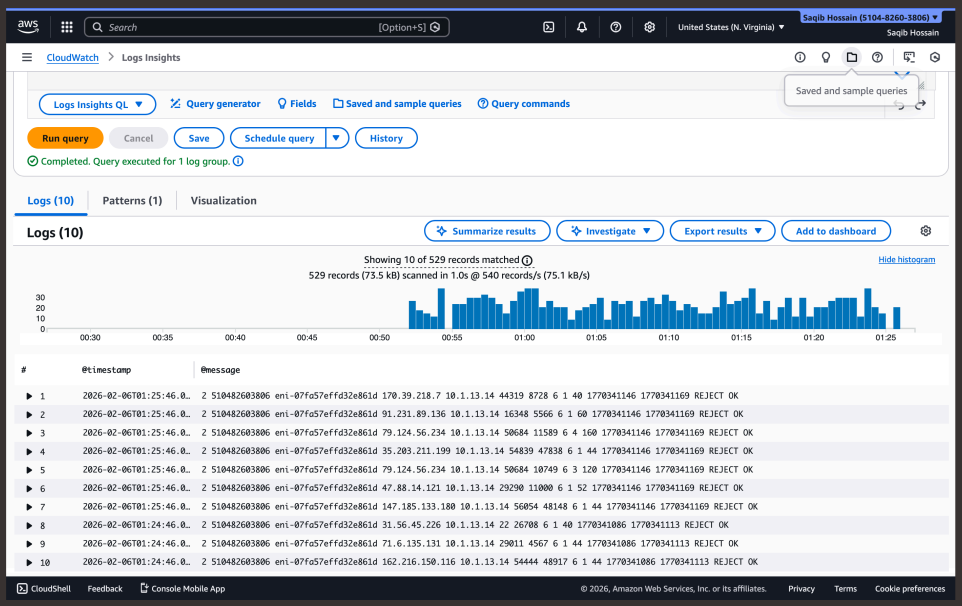
nextwork.org

VPC Monitoring with Flow Logs

saqibh49@gmail.com



saqibh49@gmail.com
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a sectioned off space within the larged AWS cloud and it is useful because it provides secure spaces to users who need to store, share and access sensitive data within a network.

How I used Amazon VPC in this project

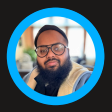
In today's project, I used Amazon VPC to teest the connection between 2 VPCs and then explore the flow logs to better understand them.

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

One thing I didn't expect in this project was how complex the flow logs would be. They sent me into a bit of a downward spiral for a minute before I took a moment to understand the basics of them.

This project took me...

This project took me about an hour.


saqibh49@gmail.com
NextWork Student

In the first part of my project...

Step 1 - Set up VPCs

In this step, I will set up my VPCs using the setup wizard because it is a much more efficient way of creating a VPC.

Step 2 - Launch EC2 instances

In this step, I will launch an EC2 instance in each of my VPCs because that will allow me to use Instance Connect to communicate between my VPCs later on.

Step 3 - Set up Logs

In this step, I will set up VPC Flow Logs because this will allow me to track and manage the types of data in my VPCs.

Step 4 - Set IAM permissions for Logs

In this step, I will create an IAM policy for my flow logs because that is how I can give permission to my flow logs to store data and send it CloudWatch.

saqibh49@gmail.com
NextWork Student

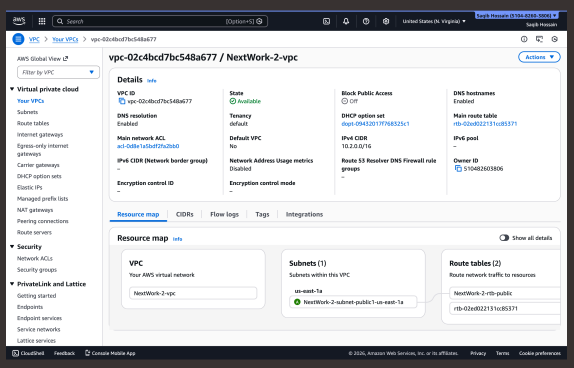
Multi-VPC Architecture

I started my project by launching 2 VPCs, each with 1 public 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 because if resources in different connected VPC's have the same IP address, it can cause issues when accessing them.

