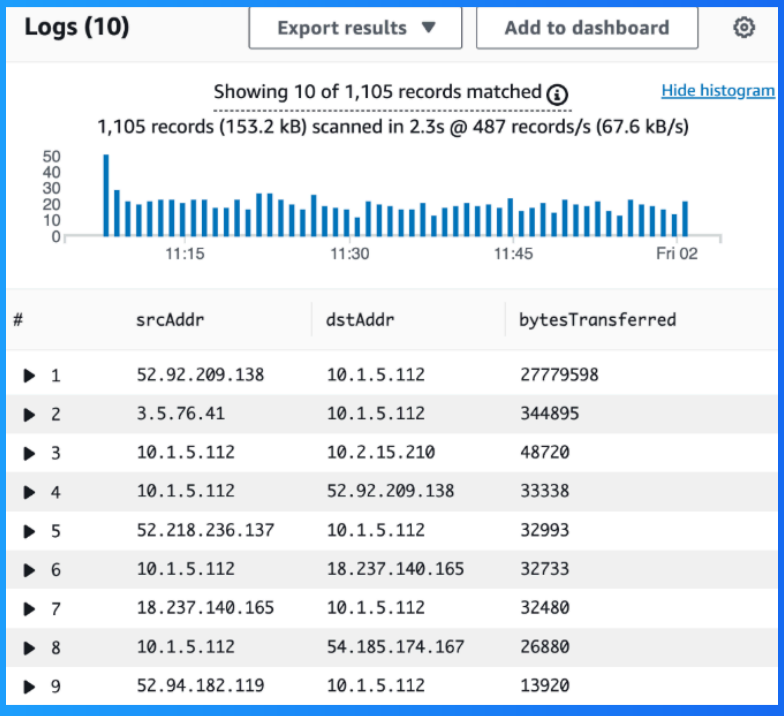
NextWork.org

VPC Monitoring with Flow Logs

SA samahae1530@gmail.com



#	srcAddr	dstAddr	bytesTransferred
▶ 1	52.92.209.138	10.1.5.112	27779598
▶ 2	3.5.76.41	10.1.5.112	344895
▶ 3	10.1.5.112	10.2.15.210	48720
▶ 4	10.1.5.112	52.92.209.138	33338
▶ 5	52.218.236.137	10.1.5.112	32993
▶ 6	10.1.5.112	18.237.140.165	32733
▶ 7	18.237.140.165	10.1.5.112	32480
▶ 8	10.1.5.112	54.185.174.167	26880
▶ 9	52.94.182.119	10.1.5.112	13920

SA
samahae1530@gmail.com
NextWork Student
NextWork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) is a service that lets the user to create their own private network inside the AWS cloud. It's like having our own secure area where you can run your applications, store data, and control who can access it.

How I used Amazon VPC in this project

first learnt to troubleshoot VPC peering connecticity issues. secondly learnt monitor network traffic using VPC flow logs.

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

log insights have a lot of built in queries that gives us many options on how we like to analyze network traffic.

This project took me...

this project took me 2 hours and half an hour for documentation.

SA
samahae1530@gmail.com
NextWork Student
NextWork.org

In the first part of my project...

Step 1 - Set up VPCs

In this step, I set up two VPCs from scratch within minutes. Network monitoring can also be performed using a single VPC and utilizes VPC peering for communication.

Step 2 - Launch EC2 instances

In this step, two EC2 instances are launched, one in each VPC. These instances are essential for the next stages of the project, as they will generate traffic that VPC Flow Logs will monitor.

Step 3 - Set up Logs

settting up vpc flow logs to start monitoring traffic also setting up storage space for flow logs.

Step 4 - Set IAM permissions for Logs

providing vpc flow logs with permissions to create logs and upload them into log group in cloudwatch.

