NextWork.org

VPC Monitoring with Flow Logs

PH phogan2886@gmail.com

PH
phogan2886@gmail.com
NextWork Student
NextWork.org

Introducing Today's Project!

What is Amazon VPC?

A VPC is a service that allows you to create a private network within AWS cloud. With VPC, you can define your own network configuration, including IP address ranges, subnets, route tables, and security settings.

How I used Amazon VPC in this project

I created two VPCs and EC2 instances within each VPC. After I created a peer connection between the two, I created a flow log to monitor the network traffic between them.

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

How easy it was to create a flow log group to monitor the traffic and how to read the logs. THe JSON portion was the most interesting when I set the parameters of what I wanted to look for.

This project took me...

This project took me about an hour.

PH
phogan2886@gmail.com
NextWork Student
NextWork.org

In the first part of my project...

Step 1 - Set up VPCs

Creating 2 VPCs using VPC and more to auto populate 2 of them

Step 2 - Launch EC2 instances

Create EC2 instances so that they can send data to each other in the project, which gives us network activity to monitor. Create EC2 instances in each VPC, so I can use them to test my VPC peering connection later

Step 3 - Set up Logs

Set up a way to track all inbound and outbound network traffic.. Set up a space that stores all of these records.

Step 4 - Set IAM permissions for Logs

Give my logs permission to write and send them to the cloud watch group that was created

PH
phogan2886@gmail.com
NextWork Student

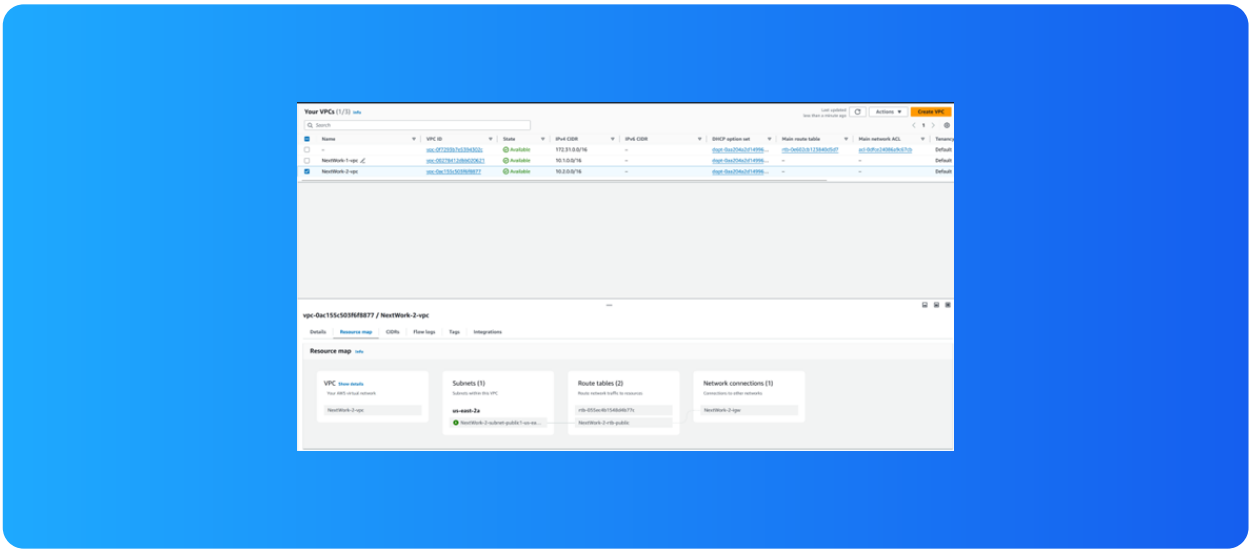
Multi-VPC Architecture

I started my project by launching 2 VPCs and assigning IP addresses of 10.1 and 10.2 to differentiate both of them

The CIDR blocks for VPCs 1 and 2 are 10.1 and 10.2. They have to be unique because they are their own separate networks.

