nextwork.org

VPC Monitoring with Flow Logs

Sanjana Tripathy

Sanjana Tripathy
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) lets you create a private, isolated network within AWS. It gives you full control over IP ranges, subnets, route tables, and gateways, allowing secure and scalable deployment of AWS resources in a virtual network.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to set up two VPCs, establish VPC peering between them, and enable VPC Flow Logs. This allowed me to monitor and analyze network traffic using Amazon CloudWatch for better visibility and troubleshooting.

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

One thing I didn’t expect in this project was how insightful CloudWatch would be. I was surprised by the amount of detailed information it provided—it was eye-opening to see how powerful monitoring tools can be. A great learning experience!

Sanjana Tripathy
NextWork Student

This project took me...

This project took me 2 hours to complete.

In the first part of my project...

Step 1 - Set up VPCs

In this step we are going to create VPCs from scratch.

Step 2 - Launch EC2 instances

In this step, will be launching instances in both created VPCs. They will be used lator when I test VPC connectivity peering.

Step 3 - Set up Logs

In this step, I'm setting up a way to track all inbound and outbound network traffic by enabling VPC Flow Logs. These logs help monitor, troubleshoot, and analyze traffic patterns. I'll also create a log group in CloudWatch to store these records.

Step 4 - Set IAM permissions for Logs

In this step, I'll grant VPC Flow Logs the required permissions to send data to CloudWatch by creating an IAM role and policy. Then, I'll enable flow logs for my subnet to start capturing and monitoring network traffic.

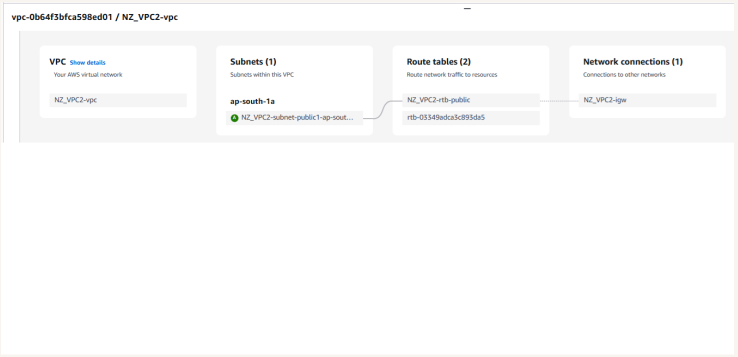
Multi-VPC Architecture

I created two VPCs from scratch using the AWS Management Console, leveraging the simplified VPC creation wizard.Each VPC had one public subnet placed in a single Availability Zone. No private subnets were created.

The IPv4 CIDR blocks for VPCs 1 and 2 must be unique to avoid IP address conflicts. VPC peering relies on distinct IP ranges so that route tables can properly direct traffic. Overlapping CIDR blocks would confuse routing and block communication.

I also launched EC2 instances in each subnet

My EC2 instance's security group allows ICMP traffic from all IP addresses to enable successful ping tests. Since ping relies on the ICMP protocol, allowing traffic from all sources ensures smooth connectivity testing across networks.

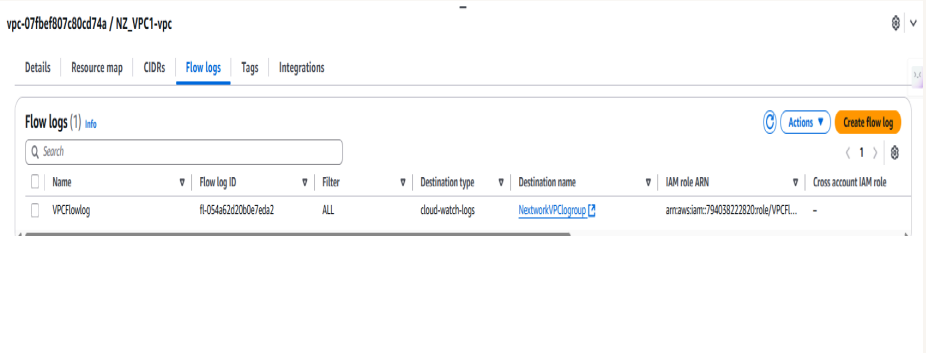

vpc-0b64f3bfca598ed01 / NZ_VPC2-vpc
VPC Show details
Your AWS virtual network
NZ_VPC2-vpc
Subnets (1)
Subnets within this VPC
ap-south-1a
NZ_VPC2-subnet-public1-ap-sout...
Route tables (2)
Route network traffic to resources
NZ_VPC2-rtb-public
rtb-03349adca5c893da5
Network connections (1)
Connections to other networks
NZ_VPC2-igw

Sanjana Tripathy
NextWork Student

Logs

Logs are detailed records of events or actions that occur within a system or application. In AWS, logs help track activity, detect issues, and ensure security by capturing information like IP addresses, traffic type, and allowed or denied connections

A log group in AWS CloudWatch is a container for organizing and storing related log streams. It helps group logs from similar resources (like EC2 or VPC flow logs), making it easier to manage, monitor, and analyze logs for performance and security.



