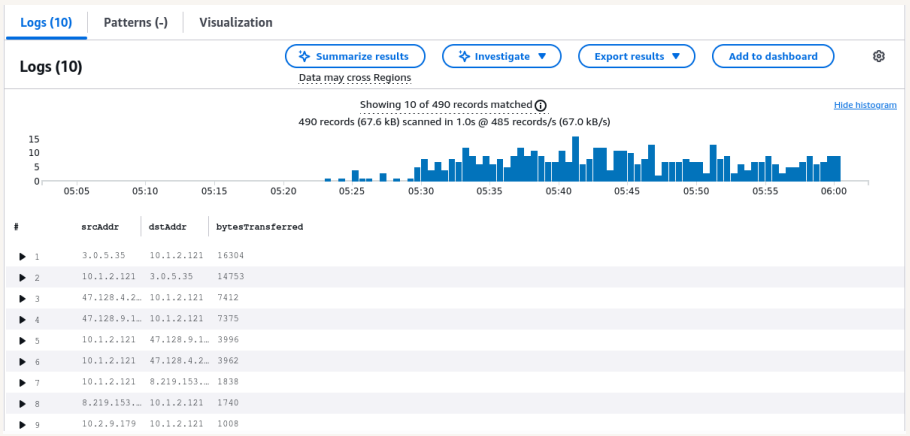
nextwork.org

VPC Monitoring with Flow Logs

Sean Calderon



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is for providing secure, reliable and scalable network infrastructure. VPC is useful for network administrators of the cloud to analyze and monitor traffic and troubleshoot using detailed logs generated.

How I used Amazon VPC in this project

In this project, I used Amazon VPC to monitor my traffic from going back and forth on VPC to VPC and analyze each generated log.

This project took me...

I took this project almost an hour. It was rewarding to see logs flowing like streams that records all traffic whether the traffic is allowed or denied.

In the first part of my project...

Step 1 - Set up VPCs

In this step, I am going to start my project from scratch and use VPC wizard to create two VPCs within seconds.

Step 2 - Launch EC2 instances

In this step, I will launch an EC2 instance in each VPC, so I can use them to test my VPC peering connection later.

Step 3 - Set up Logs

In this step, I am now ready to start my VPC monitoring journey. I am going to setup flow logs that monitors inbound and outbound traffic and also setup up where to store these logs.

Step 4 - Set IAM permissions for Logs

VPC Flow Logs doesn't have the permission to write logs and send them to CloudWatch yet. So in this step, I give VPC Flow Logs permission to write logs and send them to cloudwatch.


Sean Calderon
NextWork Student

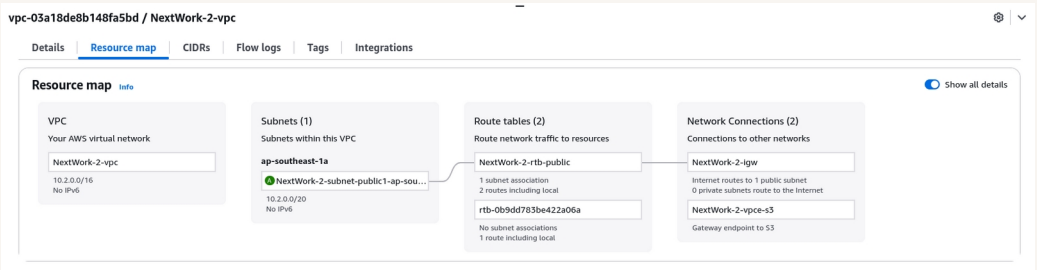
Multi-VPC Architecture

I started my project by launching two VPCs with non-overlapping CIDR blocks.

The CIDR blocks for VPCs 1 and 2 are unique and non-overlapping. They have to be unique because it is impossible to route traffic to the destination that is actually destined to another network causing network conflicts.

I also launched EC2 instances in each subnet

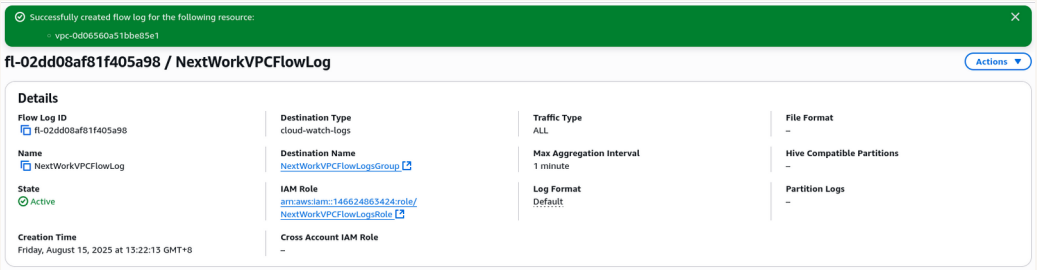
My EC2 instances' assigned security groups that allow ICMP request from neighbouring VPC's CIDR blocks. This is because I want to narrow down to CIDR blocks to prevent anyone and anywhere pinging my instances.



