NextWork.org

VPC Monitoring with Flow Logs

Alex Ten

Alex Ten
NextWork Student
NextWork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a foundational AWS service that lets us control the underline network for our resources, so that we can control traffic flow, monitor for security ,and organize our resources.

How I used Amazon VPC in this project

In todays project we achieved two big milestones. First, we learned to troubleshoot VPC peering connectivity issues. Secondly, we learned how to monitor network traffic using VPC flow logs.

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

I didnt expect to see how queries really shows you whats going on under the hood. So much data can be analyzed for troubleshooting purposes.

This project took me...

This project took me under 1 hr to do while learning how Peering, log insights and Flow Logs work.

Alex Ten
NextWork Student
NextWork.org

In the first part of my project...

Step 1 - Set up VPCs

In this step I have created the 2 VPC's from scratch in minutes. Networking monitioring a can still be done with just a single VPC.

Step 2 - Launch EC2 instances

In this step I will be creating and launching two 2 instances, one in each VPC. Our EC2 intances will generate traffic that our VPV flow logs will monitor.

Step 3 - Set up Logs

In this step we are setting up VPC flow logs to start monitoring network traffic. We are also setting up a storage space for our flow logs.

Step 4 - Set IAM permissions for Logs

In this step we provide VPC Flow Logs with the permission to create logs and upload them into our log group in CloudWatch.

A

Alex Ten
NextWork Student

NextWork.org

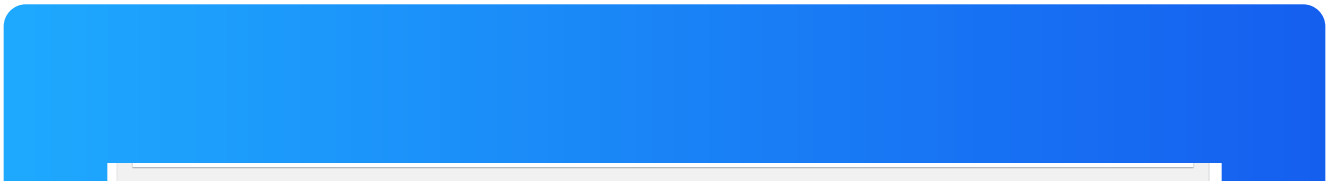
Multi-VPC Architecture

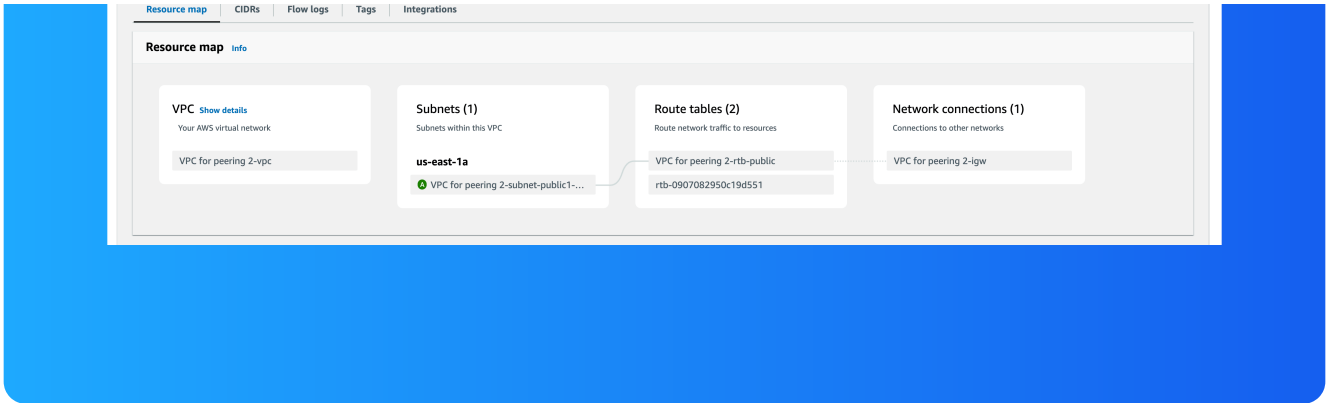
I started my project by launching 2 VPCs and created 2 public subnets. One public subnets per VPC with no private subnets.

Each subnet must have a unique CIDR block to ensure that it can be properly identified and communicate within the VPC. Overlapping CIDR blocks between subnets should be avoided to prevent routing conflicts and potential network issues."

I also launched EC2 instances in each subnet

My EC2 instances' security groups allow all SSH traffic and ICMP type traffic. EC2 Instance Connect will need to access both traffic types for connectivity tests.





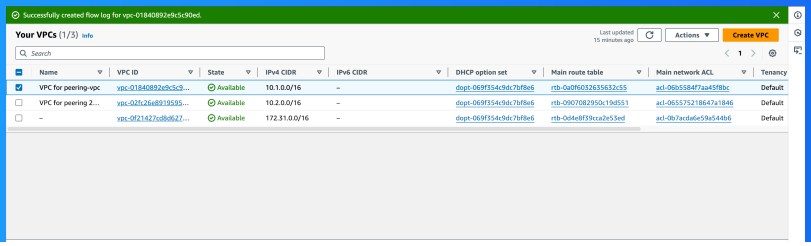
Alex Ten
NextWork Student
NextWork.org

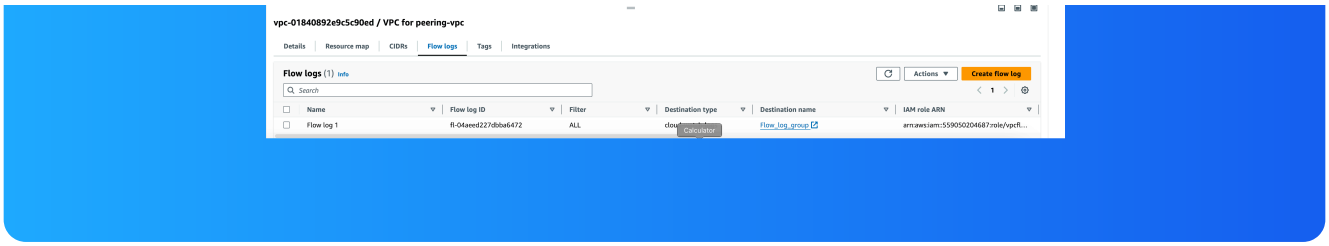
Logs

Logs are data entries for our computer system. They're detailed activity ralated to the traffic/resource/AWS service that the logs tracks.

Log groups are like folders that contain the actual log activity within the project/application/source and are often in a log group together.

I also set up a flow log for VPC 1





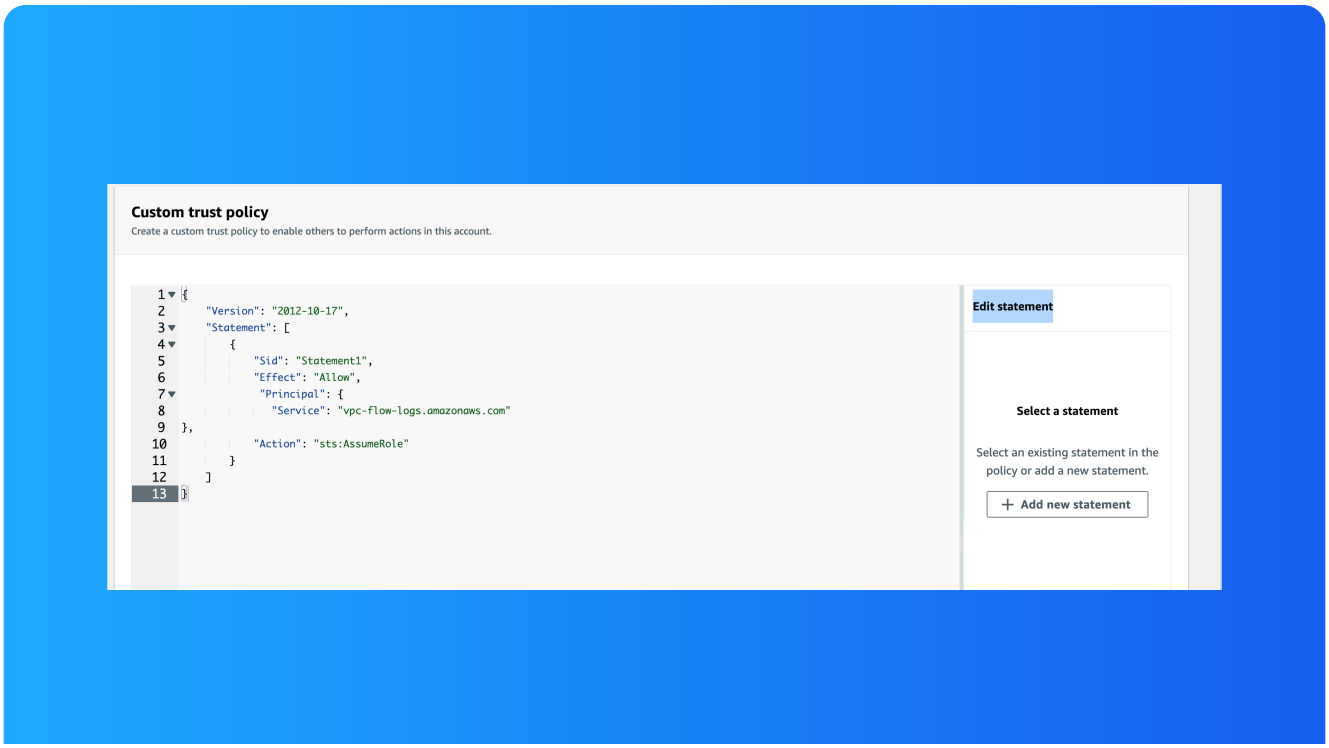
Alex Ten
NextWork Student
NextWork.org

IAM Policy and Roles

I created an IAM policy so that we can define a rule that allows policy holders e.g our VPC Flow Logs service the ability to create log streams and upload them into CloudWatch.

I also created an IAM role because services like VPC Flow Logs have to be associated with a role instead of JSON. Creating an IAm role with be necessary to give our VPC Flow Logs the access it needs to record and upload logs.

A custom trust policy is a specific type fo policy used for designing who / what is allowd to access the IAM role.



A

Alex Ten
NextWork Student

NextWork.org

In the second part of my project...

Step 5 - Ping testing and troubleshooting

In this step we are generating network traffic. This becomes important we are commuinication about cloudworks/cloud networking/or cloud engineering.

Step 6 - Set up a peering connection

In this step we are setting up a peering connection so that our VPC's can communicate with each other.