SA
samahae1530@gmail.com
NextWork Student

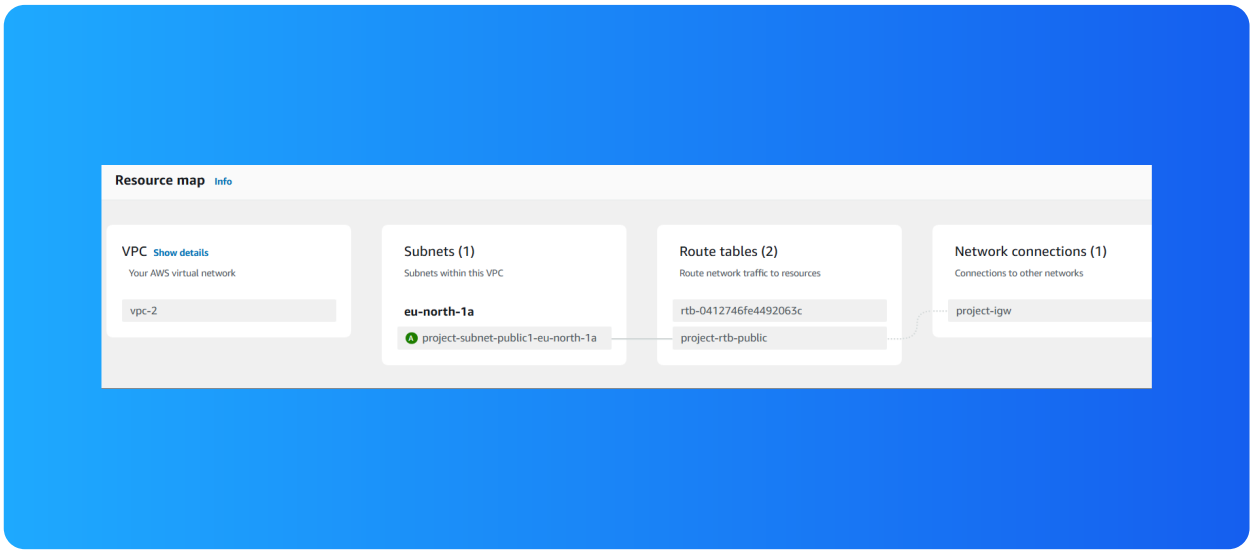
Multi-VPC Architecture

I started my project by launching two public subnets (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. They have to be unique because having overlapping CIDR blocks will cause routing/traffic issues down the line when traffic when traffic is needing to go from one vpc to another.

I also launched EC2 instances in each subnet

EC2 instances security groups allow SSH and ICMP type traffic. This is because EC2 instance connect will need to access EC2 instance using SSH traffic and need to allow ICMP traffic for connectivity tests later.

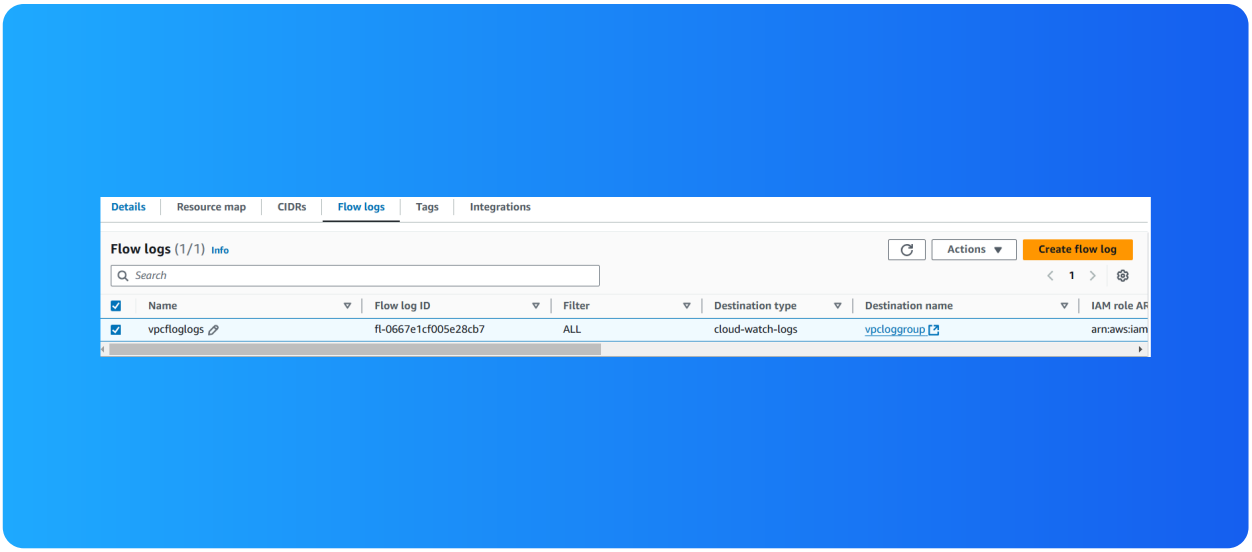


SA
samahae1530@gmail.com
NextWork Student

Logs

logs are records of events or activities that occur within applications or AWS services. They help to understand what's happening in the environment, troubleshoot issues, and monitor performance.

log groups are a way to organize and manage logs in Amazon CloudWatch Logs. A log group is essentially a container for related logs, making it easier to manage and analyze them together.



SA
samahae1530@gmail.com
NextWork Student

IAM Policy and Roles

I created an IAM policy because so that i can define a rule that allows policy holders e.g. vpc flow log 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 will be necessary to give vpc flow logs the acess it needs to record and upload logs

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

SA
samahae1530@gmail.com
NextWork Student

In the second part of my project...

Step 5 - Ping testing and troubleshooting

In this step, creating a network traffic this becomes important when communicating about cloudwork or cloud networking.

Step 6 - Set up a peering connection

setting up peering connection so that vpc 1 and 2 can communicate directly to each other.

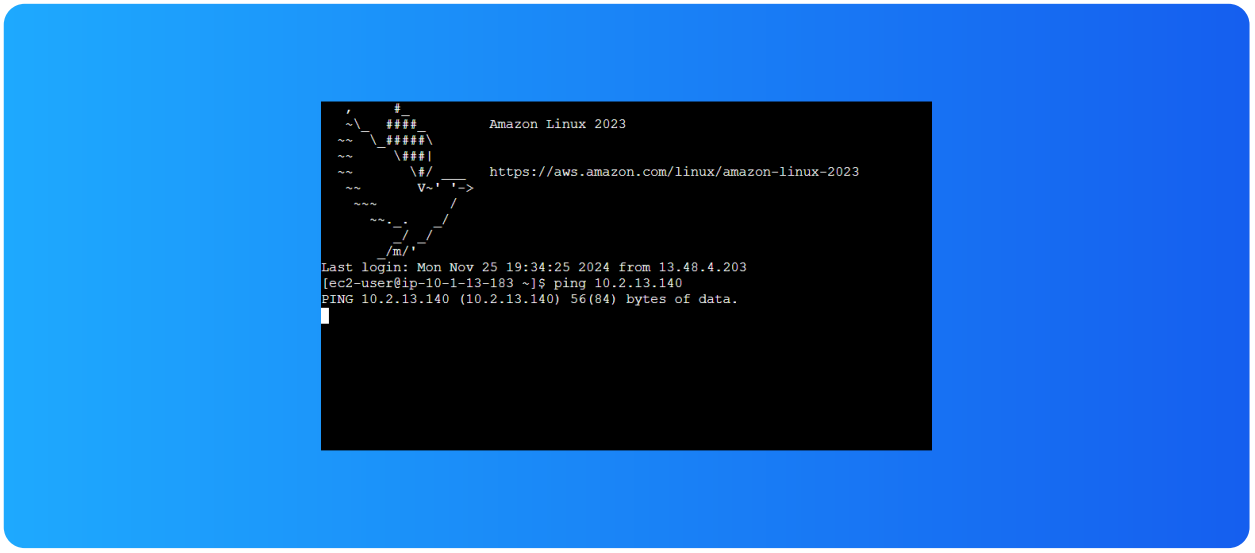
Step 7 - Analyze flow logs

In this step, tracking the network data that;s been collected from vpc and then analyze that data to extract insights.

SA
samahae1530@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 security group/network ACLS or maybe traffic is 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 allowing ICMP traffic.

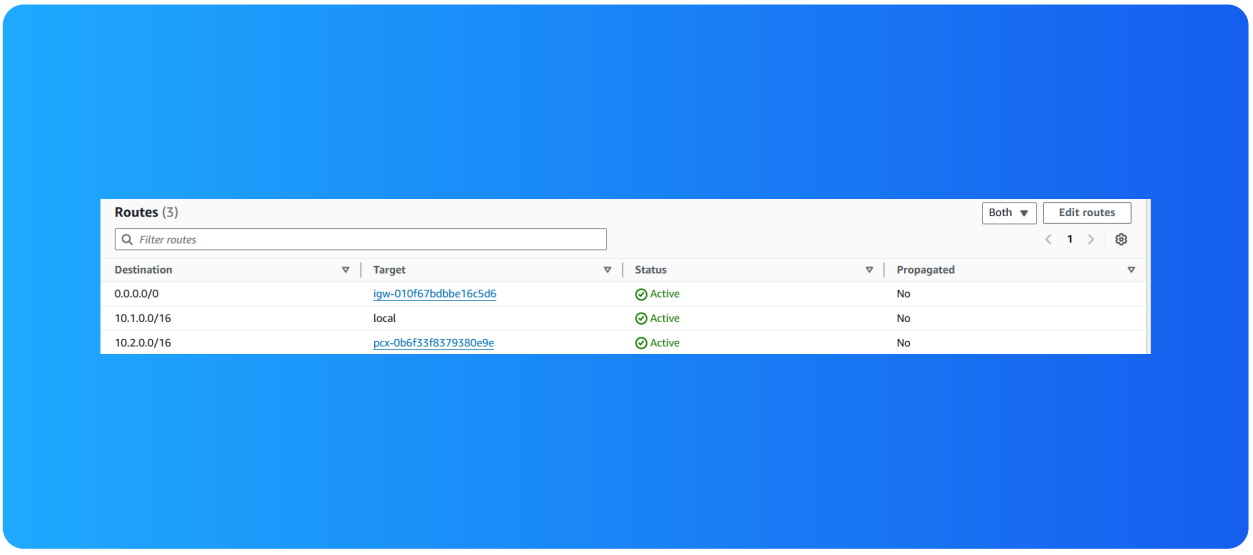
SA
samahae1530@gmail.com
NextWork Student

Connectivity troubleshooting

Looking at VPC 1's route table, I identified that the ping test with Instance 2's private address failed because the vpc doesnt have route in vpc's route table that directs traffic from one vpc to another.

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

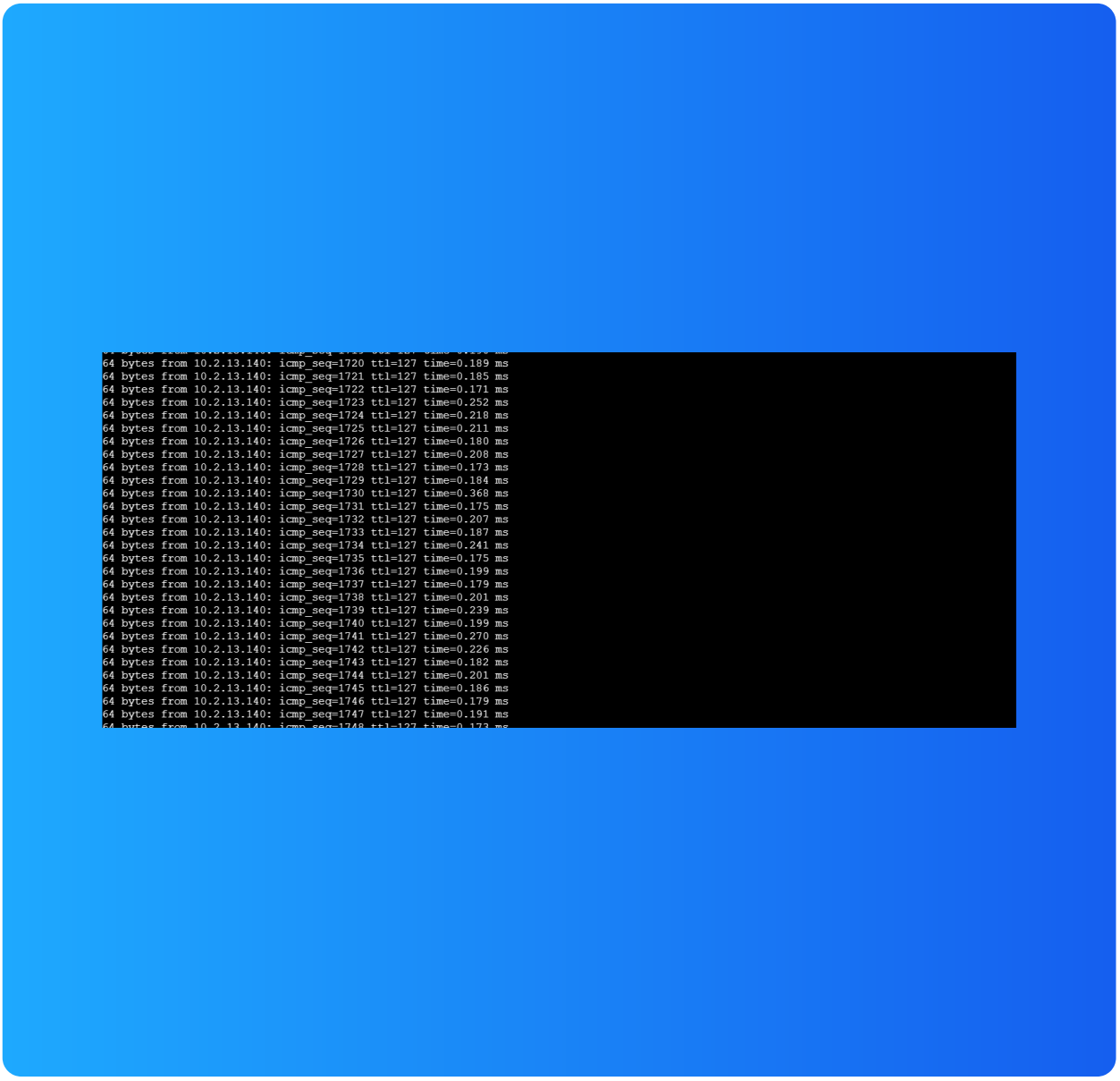
updated both VPCs' route tables so that traffic from one of the vpc's and heading to other vpc's ipv4 address can get directed to go through peering connection instead of the public internet.



