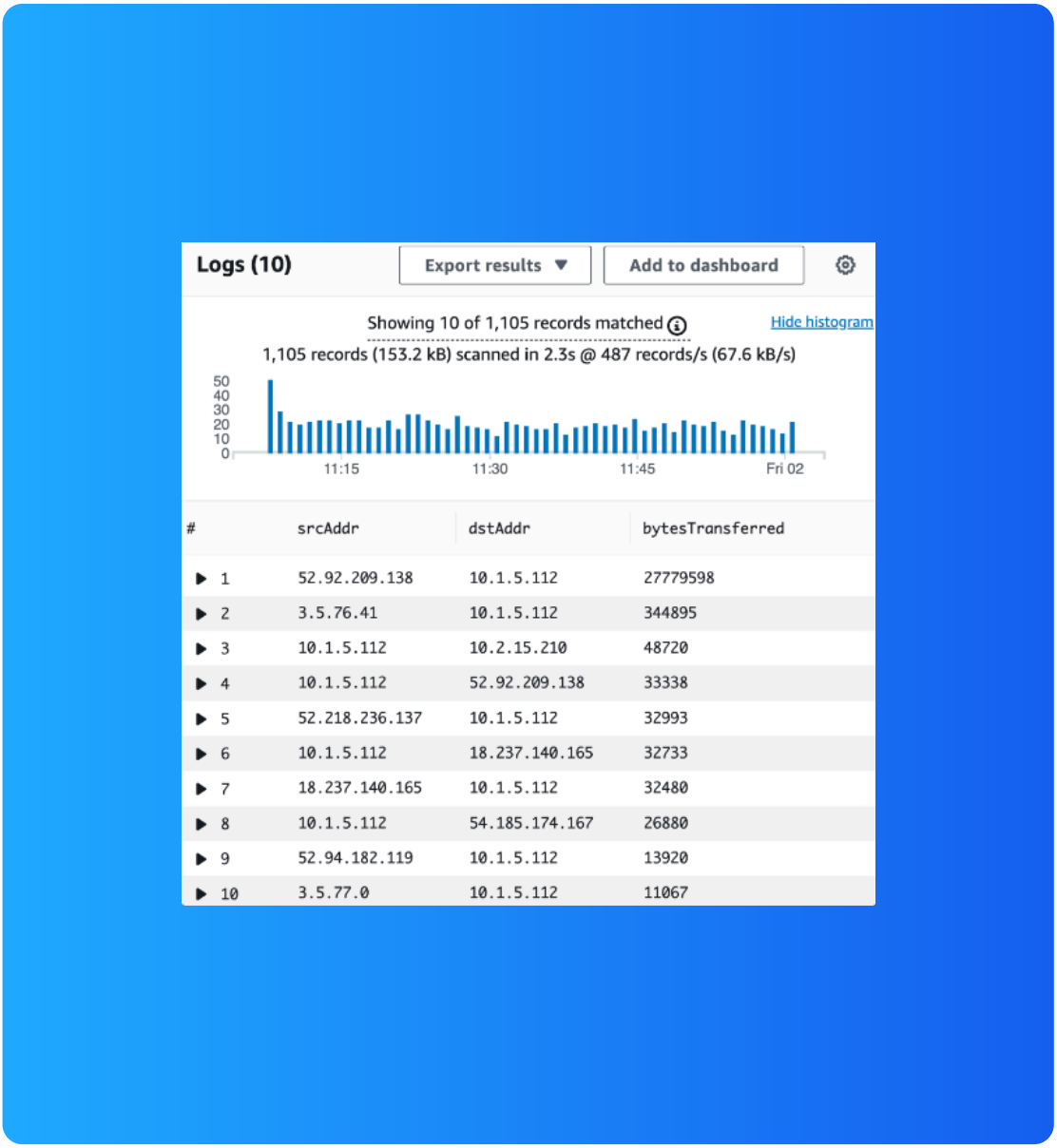
NextWork.org

VPC Monitoring with Flow Logs

NI nikhil7_94@hotmail.com



NI
nikhil7_94@hotmail.com
NextWork Student
NextWork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a private isolated network in the cloud where you can securely run resources like servers and databases. It's useful because it gives full control over network settings, security and connectivity to the internet.

How I used Amazon VPC in this project

Today I used Amazon VPC to monitor the VPC with flow logs.

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

One thing I didnt expect was you can get different queries from the flow logs.

This project took me...

I took around 2 hours with this project.

NI
nikhil7_94@hotmail.com
NextWork Student
NextWork.org

In the first part of my project...

Step 1 - Set up VPCs

Im about to create two VPCs from scratch.

Step 2 - Launch EC2 instances

Now I will create an EC2 instance in each VPC.

Step 3 - Set up Logs

In this step Im going to set up a way to track all inbound and outbound network traffic and set up a space that stores all of these records.

Step 4 - Set IAM permissions for Logs

In this step I will give VPC Flow Logs the permission to write logs and send them to CloudWatch and finish setting up your subnet's flow log.

NI
nikhil7_94@hotmail.com
NextWork Student

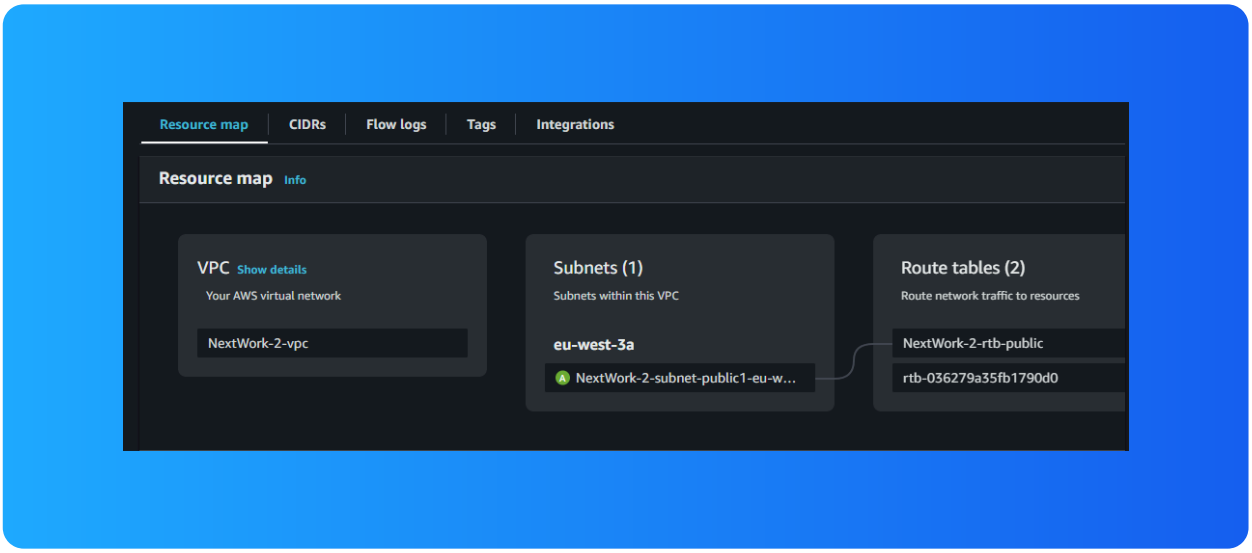
Multi-VPC Architecture

I started my project by launching 2 VPCs creating 1 public subnet in each VPC and none private subnet.

The CIDR blocks for VPCs 1 and 2 are different. They have to be unique because they cant overlap.

I also launched EC2 instances in each subnet

My EC2 instances' security groups allow botch EC2 to communicate. This is because I allowed ICMP traffic from all IP addresses.



