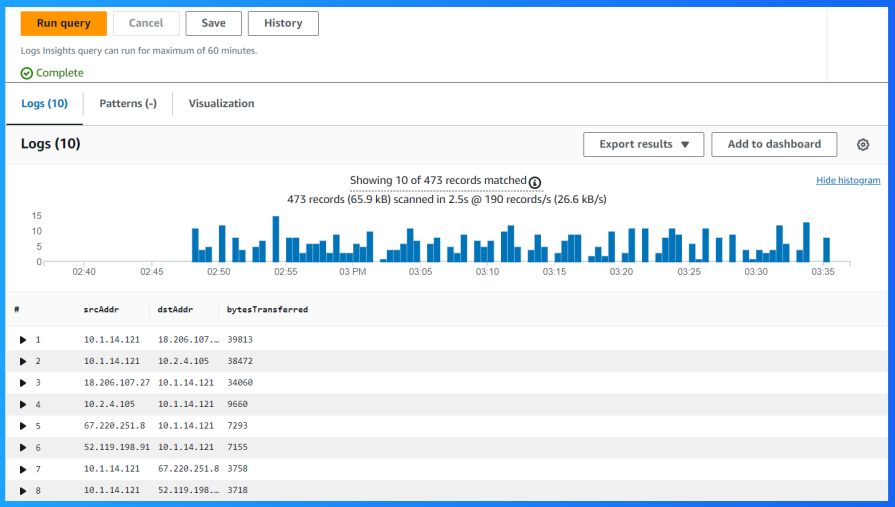
NextWork.org

VPC Monitoring with Flow Logs

Ivan Delgadillo Fernandez



Ivan Delgadillo Fernandez
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon Virtual Private Cloud (Amazon VPC) gives you full control over your virtual networking environment, including resource placement, connectivity, and security.

How I used Amazon VPC in this project

Use Amazon VPC to launch AWS resources into a virtual network that is a logically isolated section of the AWS Cloud.

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

I didn't expect configure a Peering VPC

This project took me...

120 Minutes

Ivan Delgadillo Fernandez
NextWork Student

NextWork.org

In the first part of my project...

Step 1 - Set up VPCs

I use VPC wizard to create 2 VPC, that contain only public subnet with a internet gateway.

Step 2 - Launch EC2 instances

We need to create these EC2 instances so that they can send data to each other later in the project, which gives us network activity to monitor.

Step 3 - Set up Logs

Setup VPC Flow logs and cloud Watch

Step 4 - Set IAM permissions for Logs

Now that we know that logs are digital diaries that services keep, think of flow logs as a specific type of diary for VPCs. Flow logs capture traffic going to and from the network - noting down who's visiting your VPC and the specific network interfa

