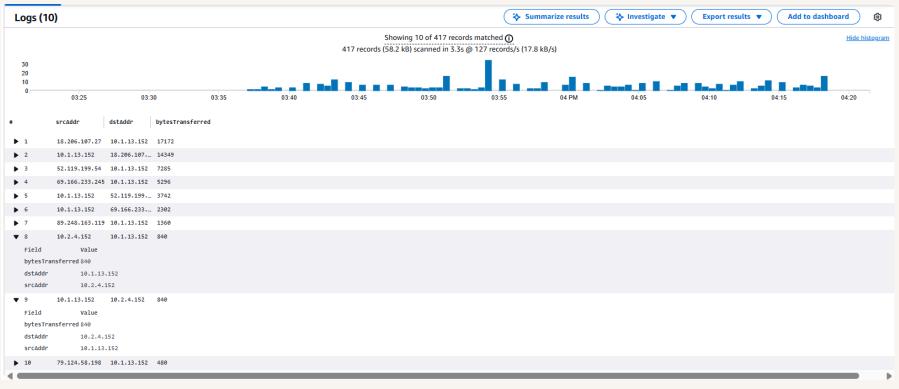
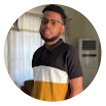
nextwork.org

VPC Monitoring with Flow Logs

Jonathan Nutsugah





Jonathan Nutsugah
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) lets you create a secure, isolated network in AWS where you control IP ranges, subnets, and traffic. It's useful for customizing network setup, enhancing security, and supporting hybrid cloud deployments.

How I used Amazon VPC in this project

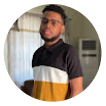
Through the management console, I used it to virtually isolate a space to keep my resources away from external access.

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

How easy it is to navigate AWS.

This project took me...

1hour 30mins


Jonathan Nutsugah
NextWork Student

In the first part of my project...

Step 1 - Set up VPCs

In this step, I'm going to create two brand-new VPCs from scratch so I have isolated, customizable networks to work with. This is important because it lets me design and control each VPC's settings, like IP ranges and subnets.

Step 2 - Launch EC2 instances

In this step, I'm going to launch an EC2 instance in each VPC. These instances will let me test the peering connection later to make sure the two VPCs can communicate properly.

Step 3 - Set up Logs

In this step, I'm going to set up VPC Flow Logs to capture all inbound and outbound network traffic in my VPC. Then, I'll create a storage space to save these logs so I can review and analyze the traffic later.

Step 4 - Set IAM permissions for Logs

In this step, I'm going to give VPC Flow Logs permission to send traffic data to CloudWatch and then complete the setup for my subnet's flow log. This is important because it lets me capture and store network activity.

Jonathan Nutsugah
NextWork Student

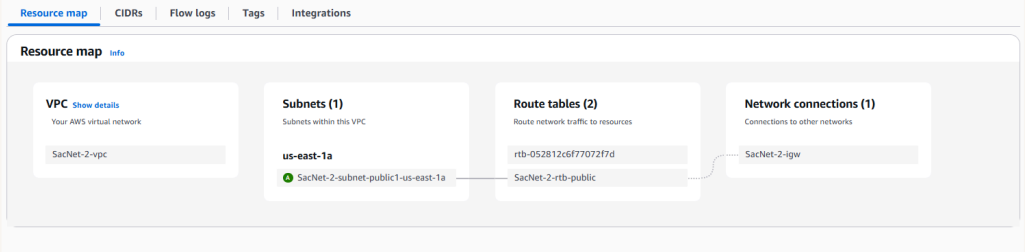
Multi-VPC Architecture

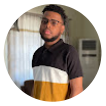
I started my project by launching 2 VPCs with 1 subnet each.

The CIDR blocks for VPCs 1 and 2 are unique. They have to be unique because overlapping IPs cause routing conflicts and stop proper communication between the VPCs.

I also launched EC2 instances in each subnet

My EC2 instances' security groups allow ICMP traffic from all IP addresses. This is because I need to enable ping tests between the instances to verify that the VPC peering connection is working correctly.