I also launched EC2 instances in each subnet

My EC2 instances' security groups allow ICMP traffic from ALL IP addresses. This is because so I can do a ping test



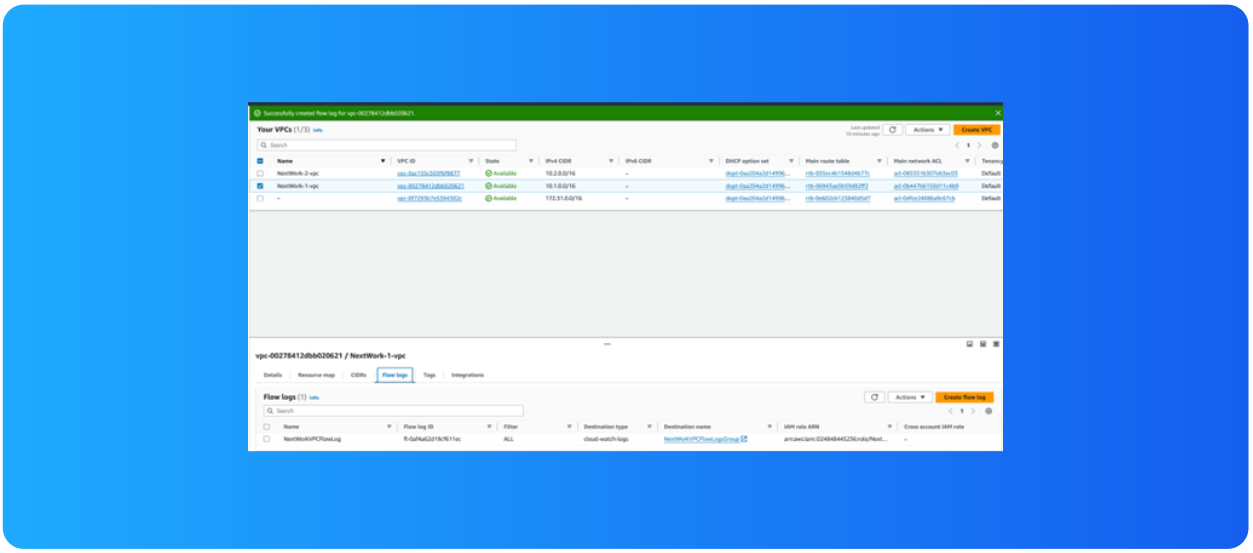
PH
phogan2886@gmail.com
NextWork Student

Logs

Logs are like a diary for your computer systems. They record everything that happens, from users logging in to errors popping up.

Log groups are a big folder in AWS where you keep related logs together. Usually, logs from the same source or application will go into the same log group, BUT logs are also region-specific.