Ivan Delgadillo Fernandez
NextWork Student

NextWork.org

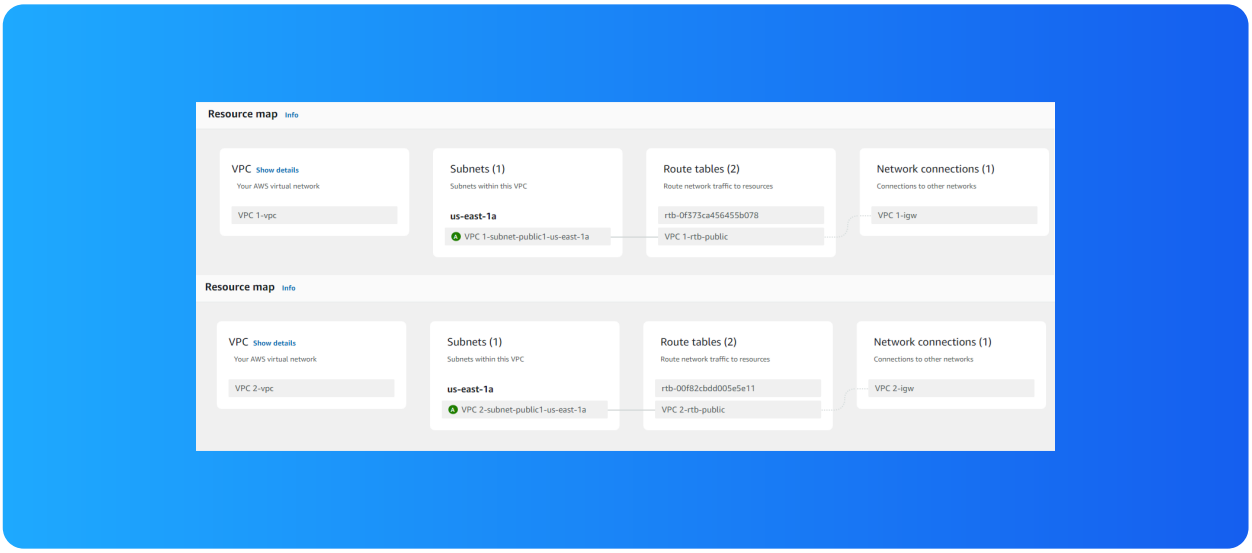
Multi-VPC Architecture

I stared my project by launching 2 VPCs using VPC wizard, I completed in 2 minutes.

The CIDR blocks for VPCs 1 and 2 are 10.1.0.0/16 and 10.2.0.0/16, they have to be unique because you needed separate different workloads.

I also launched EC2 instances in each subnet

Security Groups allow access from a source with differents ports to access a Instances EC2 like a SSH, HTTP, ICMP.



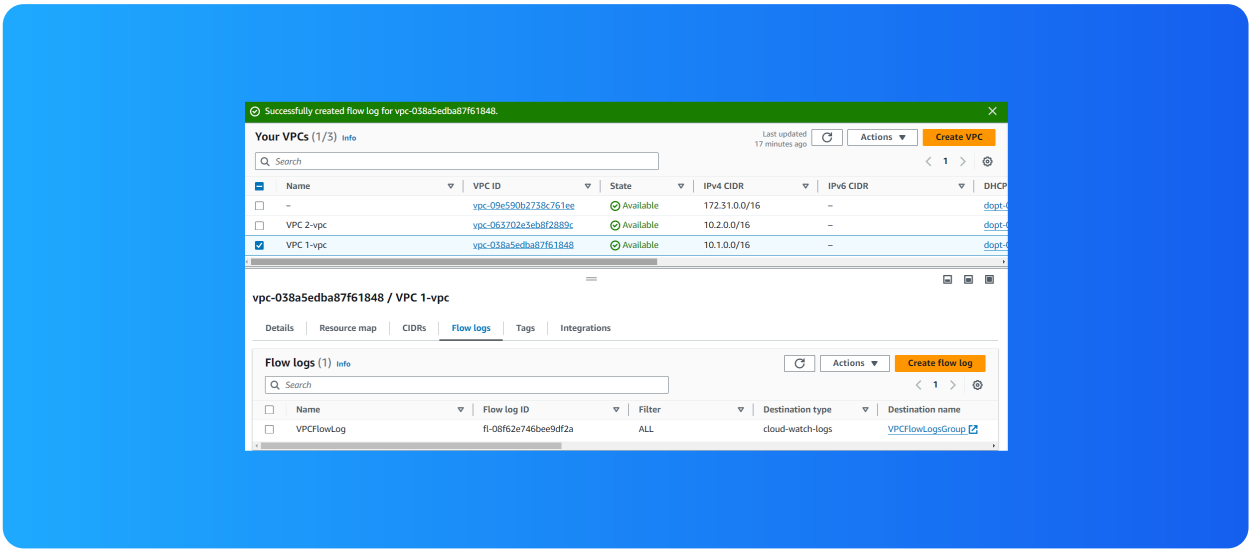
Ivan Delgadillo Fernandez
NextWork Student

Logs

Logs are like a diary for your computer systems. They record everything that happens, from users logging in to errors popping up. It's the go-to place to understand what's going on with your systems, troubleshoot problems, and keep an eye on who’s do

Think of a log group as a big folder in AWS where you keep related logs together. Usually, logs from the same source or application will go into the same log group, BUT logs are also region-specific. This means log data gets created and saved in the

I also set up a flow log for VPC 1



Ivan Delgadillo Fernandez
NextWork Student

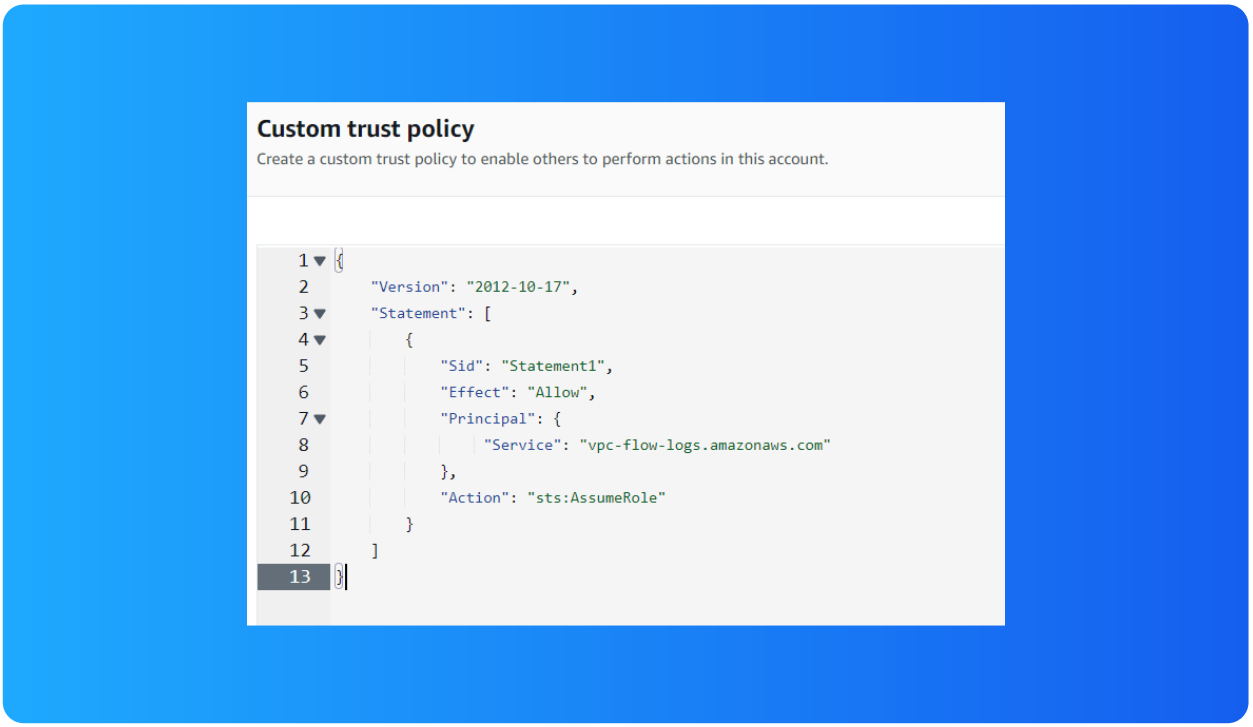
NextWork.org

IAM Policy and Roles

VPC Flow Logs by default don't have the permission to record logs and store them in your CloudWatch log group.

IAM roles made up of combinations of IAM policies

A custom trust policy is specific type of policy! They're different from IAM policies. While IAM policies help you define the actions a user/service can or cannot do, custom trust policies are used to very narrowly define who can use a role.



Ivan Delgadillo Fernandez
NextWork Student

NextWork.org

In the second part of my project...

Step 5 - Ping testing and troubleshooting

Let's generate some network traffic and see whether our flow logs can pick up on them. We're going to generate network traffic by trying to get our instance in VPC 1 to send a message to our instance in VPC 2.

Step 6 - Set up a peering connection

Let's add that peering connection in this step to bridge our VPCs together!

Step 7 - Update VPC route tables

Set up a way for traffic coming from VPC 1 to get to VPC 2. Set up a way for traffic coming from VPC 2 to get to VPC 1.

Step 8 - Analyze flow logs

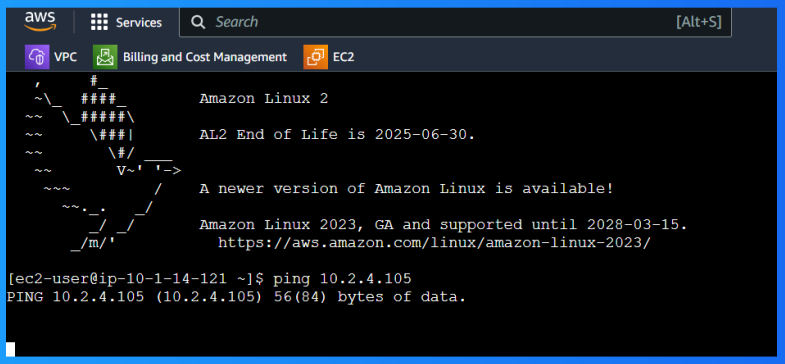
Review the flow logs recorded aboout VPC 1's public subnet. Analyse the flow logs to get some tasty insights

Ivan Delgadillo Fernandez
NextWork Student

NextWork.org

Connectivity troubleshooting

My first ping test between my EC2 instances had no replies, which means there aren't connections between my VPCs



I could receive ping replies if I ran the ping test using the other instance's public IP address

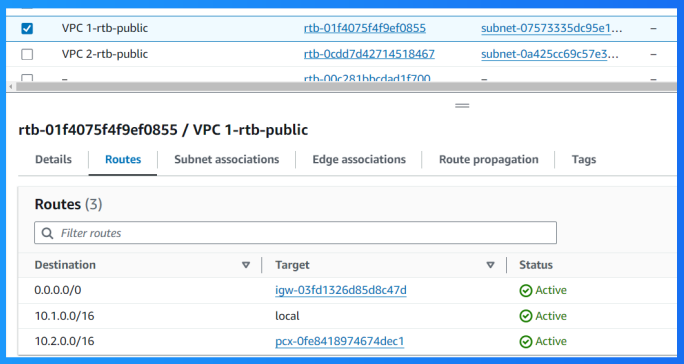
Ivan Delgadillo Fernandez
NextWork Student

Connectivity troubleshooting

Looking at VPC 1's route table, I identified that the ping test with Instance 2's private address failed because the traffic is is through the internet gateway i.e. traffic will travel through and be exposed to the public internet.

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

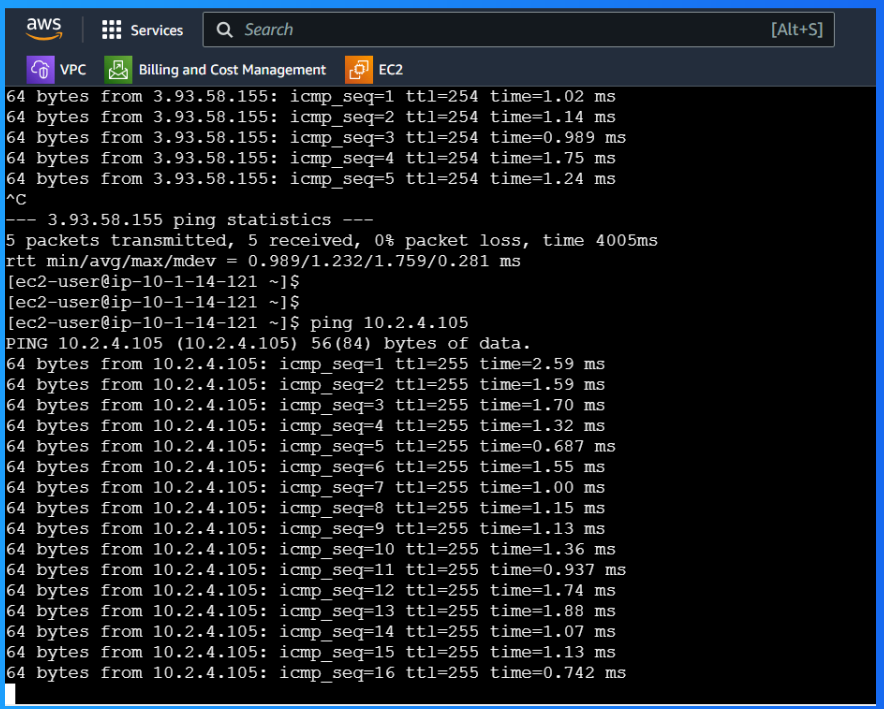
I also updated both VPCs' route tables so that both VPCs could PING to other VPC



Ivan Delgadillo Fernandez
NextWork Student

Connectivity troubleshooting

I received ping replies from Instance 2's private IP address! This means there are connection succesful

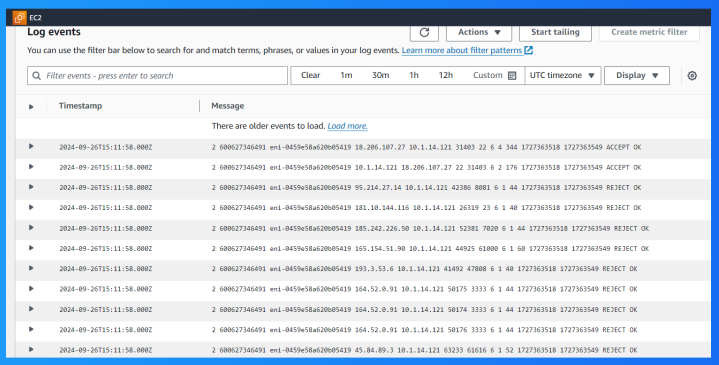


Ivan Delgadillo Fernandez
NextWork Student

Analyzing flow logs

This flow log shows that 344 bytes of data were sent successfully from the IP address 18.237.140.165 to 10.1.5.112 using TCP protocol on port 22, with 4 packets transferred and the traffic was allowed ("ACCEPT").