IAM Policy and Roles

I created an IAM policy to define the specific permissions VPC Flow Logs need to write data to CloudWatch Logs. This ensures secure and controlled access when capturing and storing network traffic logs.

I also created an IAM role because VPC Flow Logs needs permission to send log data to CloudWatch. The role defines what actions AWS services can perform, ensuring logs are securely and correctly delivered to the monitoring destination.

A custom trust policy is a JSON document that defines which AWS service or user is allowed to assume a role. In VPC Flow Logs, it allows services like vpc-flow-logs.amazonaws.com to use the IAM role to deliver logs securely to CloudWatch.

Custom trust policy

Create a custom trust policy to enable others to perform actions in this account.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Principal": {
                "Service": "vpc-flow-logs.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

In the second part of my project...

Step 5 - Ping testing and troubleshooting

In this step, we're generating network traffic from our instance in VPC 1 to our instance in VPC 2 to test if flow logs capture the activity. This also serves as a check on our VPC peering setup—validating both connectivity and logging in one go!

Step 6 - Set up a peering connection

In this step we will establish a VPC peering connection between my two created VPCs

Step 7 - Analyze flow logs

In this final step, it's time to dive into the logs and review what VPC Flow Logs captured about my network activity. I will examine the records from VPC 1's public subnet and analyze them to gain insights into traffic patterns and connectivity.

Connectivity troubleshooting

My first ping test between my EC2 instances has no replies, which means the traffic isn't reaching the destination. This suggests that something is blocking communication between the VPCs—possibly a missing route or configuration.

I can receive ping replies when using the other instance's public IP address, which means both instances have internet access and their security groups allow ICMP traffic but they're not communicating privately,indicating VPC peering isn't set up yet

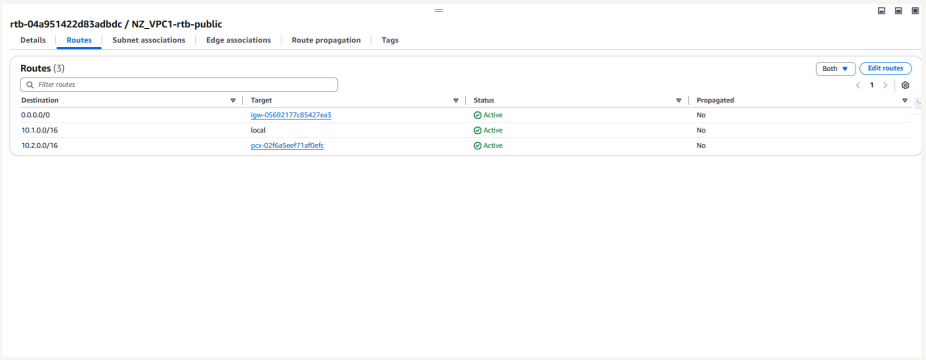
Sanjana Tripathy
NextWork Student

Connectivity troubleshooting

The ping test using Instance 2's private IP address fails because a VPC peering connection hasn't been established yet—without it, private IP communication between the two VPCs isn't possible.

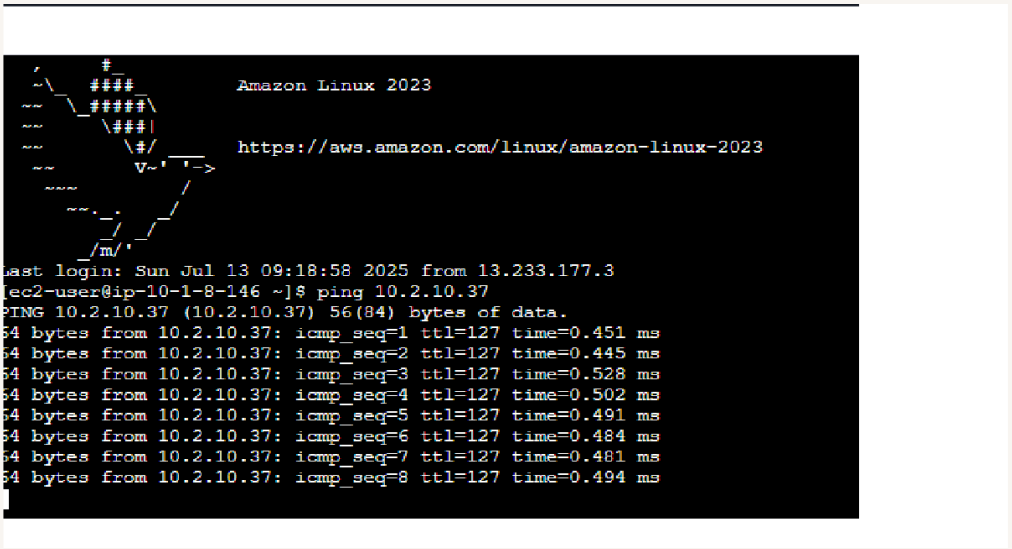
To solve this, I set up a peering connection between my VPCs