I also set up a flow log for VPC 1



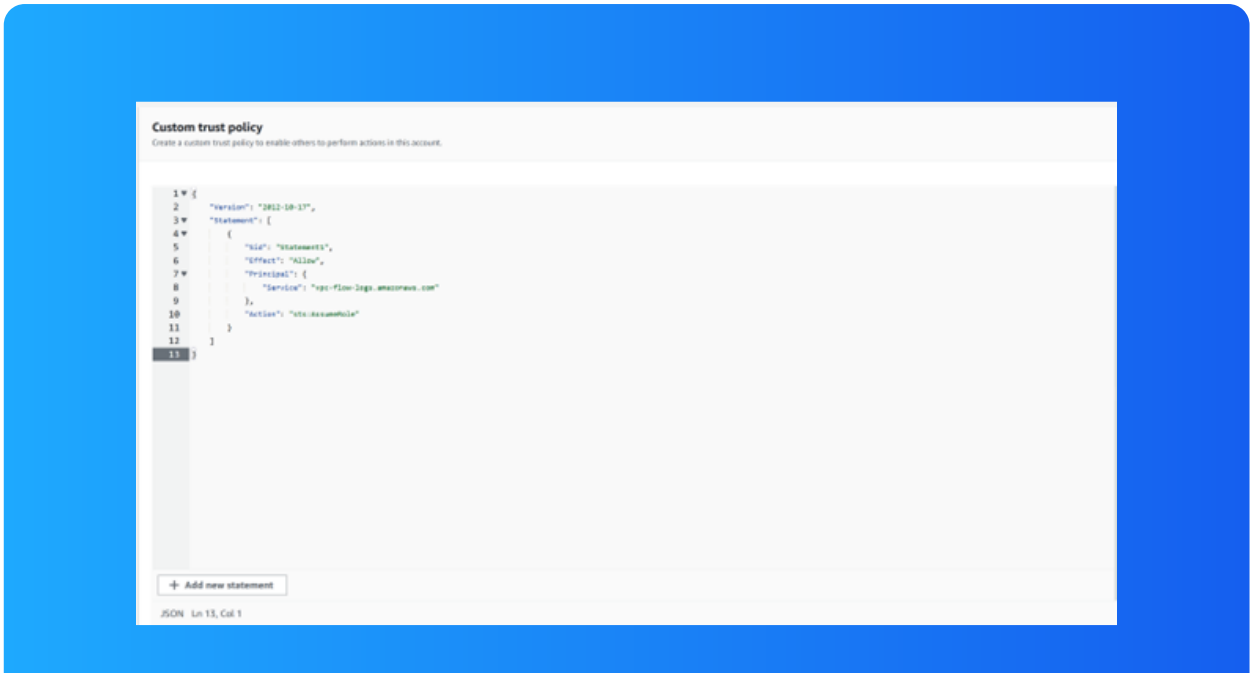
PH
phogan2886@gmail.com
NextWork Student

IAM Policy and Roles

I created an IAM policy because VPC Flow Logs by default don't have the permission to record logs and store them in your CloudWatch log group. This policy makes sure that your VPC can now send log data to your log group!

I also created an IAM role to give VPC Flow Logs the permission to write and send logs to CloudWatch. We only want Flow Logs to have this access, not just any service.

A custom trust policy is specific type of policy! They're different from IAM policies. While IAM policies help you define the actions a user/service can or cannot do, custom trust policies are used to very narrowly define who can use a role.



PH
phogan2886@gmail.com
NextWork Student
NextWork.org

In the second part of my project...

Step 5 - Ping testing and troubleshooting

Let's generate some network traffic and see whether our flow logs can pick up on them. I'm going to generate network traffic by trying to get our instance in VPC 1 to send a message to our instance in VPC 2.

Step 6 - Set up a peering connection

Set up a connection link between my VPCs so they can communicate between the 2 of them.