Logs

Logs are like a diary of a system or an application that records events and happenings that are likely generated by authentication, authorization and accounting events, and these could also be an application error, warning, or info.

Log groups are more like a folder of diary where you keep related logs together.

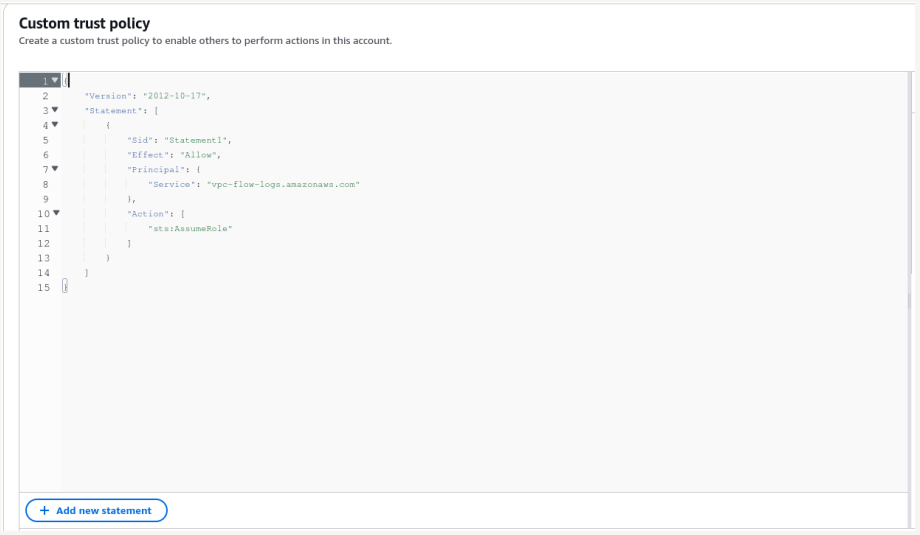


IAM Policy and Roles

I created an IAM policy because VPC Flow Logs doesn't have the permission to write logs and send them to CloudWatch yet.

I also created an IAM role because policies can't be directly attached to a service (VPC Flow Logs) but instead assigning them roles and those roles has policies attached for defining their access control.

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.


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"
]
}
]
}
+ Add new statement

In the second part of my project...

Step 5 - Ping testing and troubleshooting

In this step, I am going to generate network traffic by trying to get my instance in VPC 1 to send a message to my instance in VPC 2.

Step 6 - Set up a peering connection

In this step, I will fix the missing link that's causing this connectivity error by adding VPC peering connection to bridge my VPCs together!

Step 7 - Analyze flow logs

In this step, I will review and analyze the recorded flow logs on my VPC 1's public subnet.

Connectivity troubleshooting

My first ping test between my EC2 instances had no replies, which means there is still no dedicated route for my two VPCs.

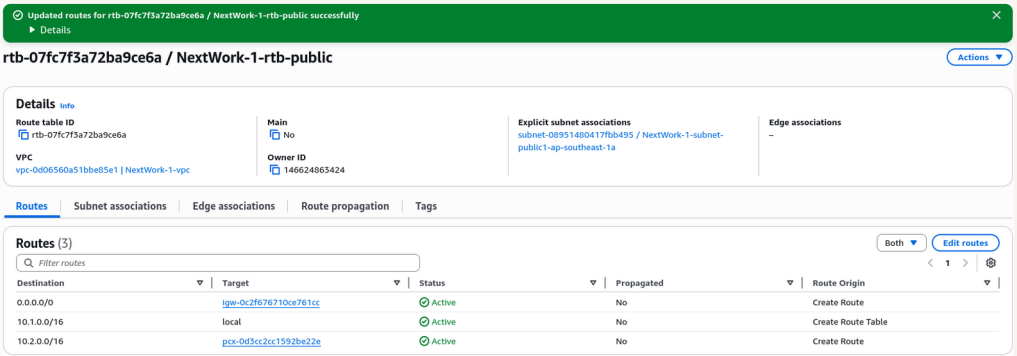
I could receive ping replies if I ran the ping test using the other instance's public IP address, which means instances from VPC 2 can reach the instances on VPC 1. However, the traffic has to go outside the internet.

Connectivity troubleshooting

Looking at VPC 1's route table, I identified that the ping test with Instance 2's private address failed because I still have a missing ingredient in my architecture which 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 they traffic can go back and forth on my network infrastructure.



Connectivity troubleshooting

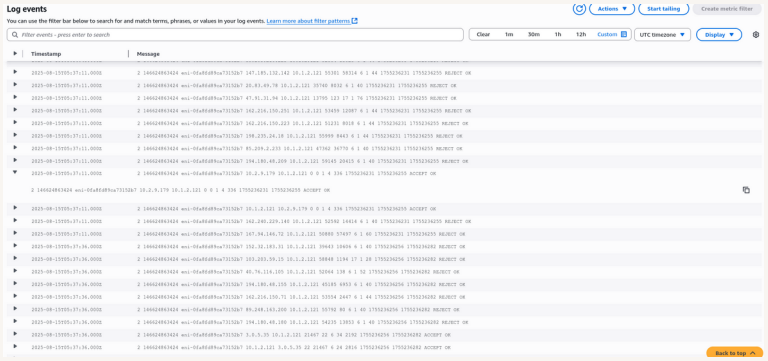
I received ping replies from Instance 2's private IP address! This means my connection or traffic can now move back and forth in my network infrastructure.

```
[ec2-user@ip-10-1-2-121 ~]$ ping 10.2.9.179
PING 10.2.9.179 (10.2.9.179) 56(84) bytes of data.
64 bytes from 10.2.9.179: icmp_seq=1 ttl=127 time=0.163 ms
64 bytes from 10.2.9.179: icmp_seq=2 ttl=127 time=0.184 ms
64 bytes from 10.2.9.179: icmp_seq=3 ttl=127 time=0.193 ms
64 bytes from 10.2.9.179: icmp_seq=4 ttl=127 time=0.270 ms
64 bytes from 10.2.9.179: icmp_seq=5 ttl=127 time=0.185 ms
64 bytes from 10.2.9.179: icmp_seq=6 ttl=127 time=0.169 ms
64 bytes from 10.2.9.179: icmp_seq=7 ttl=127 time=0.197 ms
64 bytes from 10.2.9.179: icmp_seq=8 ttl=127 time=0.184 ms
^C
--- 10.2.9.179 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7291ms
rtt min/avg/max/mdev = 0.163/0.193/0.270/0.030 ms
[ec2-user@ip-10-1-2-121 ~]$
```

Analyzing flow logs

Flow logs tell us about a traffic moving back and forth with an entrypoint interface of my VPC.

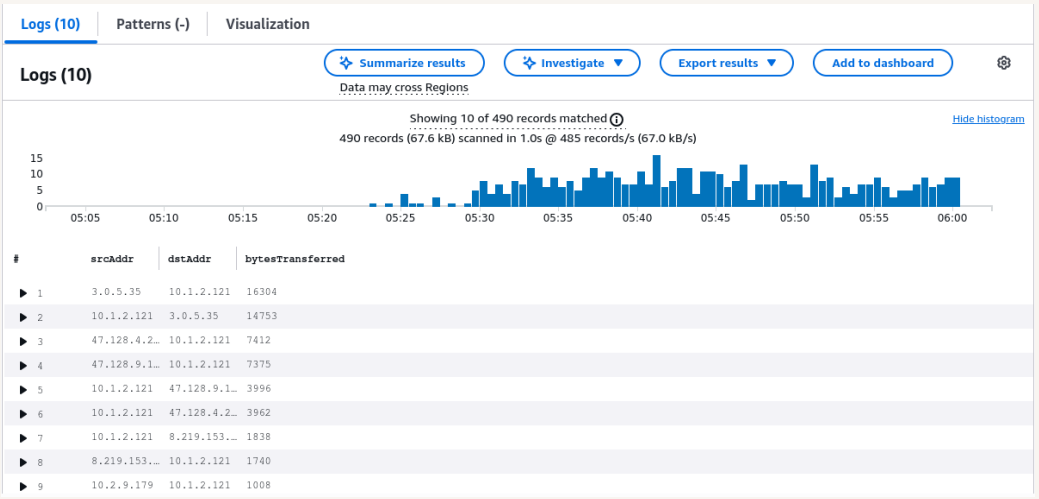
For example, the expanded flow log I've captured tells us traffic coming from a source IP address of 10.2.9.179 going to the destination IP address of 10.1.2.121 is allowed.



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 to return data with top 10 byte transfers by source and destination IP addresses. This query analyzes important returned data with detailed reports such as graphs.



The place to learn & showcase your skills

Check out nextwork.org for more projects