Step 7 - Update VPC route tables

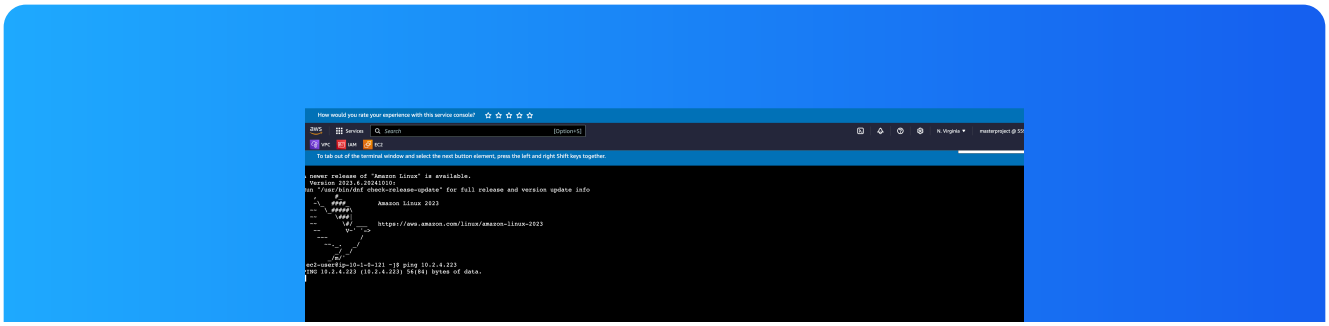
Step 8 - Analyze flow logs

In this step we are tracking the network data that's been collected on our VPC's and then analyze that data to extracts insights.

Alex Ten
NextWork Student
NextWork.org

Connectivity troubleshooting

My first ping test between my EC2 instances had no replies, which means Icmp Traffic could be blocked.It could be blocked by the security groups/network acls, or maybe our traffic is being routed to a wrong path.



I could receive ping replies if I ran the ping test using the other instance's public IP address, which means second instance is actually allowing ICMP traffic.

A

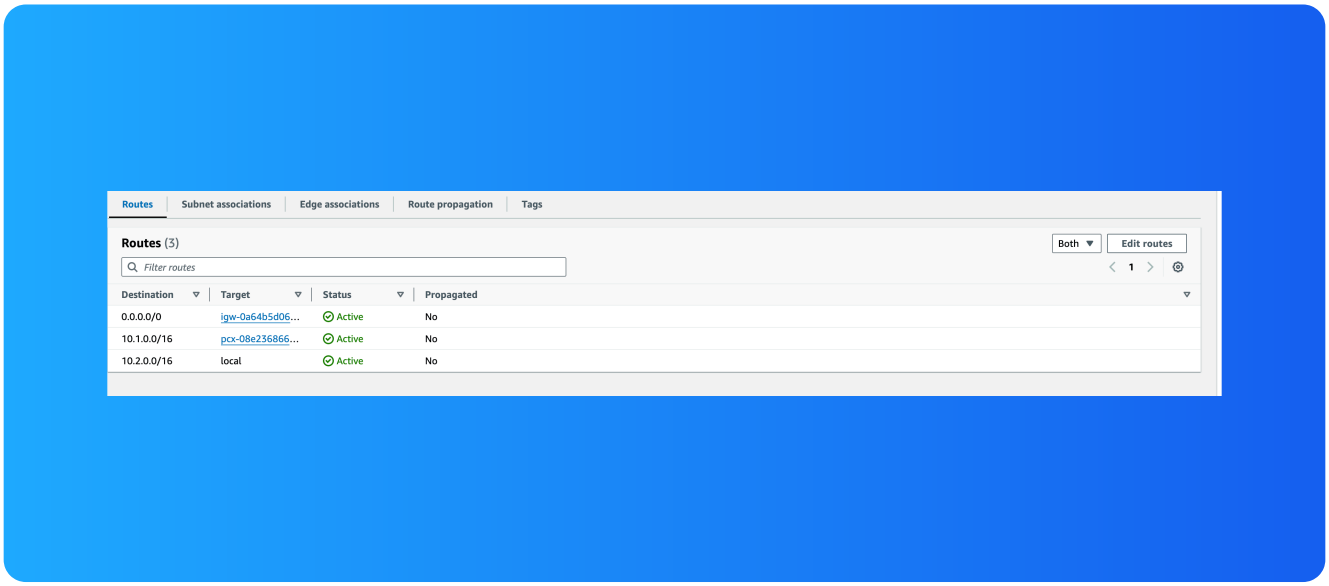
Alex Ten
NextWork Student
NextWork.org

Connectivity troubleshooting

Looking at VPC 1's route table, I identified that the ping test with Instance 2's private address failed because we do not have a route in our VPC's route tables that directs traffic from VPC to another.

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

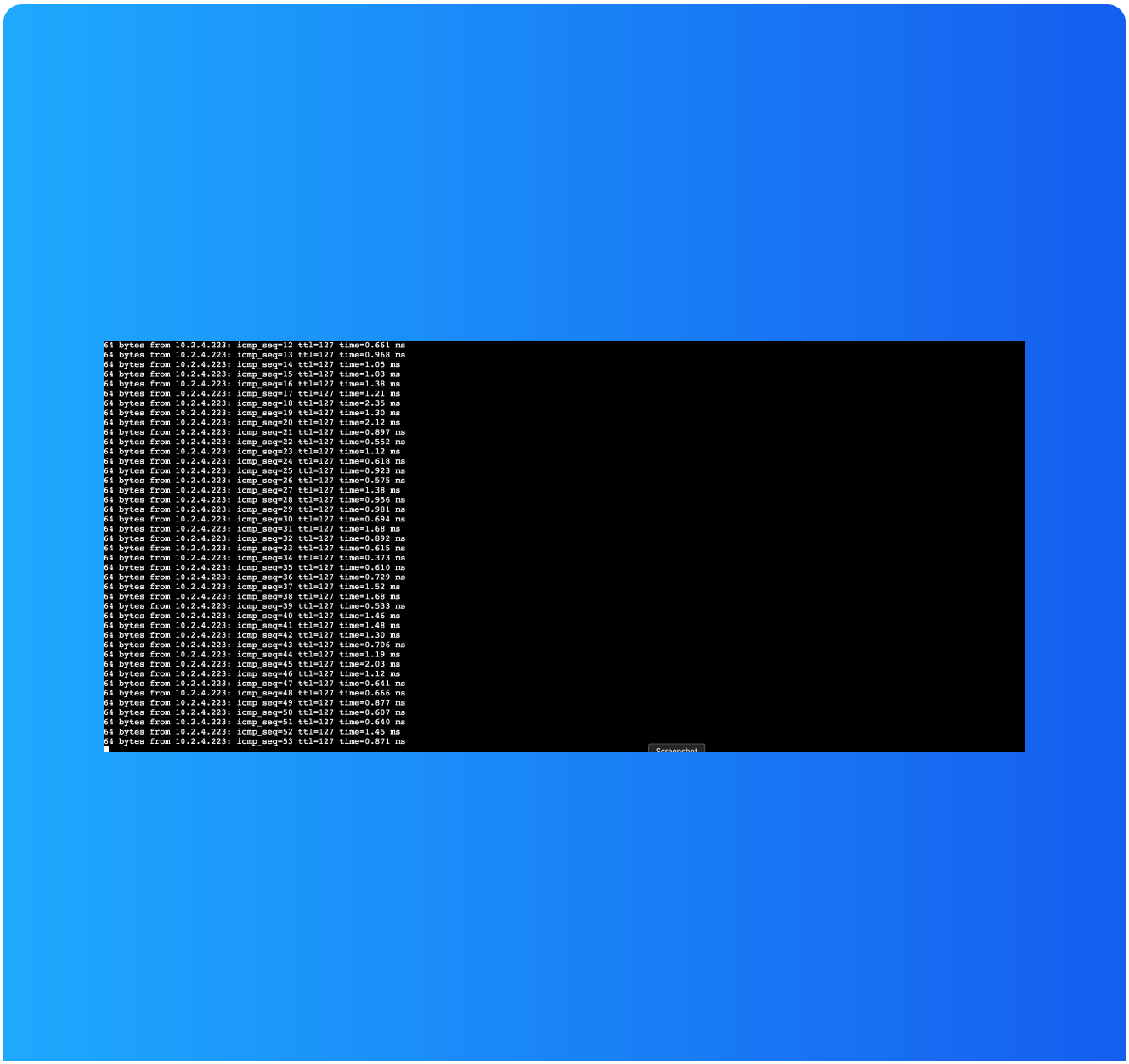
I also updated both VPCs' route tables, so that traffic of one of the VPC's heading to other VPC's private IPV4 address can get directed to go through the peering connection instead of the public internet.



Alex Ten
NextWork Student
NextWork.org

Connectivity troubleshooting

We recieved ping replies from instance 2's private IP address. This means setting up the peering connection and the route table sovled the connectivity error of our VPC's traffic not being able to navigate VPC to another.

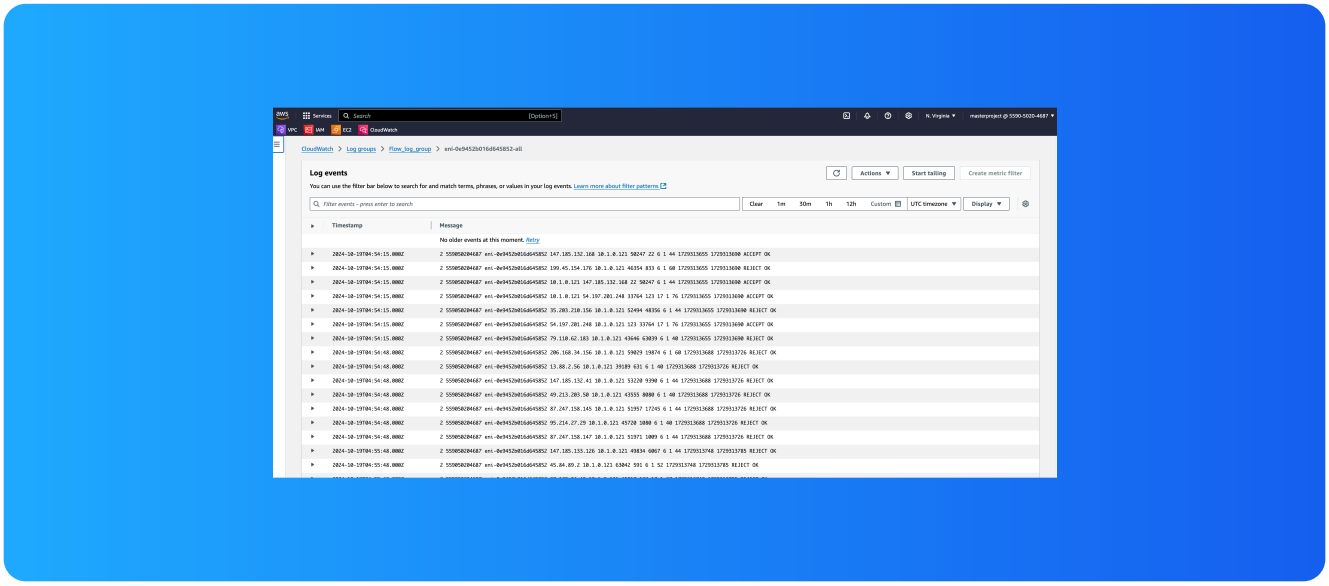


Alex Ten
NextWork Student
NextWork.org

Analyzing flow logs

Flow logs tell us about the source and destination of the network traffic and the amount of data being transffered, whether the traffic was accepted or rejected.

For example, the flow log I've captured tells us that the traffic went from that the log group associated with a network interface (ENI) with the ID "eni-0694526016d645852, also a timestamp for each event and if it was accepted or rejected.

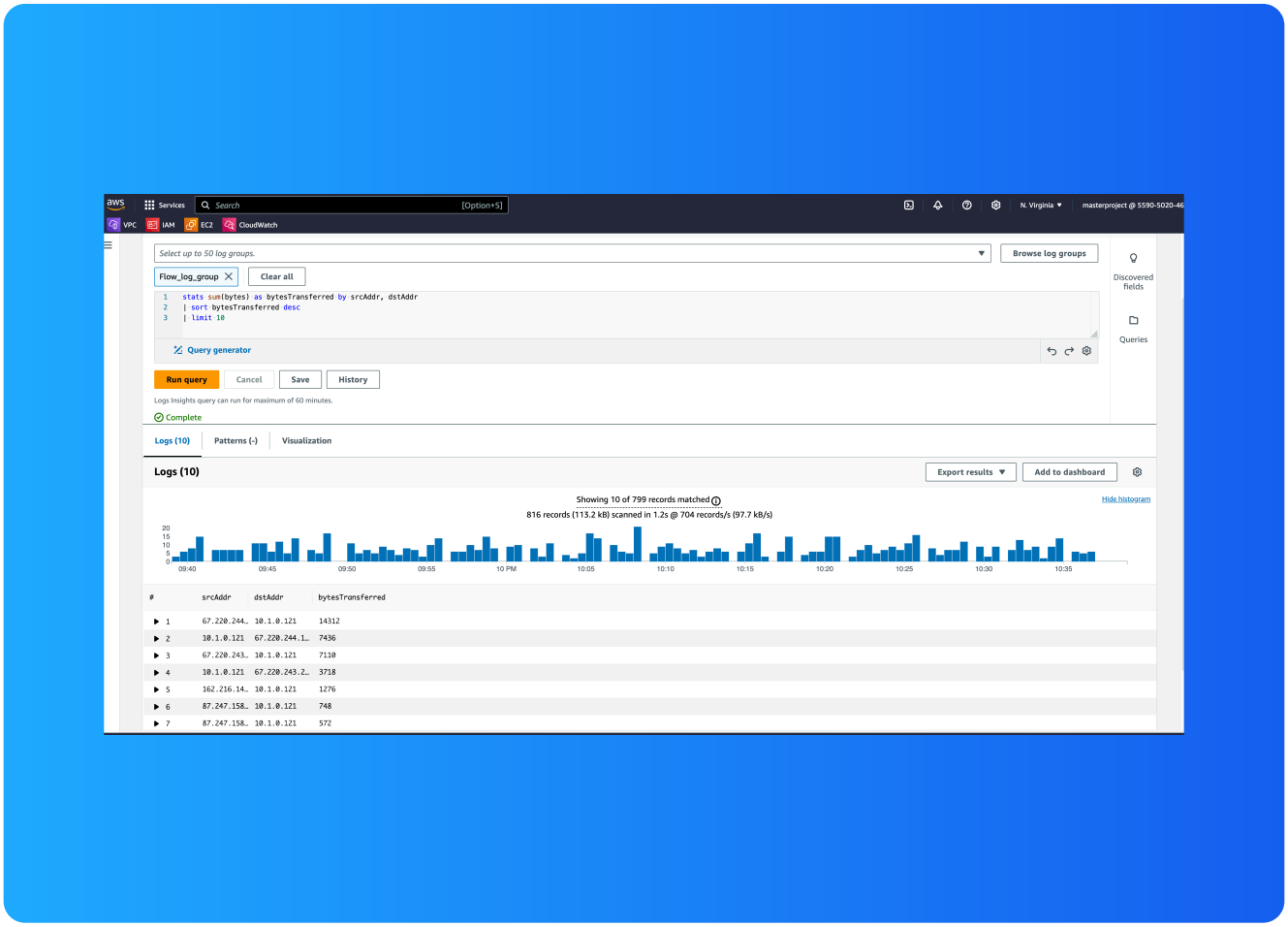


Alex Ten
NextWork Student
NextWork.org

Logs Insights

Logs Insights is a special tool within Amazon CloudWatch that helps us with analysing logs and creating visual graphs and charts through queries.

I ran the query Top 10 byte transfers by source and destination IP addresses, This query analyses the flow logs collected on EC2 Instance 1, and return the top 10 pairs of IP addresses based on the amount of data transfered between them.



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for more projects