SA
samahae1530@gmail.com
NextWork Student

Connectivity troubleshooting

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

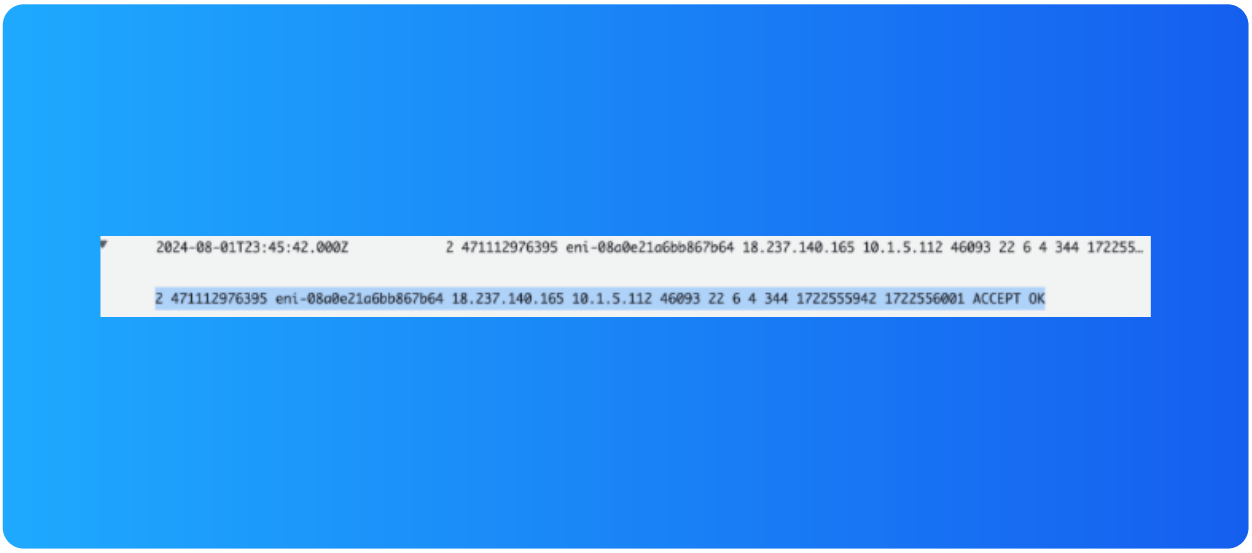


SA
samahae1530@gmail.com
NextWork Student

Analyzing flow logs

Flow logs tell us about the source and destination of 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 the traffic went from 18.237.140.165 to 10.1.5.112.