Step 7 - Update VPC route tables

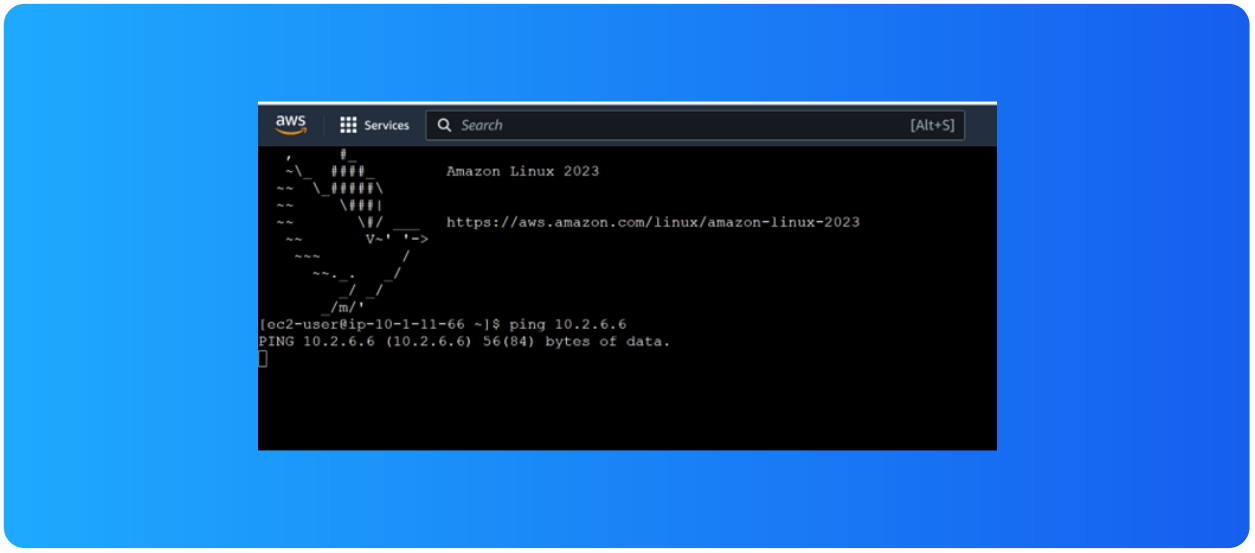
Step 8 - Analyze flow logs

Review the flow logs recorded about VPC 1's public subnet. Analyse the flow logs to get some insights

PH
phogan2886@gmail.com
NextWork Student
NextWork.org

Connectivity troubleshooting

My first ping test between my EC2 instances had no replies, which means I am not receiving a response from the other instance. The network traffic has been blocked.



'I could receive ping replies if I ran the ping test using the other instance's public IP address, which means Instance 2 is correctly configured to respond to ping requests, and Instance 1 can actually communicate with Instance 2 if it traffic goes

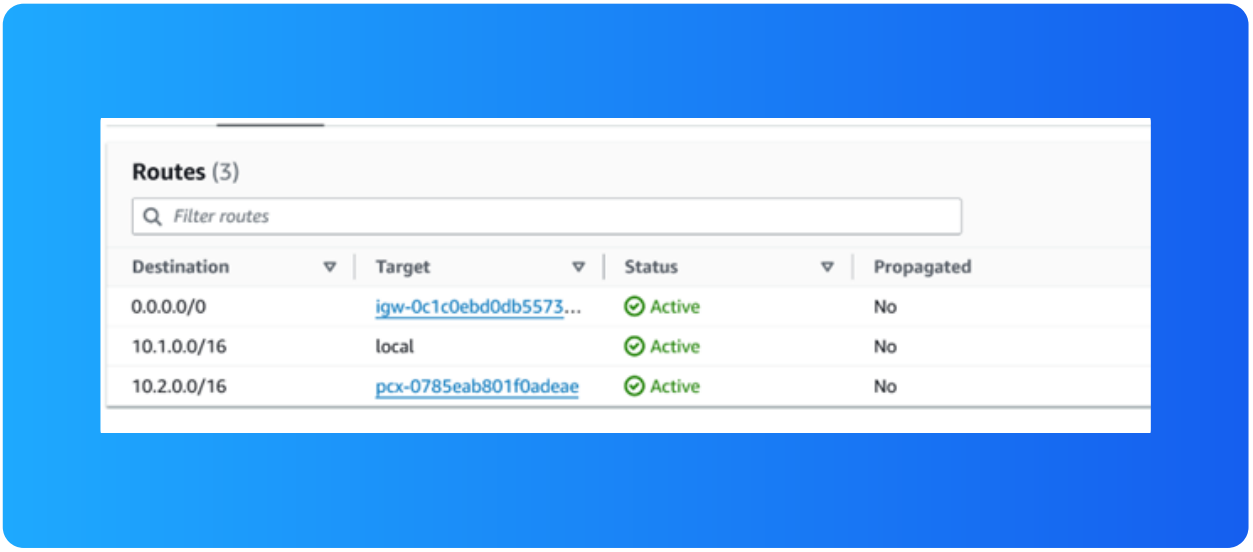
PH
phogan2886@gmail.com
NextWork Student

Connectivity troubleshooting

Looking at VPC 1's route table, I identified that the ping test with Instance 2's private address failed because missing in my architecture is the VPC peering connection that directly connects VPCs 1 and 2.