I also launched EC2 instances in each subnet

My EC2 instances' security groups allow all ICMP traffic. This is because I will be using ICMP to communicate between my instances with Instance Connect.

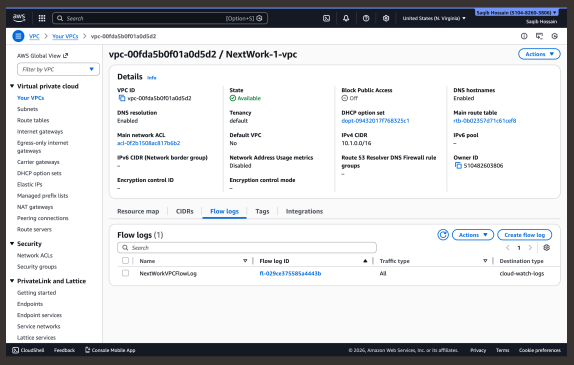


saqibh49@gmail.com
NextWork Student

Logs

Logs are essentially notes on what is going on in the VPC. For example, if someone tries to login, that will show in the logs, if theres an error somewhere, that too will be in the logs, so on and so forth.

Log groups are folders for storing logs of the same category in one place.



saqibh49@gmail.com
NextWork Student

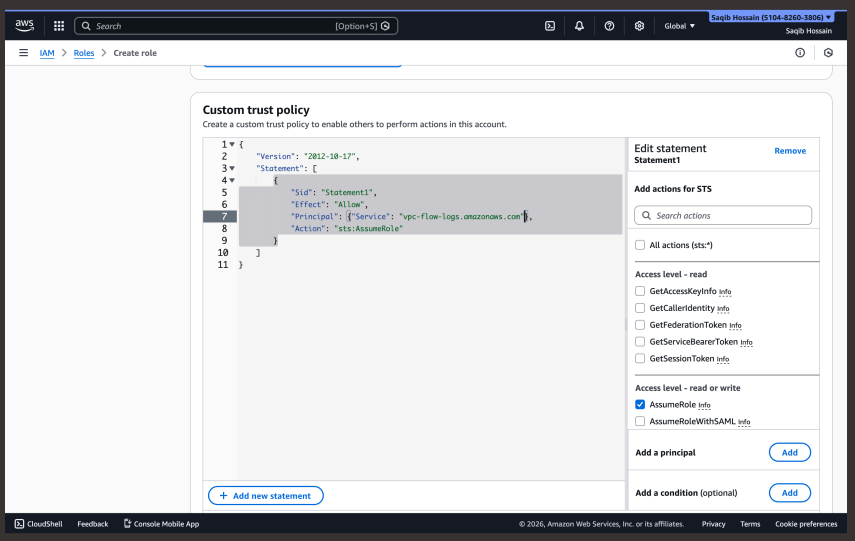
nextwork.org

IAM Policy and Roles

I created an IAM policy because thsi will allow my log flow to log data and send it wwherever it needs to go.

I also created an IAM role because this role gives me the ability to create a rule that only allows the flow logs service to use my IAM policy's allowances.

A custom trust policy is essentially a rule within a role that tells AWS which service or services can access a role.



saqibh49@gmail.com
NextWork Student

In the second part of my project...

Step 5 - Ping testing and troubleshooting

In this step, I will send a message between my 2 instances because that will create traffic that my flow logs will pickup on, allowing me to test not only my flow logs, but also my VPC connection.

Step 6 - Set up a peering connection

In this step, I will set up a peering connection because this will provide a secure way for my 2 instances to communicate that doesnt send sensitive data over the open internet.

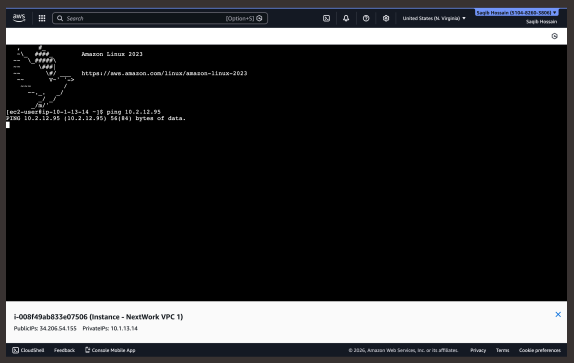
Step 7 - Analyze flow logs

In this step, I will review the flow logs because this will show me exactly what traffic came into my instances.

saqibh49@gmail.com
NextWork Student

Connectivity troubleshooting

My first ping test between my EC2 instances had no replies, which means the message was sent, but no reply was received from the other instance, meaning its not getting my message.



I could receive ping replies if I ran the ping test using the other instance's public IP address, which means the other instance is able to receive traffic from the open internet, but I need to configure it to be able to receive traffic from server 1 without going through the open internet.

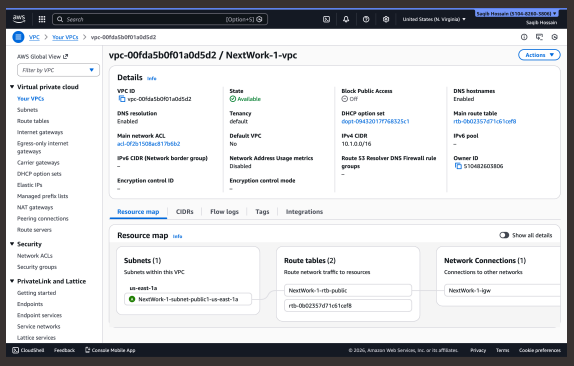
saqibh49@gmail.com
NextWork Student

Connectivity troubleshooting

Looking at VPC 1's route table, I identified that the ping test with Instance 2's private address failed because it doesn't have a direct link set up to the other instance.

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

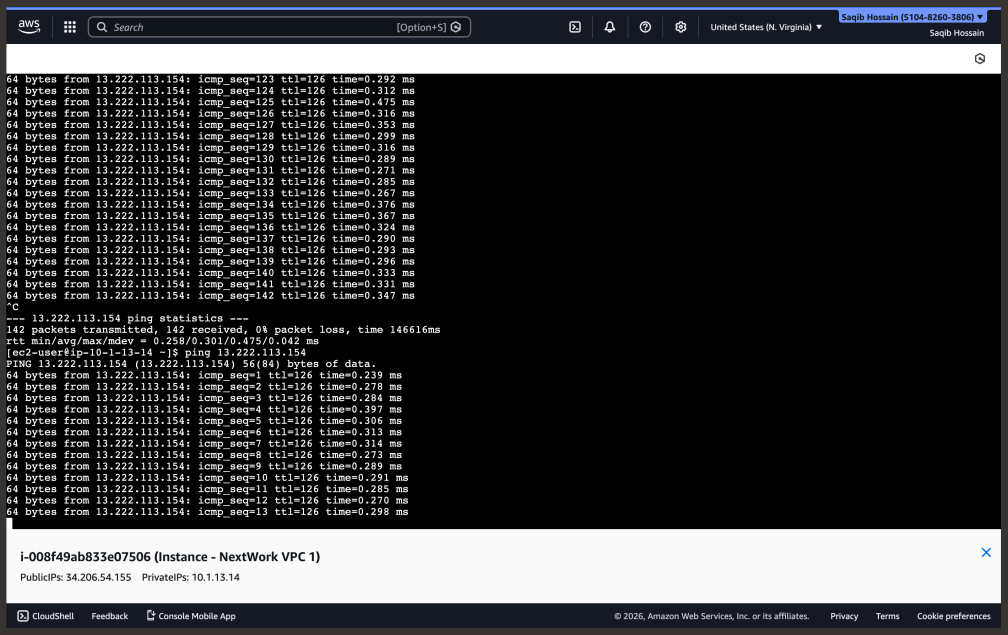
I also updated both VPCs' route tables so that a new route connecting the 2 instances directly was added toe each subnet.



saqibh49@gmail.com
NextWork Student

Connectivity troubleshooting

I received ping replies from Instance 2's private IP address! This means that both instances are connected over a secure route that doesnt have to go through the open internet.