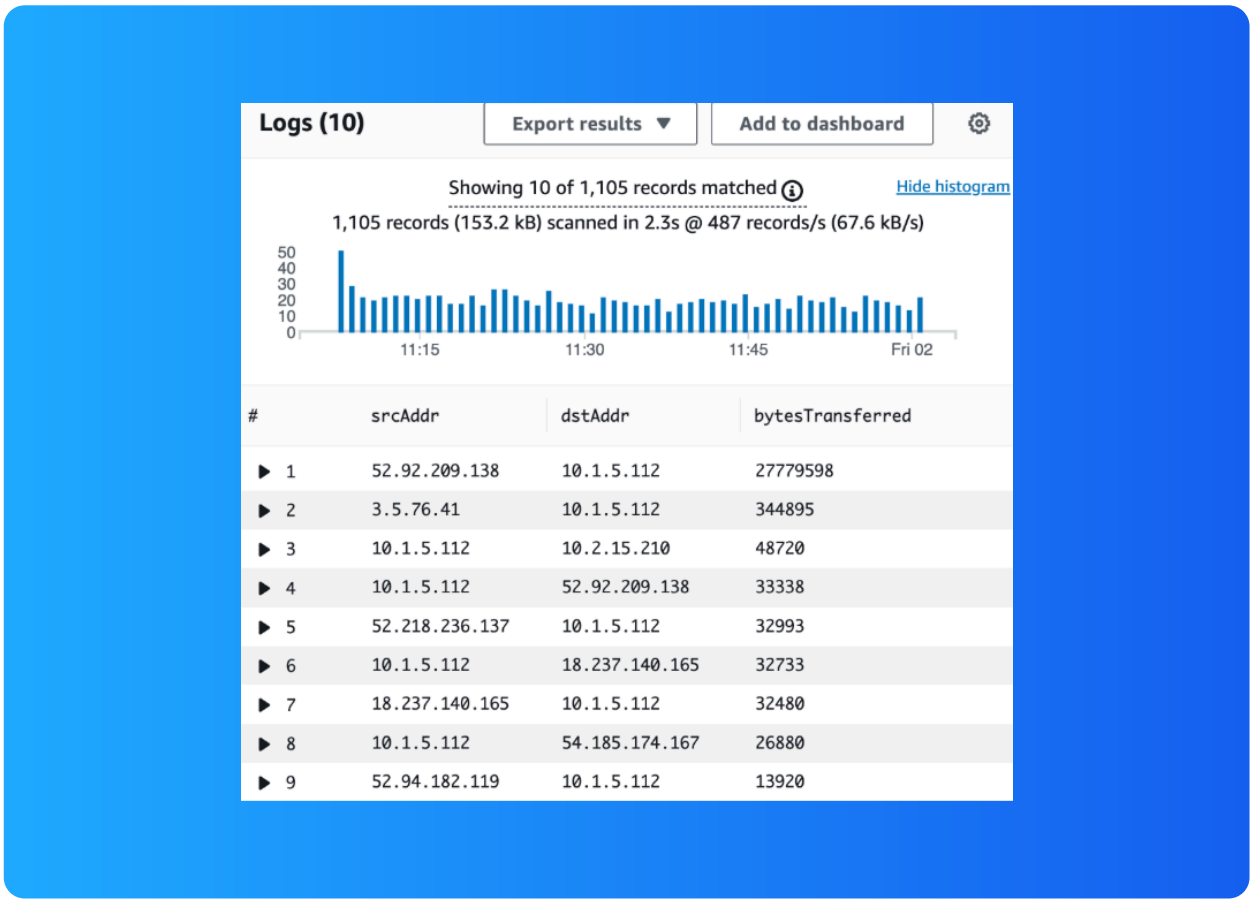


SA
samahae1530@gmail.com
NextWork Student

Logs Insights

logs insight is a special tool within amazon cloudwatch that help us with analysing logs and creating visual graphs and chart through queries.

I ran the query the top 10 byte transfers by source and destination IP addresses. This query analyzes the flow logs collected on EC2 instance 1.



#	srcAddr	dstAddr	bytesTransferred
1	52.92.209.138	10.1.5.112	27779598
2	3.5.76.41	10.1.5.112	344895
3	10.1.5.112	10.2.15.210	48720
4	10.1.5.112	52.92.209.138	33338
5	52.218.236.137	10.1.5.112	32993
6	10.1.5.112	18.237.140.165	32733
7	18.237.140.165	10.1.5.112	32480
8	10.1.5.112	54.185.174.167	26880
9	52.94.182.119	10.1.5.112	13920

Everyone should be in a job they love.

Check out nextwork.org for more projects