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

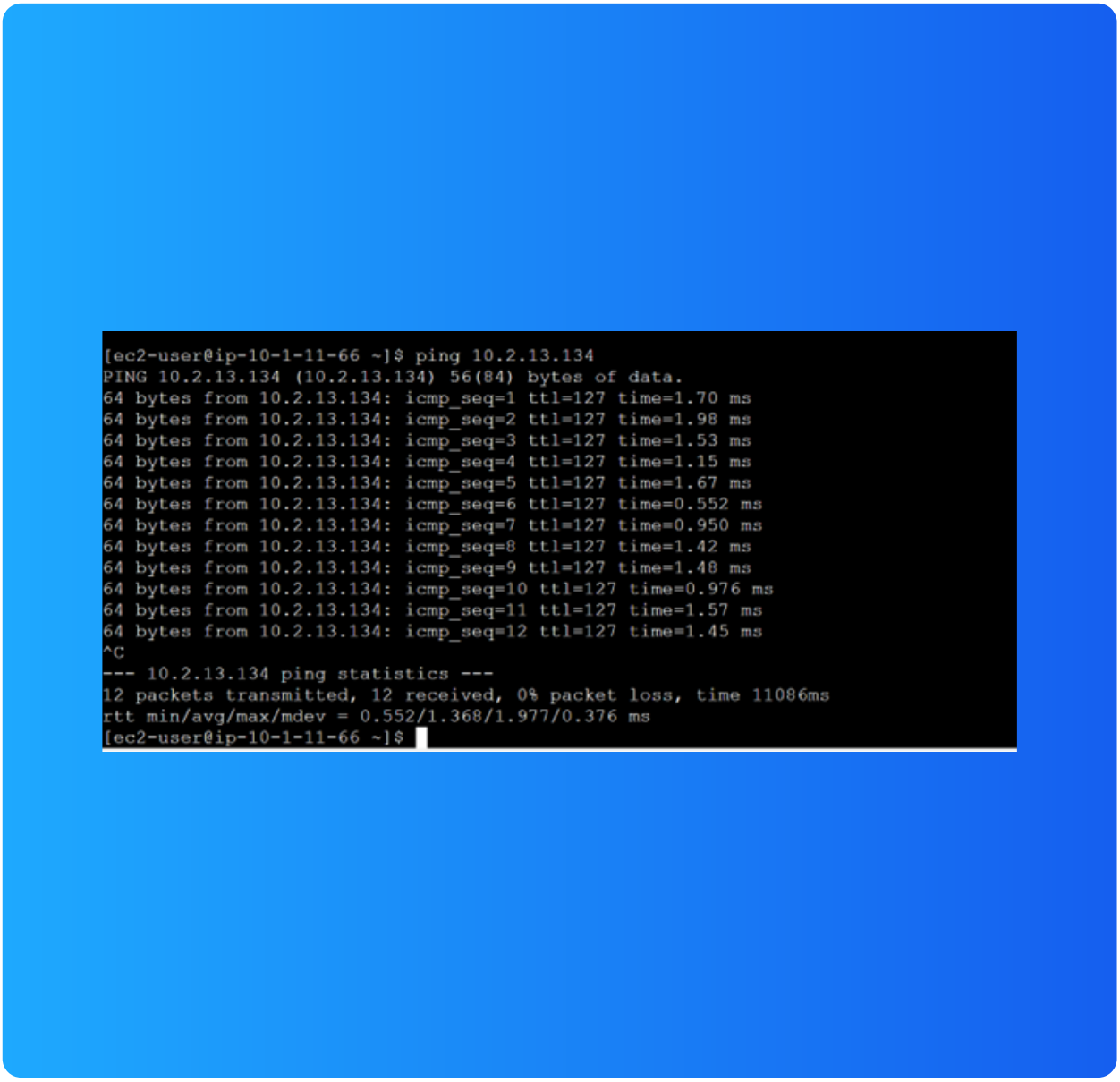
I also updated both VPCs' route tables so that they have a direct private link with each other instead of going through a public route.



PH
phogan2886@gmail.com
NextWork Student

Connectivity troubleshooting

I received ping replies from Instance 2's private IP address! This means the new private route tables have been successfully been created between the VPCs

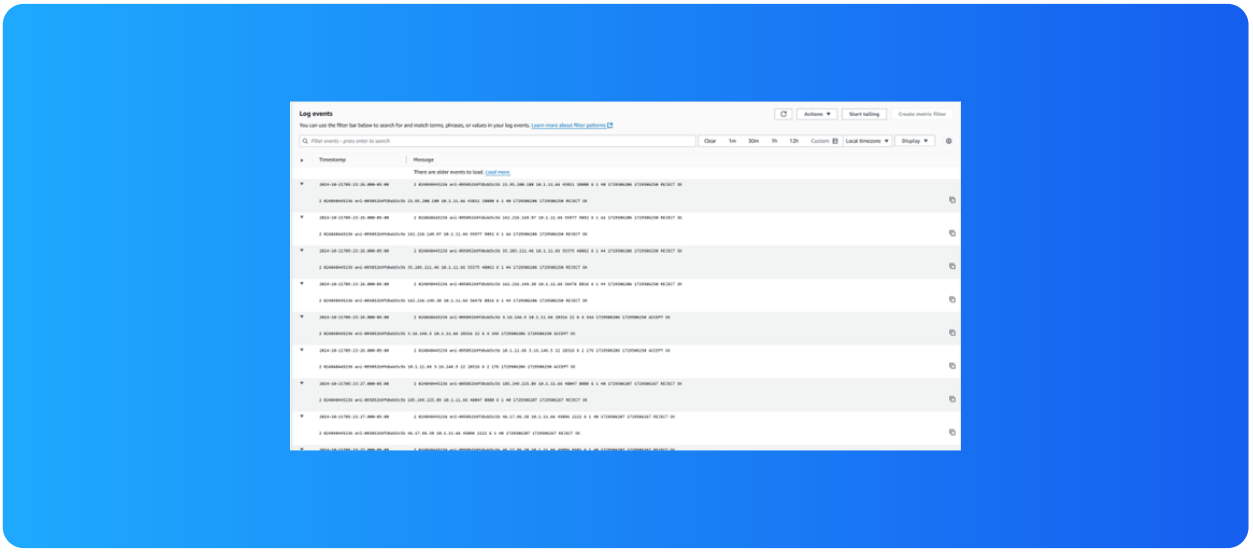


PH
phogan2886@gmail.com
NextWork Student

Analyzing flow logs

Flow logs can help you with a number of tasks, such as: Diagnosing overly restrictive security group rules. Monitoring the traffic that is reaching your instance. Determining the direction of the traffic to and from the network interfaces.

For example, the flow log I've captured tells us abou the network traffic between the two VPCs I created. Whether the attempt to ping was successful or not.

