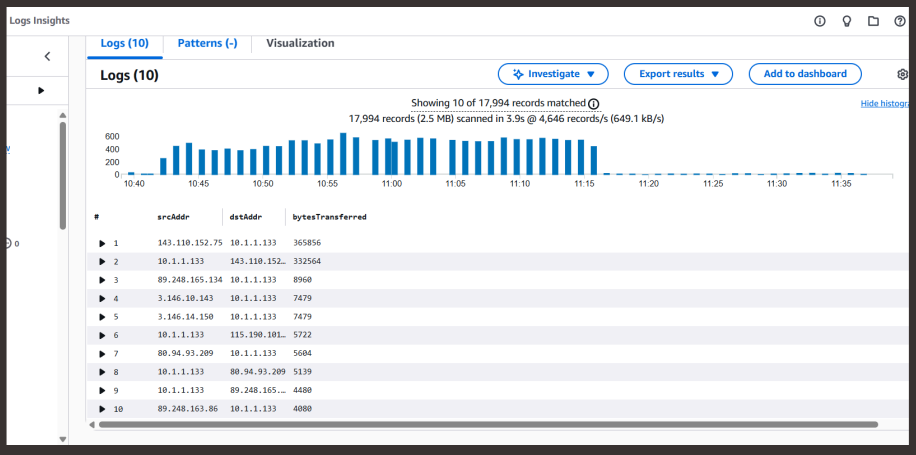
nextwork.org

VPC Monitoring with Flow Logs

Joba Amunigun
https://www.linkedin.com/in/dvoice



Joba Amunigun
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) is a private, isolated section of the AWS cloud where you can launch and manage your AWS resources—like EC2 instances, databases, and more—within a custom-defined network. You have full control over things like IP address ranges, subnets, route tables, internet gateways, and security settings. It’s useful because it allows you to create a secure and customizable network environment, similar to having your own data center, but in the cloud. With VPC, you can control how your resources connect to each other, to the internet, and to other AWS services—making it ideal for secure application hosting, compliance, scalability, and performance.

How I used Amazon VPC in this project

In today's project, I acheived two big milestones! Firstly, I learnt to troubleshoot VPC peering , connectivity issues and secondly, I learnt to monitor network traffic using VPC Flow Logs!

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

Logs Insights has lots of inbuilt Queries that gives many options on how to analyze network traffics! That was exciting

Joba Amunigun
NextWork Student

This project took me...

This project took me about 3 hours + including study time


Joba Amunigun
NextWork Student

In the first part of my project...

Step 1 - Set up VPCs

In this step , I will be creating two VPCs from scratch - Network Monitoring can still be done with single VPC, but I will be settings up two VPCs today so that i can revise some learnings from the previous project (VPC peering) too!

Step 2 - Launch EC2 instances

In this step, I will be launching two EC2 Instances - One in each VPC. Doing this is important to set up the remainder of this project - EC2 Instance will generate traffic that VPC Flow Logs will monitor.

Step 3 - Set up Logs

In this step, I am setting up VPC Flow logs to start monitoring VPC traffics (To track all inbound and outbound network traffic). and I will also be setting up storage space for my Flow Logs

Step 4 - Set IAM permissions for Logs

In this step, I will provide VPC Flow Logs the permission to write logs and upload them into my Log groups in CloudWatch

Joba Amunigun
NextWork Student

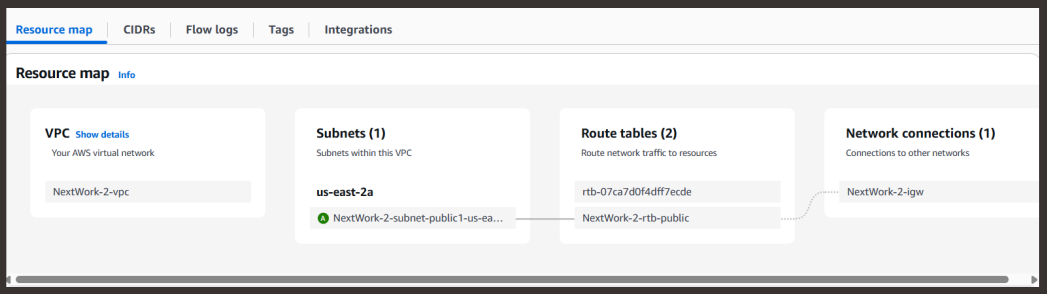
Multi-VPC Architecture

I started this project by launching 2 VPCs ! I created 2 public subnets (i.e. One in each VPC) with no Private subnets

The CIDR blocks for VPCs 1 and 2 are "10.1.0.0/16" and "10.2.0.0/16" respectively. They have to be unique so that the IP addresses of their resources don't overlap. Having overlapping IP addresses could cause routing conflicts and connectivity issues!