I updated my VPCs' route tables to enable traffic flow between the two VPCs after establishing a peering connection. Without these updates, the VPCs wouldn't know how to reach each other—even if the peering connection exists.



Connectivity troubleshooting

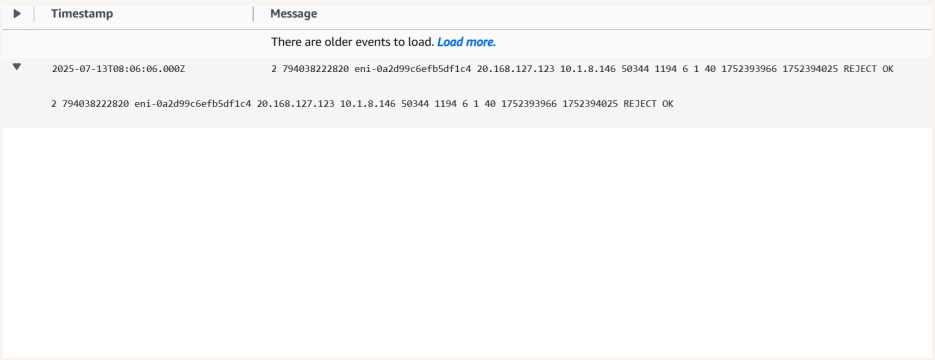
I received ping replies from Instance 2's private IP address, confirming that VPC peering is working correctly. The private instances in different VPCs can now communicate securely over their internal IPs—successfully validating our setup!



Analyzing flow logs

A flow log includes key parts like source and destination IP addresses, protocol used (e.g., TCP), port numbers, number of packets, number of bytes, action taken (e.g., ACCEPT or REJECT), data packets transferred and total no of bytes transferred.

For example, the flow log I've captured tells us:the source and destination PI addresses are 20.168.127.123 and 10.1.8.146.The protocol is TCP(6).1 data packet and total of 40 bytes of data is transferred during this session.

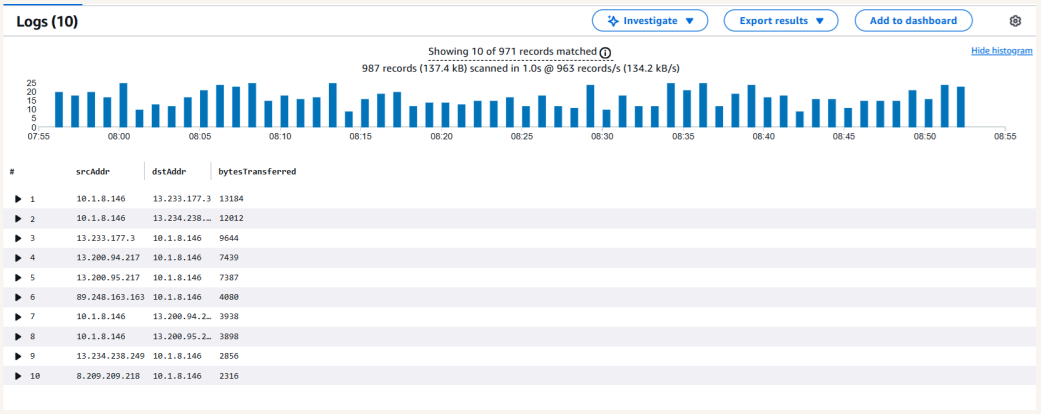


Sanjana Tripathy
NextWork Student

Logs Insights

Log Insights is a powerful feature in Amazon CloudWatch that lets you run queries on log data to quickly analyze and troubleshoot issues, spot trends, and gain real-time insights—all from within your AWS environment.

I ran the query:stats sum(bytes) as bytesTransferred by srcAddr, dstAddr | sort bytesTransferred desc | limit 10. This Query gives ten pairs of source and destination IP addresses that transferred the most data between them out of all flow logs.



The place to learn & showcase your skills

Check out nextwork.org for more projects