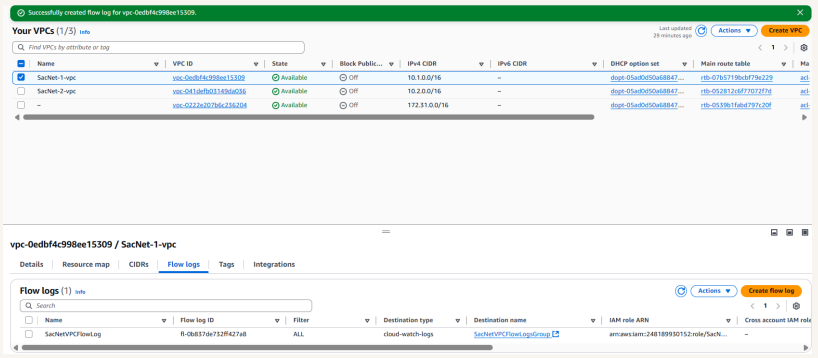


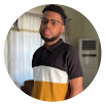
Jonathan Nutsugah
NextWork Student

Logs

Logs are records that automatically capture important events or actions happening in a system, like network activity or errors. They help me track, monitor, and troubleshoot what's going on behind the scenes.

Log groups are collections of related log streams in CloudWatch Logs that help organize and manage logs from the same source or application in one place.





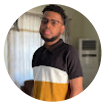
Jonathan Nutsugah
NextWork Student

IAM Policy and Roles

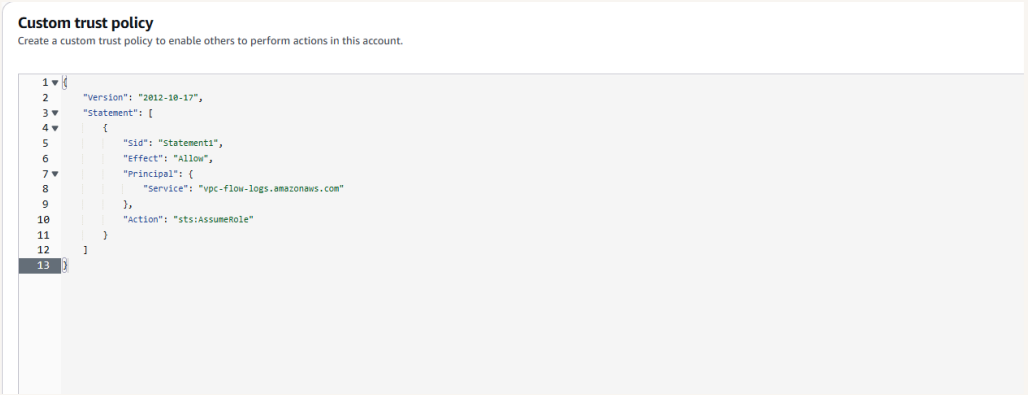
I created an IAM policy because VPC Flow Logs need permission to send log data to CloudWatch. The policy defines those permissions, allowing AWS to securely collect and store my network traffic logs.

I also created an IAM role because it lets VPC Flow Logs use the permissions from the IAM policy. By attaching the role to the flow logs service, I'm allowing it to send log data to CloudWatch on my behalf.

A custom trust policy is a set of rules that defines which AWS services or accounts are allowed to assume a specific IAM role. It ensures that only trusted entities can use the role and its permissions.



Jonathan Nutsugah
NextWork Student



In the second part of my project...

Step 5 - Ping testing and troubleshooting

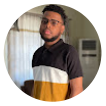
In this step, I'm going to send a test message from Instance 1 to Instance 2 to generate network traffic and see if it shows up in the flow logs. At the same time, this also helps me verify that my VPC peering connection is working.

Step 6 - Set up a peering connection

In this step, I'm creating a connection between my VPCs to let them communicate privately and securely using their private IPs.

