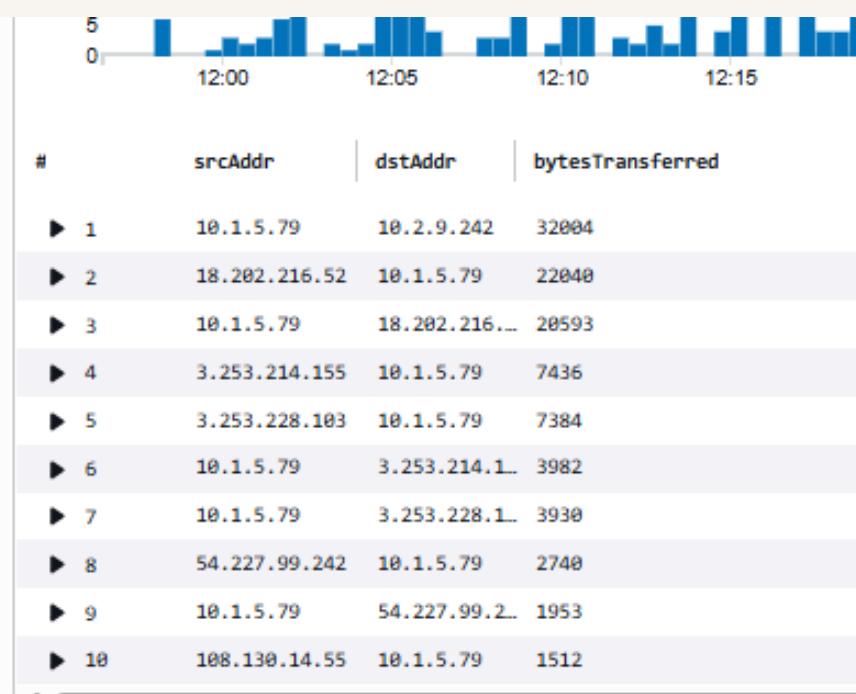




VPC Monitoring with Flow Logs

OR

ucbethuel



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 Flow log to keep track of traffic in out VPC which are stored and analyse in Amazon CloudWatch.

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

none yet

This project took me...

This project took me 2 and half hour

OR

ucbethuel
NextWork Student

nextwork.org

In the first part of my project...

Step 1 - Set up VPCs

In this step, I will be creating two VPC from scratch.

Step 2 - Launch EC2 instances

In this step, I will Launch an EC2 instance in each VPC, so we can use them to test your VPC peering connection later.

Step 3 - Set up Logs

In this step, I will 1. Set up a way to track all inbound and outbound network traffic. 2. Set up a space that stores all of these records.

Step 4 - Set IAM permissions for Logs

In this step, I will 1. Give VPC Flow Logs the permission to write logs and send them to CloudWatch. 2. Finish setting up your subnet's flow log.

OR

ucbethuel
NextWork Student

nextwork.org

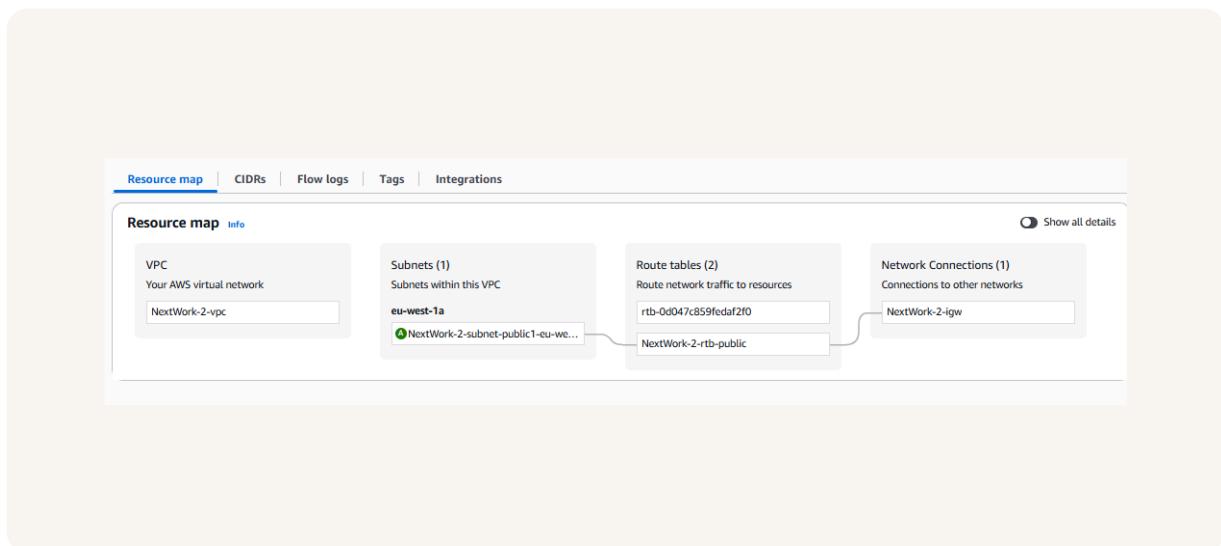
Multi-VPC Architecture

I started my project by launching my VPC using the VPC wizard, and in each VPC i have one subnet which is a public subnet connected to the internet gateway. within each at the moment, no private subnet, makes makes it a total of 1 subnet each.

The CIDR blocks for VPCs 1 and 2 are 10.1.0.0/16 and 10.2.0.0/16 respectively. They have to be unique because to avoid overlapping of IP addresses since we are peer connecting.

I also launched EC2 instances in each subnet

My EC2 instances' security groups allow ICMP traffic form any IP addresses, This is because we need to quick test the connectivity of both VPC.



OR

ucbethuel
NextWork Student

nextwork.org

Logs

Logs are activities of my computer been recorded.

Log groups are like folders that collects related logs together.

The screenshot shows the AWS CloudWatch Logs console with a success message at the top:

Successfully created flow log for the following resource:
vpc-075355d3deeb6babc

The main section displays the details of a flow log named "fl-03b586b12753ac177 / NextWorkVPCFlowLogsPolicy".

Details	Destination Type	Traffic Type	File Format
Flow Log ID fl-03b586b12753ac177	cloud-watch-logs	ALL	-
Name NextWorkVPCFlowLogsPolicy	Destination Name NextWorkVPCFlowLogsGroup	Max Aggregation Interval 1 minute	Hive Compatible Partitions
State Active	IAM Role arn:aws:iam:190680267675:role/NextWorkVP CFlowLogsRole	Log Format Default	Partition Logs
Creation Time Monday, September 8, 2025 at 12:57:45 GMT+1	Cross Account IAM Role -		

Below the details, there are tabs for "Tags" and "Integrations". The "Tags" tab is selected, showing a search bar and a "Manage tags" button. The page also includes navigation controls (page 1 of 1).

OR

ucbethuel
NextWork Student

nextwork.org

IAM Policy and Roles

I created an IAM policy because by default do not send logs entries to cloudWatch.

I also created an IAM role because my flow log needs a service role, which is yet to be created.

A custom trust policy is kind of IAM policy but not it, it used to very narrowly define who can use a role.

```
1 ▼ {
2     "Version": "2012-10-17",
3     "Statement": [
4         {
5             "Sid": "Statement1",
6             "Effect": "Allow",
7             "Principal": {
8                 "Service": "vpc-flow-logs.amazonaws.com"
9             },
10            "Action": "sts:AssumeRole"
11        }
12    ]
13 }
```

OR

ucbethuel
NextWork Student

nextwork.org

In the second part of my project...

Step 5 - Ping testing and troubleshooting

In this step, I will Get Instance - EC2 1 to send test messages to Instance - EC2 2.

Step 6 - Set up a peering connection

In this step, I will Set up a connection link between your VPCs.

