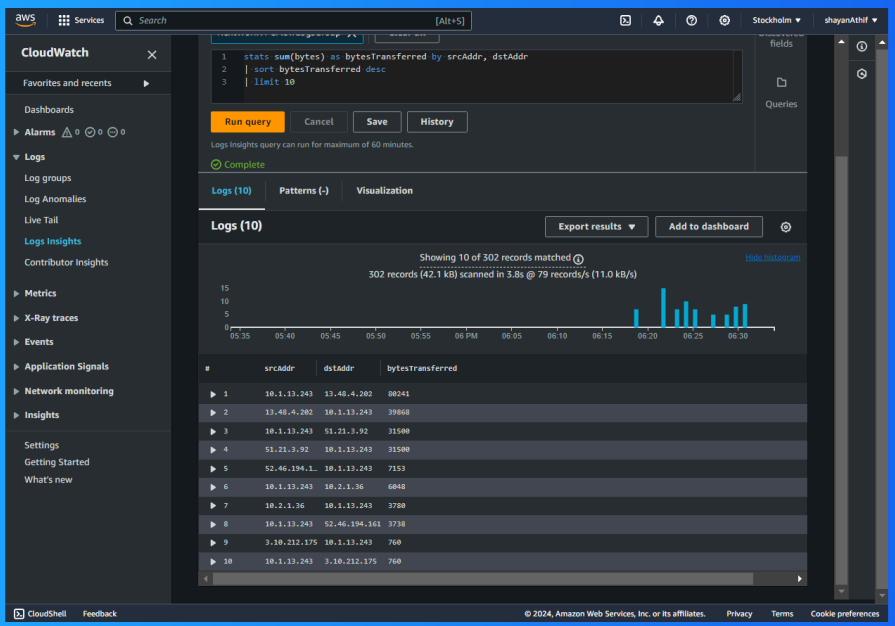
NextWork.org

VPC Monitoring with Flow Logs

sirajudeen athif



S
sirajudeen athif
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a service that allows users to create private networks within the AWS cloud. It provides enhanced security, customizable network configurations and easy scalability.

How I used Amazon VPC in this project

I used Amazon VPC to create two virtual private cloud (VPC), established a peering connection between them and monitored the network.

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

That it is very simple to use AWS, given you have some practice.

This project took me...

Around 2 hours.

S
sirajudeen athif
NextWork Student

In the first part of my project...

Step 1 - Set up VPCs

Create VPCs from scratch, establish VPC Peering Connections between them, and set up monitoring to track traffic and analyze network performance.

Step 2 - Launch EC2 instances

Launch EC2 instances in both VPCs to establish a peering connection and then, monitor network traffic and performance between them.

Step 3 - Set up Logs

We will enable AWS CloudWatch Logs to capture and record all network traffic, including requests and responses, for monitoring and analysis purposes.

Step 4 - Set IAM permissions for Logs

We're granting VPC Flow Logs permission to write logs and send them to CloudWatch, allowing us to capture and store network traffic data.

