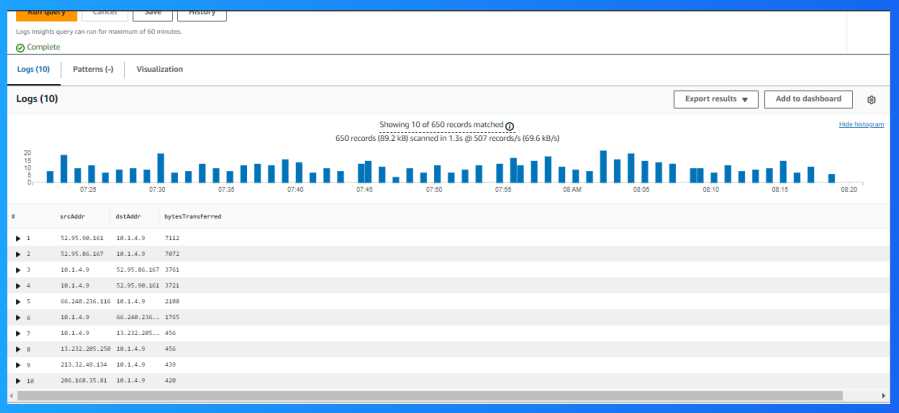
NextWork.org

VPC Monitoring with Flow Logs

Roshan Thomas



Roshan Thomas
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) allows you to create an isolated network within AWS, providing control over network settings, security, and access. It's useful for securely hosting applications, managing traffic, and integrating on-premise network

How I used Amazon VPC in this project

I used VPC to create a secure network for my EC2 instances. I set up subnets, configured routing, and used security groups to control traffic. VPC Flow Logs helped me monitor network activity and analyze data flow.

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

One thing I didn't expect was the complexity of configuring network ACLs and security groups to allow ICMP traffic for ping tests. This highlighted the importance of precise security settings for network connectivity.

This project took me...

2 Hours and 30 Mins

Roshan Thomas
NextWork Student

NextWork.org

In the first part of my project...

Step 1 - Set up VPCs

I'm going to create two VPCs to practice setting up and configuring virtual private networks in AWS. This will also help me review concepts from previous projects and prepare for more complex network architectures.

Step 2 - Launch EC2 instances

I launched one EC2 instance in each VPC to test the VPC peering connection and prepare for future network monitoring.

Step 3 - Set up Logs

I'll set up VPC Flow Logs to track network traffic and store the data. This will help me analyze data flow, identify threats, and optimize network performance.

Step 4 - Set IAM permissions for Logs

I'm going to create an IAM role and policy to grant VPC Flow Logs the necessary permissions to write logs and send them to CloudWatch. This will enable me to effectively monitor and analyze network traffic within my VPCs.

