



VPC Endpoints



tahirgroot@gmail.com

vpce-05f0ad4f87d93d7be / Groot279 VPC Endpoint			
Details	Route tables	Policy	Tags
Details			
Endpoint ID vpce-05f0ad4f87d93d7be	Status Available	Creation time Monday 26 August 2024 at 21:52:51 BST	Endpoint type Gateway
VPC ID vpc-01373105ff43d8b78 (Groot279-vpc)	Status message -	Service name com.amazonaws.eu-west-2.s3	Private DNS names enabled No

 TA

tahirgroot@gmail.com

NextWork Student

NextWork.org

Introducing Today's Project!

What is Amazon VPC?

AWS VPC is an AWS networking service provided by AWS that allows us to isolate our resources from the public internet, set up secure connections between our resources, and control traffic flow security.

How I used Amazon VPC in this project

We used Amazon VPC in this project to set up a VPC endpoint, specifically an S3 Gateway. This provides our VPC with direct access to another AWS service.

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

N/a

This project took me...

45 mins

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 a VPC, EC2 instance, and S3 bucket so that we can set up an endpoint architecture and test that setup in the last step of this project.

Step 2 - Connect to EC2 instance

The command I ran was 'aws s3 ls'. It lists the contents of an Amazon S3 bucket or a specific directory within a bucket. Displays the names, sizes, and last modified dates of the objects.

Step 3 - Set up access keys

In this step, we will set up an access key so that our EC2 instance can access the AWS environment. Access keys are almost like "login details" for EC2 instances/applications to interact with AWS services.

Step 4 - Interact with S3 bucket

In this step, we apply our access key credentials to our EC2 instance, and then we use AWS CLI and our EC2 instance to access Amazon S3



tahirgroot@gmail.com

NextWork Student

NextWork.org

Architecture set up

I started my project by launching three critical resources - a VPC, an EC2 instance and an S3 bucket.

In this step, I connect directly to the EC2 instance using the EC2 instance connect. Connecting to instances will help us access S3 and run commands later in this project.

Amazon S3 > Buckets > groot279-vpc-endpoints-cyberchef201 [Info](#)

Objects Properties Permissions Metrics Management Access Points

Objects (2) [Info](#)

[Upload](#)

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'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

<input type="checkbox"/>	Name	Type	Last modified	Size
<input type="checkbox"/>	NextWork - Denzel is awesome.png	png	August 26, 2024, 19:44:51 (UTC+01:00)	
<input type="checkbox"/>	NextWork - Lelo is awesome.png	png	August 26, 2024, 19:44:53 (UTC+01:00)	

Access keys

Credentials

To set up my EC2 instance to interact with my AWS environment, I configured the AWS access key ID, secret access key matching that key ID, default region type and then the default output format.

Access keys are a pair of secret credentials that are used to authenticate your identity and gain access to AWS services. They consist of an access key ID and a secret access key.

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

Best practice

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



TA

tahirgroot@gmail.com

NextWork Student

NextWork.org

Connecting to my S3 bucket

The command I ran was 'aws s3 ls'. It lists the contents of an Amazon S3 bucket or a specific directory within a bucket. Displays the names, sizes, and last modified dates of the objects.

The terminal responded with a list of my account's S3 buckets. This indicated that our access keys were set up correctly. The access keys I set up correctly give my EC2 instance access to my AWS account and environment.

```
[ec2-user@ip-10-0-10-244 ~]$ aws s3 ls  
2024-08-26 18:41:59 groot279-vpc-endpoints-cyberchef201
```

TA

tahirgroot@gmail.com

NextWork Student

NextWork.org

Connecting to my S3 bucket

I also tested the command 'aws s3 ls s3://groot279-vpc-endpoints-cyberchef201', which returned a list of all the objects inside that s3 bucket.

```
[ec2-user@ip-10-0-10-244 ~]$ aws s3 ls s3://groot279-vpc-endpoints-cyberchef201
2024-08-26 18:44:51      2431554 NextWork - Denzel is awesome.png
2024-08-26 18:44:53      2399812 NextWork - Lelo is awesome.png
```

Uploading objects to S3

To upload a new file to my bucket, I first ran the command 'sudo touch /tmp/Groot279.txt'. This command creates an empty file name groot279.txt and saves it locally in the EC2 instance.

The second command I ran was 'aws s3 cp /tmp/nextwork.txt s3://nextwork-vpc-endpoints-yourname' This command will copy the file I created i.e.groot279.txt and upload that to my S3 bucket

The third command I ran was 'aws s3 ls s3://groot279-vpc-endpoints-cyberchef201', which validated that a new file was created and updated into our s3 bucket

```
[ec2-user@ip-10-0-10-244 ~]$ sudo touch /tmp/groot279.txt
[ec2-user@ip-10-0-10-244 ~]$ aws s3 cp /tmp/nextwork.txt s3://groot279-vpc-endpoints-cyberchef201
The user-provided path /tmp/nextwork.txt does not exist.
[ec2-user@ip-10-0-10-244 ~]$ aws s3 cp /tmp/groot279.txt s3://groot279-vpc-endpoints-cyberchef201
upload: ../../tmp/groot279.txt to s3://groot279-vpc-endpoints-cyberchef201/groot279.txt
[ec2-user@ip-10-0-10-244 ~]$ aws s3 ls s3://groot279-vpc-endpoints-cyberchef201
2024-08-26 18:44:51    2431554 NextWork - Denzel is awesome.png
2024-08-26 18:44:53    2399812 NextWork - Lelo is awesome.png
2024-08-26 19:47:11      0 groot279.txt
```

In the second part of my project...