S
sirajudeen athif
NextWork Student

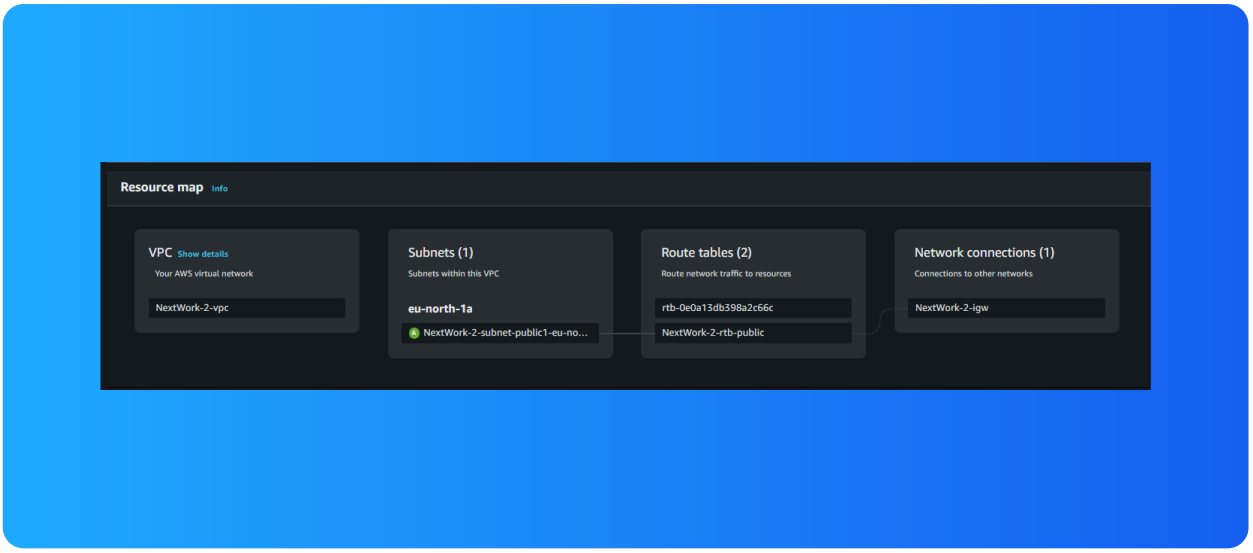
Multi-VPC Architecture

I launched 2 VPCs, each with a single Public Subnet, and configured them for use.

The CIDR blocks for VPCs 1 and 2 are 10.1.0.0/16 and 10.2.0.0/16, respectively. They must be unique because AWS reserves one IPv4 CIDR block per account, ensuring each network gets its own IP address range.

I also launched EC2 instances in each subnet

Initially, Security Group rules only allowed SSH inbound traffic. We added an explicit ICMP rule to enable pinging between instances, allowing for later network testing and verification.



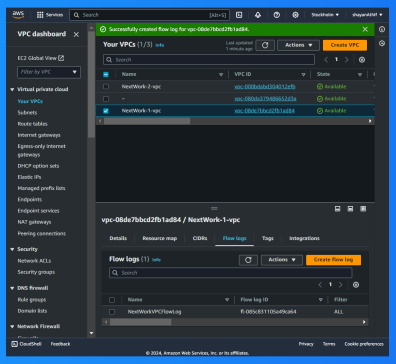
S
sirajudeen athif
NextWork Student

Logs

Logs act as a detailed account of all system activities, recording every event, interaction, and transaction that occurs within the system.

Log Groups are folders where AWS keeps related logs together, making it easy to organize and view the logs for my system.

I also set up a flow log for VPC 1



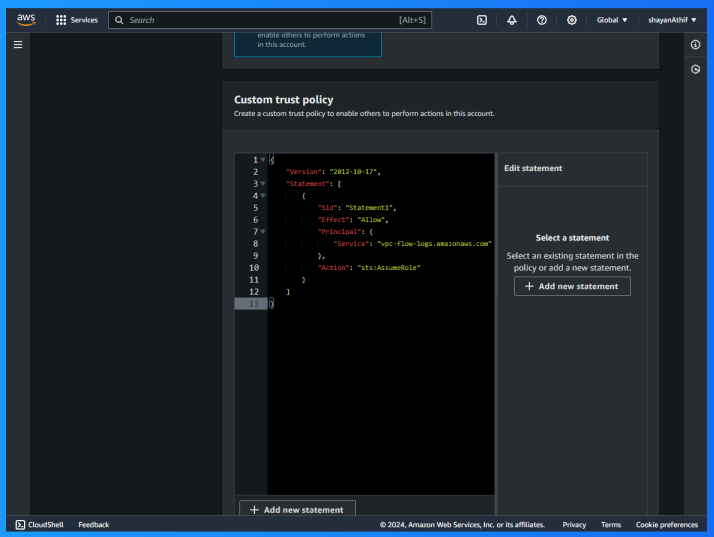
sirajudeen athif
NextWork Student

IAM Policy and Roles

By default, VPC Flow Logs can't write logs to CloudWatch. We need to give it permissions to do so, ensuring our VPC can now send its log data to the correct CloudWatch log group.