Step 7 - Analyze flow logs

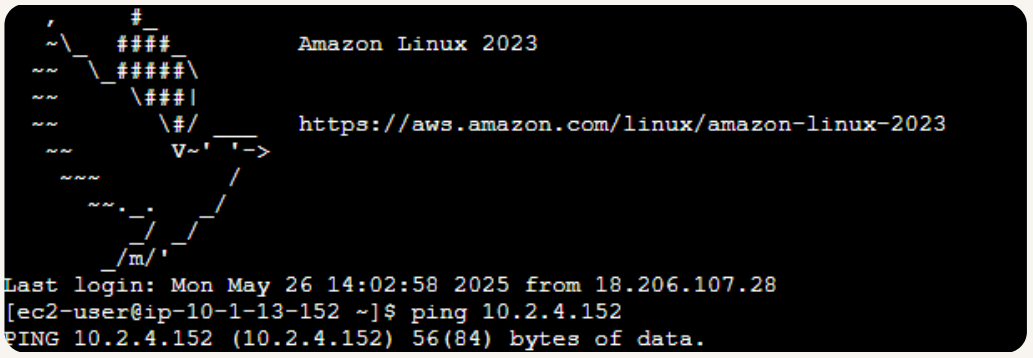
In this step i am about to analyze captured logs to gain insight on the kind of activity happening in our environment.



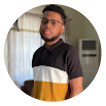
Jonathan Nutsugah
NextWork Student

Connectivity troubleshooting

My first ping test between my EC2 instances had no replies, which means the instances couldn't communicate. This could be due to issues like incorrect security group rules, missing route table entries, or misconfigured network settings.



I could receive ping replies if I ran the ping test using the other instance's public IP address, which means Instance 2 is set up to respond to ping requests, and Instance 1 can reach it over the public internet.



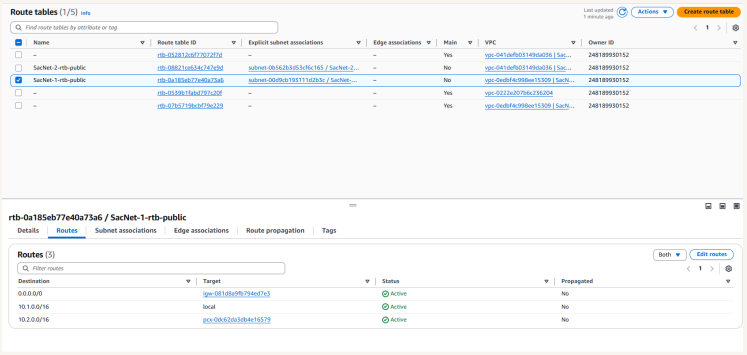
Jonathan Nutsugah
NextWork Student

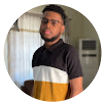
Connectivity troubleshooting

Looking at VPC 1's route table, I identified that the ping test with Instance 2's private address failed because there was no route telling VPC 1 how to reach Instance 2’s private IP through the peering connection.

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

I also updated both VPCs' route tables so that each VPC has a route to send traffic to eachother.

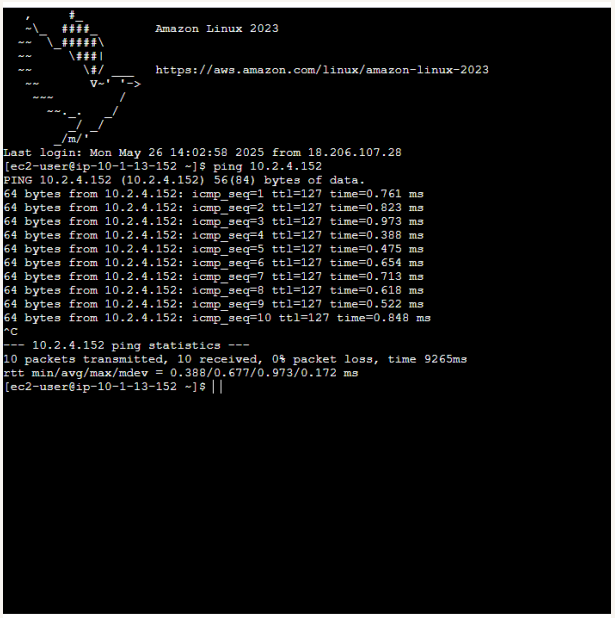


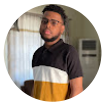


Jonathan Nutsugah
NextWork Student

Connectivity troubleshooting

I received ping replies from Instance 2's private IP address! This means our VPCs can communicate privately.