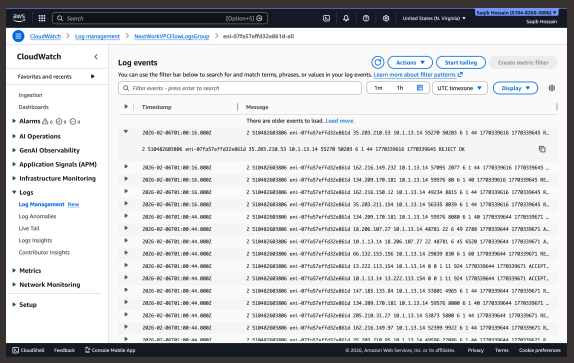


saqibh49@gmail.com
NextWork Student

Analyzing flow logs

Flow logs tell us the amount of data that was sent from which IP address to which IP address, from which port, how many packets it contained, and whether it was allowed or rejected.

For example, the flow log I've captured tells us that the data was sent from 35.203.210.53 to 10.1.13.14, it was received at pot 6 and it was only 1 packet. Finally, it says that it was rejected but the data was logged successfully, as marked by the OK.



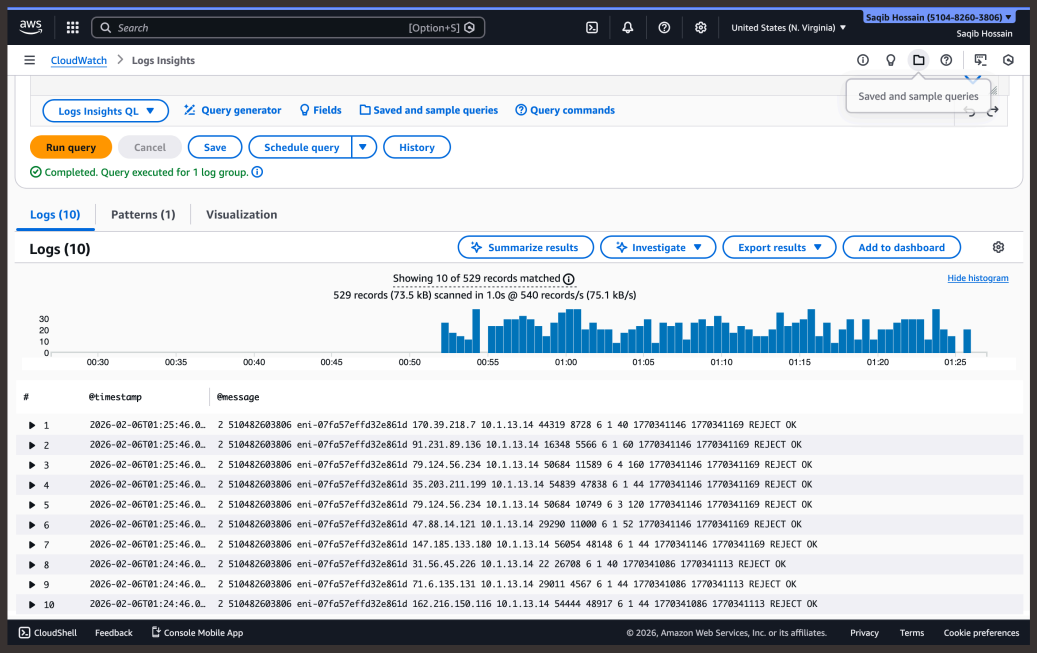
saqibh49@gmail.com
NextWork Student

nextwork.org

Logs Insights

Logs Insights is a way to search through logs using queries.

I ran the query: fields @timestamp, @message | sort @timestamp desc | limit 10
This query analyzes 10 of the most recent logs.



nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects