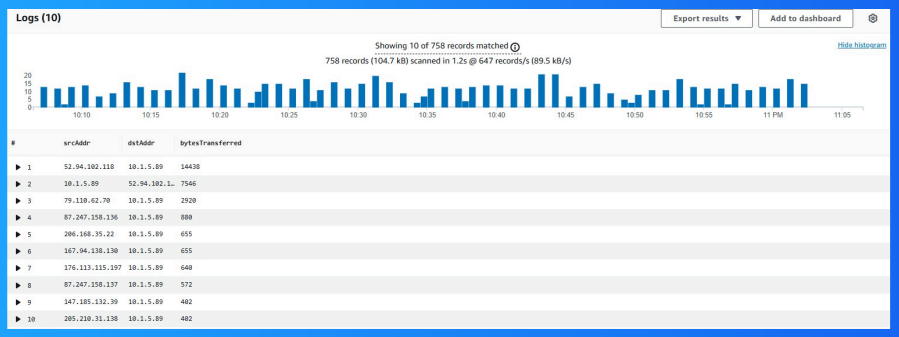
NextWork.org

VPC Monitoring with Flow Logs

Nikhil Bhan



N

Nikhil Bhan
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) allows users to create a private and isolated network in their AWS account. They can manage and organize resources as well as configure permissions and access to those resources.

How I used Amazon VPC in this project

In this project I used Amazon VPC to create a network where instances can communicate in two VPCs with a Peering Connection; I also created a VPC Flow Log with permissions to analyze the traffic in VPC 1 and send them to CloudWatch for me to view.

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

I wasn't expecting how much fun it would be to use CloudWatch and review the traffic in my VPC; this allowed me to see what happens in a VPC when traffic is sent and received.

This project took me...

This project took me 2 hours to complete and I used another 25 minutes to write my documentation.

N
Nikhil Bhan
NextWork Student

In the first part of my project...

Step 1 - Set up VPCs

In this step I'm going to create 2 VPCs to set up a VPC Peering Connection.

Step 2 - Launch EC2 instances

In this step I'll create an EC2 instance in each of my VPCs. I'm doing this so I'll be able to test the VPC Peering Connection later on.

Step 3 - Set up Logs

In this step I'll set up a VPC Flow Log that will track all inbound and outbound network traffic. I'll also set up a location where all the network traffic records will be stored.

Step 4 - Set IAM permissions for Logs

In this step I'll provide my VPC Flow Log the permissions it needs to write logs and send them to CloudWatch. After I perform these steps I'll be able to finish setting up my subnet's flow log.

