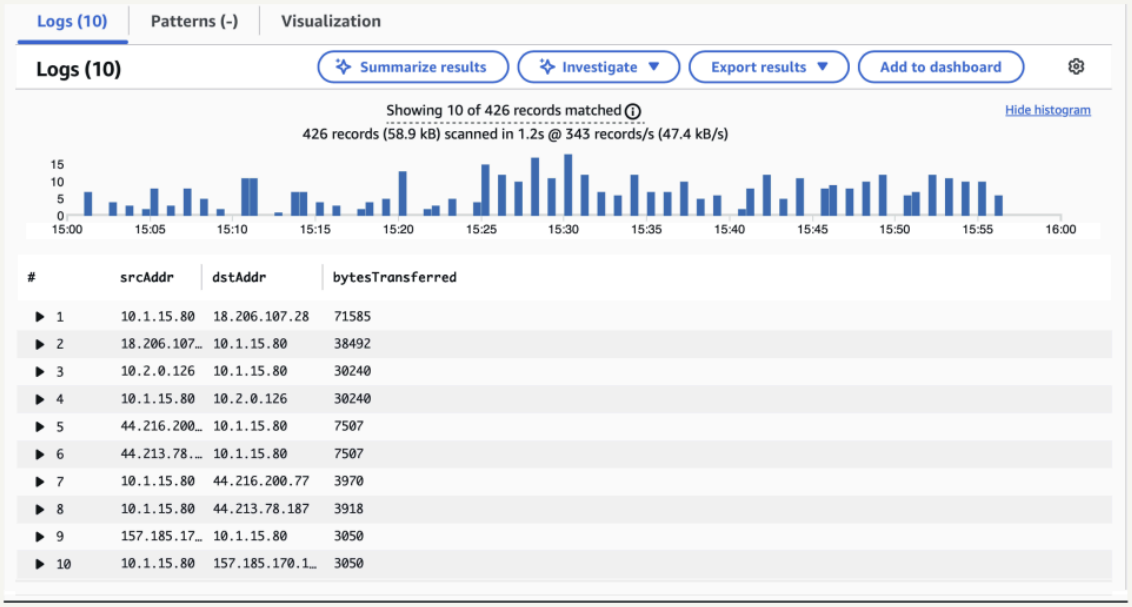
VPC Monitoring with Flow Logs

Erik Gonzalez



Introducing Today's Project!

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to analyze logs from different traffic sources and study their details. I used VPCs, and created policies, and IAM roles and subnets.

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

One thing I didn't expect in this project was how similar the logs are compared to a SIEM like Splunk.

This project took me...

This project took me about 2 and a half hours to complete.

In the first part of my project...

Step 1 - Set up VPCs

In this step, I will set up two VPCs in minutes using the VPC wizard.

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 and set up a space that stores all of these records.

Step 4 - Set IAM permissions for Logs

In this step, I will grant VPC Flow Logs the permission to write logs and send them to CloudWatch and finish setting up my subnet's flow log.

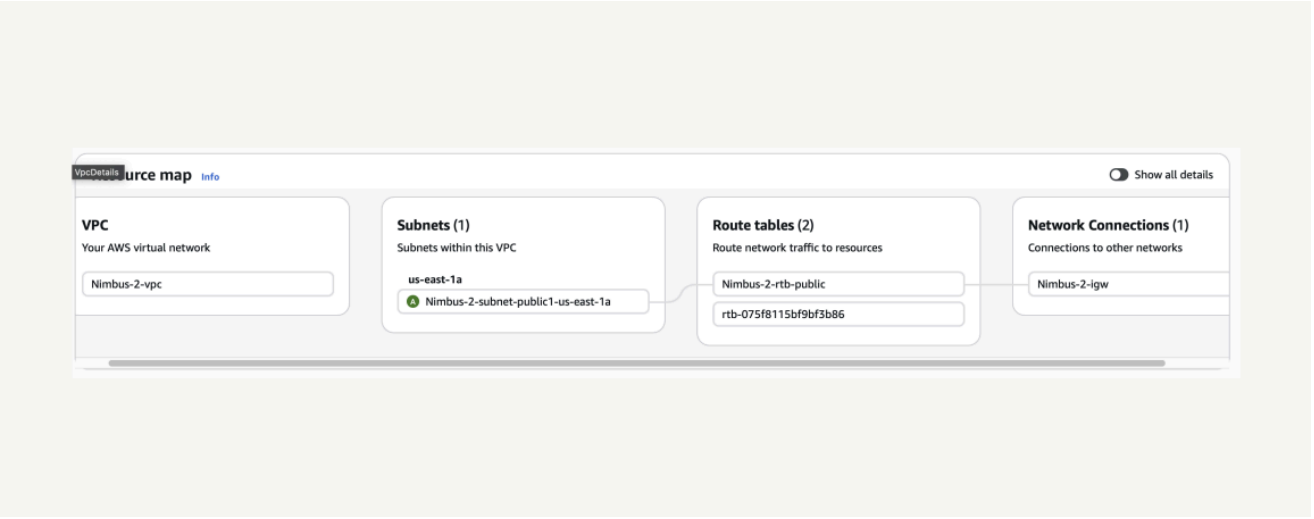
Multi-VPC Architecture

I started my project by launching two VPCs with one AZ, one public subnet and zero private subnets.

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 overlapping subnets will cause conflict with one another.

I also launched EC2 instances in each subnet

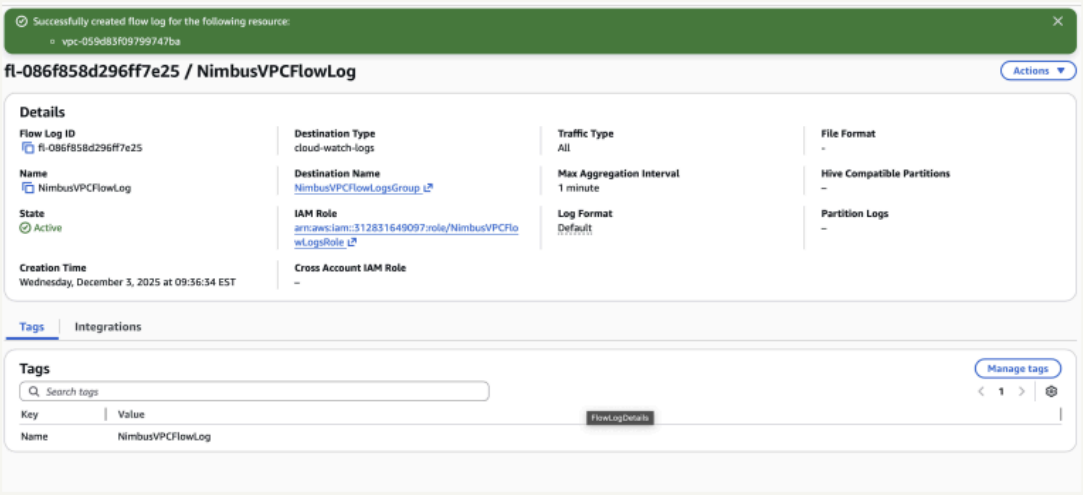
My EC2 instances' security groups allow all ICMP traffic to flow.



Logs

Logs are real-time records/entries of collected data from incoming sources. 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 doing what.

Log groups are like big folders in AWS where you keep related logs together.



IAM Policy and Roles

I created an IAM policy because I wanted to define a rule that allows all policy holders e.g. the VPC Flow Logs service the ability to create log streams and upload them into CloudWatch.

I also created an IAM role because services like VPC flow have to be associated with a role instead of JSON. Creating an IAM role will be necessary to give my VPC flow logs the access it needs to record and upload logs.

A custom trust policy is a specific type of policy that is used for designing who/what is allowed access to the IAM role.

In the second part of my project...

Step 5 - Ping testing and troubleshooting

In this step, I will get Instance 1 to send test messages to Instance 2 to test if they can communicate.

Step 6 - Set up a peering connection

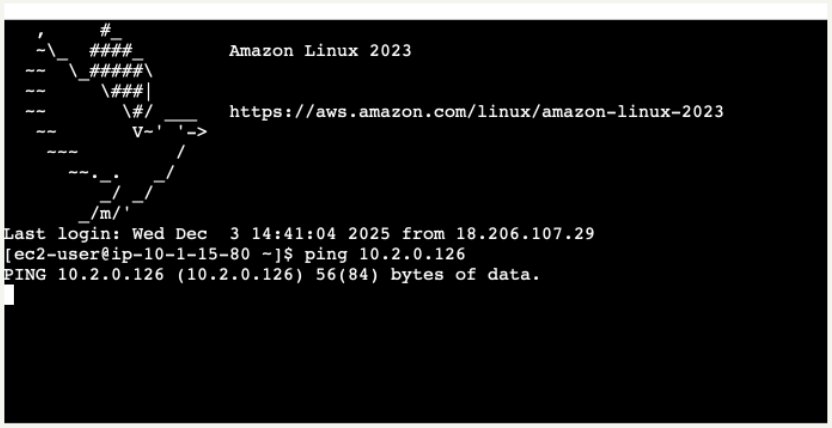
In this step, I will set up a peering connection so that VPCs 1 and 2 can talk directly with each other.

Step 7 - Analyze flow logs

In this step, I will review the flow logs recorded about VPC 1′s public subnet and analyse the flow logs to get some valuable insights.

Connectivity troubleshooting

My first ping test between my EC2 instances had no replies, which means ICMP traffic could be blocked by security groups/network ACLs; or maybe the traffic is being routed to the wrong path.



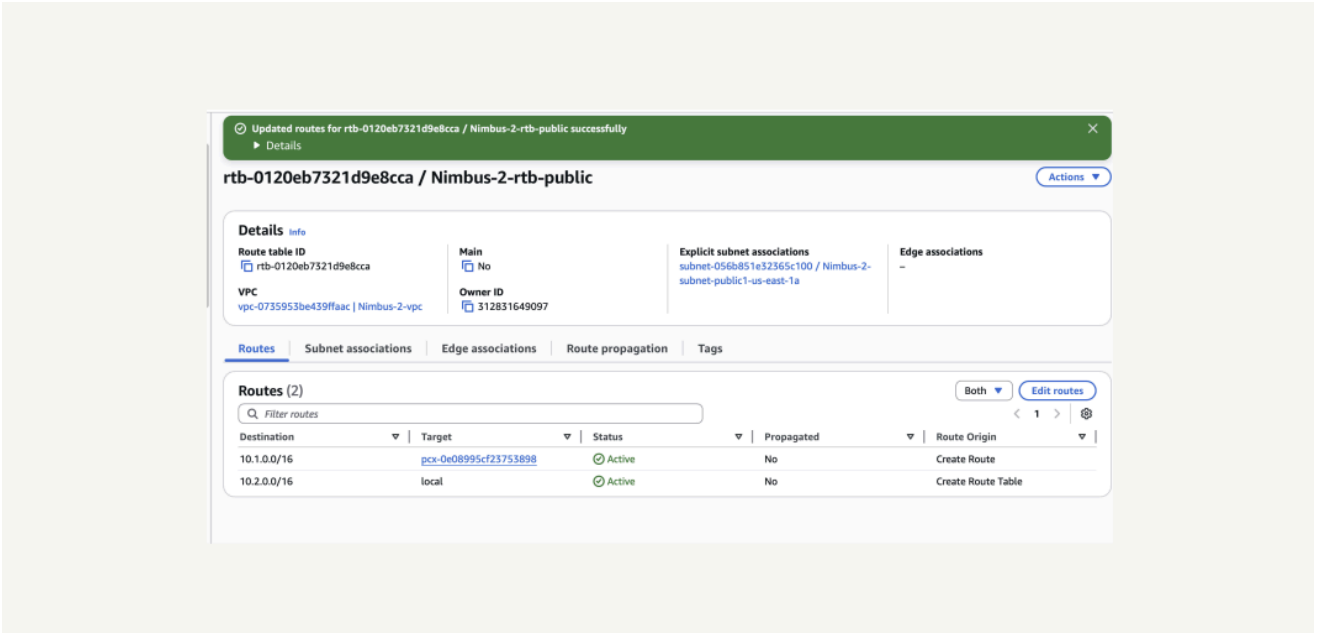
I could receive ping replies if I ran the ping test using the other instance's public IP address, which means my second instance is actually allowing ICMP traffic.

