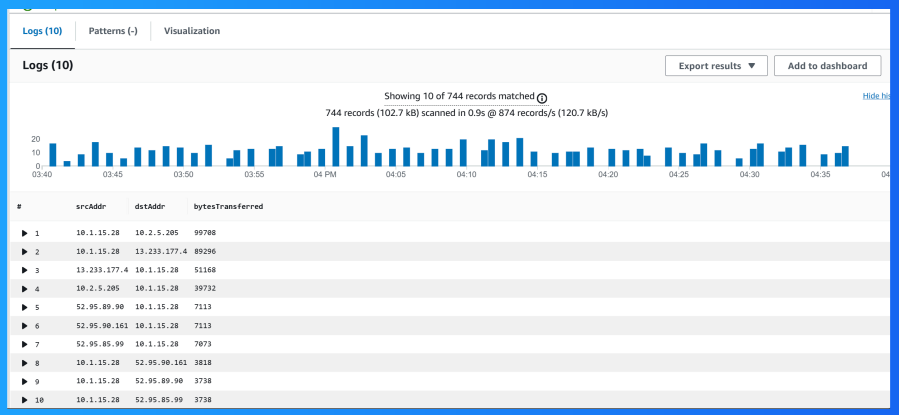
NextWork.org

VPC Monitoring with Flow Logs

MA mallangiharinathreddy727@gmail.com



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, organise our resources.

How I used Amazon VPC in this project

In today's project , we acheived two big milestones! First we learnt to troubleshoot VPC peering connectivity issues. Secondly we learnt how to monitor network traffic using VPC Flow Logs.

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

Logs insights has lots of bulit in queires that give us many options on how we w'd like to analyse our network traffic.

This project took me...

This project took me 2 and Half hour to complete.

In the first part of my project...

Step 1 - Set up VPCs

In this step we will set up two VPC from scratch in minutes. Networking Monitoring can still be done with just a single VPC, but it's great to have the extra challenge and tackle VPC peering in this project too!

Step 2 - Launch EC2 instances

In this step we launch EC2 istances- one in each VPC. Doing this is important to set up the remainder of our project - Our EC2 instances will generate the traffic that VPC Flow Logs will monitor.

Step 3 - Set up Logs

In this step, we are setting up VPC Flow Logs to start monitring Networking traffic. we are 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 permmission to create logs and upload them into our log group in CloudWatch.

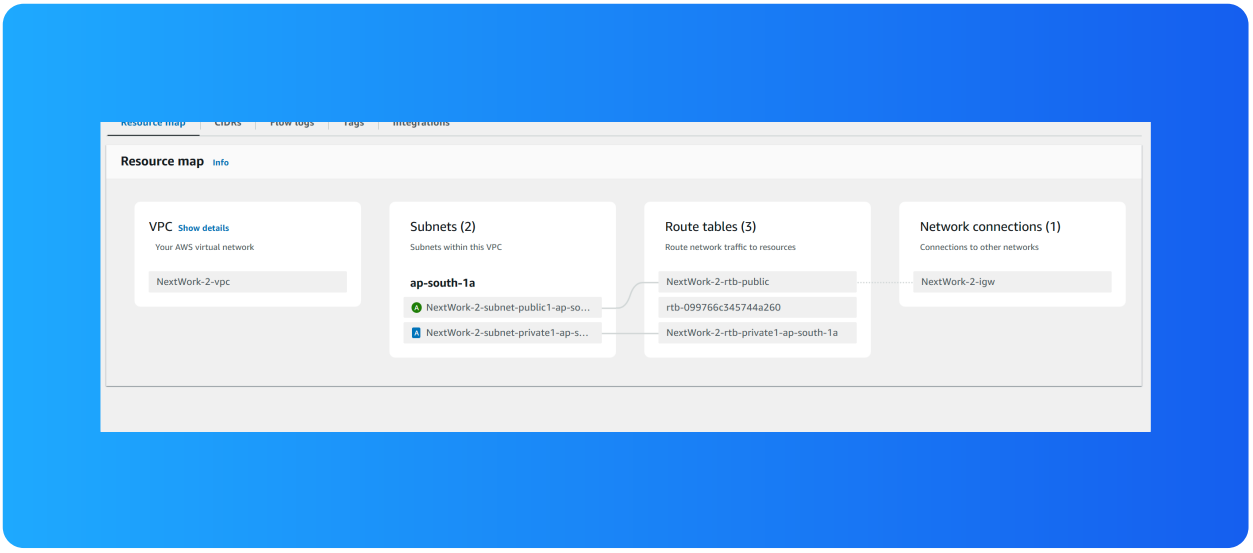
Multi-VPC Architecture

I started my project by launching two VPC's! 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 blocks will cause network routing/traffic issues down the line when traffic is needing to from one VPC to other VPC.