N

Nikhil Bhan
NextWork Student

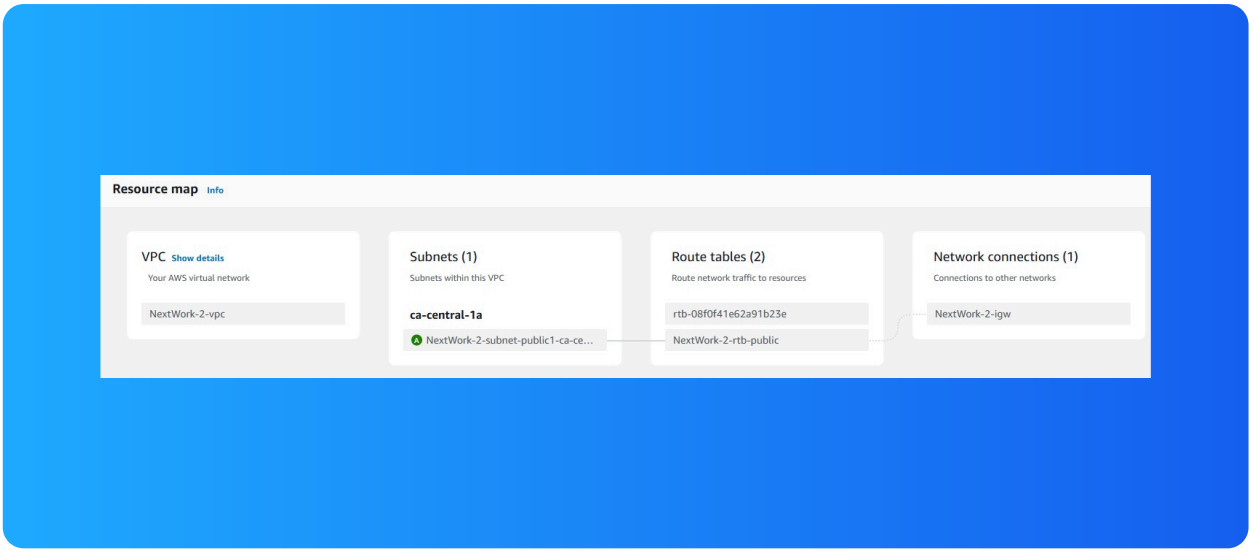
Multi-VPC Architecture

I started my project by launching 2 VPCs in my AWS account.

The CIDR blocks for VPCs 1 and 2 are 10.1.0.0/16 and 10.2.0.0/16. They have to be unique because I'll be connecting these VPCs together when I create the Peering Connection; if there are duplicate IP addresses, there would be networking issues.

I also launched EC2 instances in each subnet

My EC2 instances' security groups allow all ICMP activity to be received. This is because I will be testing the peering connection between my VPCs so I'll need to use the PING command to view ICMP traffic between the EC2 instances.



N

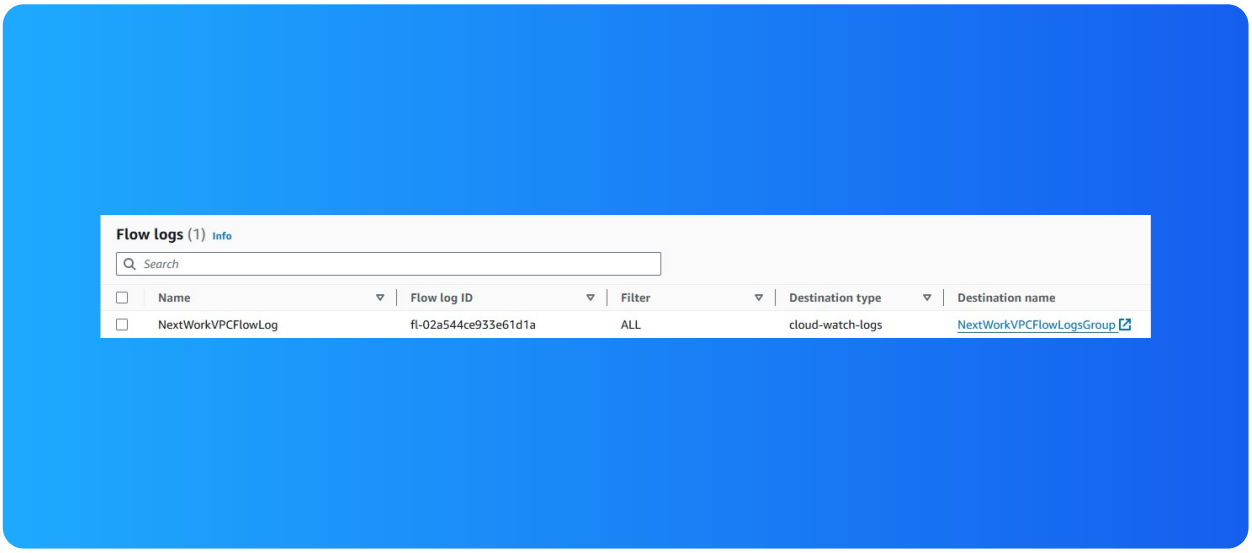
Nikhil Bhan
NextWork Student

Logs

Logs are recorded events on a computer system; they record all activities on the system and the user can leverage them to troubleshoot issues, verify system functionality and monitor system activities.

Log groups are folders where similar logs are grouped together. These log groups can store logs that come from the same source or application; logs can also belong to different regions and the user can view them from CloudWatch dashboards.

I also set up a flow log for VPC 1



N

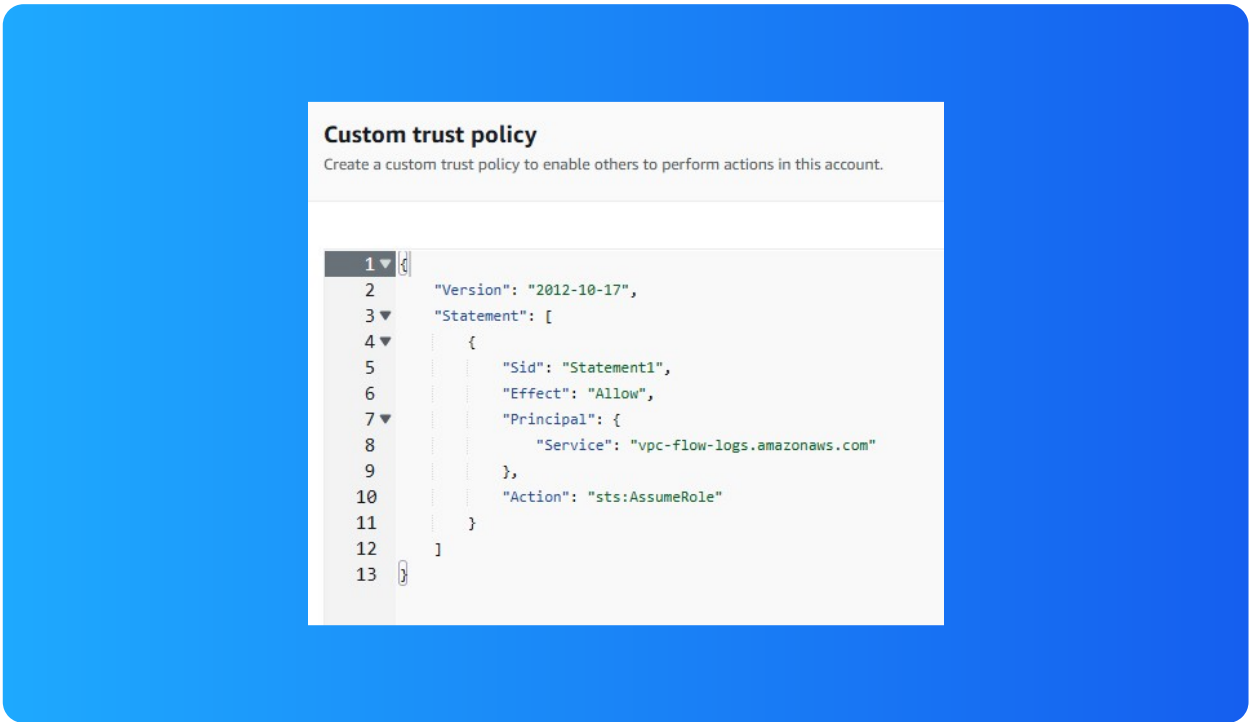
Nikhil Bhan
NextWork Student

IAM Policy and Roles

I created an IAM policy because my VPC Flow Log doesn't have permission to record logs and send them to CloudWatch. By making this IAM policy I'll be able to provide my VPC Flow Log the appropriate permissions.

I also created an IAM role because I'll need to attach the NextWorkVPCFlowLogsPolicy to it. I can then assign this IAM role to the flow log in my VPC.

A custom trust policy is a special type of policy. This is completely different from a typical IAM policy. Custom trust policies are used to define the user or application that are allowed to use a role.



N
Nikhil Bhan
NextWork Student

In the second part of my project...

Step 5 - Ping testing and troubleshooting

In this step I'm going to send test messages from my instance in VPC 1 to the instance in VPC 2.

Step 6 - Set up a peering connection

In this step I will create a connection link between my VPCs by creating a Peering Connection.