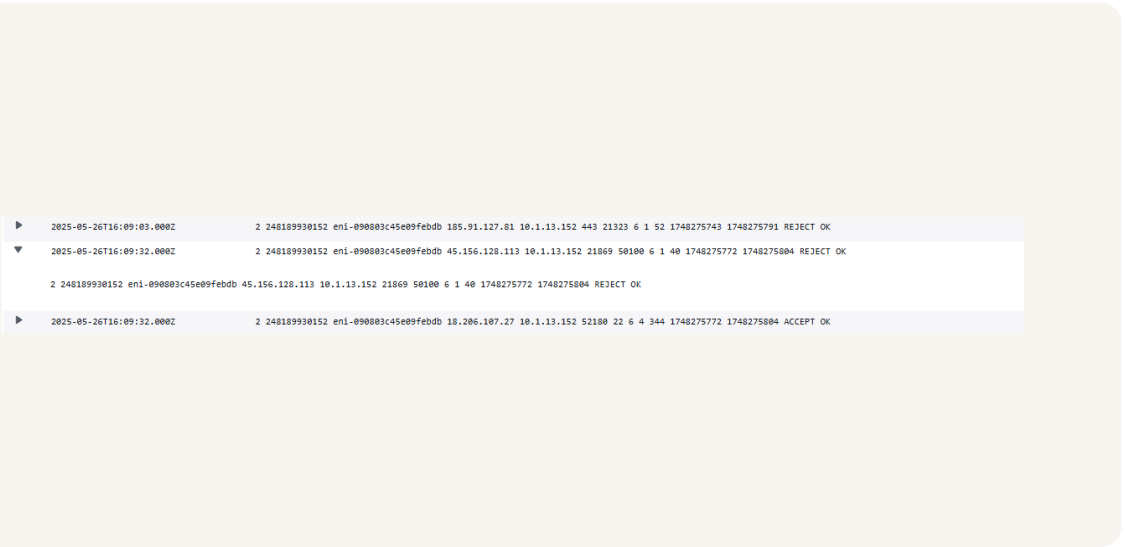


Jonathan Nutsugah
NextWork Student

Analyzing flow logs

Flow logs tell us about network traffic details like source and destination IPs, ports, protocols, traffic direction, actions taken (accepted or rejected), and timestamps. These parts help track how data moves through the VPC.

For example, the flow log I've captured tells us a ping attempt was rejected.

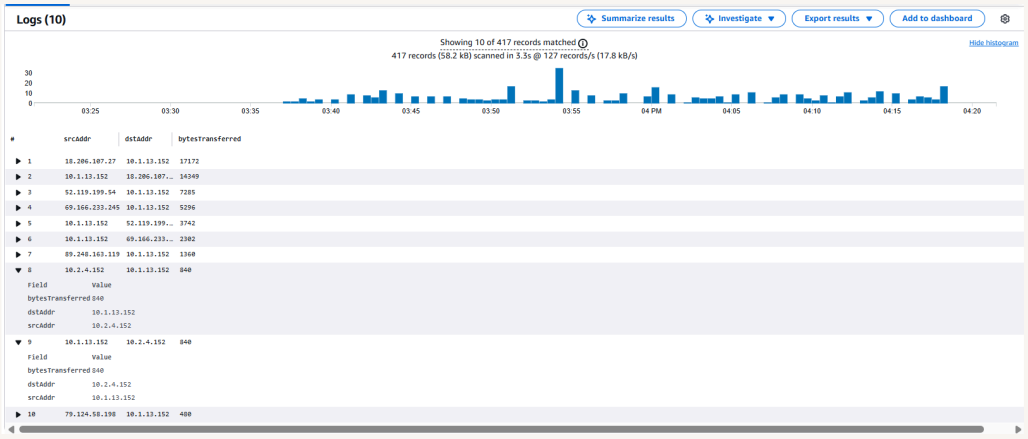


Jonathan Nutsugah
NextWork Student

Logs Insights

Logs Insights is a tool in CloudWatch that lets you search, analyze, and visualize log data using queries. It helps quickly find patterns, troubleshoot issues, and understand what's happening in your system.

The query I ran was "Top 10 byte transfers by source and destination IP addresses" from the Flow Logs section in Log Insights. This query shows me which IP pairs transferred the most data, helping me identify the top sources and destinations.



The place to learn & showcase your skills

Check out nextwork.org for more projects