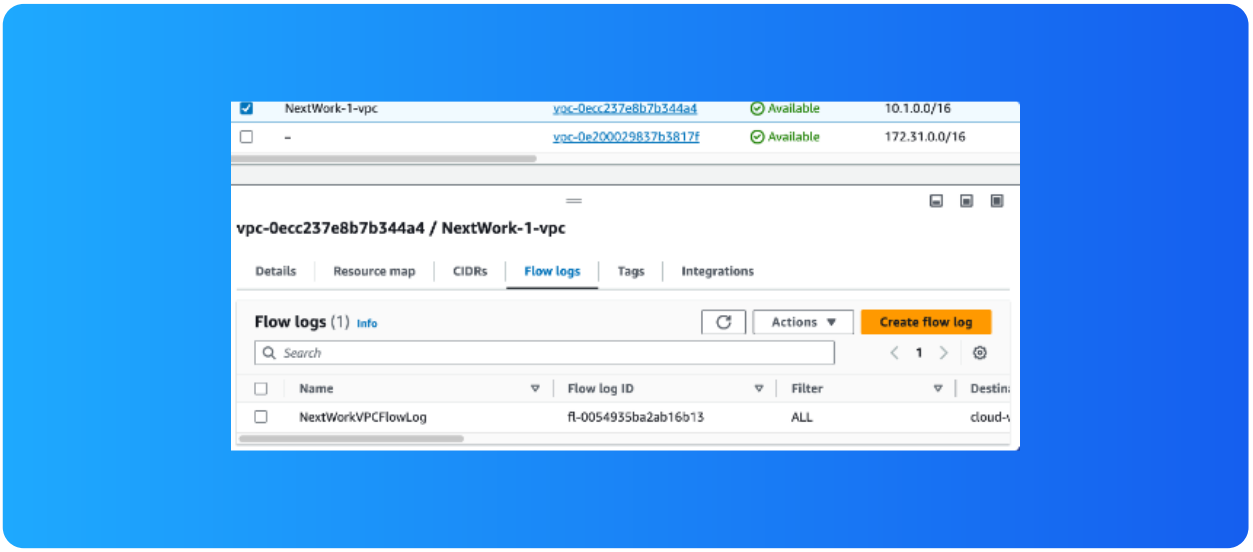
NI
nikhil7_94@hotmail.com
NextWork Student

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 the location where all the logs are stored.

I also set up a flow log for VPC 1



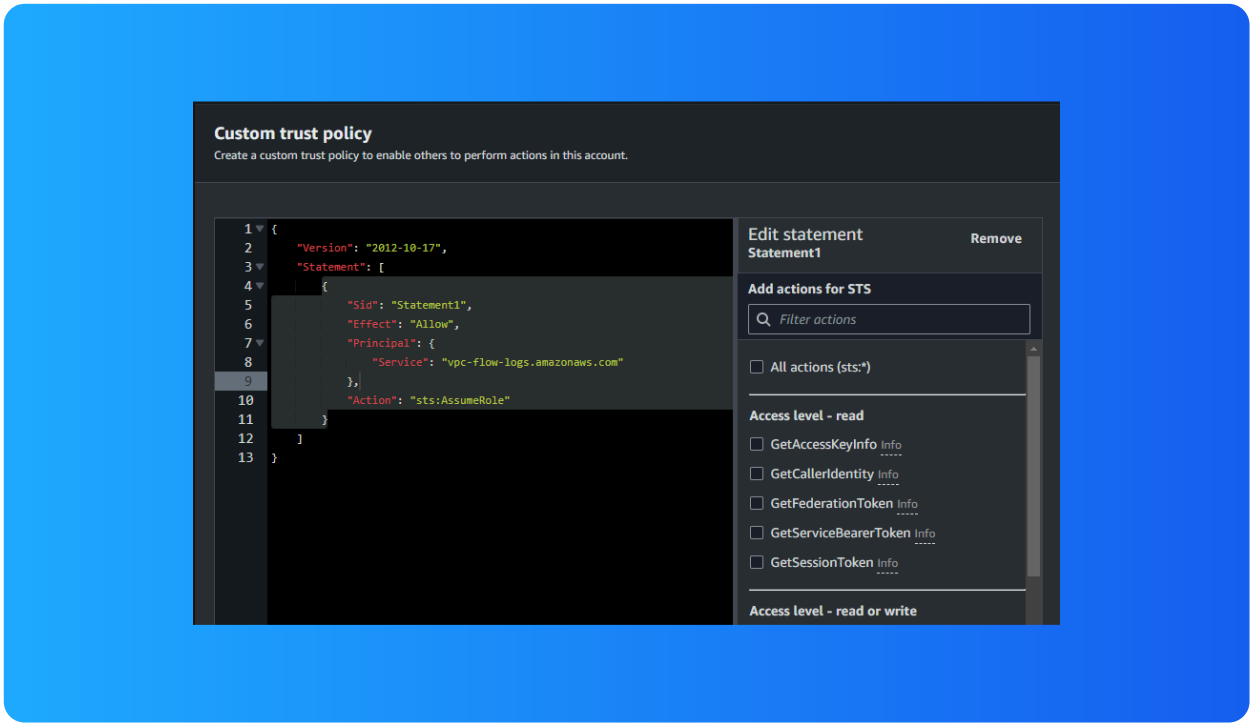
NI
nikhil7_94@hotmail.com
NextWork Student

IAM Policy and Roles

I created an IAM policy because VPC Flow Logs doesn't have the permission to write logs and send them to CloudWatch. I need an IAM policy with this permission.

I also created an IAM role because I cant assign the policy without a role.

A custom trust policy is a specific type of policy.



NI
nikhil7_94@hotmail.com
NextWork Student
NextWork.org

In the second part of my project...

Step 5 - Ping testing and troubleshooting

In this step I will get Instance 1 to send test messages to Instance 2.

Step 6 - Set up a peering connection

Now I will set up a connection link between your VPCs.

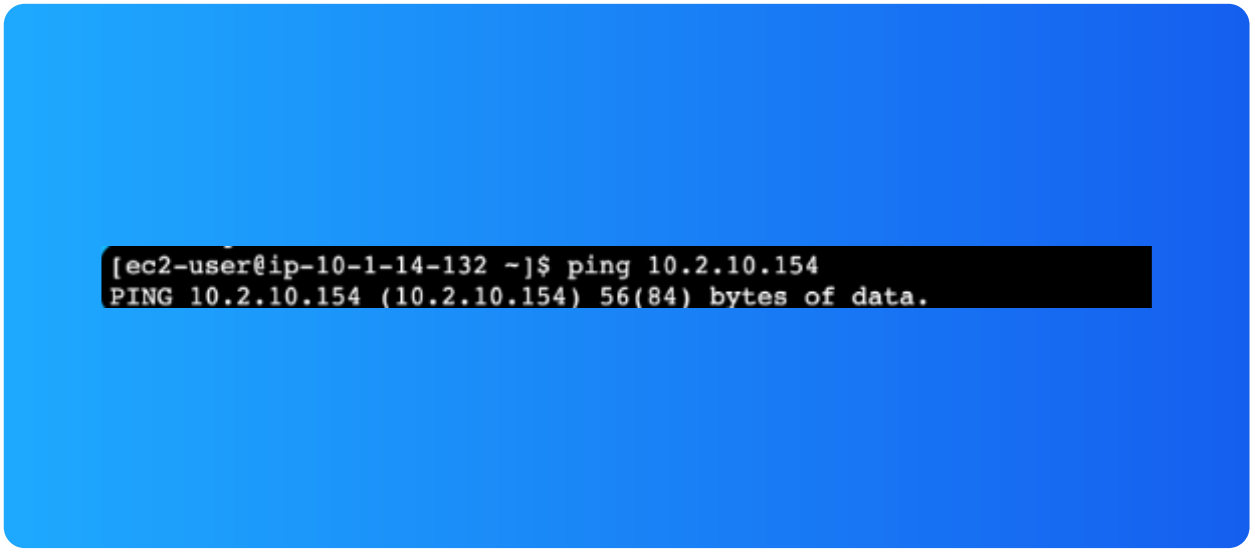
Step 7 - Analyze flow logs

In this step I will review the flow logs recorded about VPC 1's public subnet and analyse the flow logs to get insights.

NI
nikhil7_94@hotmail.com
NextWork Student

Connectivity troubleshooting

My first ping test between my EC2 instances had no replies, which means there is still no communication between my EC2 instances. There is an issue with some configuration.



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.

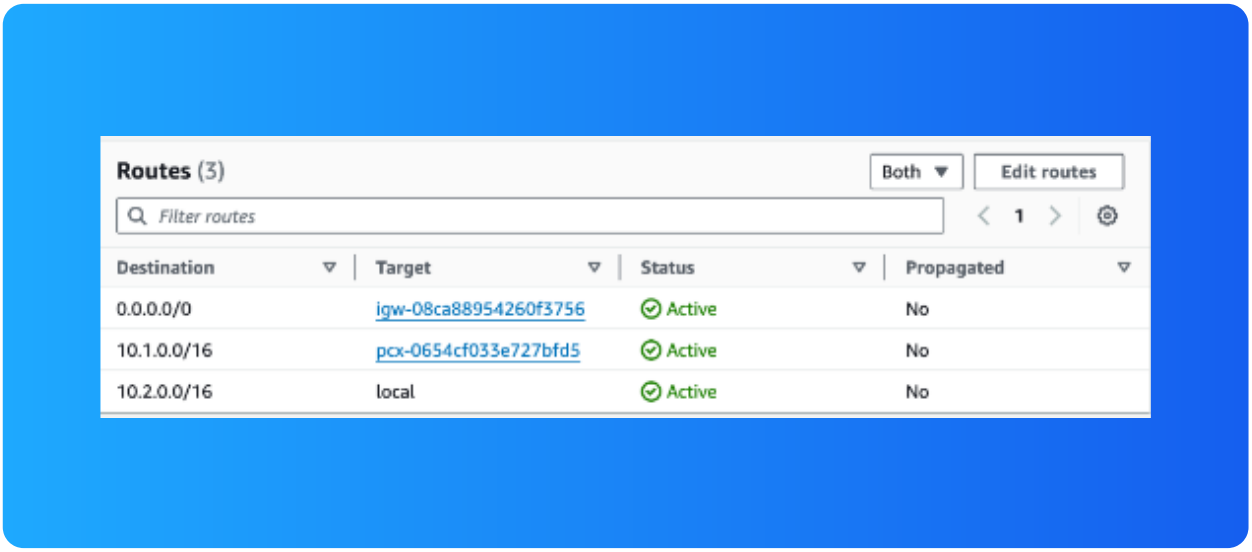
NI
nikhil7_94@hotmail.com
NextWork Student

Connectivity troubleshooting

Looking at VPC 1's route table, I identified that the ping test with Instance 2's private address failed because I didnt have set up a VPC peering connection.

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

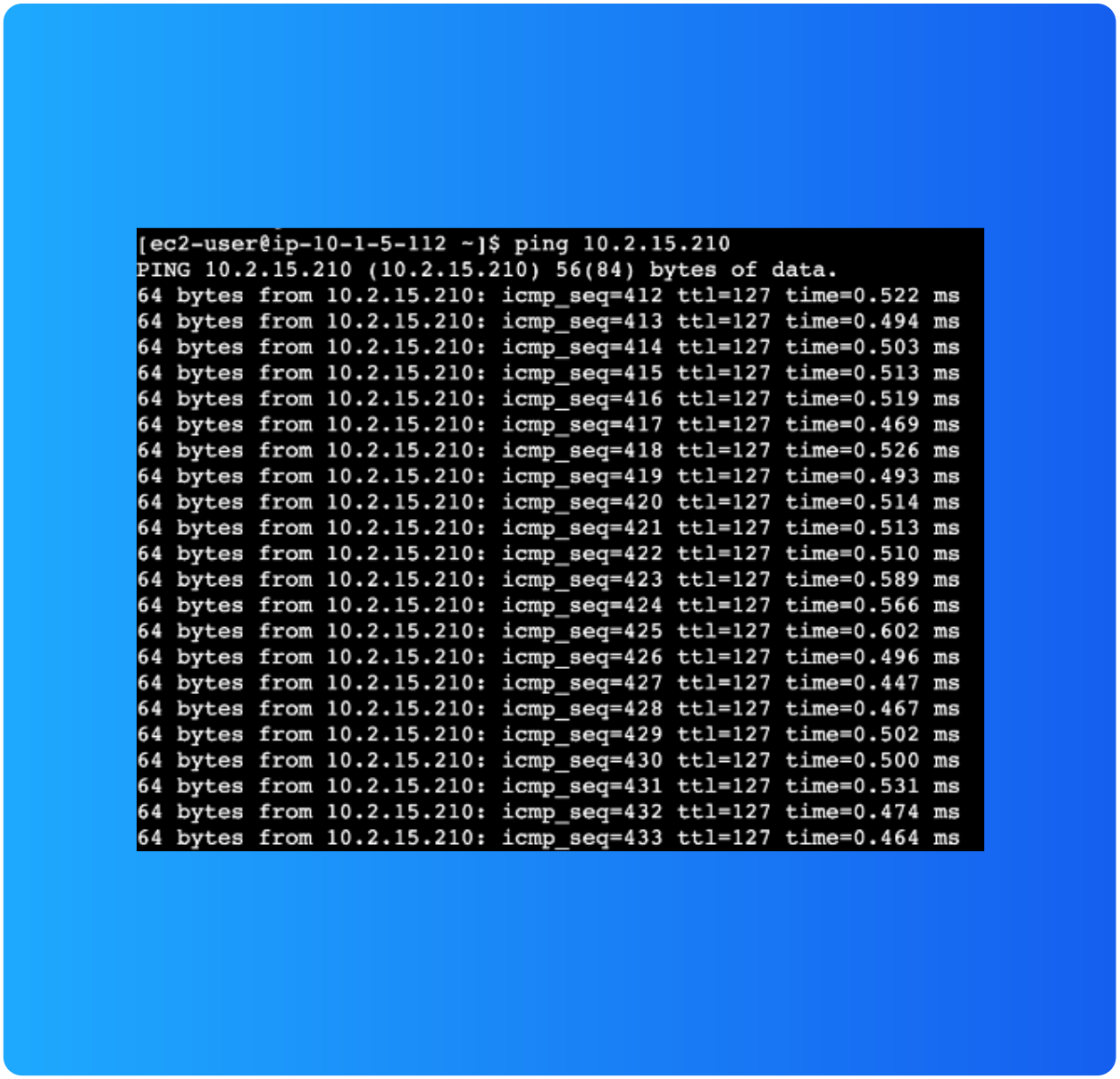
I also updated both VPCs' route tables so that The Destination is the CIDR block 10.1.0.0/16.



NI
nikhil7_94@hotmail.com
NextWork Student

Connectivity troubleshooting

I received ping replies from Instance 2's private IP address! This means now its communicating correctly.

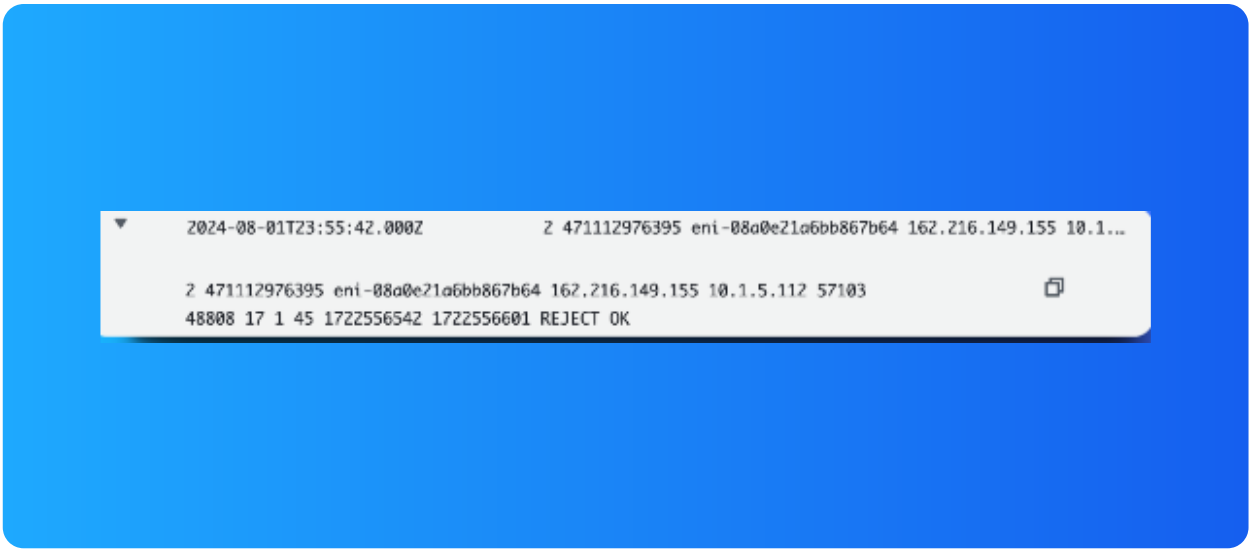


NI
nikhil7_94@hotmail.com
NextWork Student

Analyzing flow logs

Flow logs tell us about network traffic details to and from resources in a VPC including IP addresses, traffic direction and packet information.

For example, the flow log I've captured tells us this flow log shows that 344 bytes of data were sent successfully from the IP address 18.237.140.165 to 10.1.5.112 using TCP protocol on port 22 with 4 packets sent and the traffic was allowed.

