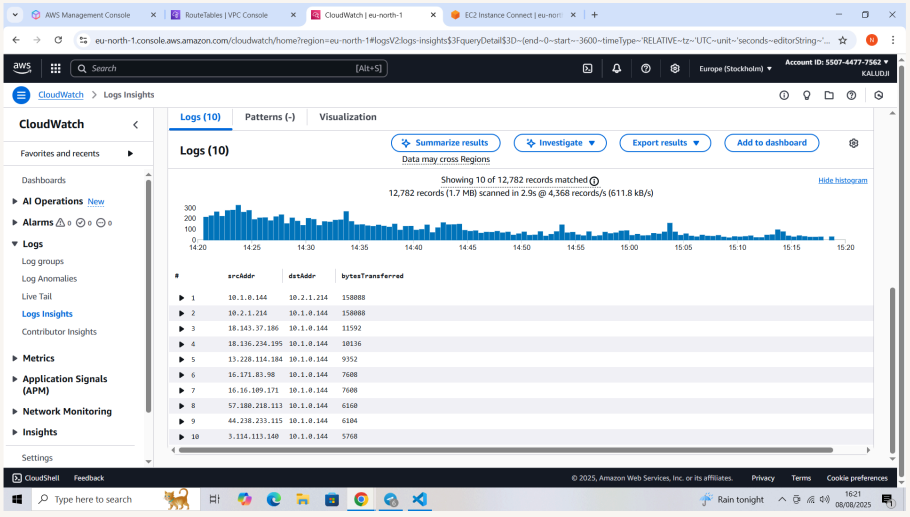
nextwork.org

VPC Monitoring with Flow Logs

Nchindo Boris



Nchindo Boris
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a networking service that lets you create a logically isolated section of the AWS cloud.

How I used Amazon VPC in this project

I used Amazon VPC in this project to monitor flow logs with CloudWatch

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

I didn't expect in this project to be easy and interesting as it was

This project took me...

It took me 1 hour to complete this project

In the first part of my project...

Step 1 - Set up VPCs

In this step I will create two VPCs from scratch!

Step 2 - Launch EC2 instances

In this step I will Launch an EC2 instance in each VPC, so we can use them to test your VPC peering connection later.

Step 3 - Set up Logs

In this step I will; - Set up a way to track all inbound and outbound network traffic. - 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. - Finish setting up your subnet's flow log.

Nchindo Boris
NextWork Student

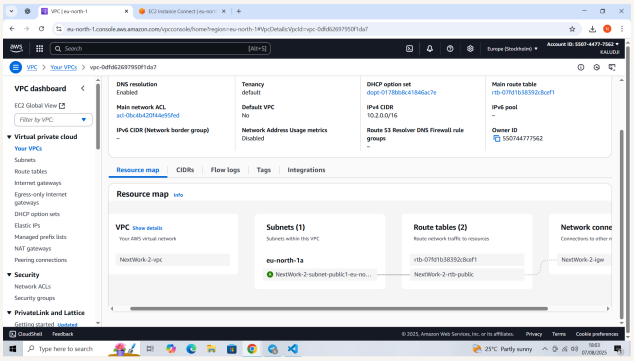
Multi-VPC Architecture

I started my project by launching 2 VPCs

The CIDR blocks for VPCs 1 and 2 are 10.2.0.0/16 and 10.1.0.0/16. They have to be unique so the IP addresses of their resources don't overlap.

I also launched EC2 instances in each subnet

My EC2 instances' security groups allow ICMP traffic from ALL IP addresses.

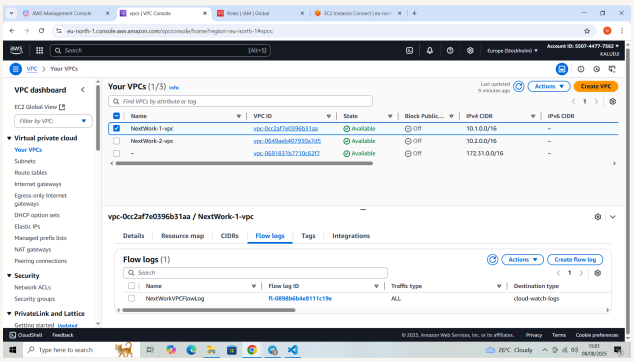


Nchindo Boris
NextWork Student

Logs

Logs are like a diary for your computer systems. They record everything that happens, from users logging in to errors popping up.

Log group is like a big folder in AWS where you keep related logs together.



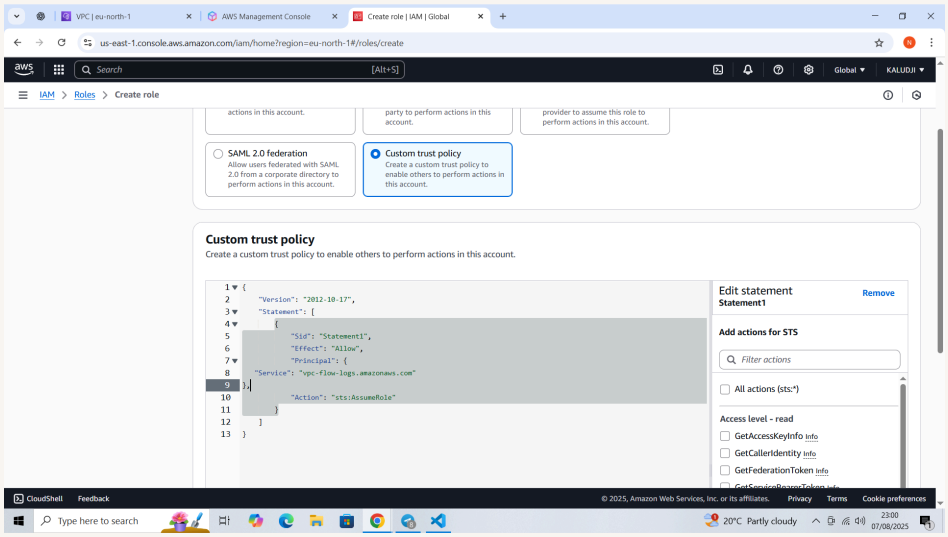
Nchindo Boris
NextWork Student

IAM Policy and Roles

I created an IAM policy to make sure that your VPC can now send log data to your log group!

I also created an IAM role because I want to Assign the IAM role to services

A custom trust policy is used to very narrowly define who can use a role.



In the second part of my project...

Step 5 - Ping testing and troubleshooting

In this step, I am going to Get Instance 1 to send test messages to Instance 2.

Step 6 - Set up a peering connection

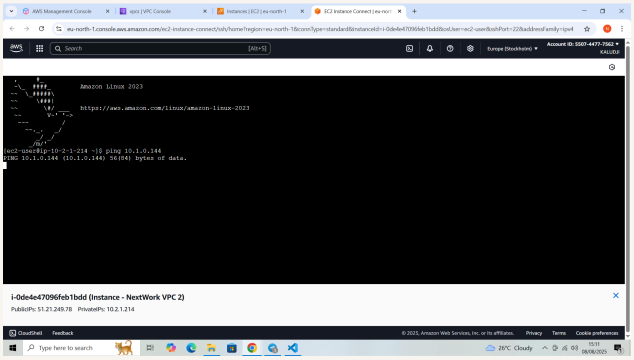
In this step, I am going to Set up a connection link between your VPCs.

Step 7 - Analyze flow logs

In this step, I am going to: - Review the flow logs recorded aboout VPC 1's public subnet. - Analyse the flow logs to get some tasty insights

Connectivity troubleshooting

My first ping test between my EC2 instances had no replies, which means there's a problem with the connection.



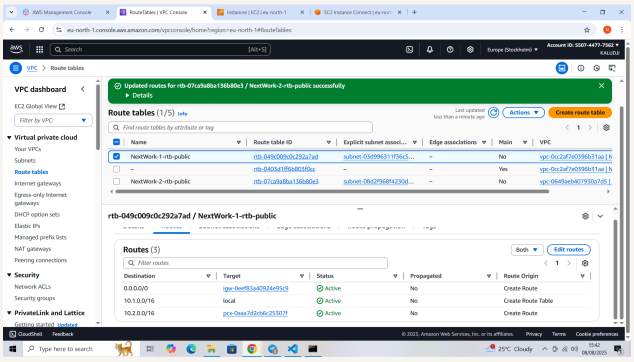
I receive ping replies after the ping test using the other instance's public IP address, which means Instance 2 is correctly configured to respond to ping requests, and Instance 1 can actually communicate with Instance 2 on the public internet

Connectivity troubleshooting

Looking at VPC 1's route table, I identified that the ping test with Instance 2's private address failed because a VPC peering connection that directly connects VPCs 1 and 2 is lacking. I should set up a new route that directs traffic to our peering

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

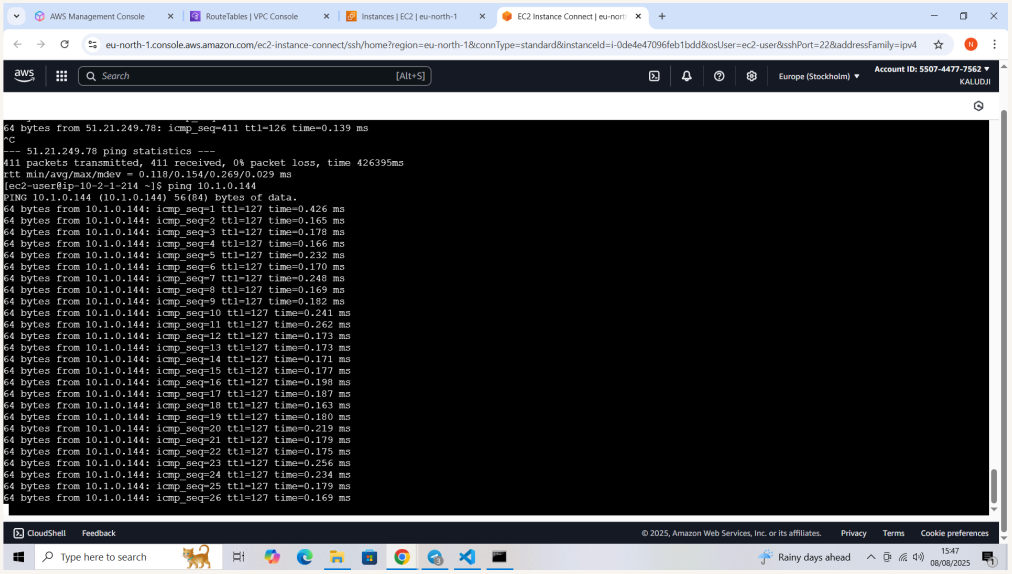
I also updated both VPCs' route tables because traffic in VPC 1 won't know how to get to resources in VPC 2 without a route in my route table. I need to set up a route that directs traffic bound for VPC 2 to the peering connection



Nchindo Boris
NextWork Student

Connectivity troubleshooting

I received ping replies from Instance 2's private IP address! This means successfully resolved the connectivity issue by setting up a peering architecture between VPC 1 and VPC 2!. The EC2 instances can now communicate using their private IP addresse

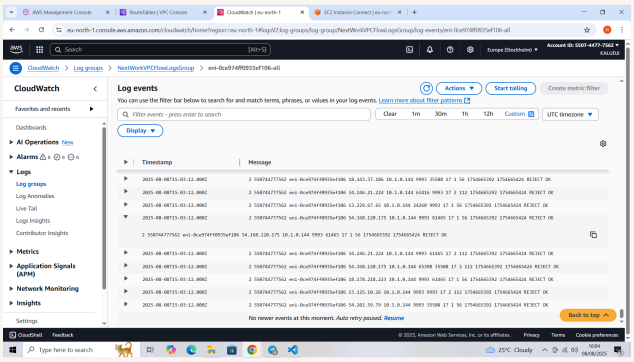


Nchindo Boris
NextWork Student

Analyzing flow logs

Flow logs tell us about - Flow log version - Account ID - ID of the ENI - Source & Destination IP address - Source & Destination port number - Protocol number - Number of packets & bytes transferred - Start and End time of the flow - ACCEPT or REJECT

For example, the flow log I've captured tells us; 2 550744777562 eni-0ce974ff0935ef106 54.168.120.175 10.1.0.144 9993 61465 17 1 56 1754665392 1754665424 REJECT OK

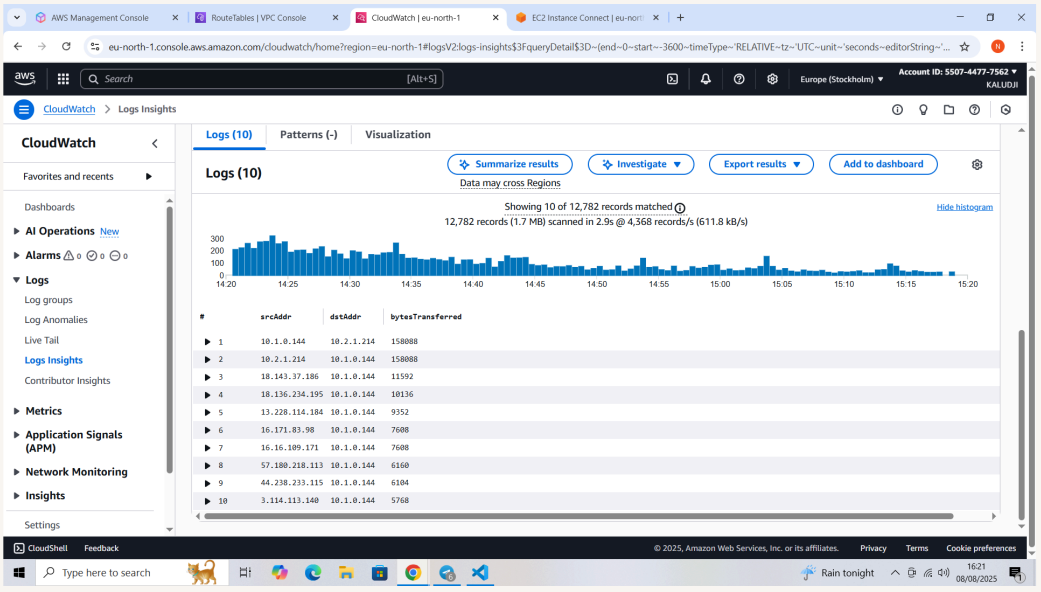


Nchindo Boris
NextWork Student

Logs Insights

Logs Insights is a CloudWatch feature that analyzes your logs. In Log Insights, you use queries to filter, process and combine data to help you troubleshoot problems or better understand your network traffic!

I ran the query "Top 10 byte transfers by source and destination IP addresses". This query analyzes the ten pairs of source and destination IP addresses that transferred the most data between them.



The place to learn & showcase your skills

Check out nextwork.org for more projects