Roshan Thomas
NextWork Student

NextWork.org

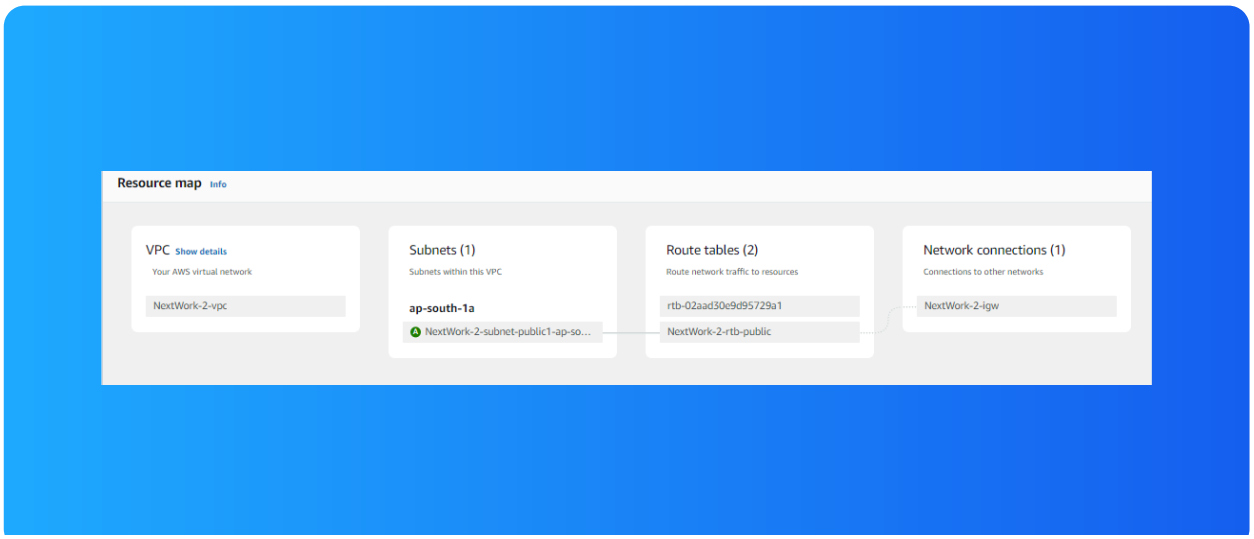
Multi-VPC Architecture

I started my project by launching two VPCs. Each VPC has two subnets: a public subnet and a private subnet. This setup allows for both internet connectivity and isolation of resources within the private subnet.

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 to ensure that the IP addresses within each VPC do not overlap and avoid conflicts when the VPCs are peered or connected to other networks.

I also launched EC2 instances in each subnet

My EC2 instances' security groups allow inbound ICMP traffic from all IP addresses (0.0.0.0/0). This is because ICMP messages are used for ping tests, which are essential for verifying network connectivity between the instances and other resources.



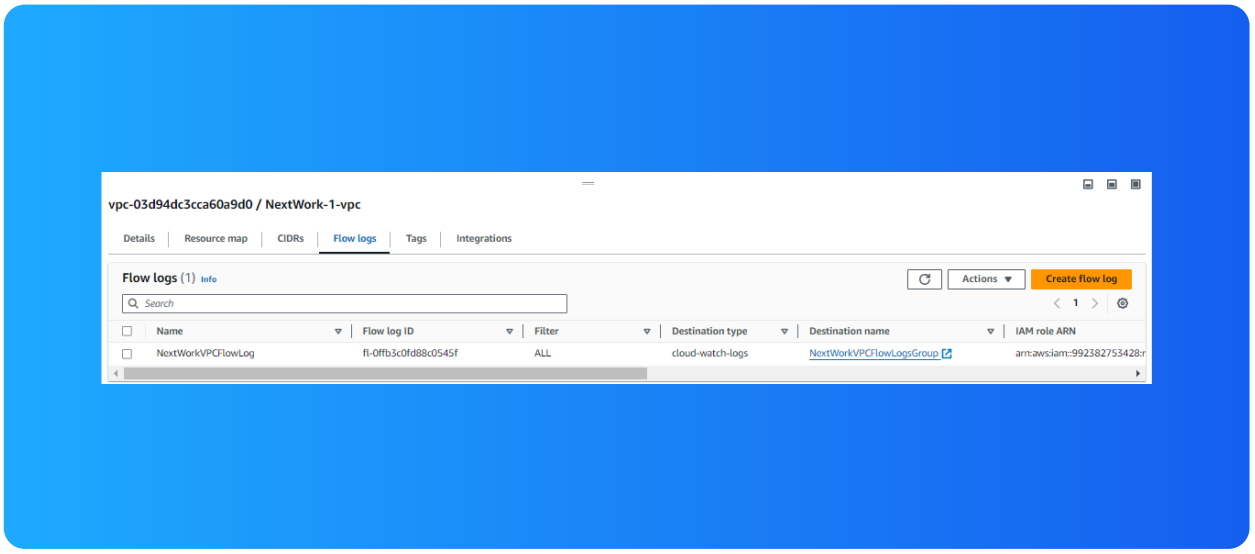
Roshan Thomas
NextWork Student

Logs

Logs are records of events or activities that occur within a system. They provide valuable information about a system's behavior, including errors, warnings, and performance metrics.

Log groups are containers that organize and store log streams. They allow you to group related logs together for easier management and analysis.

I also set up a flow log for VPC 1



Roshan Thomas
NextWork Student

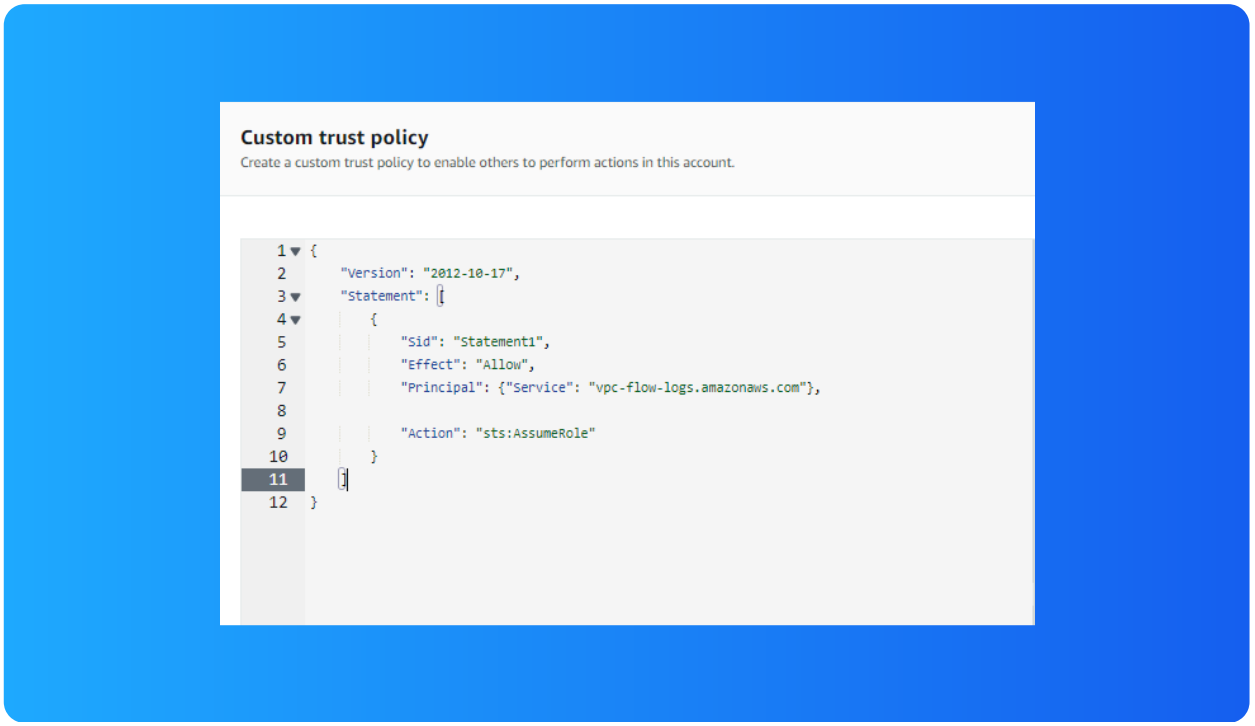
NextWork.org

IAM Policy and Roles

I created an IAM policy to grant VPC Flow Logs the necessary permissions to write logs and send them to CloudWatch. This allows me to effectively monitor and analyze network traffic within my VPCs.

I also created an IAM role because it provides a secure way to grant VPC Flow Logs the necessary permissions to write logs and send them to CloudWatch. This helps prevent unauthorized access to sensitive log data.

A custom trust policy is a JSON document that specifies which entities are allowed to assume an IAM role. It grants permissions to specific AWS services or other principals to use the role's associated permissions.



Roshan Thomas
NextWork Student

In the second part of my project...

Step 5 - Ping testing and troubleshooting

I'll use EC2 Instance Connect to access Instance 1 and send test messages to Instance 2 to generate network traffic and test the VPC peering connection.

Step 6 - Set up a peering connection

I'm going to set up a peering connection between my two VPCs. This will create a link between the networks, allowing resources in each VPC to communicate with each other.

Step 7 - Update VPC route tables

Step 8 - Analyze flow logs

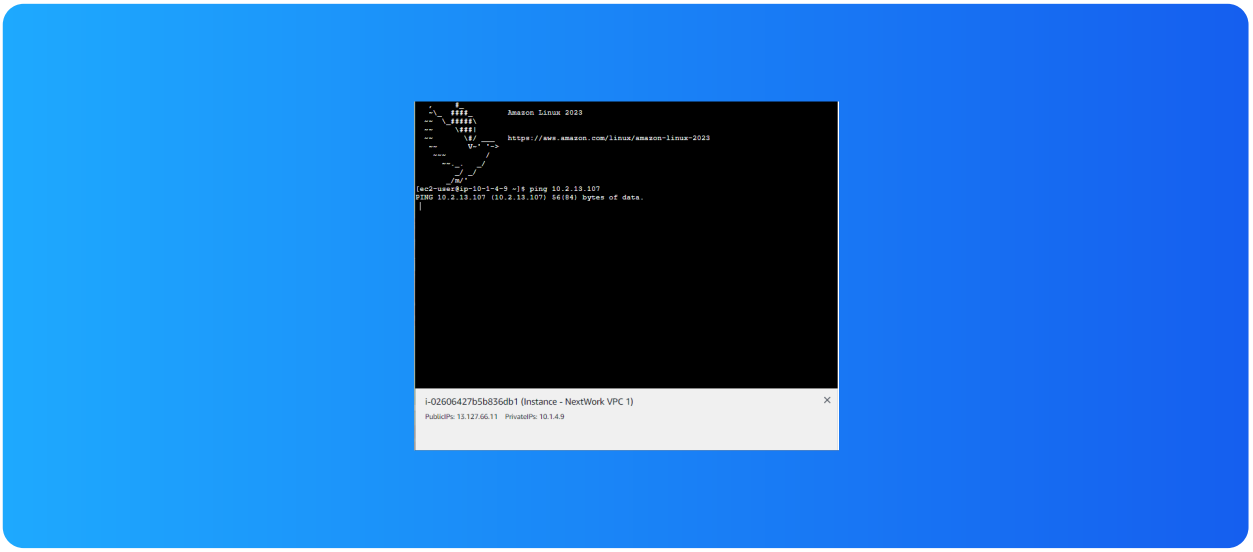
I'm going to review the flow logs recorded for VPC 1's public subnet to analyze network traffic activity within that subnet. This will help me understand data flow patterns, identify security threats, and optimize network performance.

Roshan Thomas
NextWork Student

NextWork.org

Connectivity troubleshooting

My first ping test between my EC2 instances had no replies, which means there might be a problem with the connection between them. This could be due to blocked ICMP traffic or misconfigured network settings.



I could receive ping replies using the public IP address, indicating a successful private network peering connection. However, there might be an issue with security settings restricting ICMP traffic within the private subnet.

Roshan Thomas
NextWork Student

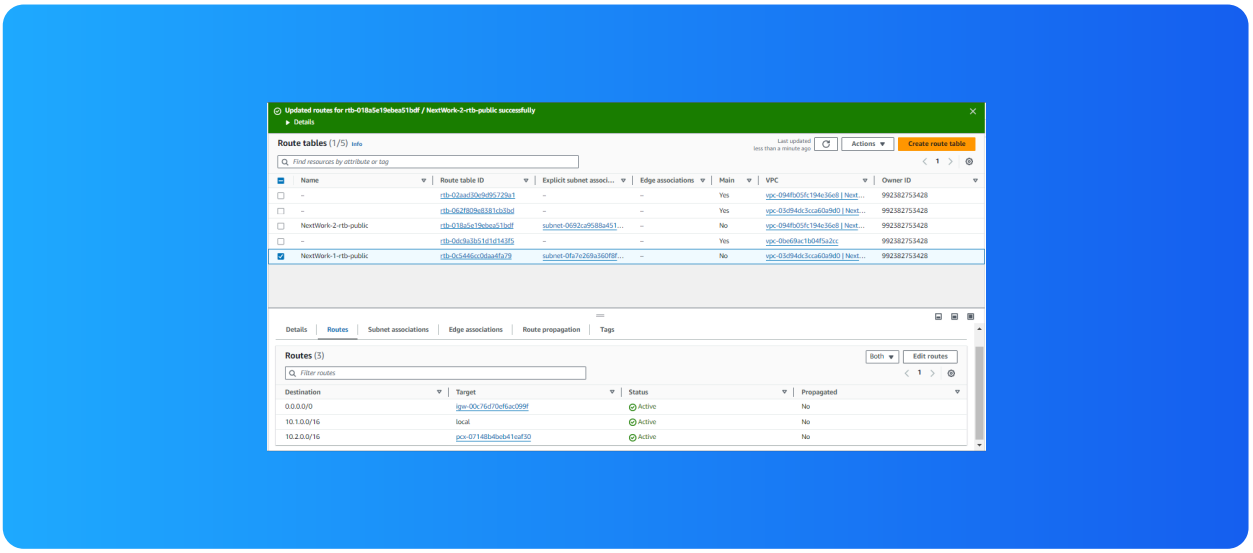
NextWork.org

Connectivity troubleshooting

Looking at VPC 1's route table, I identified that the ping test failed due to a missing route to VPC 2's private subnet. This indicates a misconfiguration in the routing settings.

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

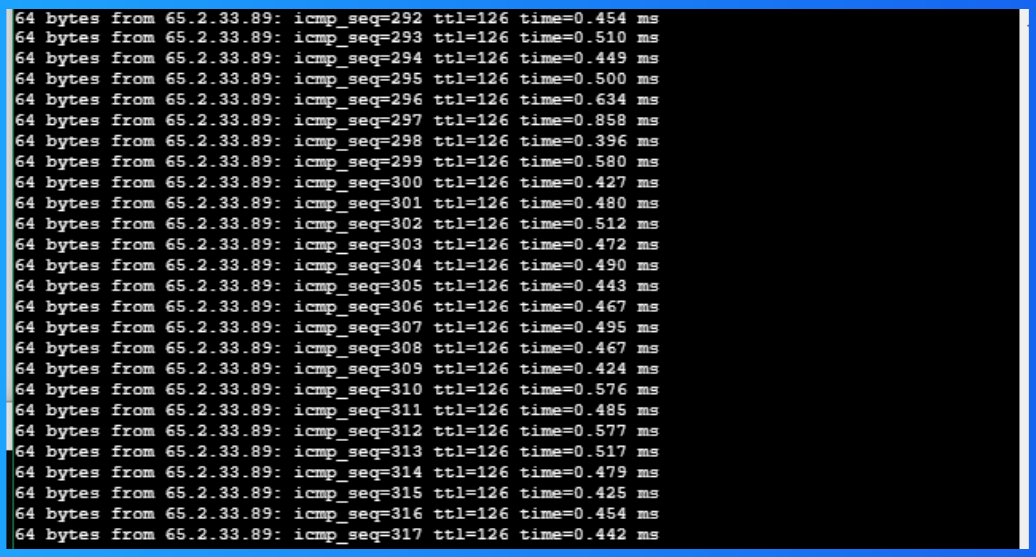
I also updated both VPCs' route tables so that resources in each VPC could reach the other VPC through the newly created peering connection. This ensured that network traffic could flow between the instances in the two VPCs.



Roshan Thomas
NextWork Student

Connectivity troubleshooting

I received ping replies from Instance 2's private IP address! This means that the network peering connection is now working correctly, and resources in the two VPCs can communicate with each other.

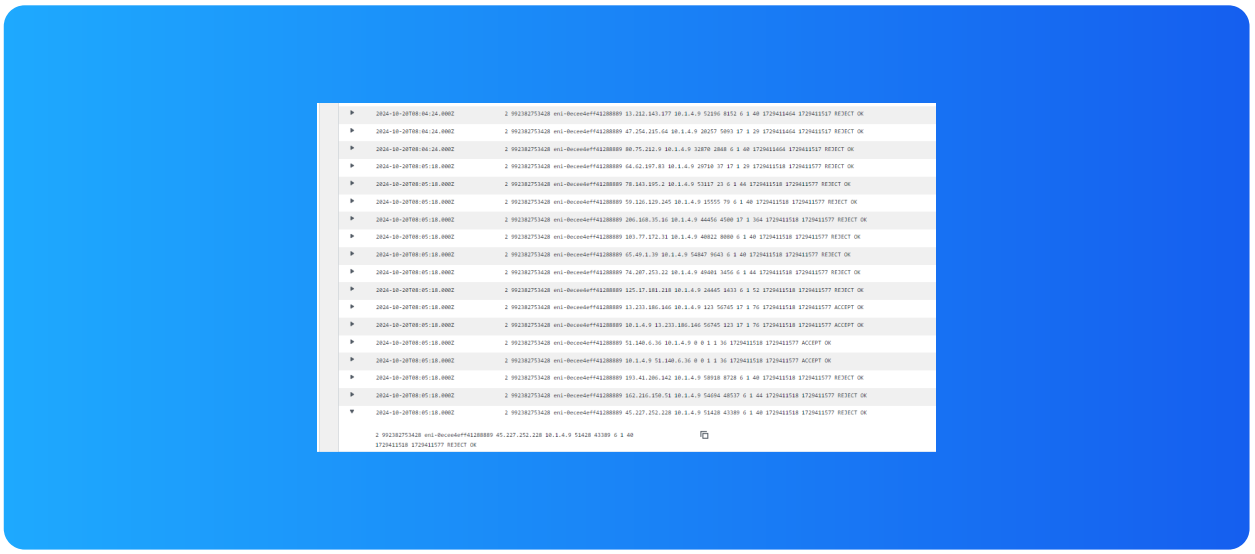


Roshan Thomas
NextWork Student

Analyzing flow logs

Flow logs provide insights into network traffic, including source and destination IP addresses, protocols, packet counts, bytes transferred, and timestamps.