I created an IAM role because you can't assign an IAM policy directly to a service, you have to assign ROLES to a service.

Custom Trust Policies are a specific type of policy that allows us to precisely control who can use an IAM Role.



S
sirajudeen athif
NextWork Student

In the second part of my project...

Step 5 - Ping testing and troubleshooting

We're setting up a VPC Peering Connection to create a secure, private link between the two VPCs, bypassing the internet and allowing them to communicate directly with each other.

Step 6 - Set up a peering connection

we will be establishing the peering connection between the two VPCs.

Step 7 - Update VPC route tables

Now that the peering connection is all set up, we now need to set up a way for the traffic coming from both the VPCs.

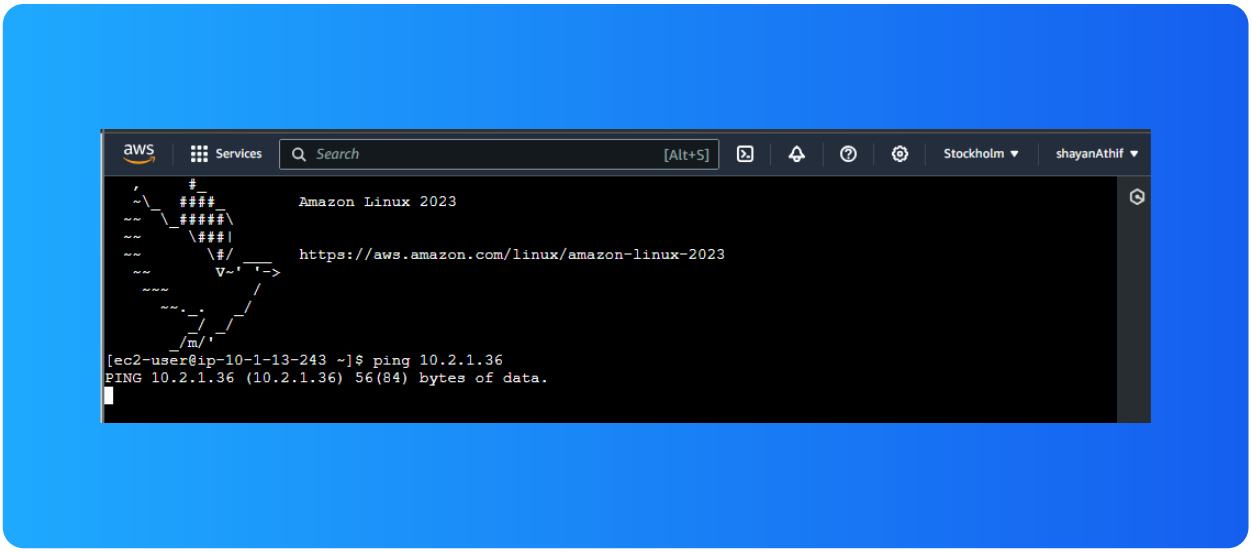
Step 8 - Analyze flow logs

we will be reviewing the flow logs recorded by the VPCs public subnet.

S
sirajudeen athif
NextWork Student

Connectivity troubleshooting

The first ping test didn't work, meaning I sent the ICMP request but got no response from the other EC2 instance, indicating a connectivity issue.



Running the ping test with the other instance's public IP allowed replies, confirming Instance 2 responds. This enables communication between both the instances using public IPs.

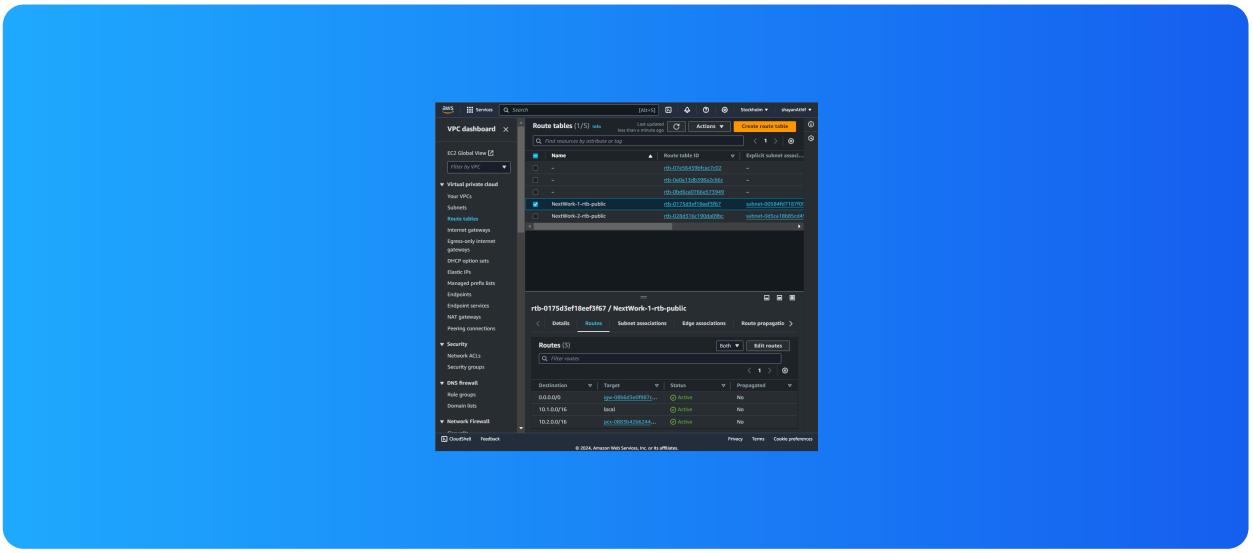
S
sirajudeen athif
NextWork Student

Connectivity troubleshooting

In VPC 1's route table, a route to 0.0.0.0/0 was found that directs traffic from anywhere, including Instance 2, through a public gateway. This prevents a direct connection and causes the ping test to fail.

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

I also updated both VPCs' route tables because even with a Peering Connection established, there's no direct route from VPC 1 to VPC 2 unless a route in the route table of VPC 1 was added.

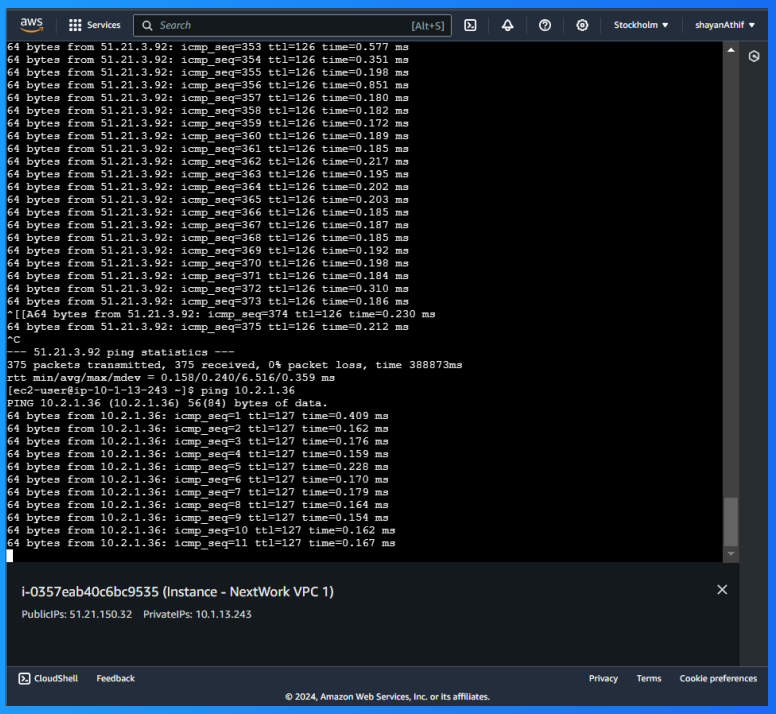


S

sirajudeen athif
NextWork Student

Connectivity troubleshooting

I received ping replies from Instance 2's private IP address! This means we have successfully created a connection between the two VPCs.



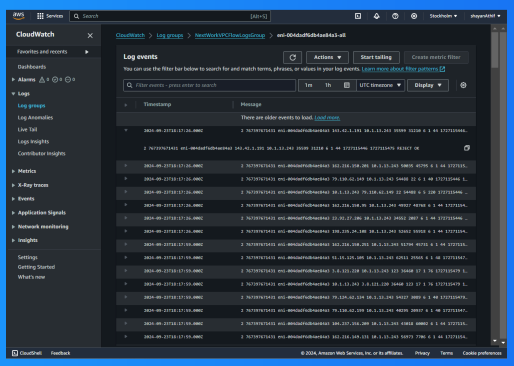
S

sirajudeen athif
NextWork Student

Analyzing flow logs

Flow logs provide detailed network metrics, including source/destination IP addresses, protocols, packet lengths, and more.

For example, the flow log I've captured tells us that it was an unsuccessful data transfer: 44 bytes via TCP (port 22) from 143.42.1.191 to 10.1.13.243, with 1 packet, in "REJECT" traffic category.

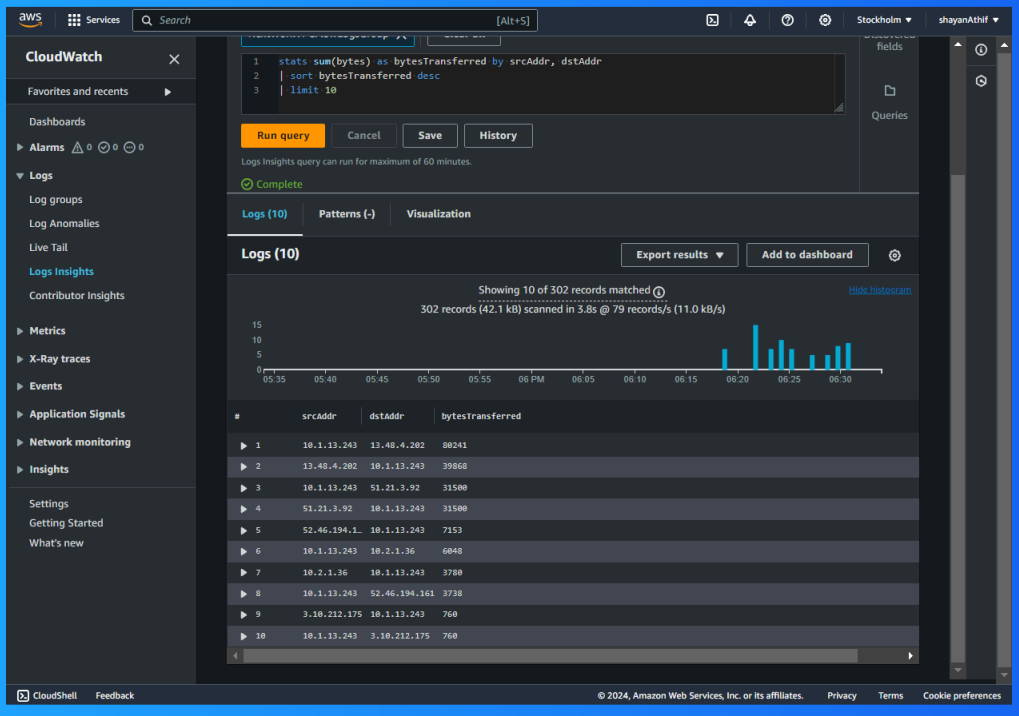


sirajudeen athif
NextWork Student

Logs Insights

Log Insights uses CloudWatch queries to filter, analyze, and combine log data, helping with troubleshooting and understanding network traffic patterns.

I ran the query to select the top 10 byte transfers by source and destination IP addresses. This query analyzes the top 10 biggest data transfers between IP addresses in this network.



Everyone should be in a job they love.

Check out nextwork.org for more projects