Connectivity troubleshooting

Looking at VPC 1's route table, I identified that the ping test with Instance 2's private address failed because I do not have a route in my VPC's route table that directs traffic from one VPC to another.

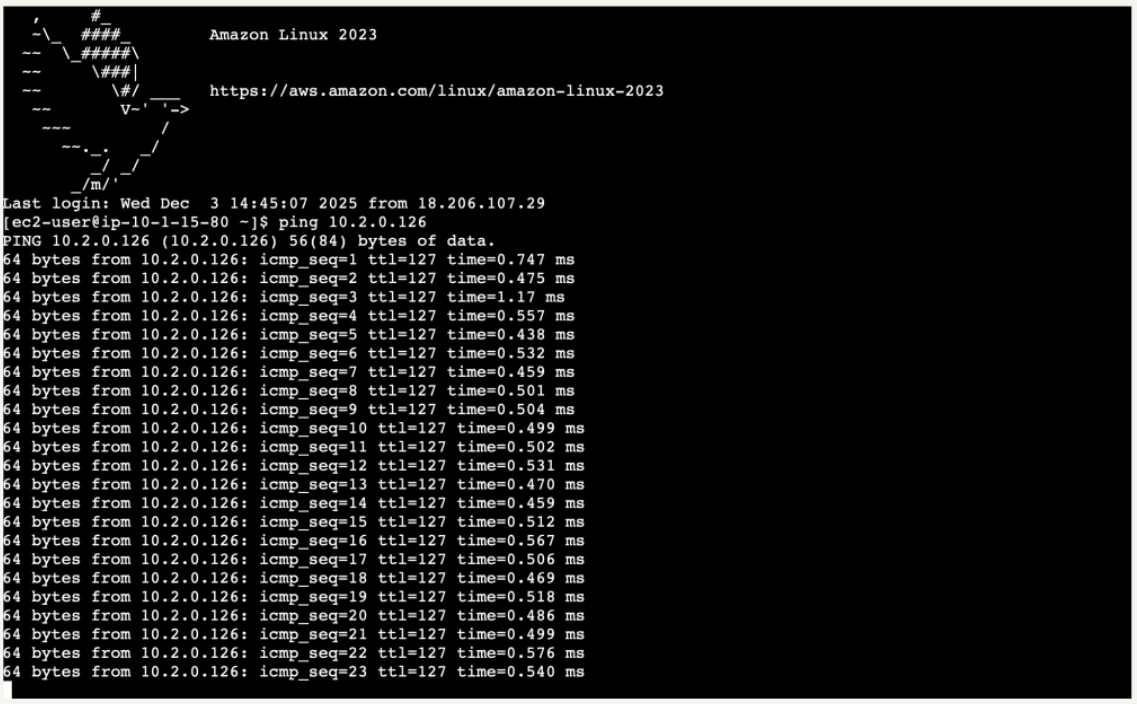
To solve this, I set up a peering connection between my VPCs

I also updated both VPCs' route tables, so that traffic from one of the VPCs and heading to the other VPC's private IPv4 address can get directed to go through the peering connection instead of the public internet.



Connectivity troubleshooting

I received ping replies from Instance 2's private IP address! This means setting up the peering connection and then the route table solved the connectivity error of the VPC's traffic not being able to navigate from one VPC to another.



Analyzing flow logs

Flow logs tell us about the source and destination of the network traffic, the amount of data being transferred, whether the traffic was accepted/rejected.

For example, the flow log I've captured tells us that traffic went from 10.1.15.80 to 157.185.170.119 and it was accepted.

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 'Return the top 10 byte transfers by source and destination IP addresses.' This query analyzes the top 10 biggest data transfers between IP addresses in my network. My private IP addresses and EC2 instances are recorded here! 10.1.15.80 - VPC 1 10.2.0.126 - VPC 2