For example, the flow log shows a successful connection from a source IP address to my EC2 instance. It includes details like protocol, ports, and status.

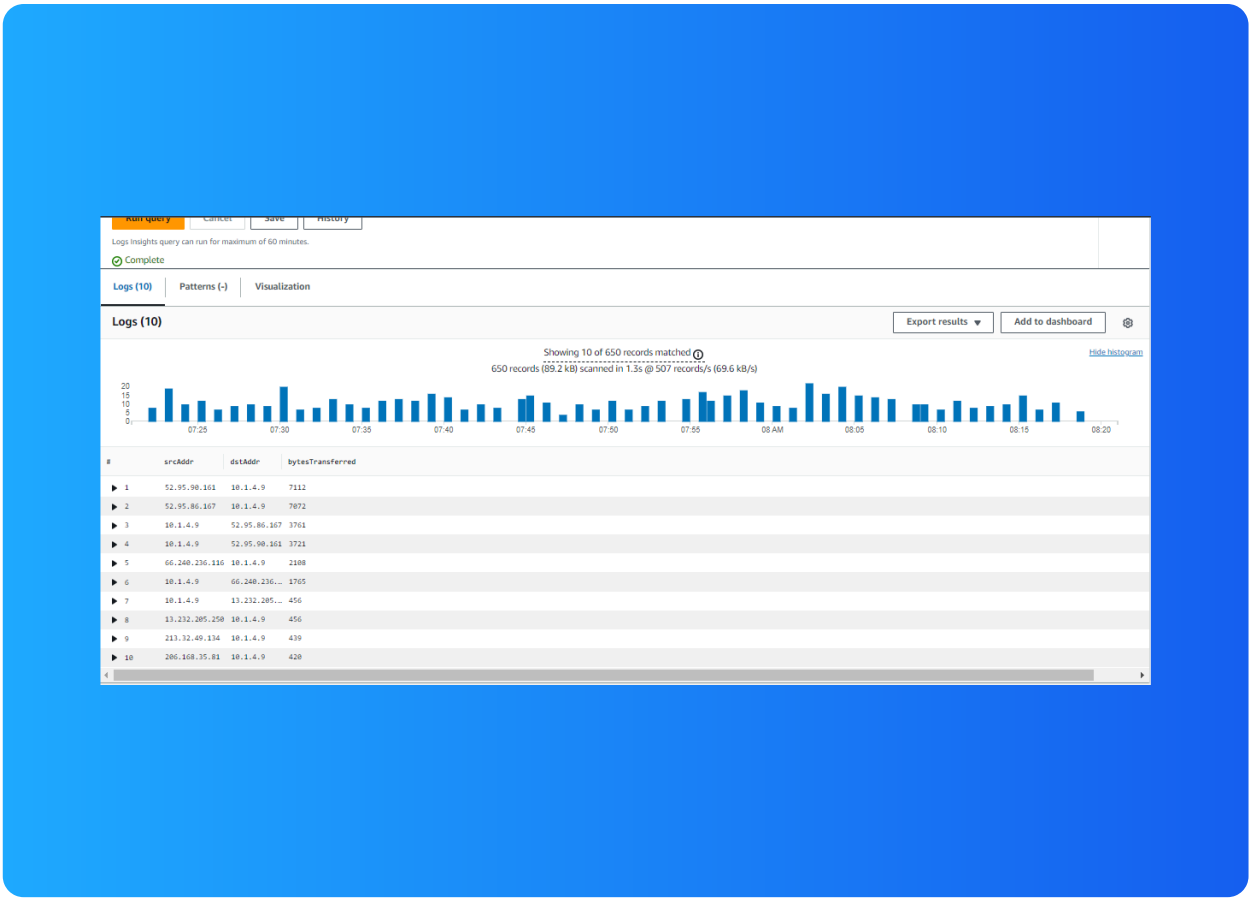


Roshan Thomas
NextWork Student

Logs Insights

Logs Insights is a powerful tool that allows you to interactively search, analyze, and visualize log data in CloudWatch Logs. It provides a user-friendly interface for querying log data, discovering log fields, and performing various analysis tasks.

I ran the query fields: source IP, destination IP, protocol, status | stats count() to analyze flow log data and understand traffic patterns.



Everyone should be in a job they love.

Check out nextwork.org for more projects