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 need to access our EC2 instance using SSH - type traffic, and because we need to allow ICMP traffic for connectivity tests later.

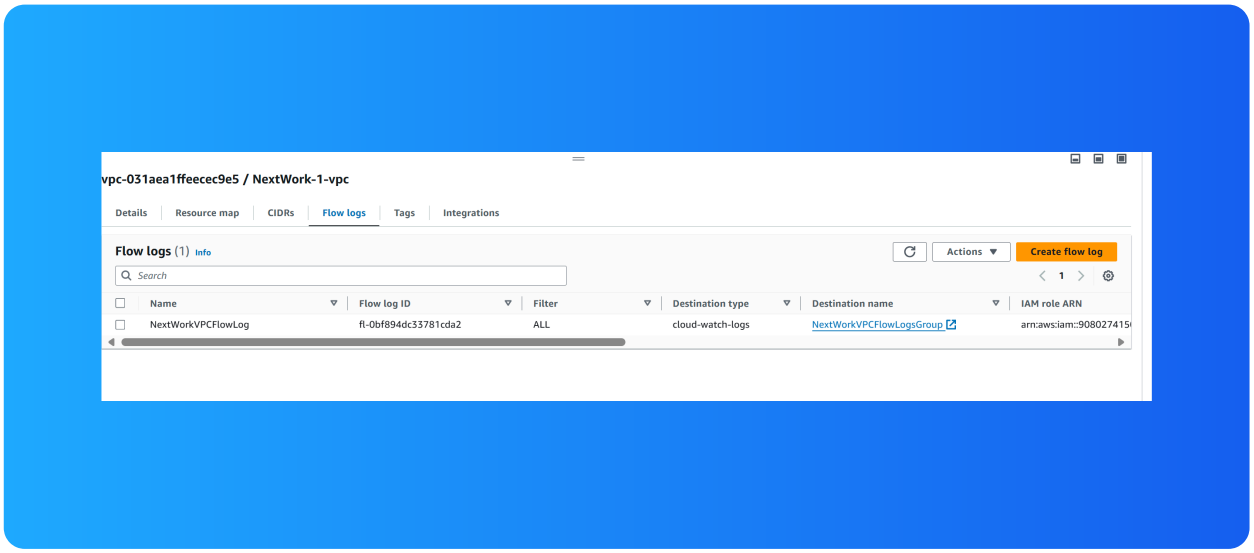


Logs

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 and problems.

Log groups are grouping of Logs i.e. logs that belong to the project/application/source are often in a log group together.

I also set up a flow log for VPC 1

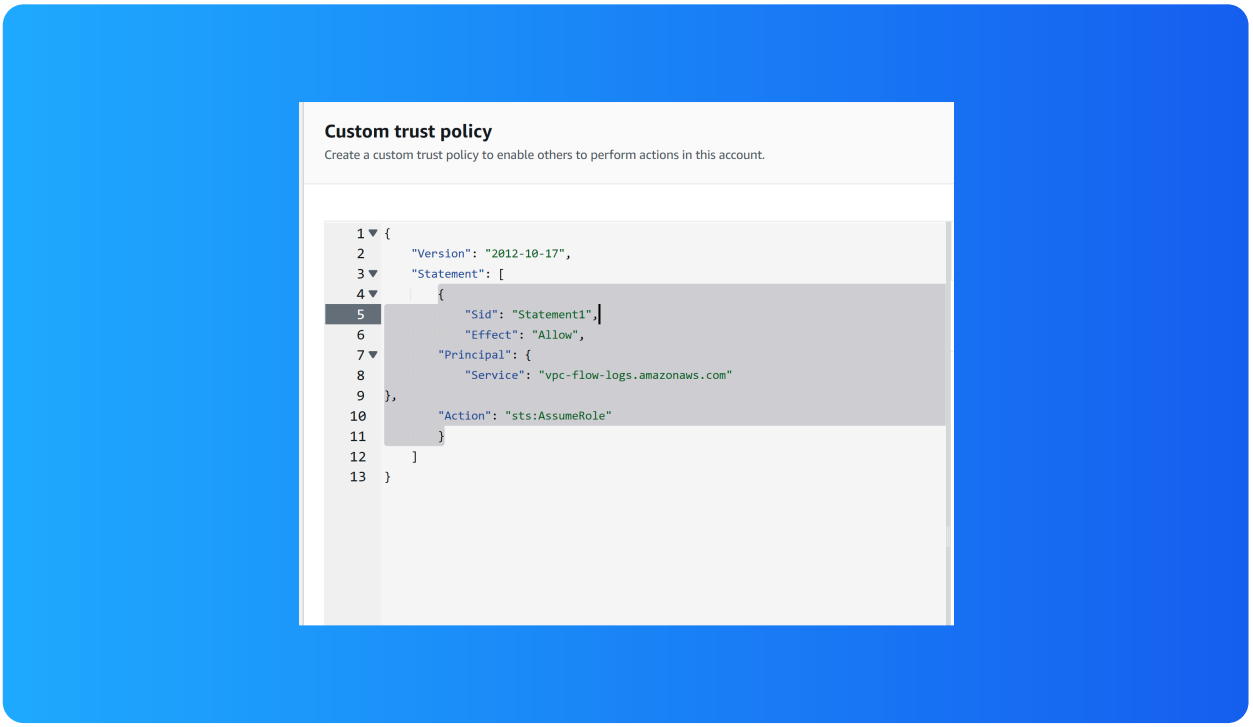


IAM Policy and Roles

I created an IAM policy so that we can define a rule that allows policy holders eg. 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 Flows have to be associated with a role instead 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.



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 CloudNetworks/Networking/Cloud Engineering.

Step 6 - Set up a peering connection

In this step we are setting up a peering connection so that VPC 1 and 2 can talk directly with each other.

Step 7 - Update VPC route tables

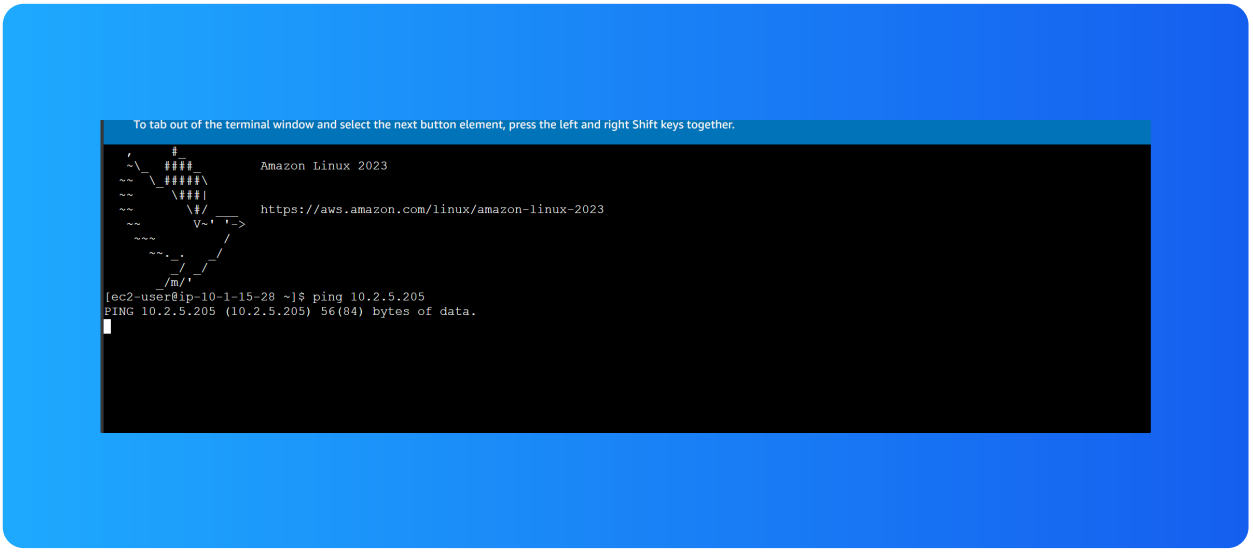
In this step we are updating the route tables for our two VPCs so that traffic bound for the other VPC can be directed to the peering connection instead of the public internet!

Step 8 - Analyze flow logs

In this step, we are tracking the nework data that's been collected on our VPCs, and then analyse that data to extract insights.

Connectivity troubleshooting

My first ping test between my EC2 instances had no replies, which means ICMP traffic would be blocked by security group/network ACLs; or may our traffic is being routed to a wrong path.



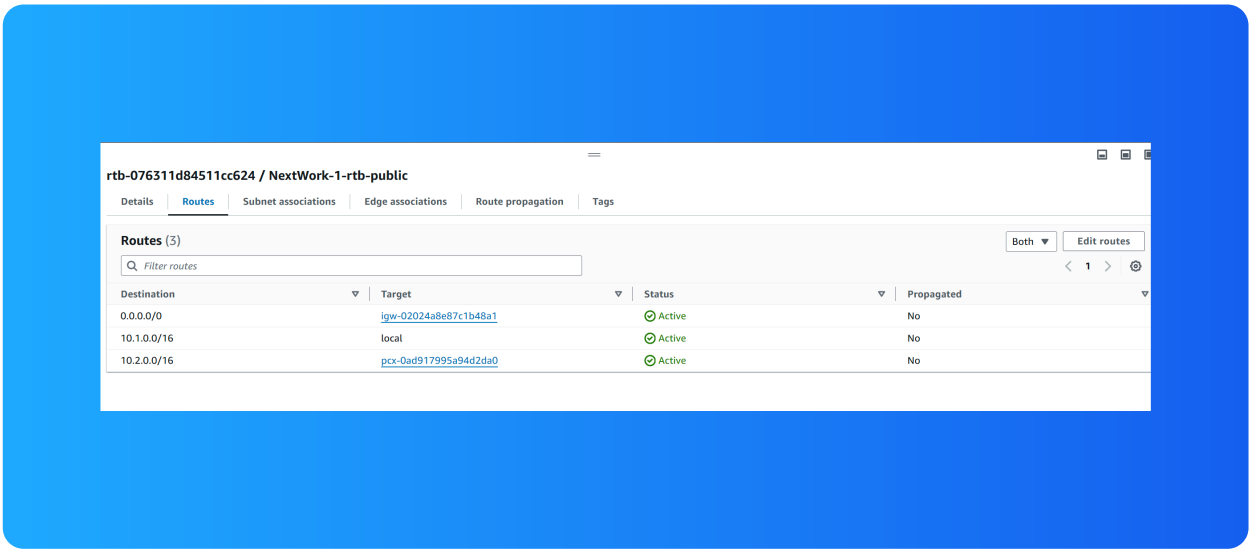
'I could receive ping replies if I ran the ping test using the other instance's public IP address, which means our second instance is actually allowing ICMP and SSH traffic.

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 route tables that directs traffic from one VPC to another.

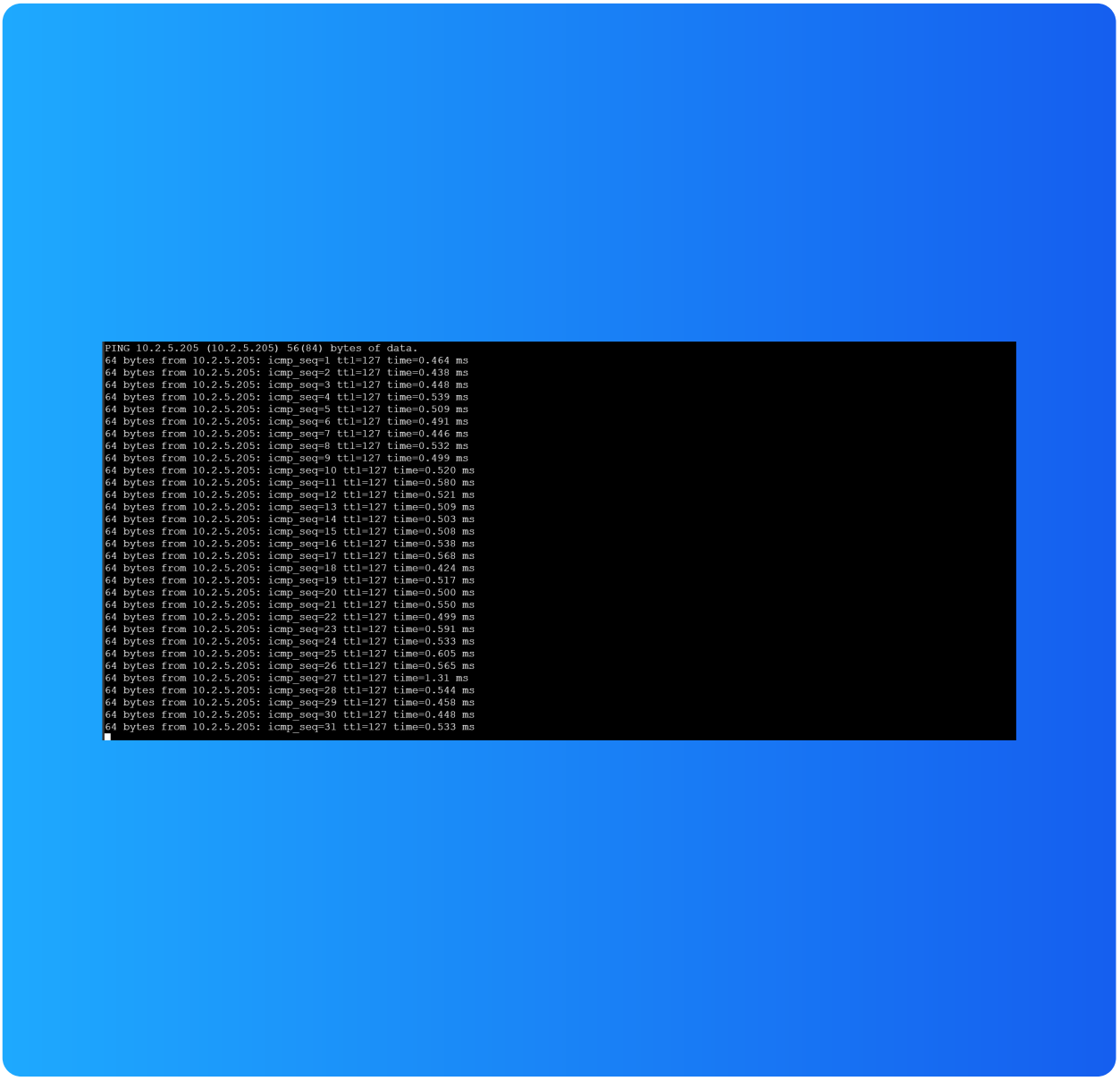
To solve this, I set up a peering connection between my VPCs

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



Connectivity troubleshooting

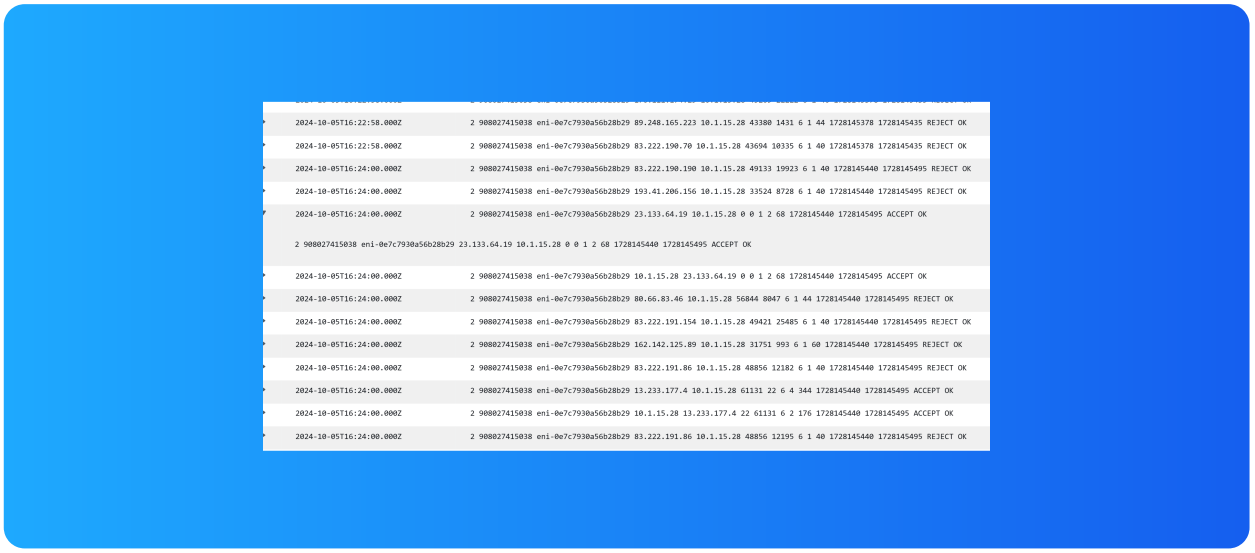
I received ping replies from Instance 2's private IP address! This means setting up the peering connection and then the route table solved the connectivity error of your VPCs traffic not being able to navigate from one VPC to another.



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.

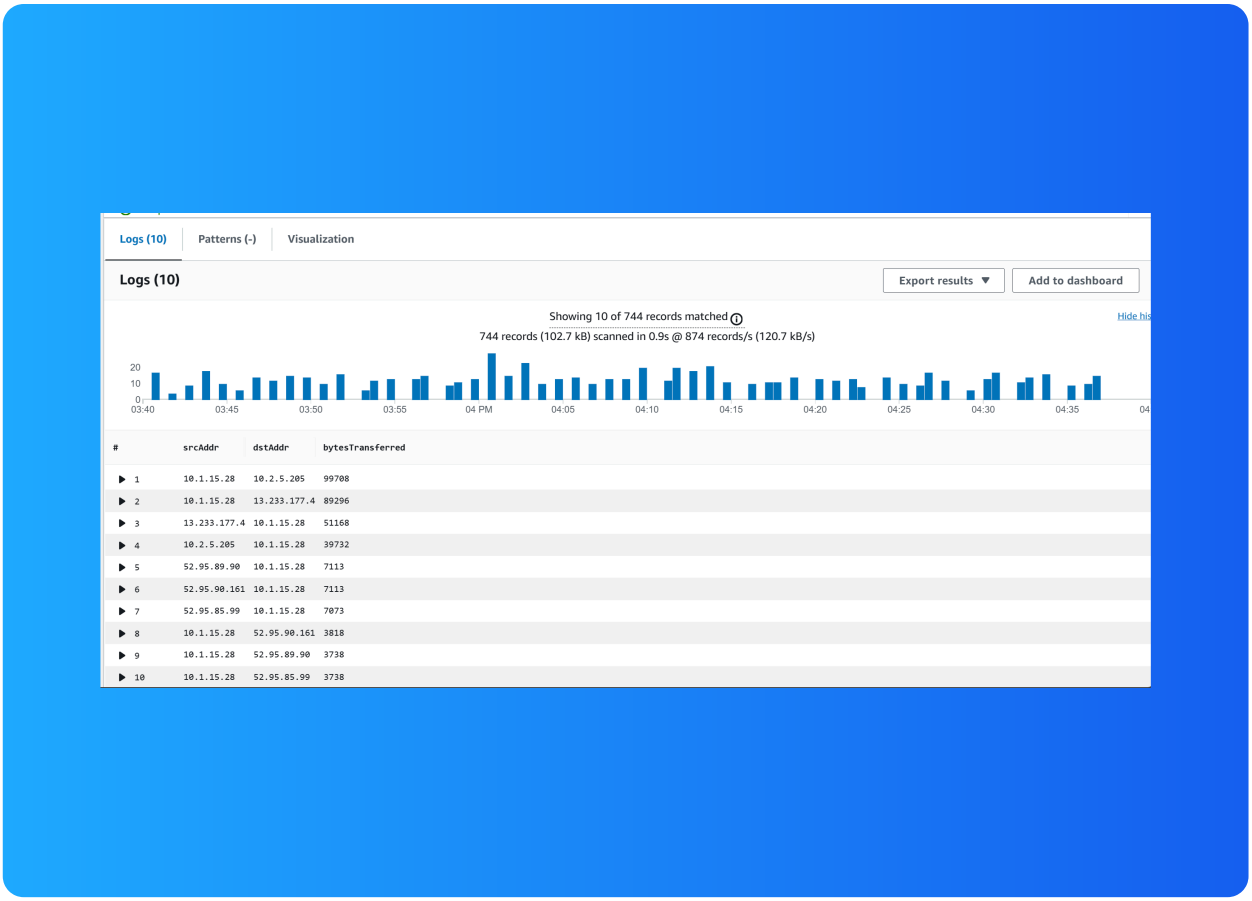
For example, the flow log I've captured tells us that traffic went from 23.133.64.19 to 10.1.15.28. we can also extract that the traffic was accepted by the security groups,network ACLs of my VPC.



Logs Insights

Logs Insights is a special tool within Amazon CoudWatch 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 analyzes the flow logs clollected on EC2 Instance 1, and return the top 10 pairs of IP addressess based on the amount of data transferred between them!



Everyone should be in a job they love.

Check out nextwork.org for more projects