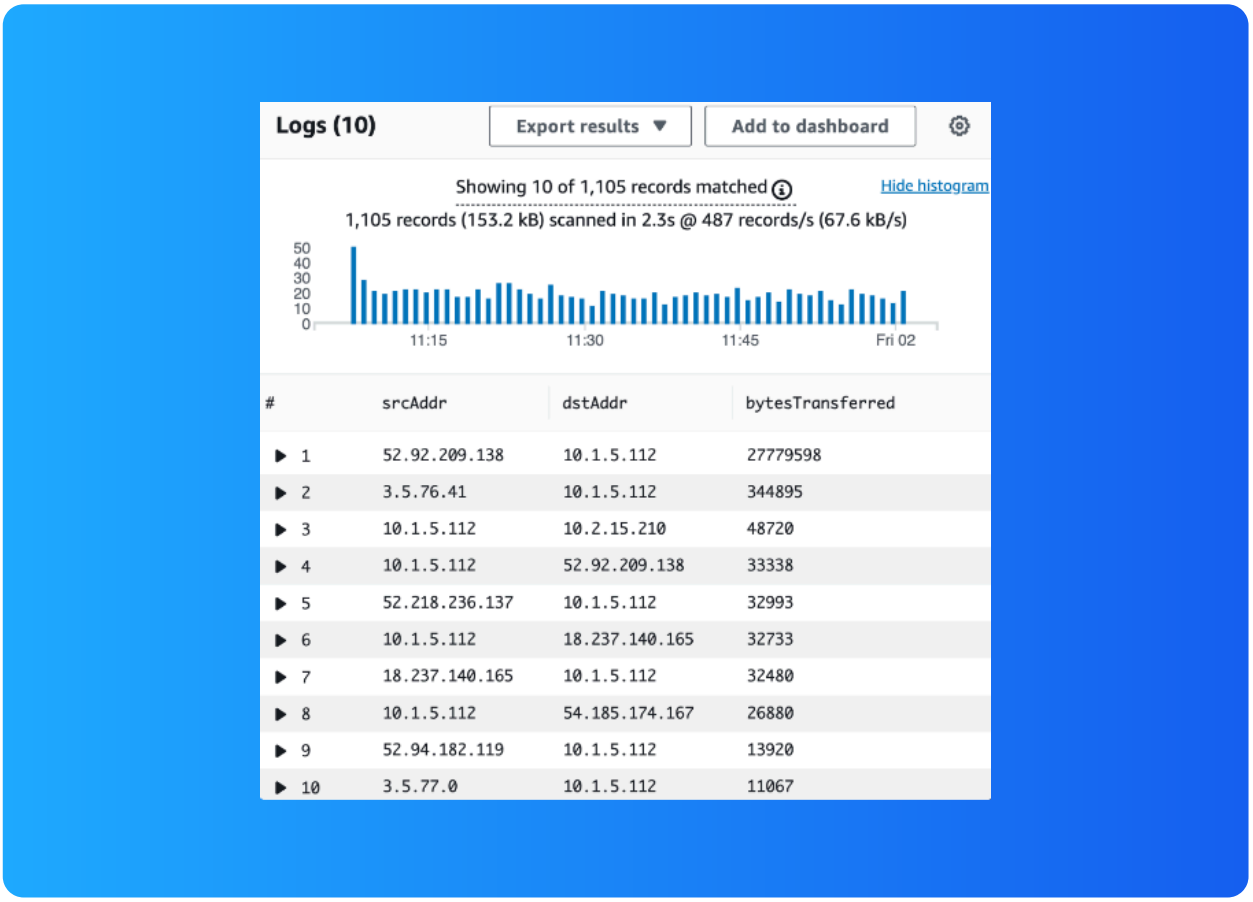


NI
nikhil7_94@hotmail.com
NextWork Student

Logs Insights

Logs Insights is a CloudWatch feature that analyzes your logs.

I ran the query "Top 10 byte transfers by source and destination IP addresses". This query analyzes is all about discovering the top 10 biggest data transfers between IP addresses in my network.



#	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
▶ 10	3.5.77.0	10.1.5.112	11067

Everyone should be in a job they love.

Check out nextwork.org for more projects