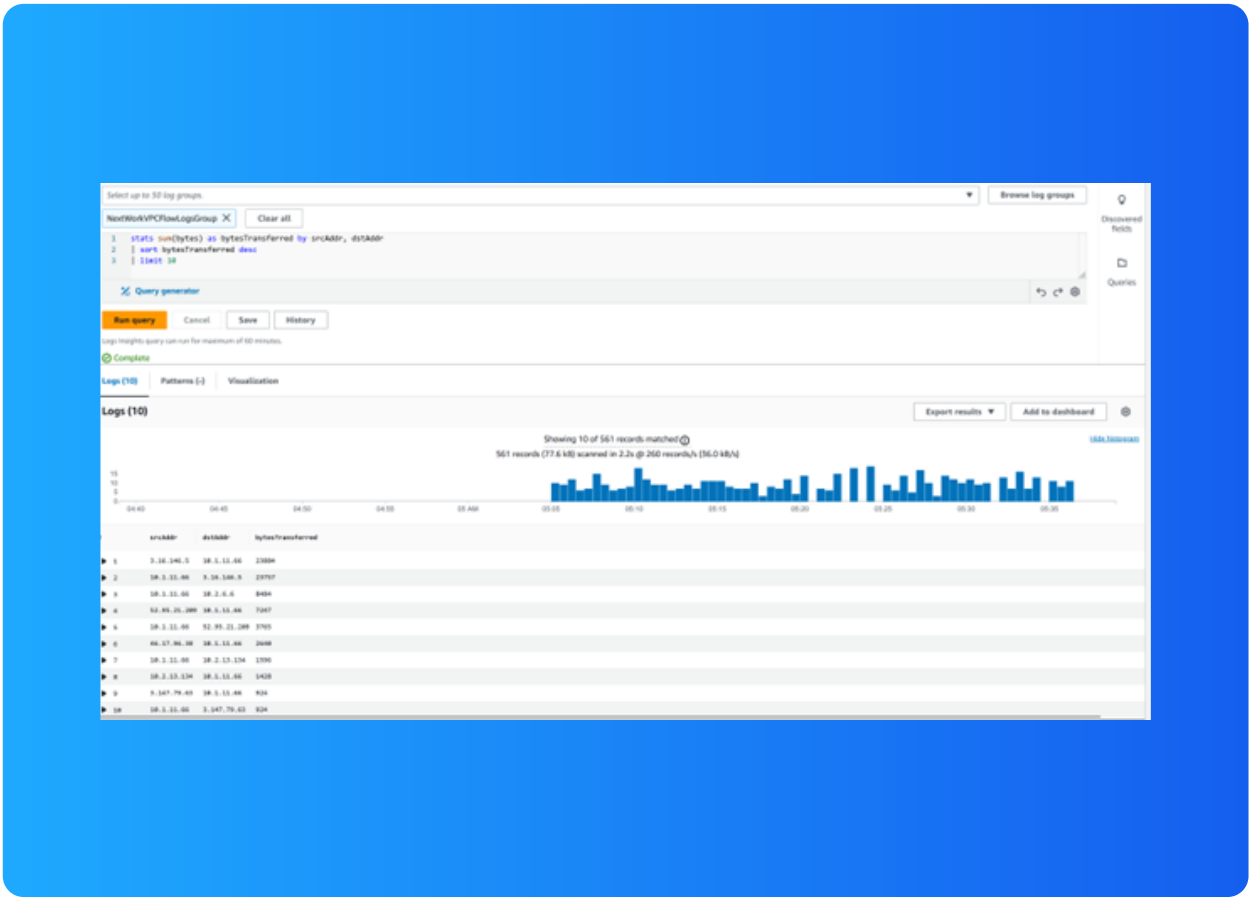


PH
phogan2886@gmail.com
NextWork Student

Logs Insights

AWS Logs Insights is a tool in Amazon Web Services that helps you analyze and search through log data stored in CloudWatch Logs. It makes it easy to quickly find information, visualize data, and troubleshoot issues.

I ran the query VPC Flow Logs Top 10 byte transfer by source and destination IP Addresses. This query analyzes the top 10 biggest data transfers between IP addresses in your network! You'll find out which resources are moving the most data.



Everyone should be in a job they love.

Check out nextwork.org for more projects