away, even when i revise back to "Allow".

```
2-user@ip-10-0-0-48 ~]$ aws s3 ls s3://nextwork-vpc-project-ucbethuel
error occurred (AccessDenied) when calling the ListObjectsV2 operation: User: arn:aws:iam::190680267675:user/ucbethuel-IAM-admin is not authorized to perform: s3>ListBucket
on resource: "arn:aws:s3:::nextwork-vpc-project-ucbethuel" with an explicit deny in a VPC endpoint policy
2-user@ip-10-0-0-48 ~]$
```



nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects