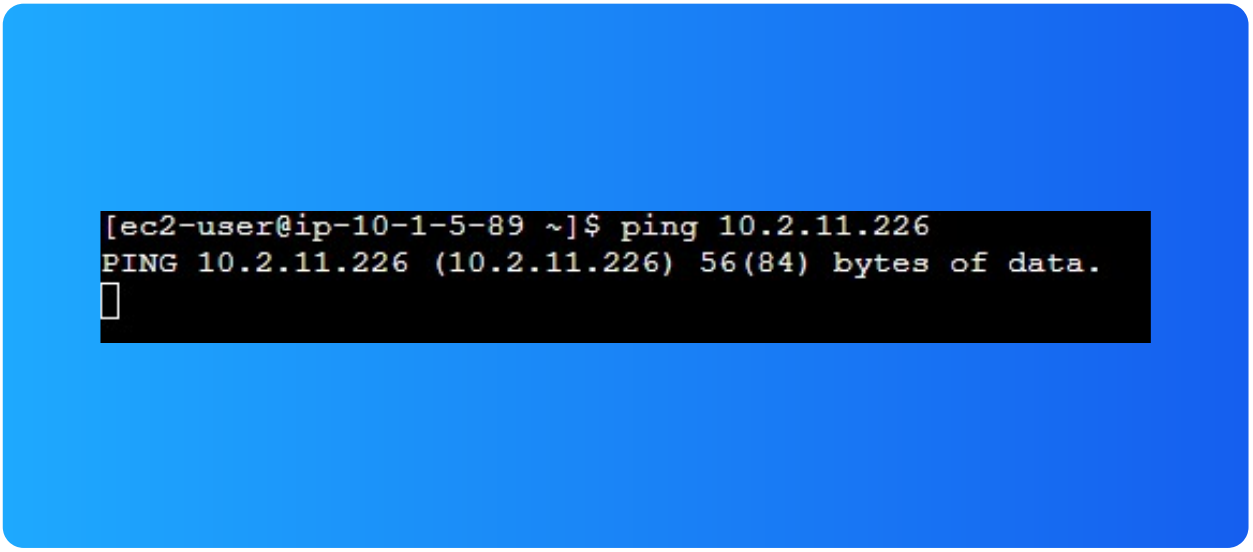
Step 7 - Analyze flow logs

In this step I'm going to review the flow logs that were recorded on the public subnet in VPC 1. I'll analyze these flow logs to gain some insight on what's happening in VPC 1.

N
Nikhil Bhan
NextWork Student

Connectivity troubleshooting

My first ping test between my EC2 instances had no replies, which means that the ICMP traffic leaving my instance in VPC 1 is unable to reach my instance in VPC 2. This concludes that there's a communication breakdown somewhere in the network.



I could receive ping replies if I ran the ping test using the other instance's public IP address, which means that the instance in VPC 2 can respond to ping requests. It also means both instances can communicate through the Internet.

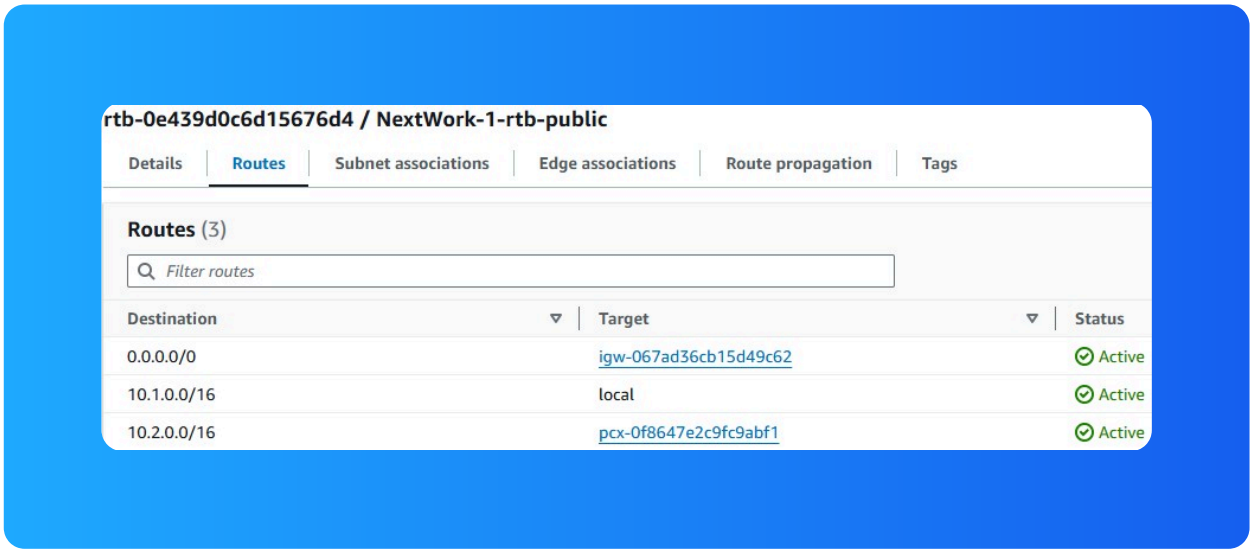
Nikhil Bhan
NextWork Student

Connectivity troubleshooting

Looking at VPC 1's route table, I identified that the ping test with Instance 2's private address failed because there was no direct connection between the two VPCs. Therefore, I'll need to create and configure a VPC Peering Connection.

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

I also updated both VPCs' route tables so that traffic will be able to travel from one VPC to the other one by going through the peering connection I had created.

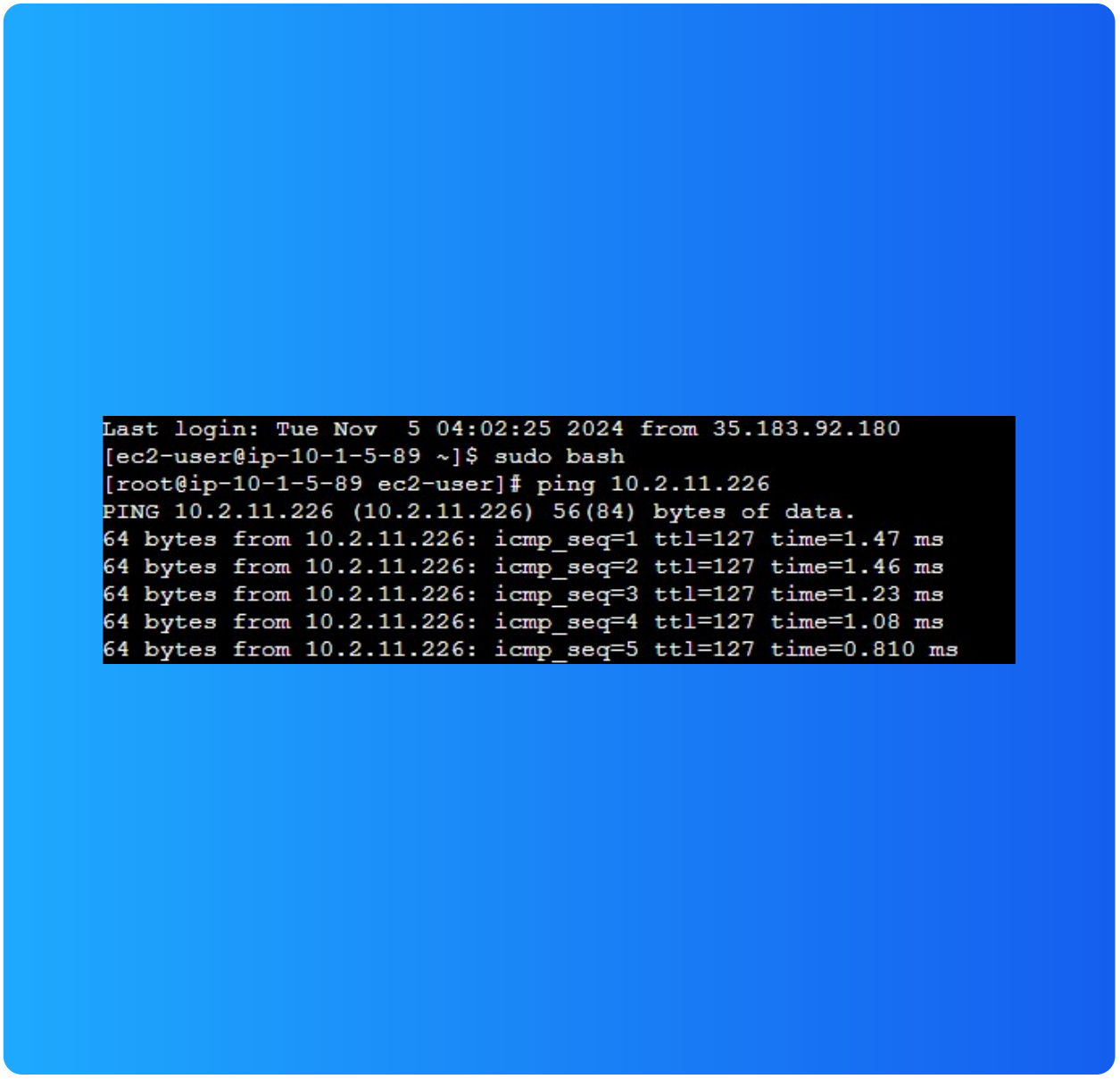


N

Nikhil Bhan
NextWork Student

Connectivity troubleshooting

I received ping replies from Instance 2's private IP address! This means that the instances can send and receive traffic between the two VPCs by using the peering connection I created.