Step 5 - Set up a Gateway

In this step we are setting up a vpc endpoint so that communication between our vpc (especially S3) and other services is direct and secure

Step 6 - Bucket policies

In this step, we are testing our endpoint connection by blocking off all traffic to our s3 bucket except for traffic coming from our endpoint

Step 7 - Update route tables

In this step, we test our endpoint connection between our bucket and Ec2 instance.

Step 8 - Validate endpoint conection

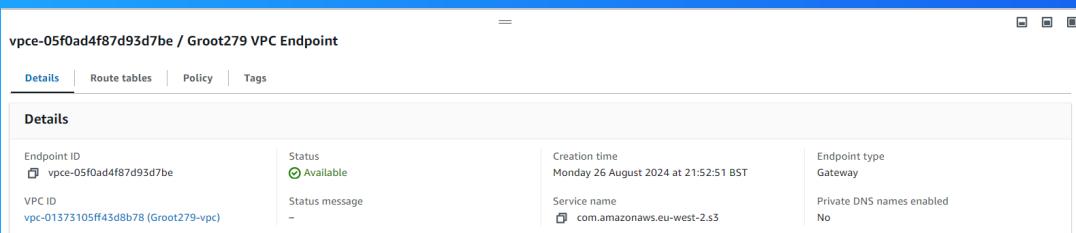
In this step, we will validate our VPC endpoint setup one more time and use endpoint policies to restrict my Ec2 instance's access to my AWS environment.

Setting up a Gateway

I set up an S3 Gateway, an endpoint designed explicitly for Amazon s3. s3 Gateway work by updating the route table of associated subnets. So, s3 bound traffic goes through the gateway instead of the internet.

What are endpoints?

An endpoint in AWS is a service that allows private connections between your VPC and other AWS services without sending traffic over the Internet.



Bucket policies

A bucket policy is a type of policy that specifies the permissions and access controls for an Amazon S3 bucket. It defines who can access the bucket and what actions they can perform on objects within it.

My bucket policy will deny traffic from all sources except for traffic coming my VPC 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:::groot279-vpc-endpoints-cyberchef201",
10       "arn:aws:s3:::groot279-vpc-endpoints-cyberchef201/*"
11     ],
12▼      "Condition": {
13        "StringNotEquals": {
14          "aws:sourceVpce": "vpce-05f0ad4f87d93d7be"
15        }
16      }
17    }
18  ]
19}
20}
```



tahirgroot@gmail.com

NextWork Student

NextWork.org

Bucket policies

Right after saving my bucket policy, my S3 bucket page showed 'denied access' warnings. This was because my policy has been updated from 'Allow' to 'deny'

I also had to update my route table because my route table, by default, didn't provide a route for traffic in my public subnet to the VPC endpoint.

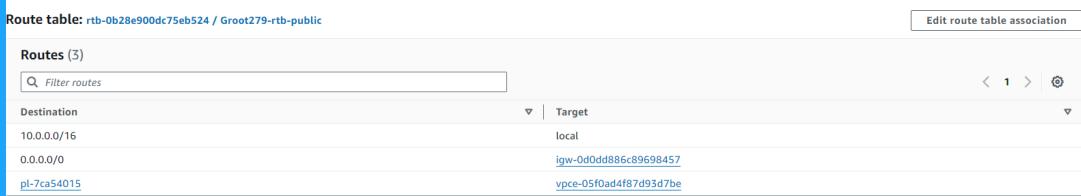
The screenshot shows the 'Permissions overview' section of an AWS S3 bucket's configuration. It highlights two areas where permission is denied:

- Block public access (bucket settings):** A red box surrounds a 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 [?]. ▶ API response".
- Bucket policy:** Another red box surrounds a 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 [?]. ▶ API response".

Route table updates

To update my route table, I visited the endpoints page of my vpc console, and we modified the route table from there to associate our vpc's public subnet.

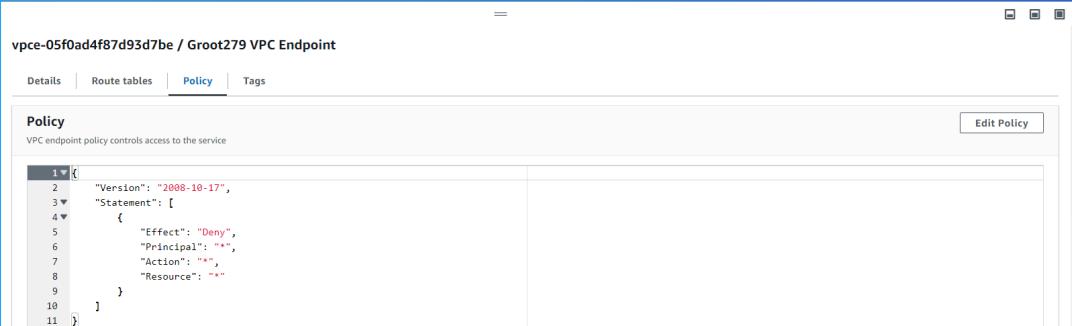
After updating my public subnet's route table, My EC2 instance could connect with my S3 bucket, and access was no longer denied!



Endpoint policies

An endpoint policy is a type of policy designed to specify the range of resources permitted by the endpoint.

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 was again denied access to S3 when I tried to run another 'aws S3' command.



The screenshot shows the AWS VPC Endpoint console for the endpoint `vpc-e-05f0ad4f87d93d7be / Groot279 VPC Endpoint`. The `Policy` tab is selected, displaying a JSON-based policy document. The policy contains a single statement that denies access to all actions on all resources for all principals. The code is as follows:

```
1 {  
2     "Version": "2008-10-17",  
3     "Statement": [  
4         {  
5             "Effect": "Deny",  
6             "Principal": "*",  
7             "Action": "*-*",  
8             "Resource": "*-*"  
9         }  
10    ]  
11 }
```



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for
more projects