Step 7 - Analyze flow logs

In this step, I will 1. Review the flow logs recorded about VPC 1's public subnet. 2. Analyse the flow logs to get some tasty insights

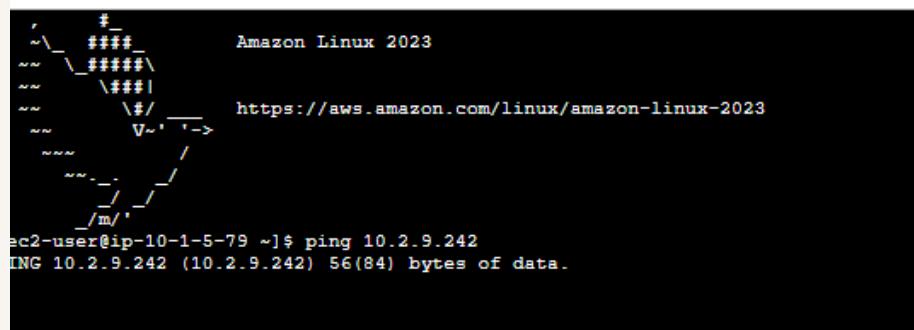
OR

ucbethuel
NextWork Student

nextwork.org

Connectivity troubleshooting

My first ping test between my EC2 instances had no replies, which suggest there could be a problem, let me troubleshoot.



```
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023

ec2-user@ip-10-1-5-79 ~]$ ping 10.2.9.242
PING 10.2.9.242 (10.2.9.242) 56(84) bytes of data.
```

I could receive ping replies if I ran the ping test using the other instance's public IP address, which means both VPC can communicate over the internet.

OR

ucbethuel
NextWork Student

nextwork.org

Connectivity troubleshooting

Looking at VPC 1's route table, I identified that the ping test with Instance 2's private address failed because base on self discovery, we are yet to create a "peering connection" and also update the route table of each vpc.

To solve this, I set up a peering connection between my VPCs

I also updated both VPCs' route tables so that in order to direct traffic to the appropriate destination.

Routes (3)			
<input type="text"/> Filter routes			
Destination	Target	Status	Propagated
0.0.0.0/0	igw-0a4c55030f6627721	Active	No
10.1.0.0/16	local	Active	No
10.2.0.0/16	pxc-098991d44a7749e84	Active	No

OR

ucbethuel
NextWork Student

nextwork.org

Connectivity troubleshooting

I received ping replies from Instance 2's private IP address! This means both vpc can now communicate internally.

```
> min/avg/max/mdev = 0.201/0.243/0.312/0.022 ms
-2-user@ip-10-1-5-79 ~]$ ping 10.2.9.242
PING 10.2.9.242 (10.2.9.242) 56(84) bytes of data.
bytes from 10.2.9.242: icmp_seq=256 ttl=127 time=0.216 ms
bytes from 10.2.9.242: icmp_seq=257 ttl=127 time=0.219 ms
bytes from 10.2.9.242: icmp_seq=258 ttl=127 time=0.209 ms
bytes from 10.2.9.242: icmp_seq=259 ttl=127 time=0.193 ms
bytes from 10.2.9.242: icmp_seq=260 ttl=127 time=0.197 ms
bytes from 10.2.9.242: icmp_seq=261 ttl=127 time=0.217 ms
bytes from 10.2.9.242: icmp_seq=262 ttl=127 time=0.205 ms
bytes from 10.2.9.242: icmp_seq=263 ttl=127 time=0.195 ms
bytes from 10.2.9.242: icmp_seq=264 ttl=127 time=0.203 ms
bytes from 10.2.9.242: icmp_seq=265 ttl=127 time=0.207 ms
bytes from 10.2.9.242: icmp_seq=266 ttl=127 time=0.201 ms
bytes from 10.2.9.242: icmp_seq=267 ttl=127 time=0.214 ms
bytes from 10.2.9.242: icmp_seq=268 ttl=127 time=0.204 ms
bytes from 10.2.9.242: icmp_seq=269 ttl=127 time=0.196 ms
bytes from 10.2.9.242: icmp_seq=270 ttl=127 time=0.220 ms
bytes from 10.2.9.242: icmp_seq=271 ttl=127 time=0.222 ms

- 10.2.9.242 ping statistics ---
1 packets transmitted, 16 received, 94.0959% packet loss, time 280762ms
> min/avg/max/mdev = 0.193/0.207/0.222/0.009 ms
-2-user@ip-10-1-5-79 ~]$
```

OR

ucbethuel
NextWork Student

nextwork.org

Analyzing flow logs

Flow logs tell us about the inbound and outbound traffic of a network.

For example, the flow log I've captured tells us that a traffic from ip:18.202.216.52 went to ip:10.1.5.79 through the port 22 of tcp, with a 31 data packet which amount to 3248 bytes of data. Also the transfer was accepted and ok.

▶ 2025-09-08T12:14:36.000Z	2 190680267675 eni-0bad358fb0d4c0be6 66.175.212.88 10.1.5.79 61000 2323 6 1 40 175733367 1757333688 REJECT OK
▼ 2025-09-08T12:15:06.000Z	2 190680267675 eni-0bad358fb0d4c0be6 18.202.216.52 10.1.5.79 40812 22 6 31 3248 17573337 1757333727 ACCEPT OK
	2 190680267675 eni-0bad358fb0d4c0be6 18.202.216.52 10.1.5.79 40812 22 6 31 3248 1757333706 1757333727 ACCEPT OK
▶ 2025-09-08T12:15:06.000Z	2 190680267675 eni-0bad358fb0d4c0be6 10.1.5.79 18.202.216.52 22 40812 6 24 4289 17573337 1757333727 ACCEPT OK
▶ 2025-09-08T12:15:06.000Z	2 190680267675 eni-0bad358fb0d4c0be6 135.237.126.99 10.1.5.79 41902 623 6 1 40 1757333706 Back to

OR

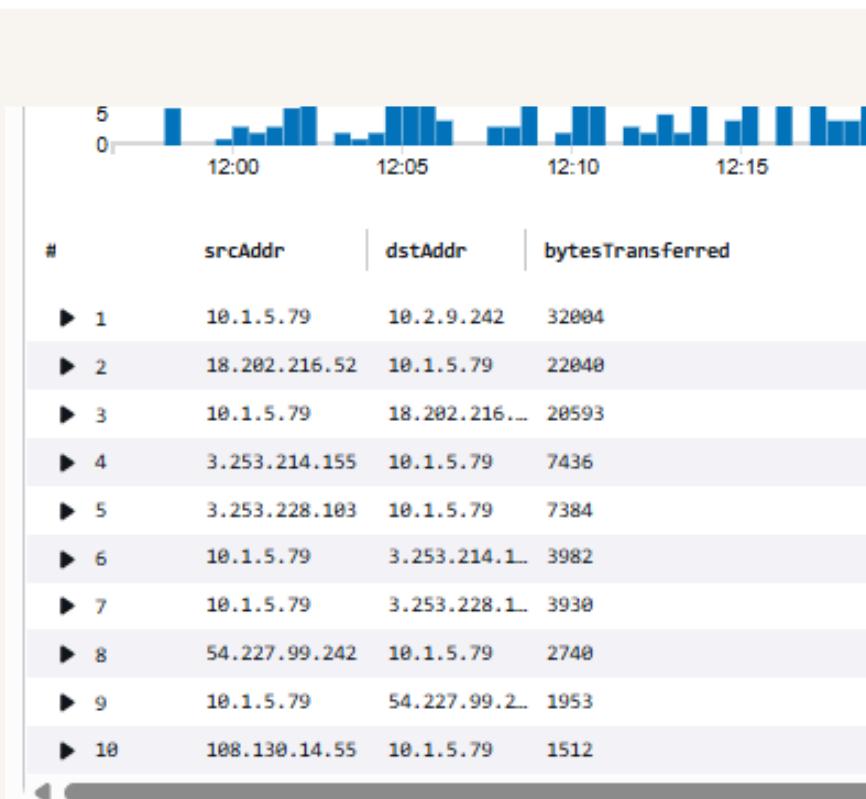
ucbethuel
NextWork Student

nextwork.org

Logs Insights

Logs Insights helps us to visualize and run queries pertaining to our traffic registered.

I ran the query top 10 inbound and outbound. This query analyzes top ten inbound and outbound traffic captured.





nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects