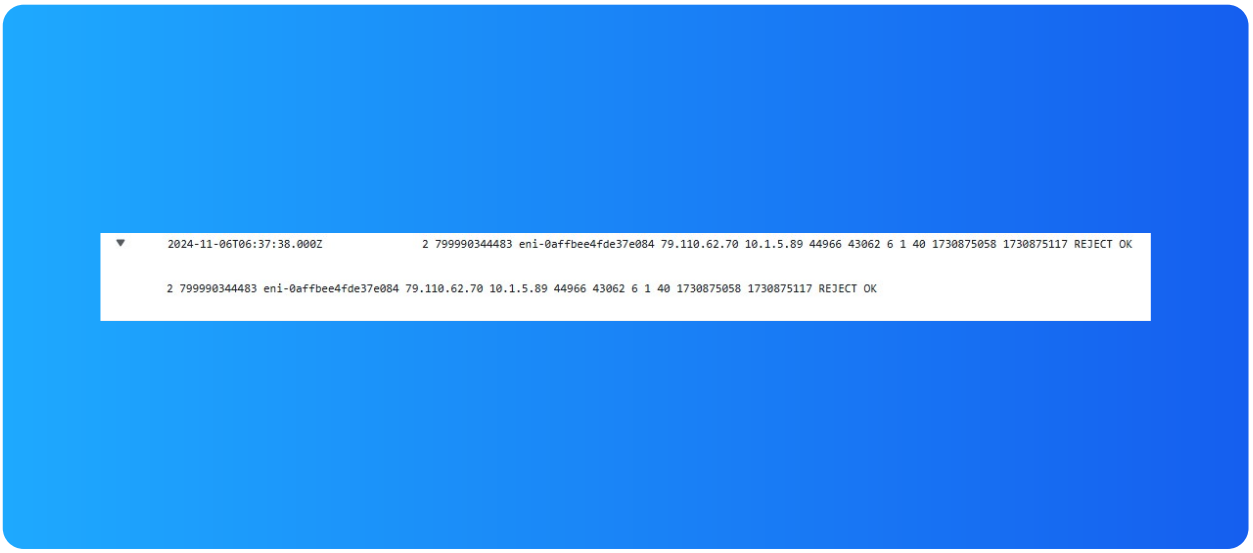


Nikhil Bhan
NextWork Student

Analyzing flow logs

Flow logs tell us about how much data and packets are being sent from the source IP address to the destination IP address, as well as what protocol and port were used for the data transfer. They also show if the transfer was Accepted or Rejected.

For example, the flow log I've captured tells us that on November 6 a data packet was rejected from entering the EC2 instance in VPC 1 at the IP address 10.1.5.89. It was coming from the IP address 79.110.62.70 via a TCP connection on port 44966.



Nikhil Bhan
NextWork Student

Logs Insights

Logs Insights is a feature in CloudWatch that can analyze logs. With Log Insights the user can develop queries to process, filter and combine data to troubleshoot any issues or understand the network traffic in the AWS environment.

I ran the query "Top 10 Byte Transfers by Source and Destination IP Addresses" in CloudWatch. This query analyzes the network traffic and provides me with a list of the highest data transfers between the IP addresses in my AWS network.

#	srcAddr	dstAddr	bytesTransferred
1	52.94.102.118	10.1.5.89	14438
2	10.1.5.89	52.94.102.1…	7546
3	79.110.62.70	10.1.5.89	2920
4	87.247.158.136	10.1.5.89	880
5	206.168.35.22	10.1.5.89	655
6	167.94.138.130	10.1.5.89	655
7	176.113.115.197	10.1.5.89	640
8	87.247.158.137	10.1.5.89	572
9	147.185.132.39	10.1.5.89	402
10	205.210.31.138	10.1.5.89	402

Everyone should be in a job they love.

Check out nextwork.org for more projects