For example, you might find one that says REJECT OK instead of ACCEPT OK at the end. These would represent the ping messages that failed to reach Instance 2!



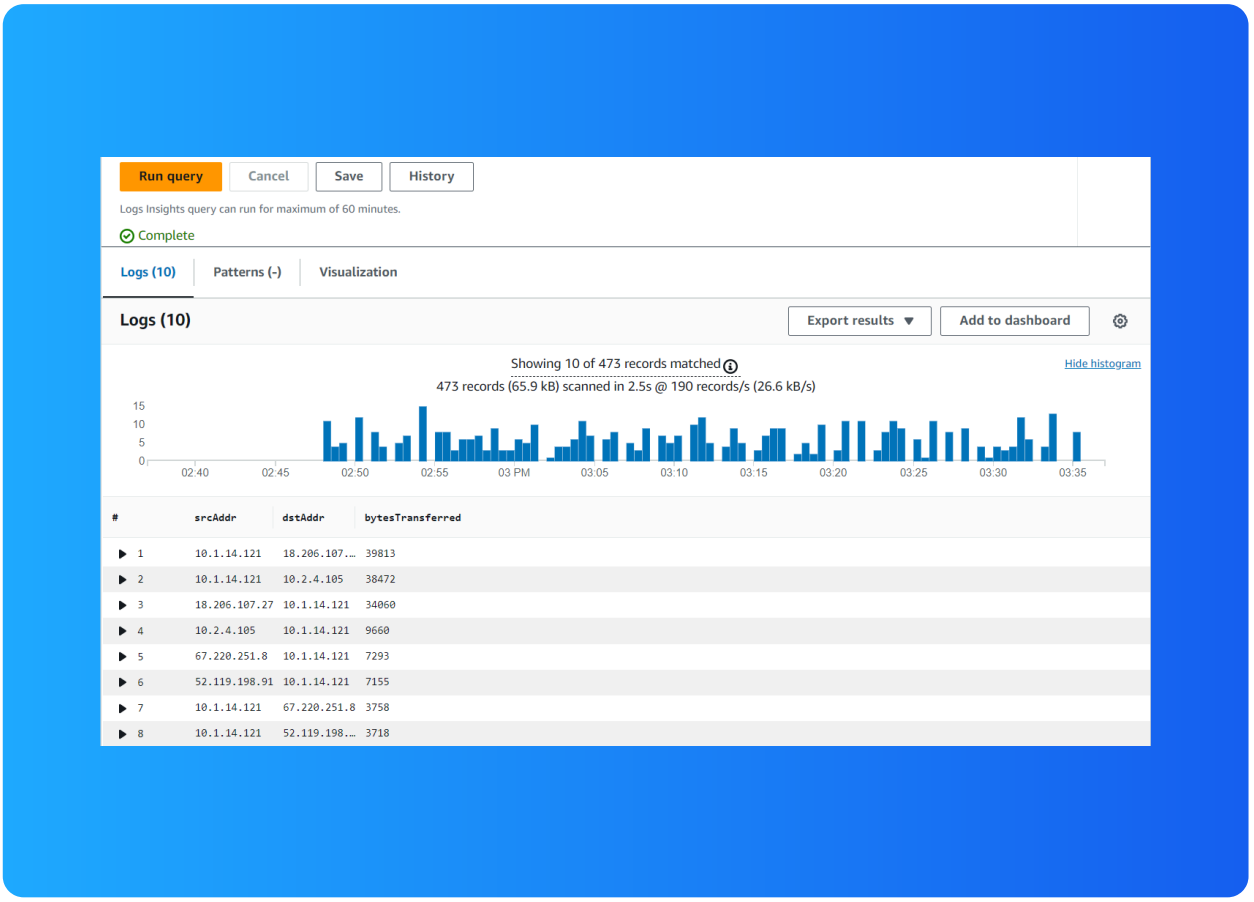
Ivan Delgadillo Fernandez
NextWork Student

NextWork.org

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!

Queries are like commands you run to analyze your logs! You can use queries to filter logs, group data, and perform calculations like sums and averages.



Everyone should be in a job they love.

Check out nextwork.org for more projects