I also launched EC2 instances in each subnet

My EC2 instances' security groups allows SSH traffic and ICMP type traffic. This is because EC2 Instance will need access to the EC2 Instance using SSH type traffic and I will need ICMP type traffic for connectivity test later.

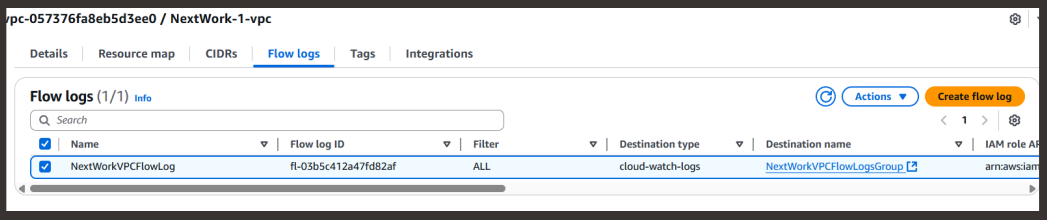


Joba Amunigun
NextWork Student

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 doing what.

Log groups is like 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 region it was created, although you can use CloudWatch dashboards to bring together logs from different regions.




Joba Amunigun
NextWork Student

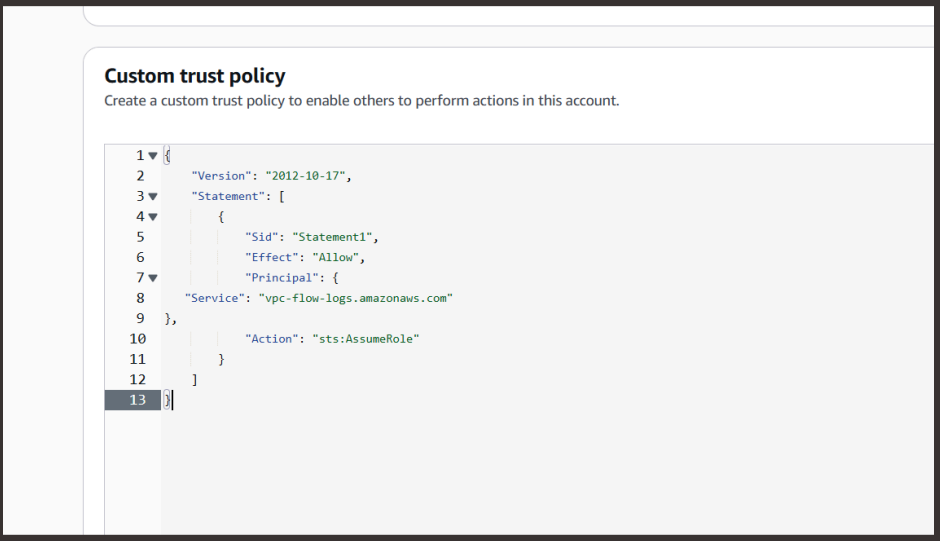
IAM Policy and Roles

I created an IAM policy because VPC Flow Logs by default don't have the permission to record logs and store them in my CloudWatch log group. This policy makes sure that my VPC can now send log data to your log group

I also created an IAM role because services like VPC Flow Logs have to be associated with a role instead of JSON and 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! Used to very narrowly define who can use a role. Here's another way to think about it: using a custom trust policy is like using a special VIP list - only the services you pinpoint in your policy would be allowed to use your role.

Joba Amunigun
NextWork Student



In the second part of my project...

Step 5 - Ping testing and troubleshooting

Right now, I'm going to trigger some network traffic from my EC2 in VPC 1 to the EC2 in VPC 2. This will test that my VPC peering is properly set up and that my flow logs are capturing traffic metadata. If I see entries in my log group showing the packet flow, I'll know both are working correctly

Step 6 - Set up a peering connection

In this step, I am going to be setting up a pairing connection link so that VPCs 1 and 2 can communicate with each other.

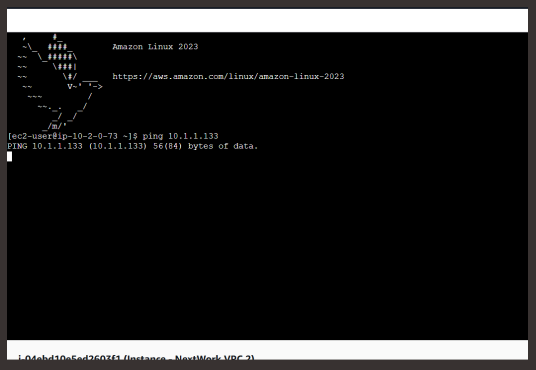
Step 7 - Analyze flow logs

In this step, I'm going to review the flow logs from VPC 1's public subnet to see what traffic has been recorded. I'll analyze the data to understand how my instances communicated, check if traffic was accepted or rejected, and make sure the monitoring setup is giving me useful insights about my network

Joba Amunigun
NextWork Student

Connectivity troubleshooting

My first ping test between my EC2 instances had no replies, which means that there's a problem with the connection. Hence,the instance in VPC 2 is not recieving any message from instance in VPC 2.- Also since i am testing my VPC peering setup at the same time it equally means that a connection is yet to be established



I could receive ping replies if I ran 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 if it traffic goes across the public internet!

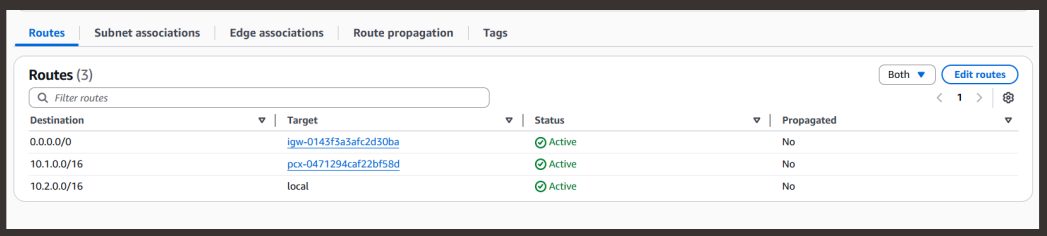
Joba Amunigun
NextWork Student

Connectivity troubleshooting

Looking at VPC 1's route table, I identified that the ping test with Instance 2's private address failed because there is no direct route to VPC 2 from VPC 1 in the route table - The missing ingredient in our architecture is the VPC peering connection that directly connects VPCs 1 and 2.

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

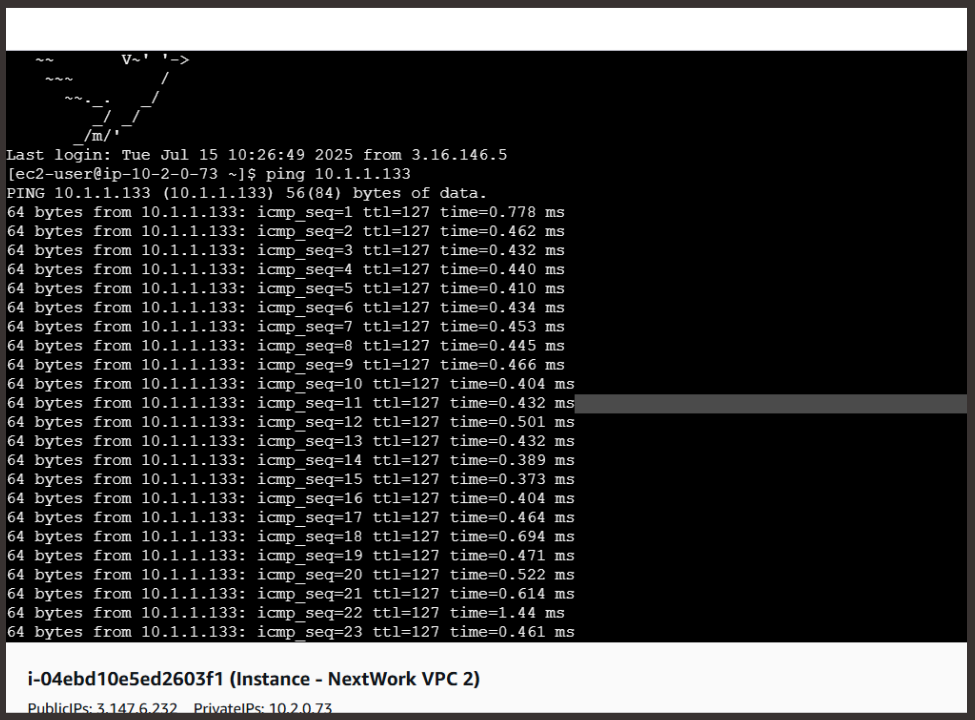
I also updated both VPCs' route tables so that traffic in VPC 1 would know how to get to resources in VPC 2 - Even if peering connection has been accepted, traffic in VPC 1 won't know how to get to resources in VPC 2 without a route in the route table! Hence,there is a need to set up a route that directs traffic bound for VPC 2 to the peering connection I have set up.



Joba Amunigun
NextWork Student

Connectivity troubleshooting

I received ping replies from Instance 2's private IP address! This means my VPCs are talking to each other! Hence! The connectivity issue has been resolved by setting up a peering architecture between VPC1 and VPC2!




Joba Amunigun
NextWork Student

Analyzing flow logs

Flow logs tell us about the details of traffic going in and out of resources in our VPC, such as EC2 instances. Each flow log entry is made up of multiple parts that help us understand the traffic behavior. The version tells us the format of the log record, while the AWS account ID identifies which account the network interface belongs to. The network interface ID (ENI) shows which interface handled the traffic. The source IP is where the traffic came from, and the destination IP is where the traffic was going. The source and destination ports tell us which ports were used on each end, and the protocol (e.g., TCP or UDP) tells us what kind of communication was used. We also see how many packets were sent and the total bytes transferred. The start and end times show when the traffic occurred, using Unix timestamps. The action field tells us if the traffic was allowed or blocked (ACCEPT or REJECT), and the log status shows whether the flow log was successfully recorded—like "OK" for succ

For example, the flow log I've captured tells us that 1 packet carrying 44 bytes of data was sent from IP address 143.110.152.75 to destination IP 10.1.1.133 using TCP protocol (protocol 6) on source port 56142 and destination port 20167. The traffic occurred between the timestamps 1752577951 and 1752578009 (Unix time), and it was allowed through, as indicated by the "ACCEPT" status. The log status is "OK", meaning this traffic flow was successfully recorded. The network interface handling this traffic was eni-0ba4fb34d7e9a41ff.

Timestamp	Message
	There are older events to load. *Load more.*
2025-07-15T11:12:31.000Z	2 394971810761 eni-0ba4fb34d7e9a41ff 143.110.152.75 10.1.1.133 56142 20167 6 1 44 1752577951 1752578009 ACCEPT OK

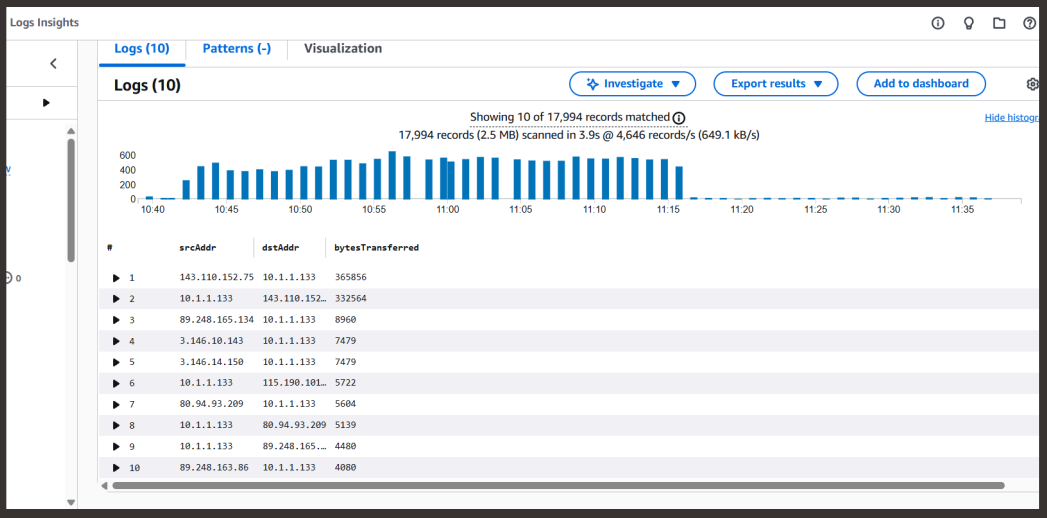
2 394971810761 eni-0ba4fb34d7e9a41ff 143.110.152.75 10.1.1.133 56142 20167 6 1 44 1752577951 1752578009 ACCEPT OK

Joba Amunigun
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 flow logs collected on EC2 Instance 1,and will return the top 10 biggest data transfers between IP addresses in my network .



nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects