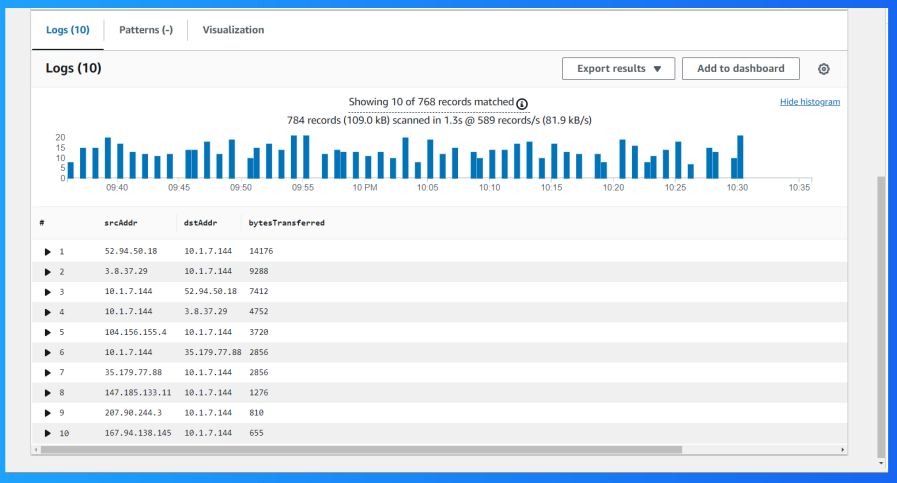
NextWork.org

VPC Monitoring with Flow Logs

TA tahirgroot@gmail.com



TA
tahirgroot@gmail.com
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

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

How I used Amazon VPC in this project

In today's project, I achieved two big milestones! First, I learnt to troubleshoot vpc peering connectivity issues. I learnt how to monitor network traffic using vpc flow logs.

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

n/a

This project took me...

1 hour

TA
tahirgroot@gmail.com
NextWork Student

In the first part of my project...

Step 1 - Set up VPCs

in this step we will Create two VPCs from scratch! in minutes. Network Monitoring can still be done with just a single VPC, but its great to have the extra challenge and tackle vpc peering in this project too!

Step 2 - Launch EC2 instances

in this step we launch two EC2 instances one in each vpc. Doing this is important to setup the reminder of our project- my Ec2 instances will generate traffic that vpc 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

we provide flow logs with the permission to create logs and upload them into our log group in cloudwatch

TA
tahirgroot@gmail.com
NextWork Student

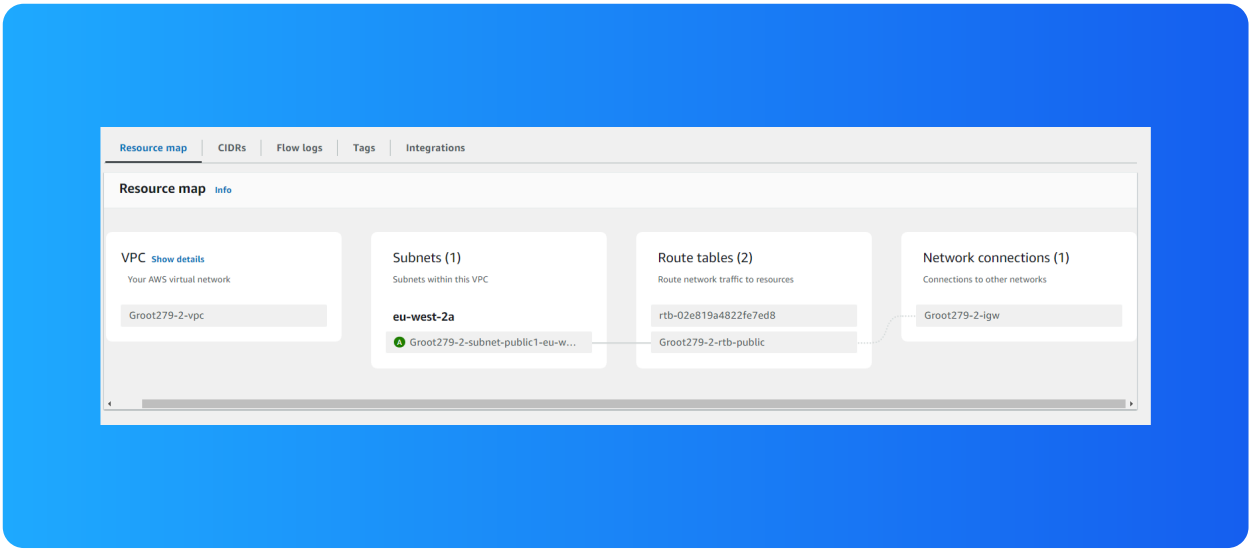
Multi-VPC Architecture

i started my project by launching two vpcs! We created two public subnets (i.e one public subnet in each vpc) with no private subnets

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 having overlapping cidr block will cause network routing/traffic issues down the line when traffic is needing to go from one vpc to another.

I also launched EC2 instances in each subnet

My EC2 instances' security groups allow ssh and icmp type traffic This is because Ec2 instance connect will need to access our EC2 instance using SSH-type traffic an d because we need to allow icmp type trafic for connectivity test later.

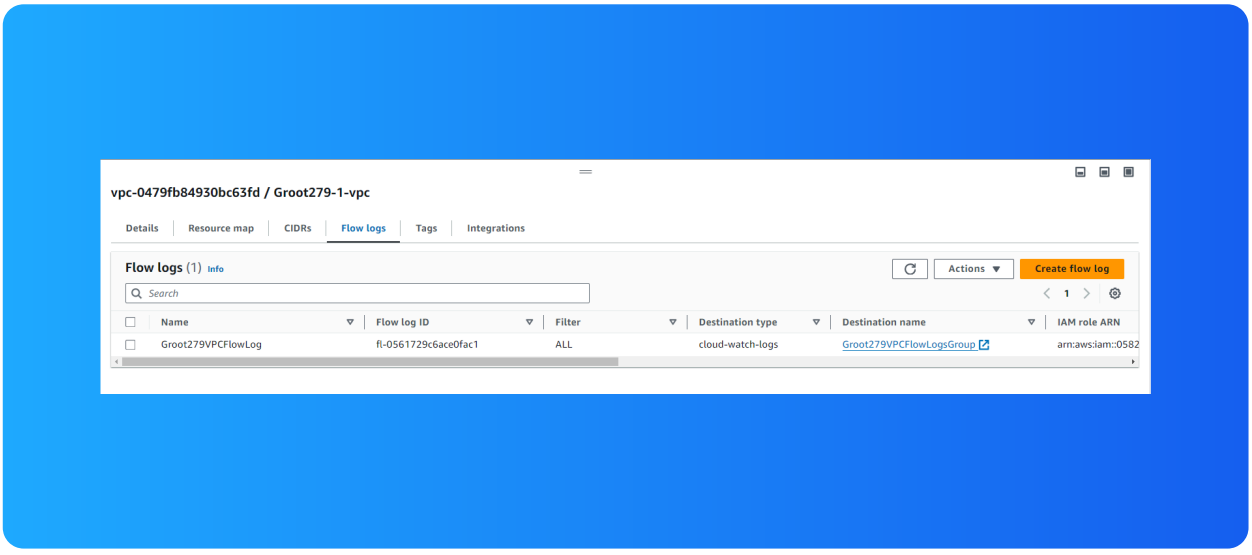


Logs

Logs are like a diary for your computer systems. They record everything that happens, from users logging in to errors popping up. It's the go-to place to understand what's going on with your systems, troubleshoot problems, and keep an eye.

Think of a log group as a big folder in AWS where you keep all your related logs together. Usually, logs from the same source or application will go into the same log group.

I also set up a flow log for VPC 1



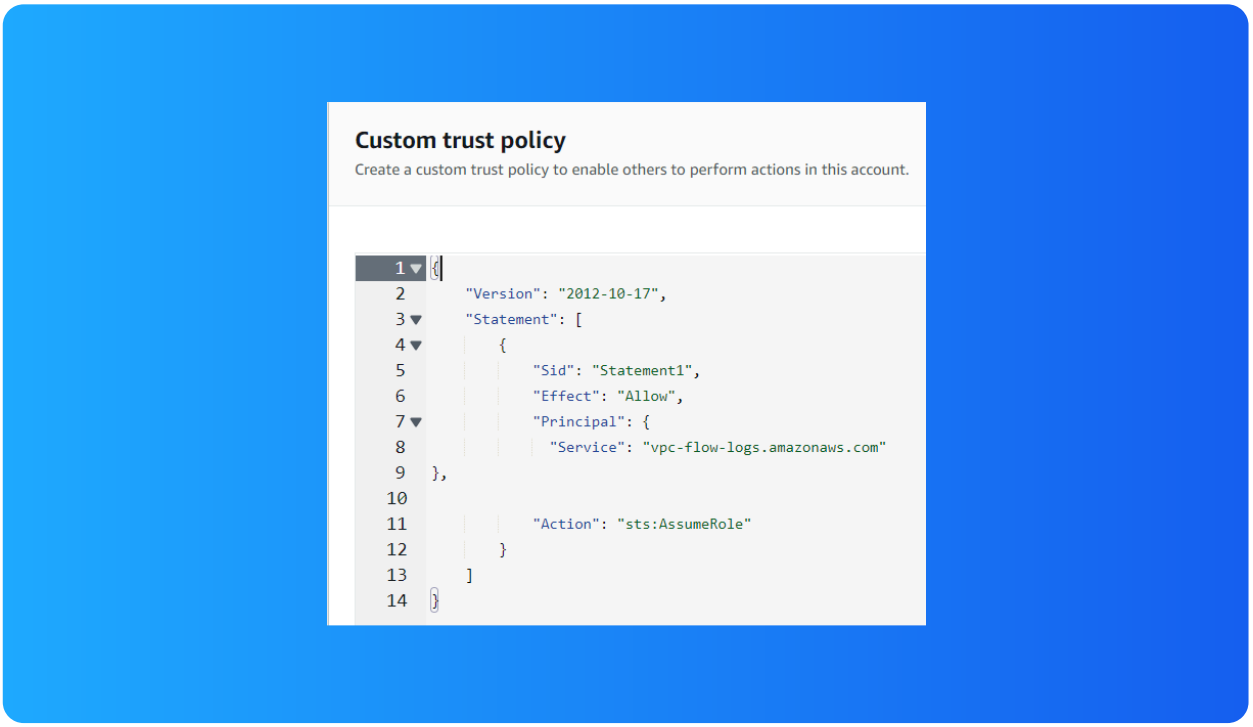
TA
tahirgroot@gmail.com
NextWork Student

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 cloud watch

I also created an IAM role because services like vpc flows have to be associated with a role instaed of JSON! Creating an IAM role will 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 of policy used for designing who/what is allowed access to the IAM role.



TA
tahirgroot@gmail.com
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 when we are communicating about cloud networks/or cloud engineering

Step 6 - Set up a peering connection

in this step, we are setting up a peering connection so that VPcs 1 and 2 can talk directly with each other

Step 7 - Update VPC route tables

In this step, we are updating the route tables for our two vpcs so that traffic bound for the other vpc can be directed to the peering connection instead of the internet

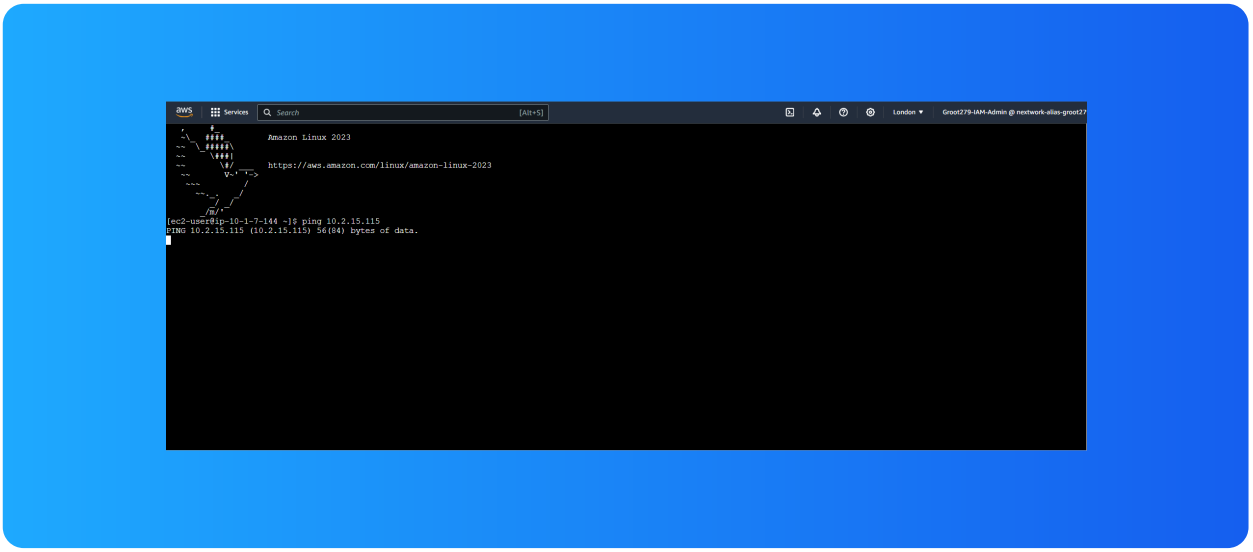
Step 8 - Analyze flow logs

in this step, I am reviewing the network data thats's been collected on my vpcs and then anlayse that data to extract insights.

TA
tahirgroot@gmail.com
NextWork Student

Connectivity troubleshooting

My first ping test between my EC2 instances had no replies, which means ICMP traffic could be blocked by secuirty group/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 meansour second instance is actually allowing ICMP and SSH traffic.

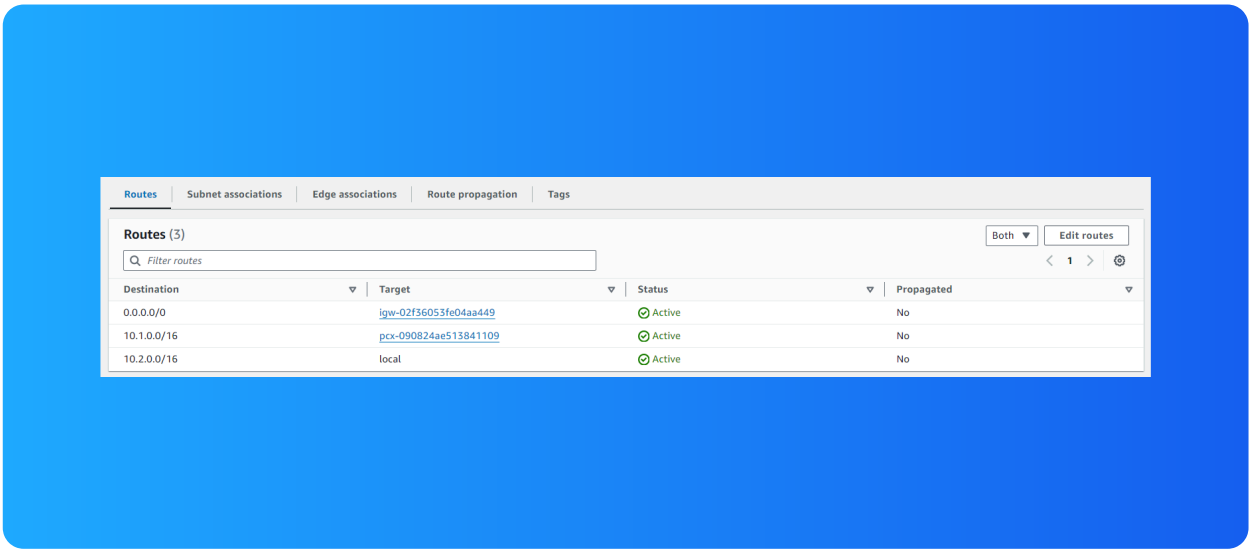
TA
tahirgroot@gmail.com
NextWork Student

Connectivity troubleshooting

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

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

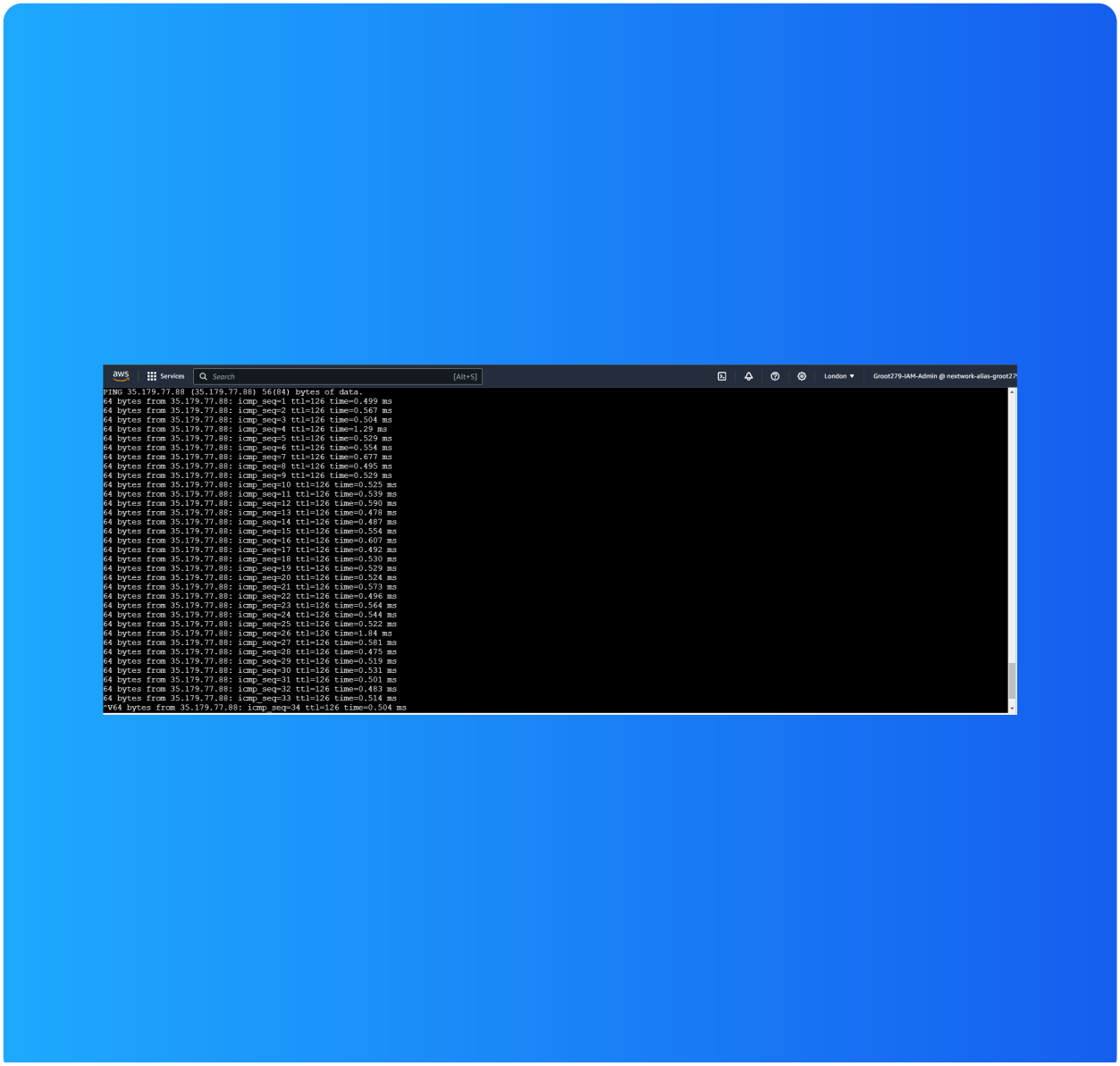
I also updated both VPCs' route tables, so that traffic from one of the VPCs can be heading to the other VPC private IPV4 address can get directed to go through the peering connection instead of the public internet.



TA
tahirgroot@gmail.com
NextWork Student

Connectivity troubleshooting

I received ping replies from Instance 2's private IP address! This means setting up the peering connections and then the route table solved the connectivity error of my vpc's traffic not being able to navigate from one vpc to another



TA
tahirgroot@gmail.com
NextWork Student

Analyzing flow logs

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

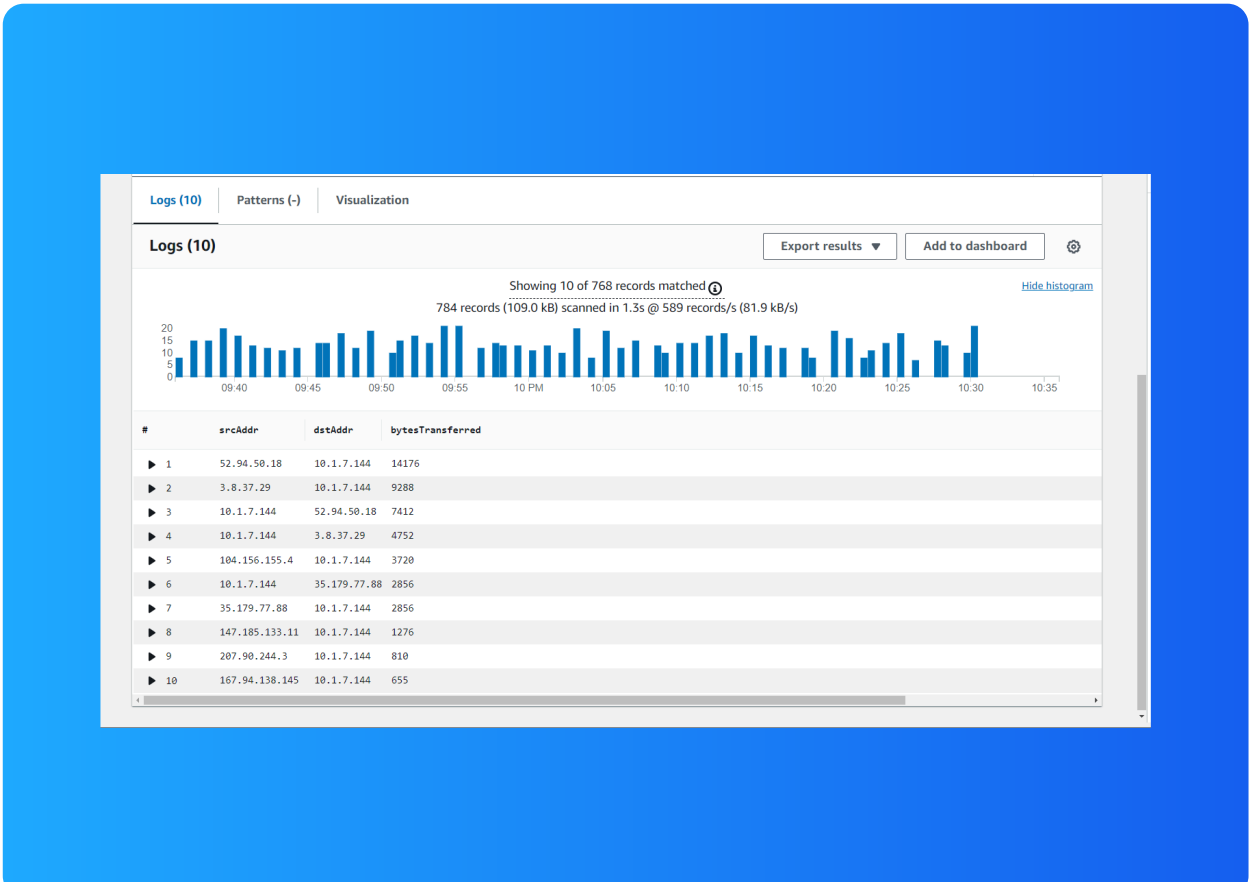
For example, the flow log I've captured tells us that traffic 76 bytes was transferred from source IP 13.40.182.125 (port 123) to destination IP 10.1.7.144 (port 53047) using protocol 17 (likely UDP).

TA
tahirgroot@gmail.com
NextWork Student

Logs Insights

Logs Insights is a powerful tool that allows you to interactively search, analyze, and query log data stored in CloudWatch Logs. It provides a query language similar to SQL, making it easy to extract valuable insights from your log data.

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



Everyone should be in a job they love.

Check out nextwork.org for more projects