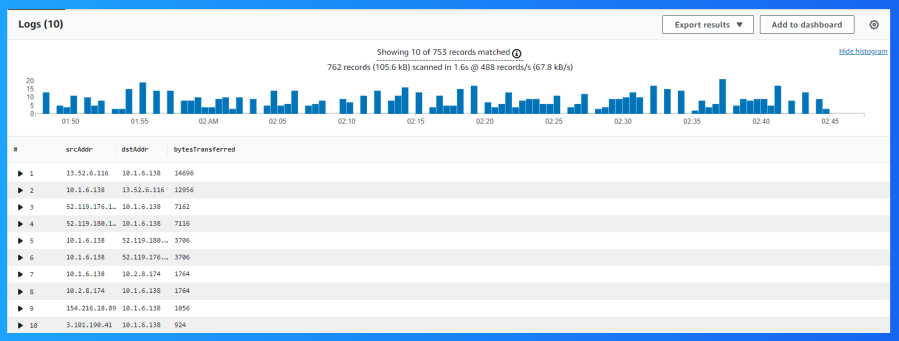
NextWork.org

VPC Monitoring with Flow Logs

mmoorejr24@gmail.com



mmoorejr24@gmail.com
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

AWS VPC is a virtual network dedicated to your AWS account, allowing you to provision and manage a logically isolated section of the AWS cloud where you can launch AWS resources.

How I used Amazon VPC in this project

I used two Amazon VPCs for peer connecting to monitor logs using the CloudWatch service.

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

I didn't expect this project to be so awesome.

This project took me...

This project took me about two hours and forty minutes to complete.

mmoorejr24@gmail.com
NextWork Student

In the first part of my project...

Step 1 - Set up VPCs

In this step we will set up two VPCs from scratch in minutes. Network monitoring can still be done with just a single VPC, but it's great to have the extra challenge and tackle VPC peering in this project too!

Step 2 - Launch EC2 instances

In this step, we launch two EC2 instances - one in each VPC. Doing this is important to set up the remainder of our project. Our EC2 instances will generate traffic that the VPC Flow Logs with monitor.

Step 3 - Set up Logs

In this step, we are setting up VPC flow logs to start monitoring network traffic. We are also setting up a storage space for our flow logs.

Step 4 - Set IAM permissions for Logs

In this step, we provide VPC Flow Logs with the permission to create logs and upload them into our log group in CloudWatch.

mmoorejr24@gmail.com
NextWork Student

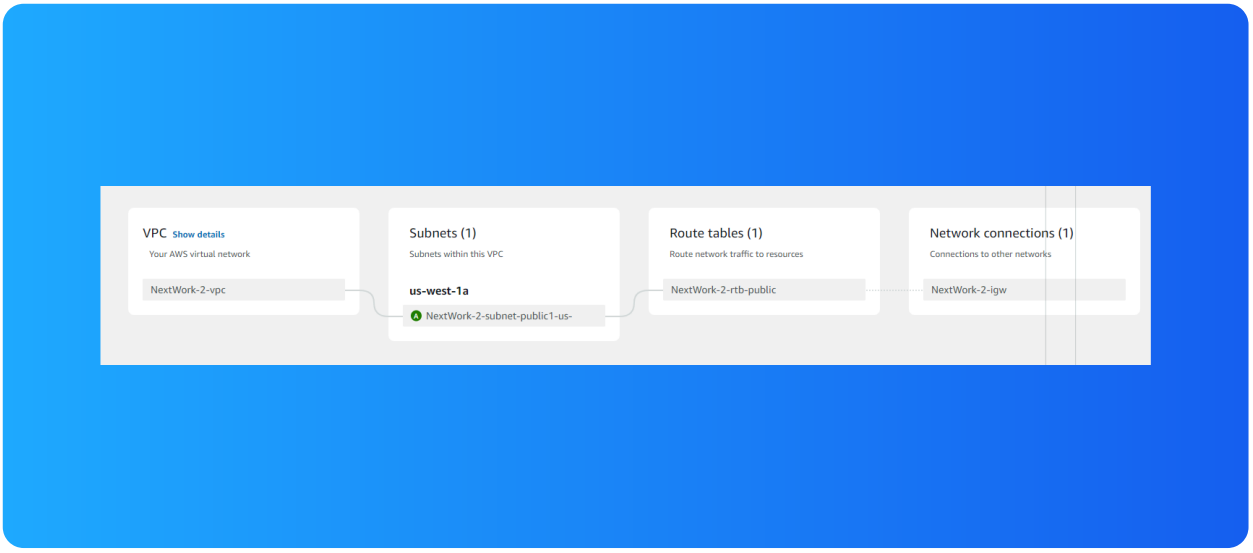
Multi-VPC Architecture

I started my project by launching two VPCs! We created two public subnets (i.e. one public subnet 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. They have to be unique because having overlapping CIDR blocks will cause network/routing traffic issues down the line when traffic is needing to go from one VPC to another.

I also launched EC2 instances in each subnet

My EC2 instances' security groups allow SSH and ICMP type traffic. This is because EC2 Instance Connect will need to access our EC2 instance using SSH-type traffic, and because we need to allow ICMP type traffic for connectivity tests later.



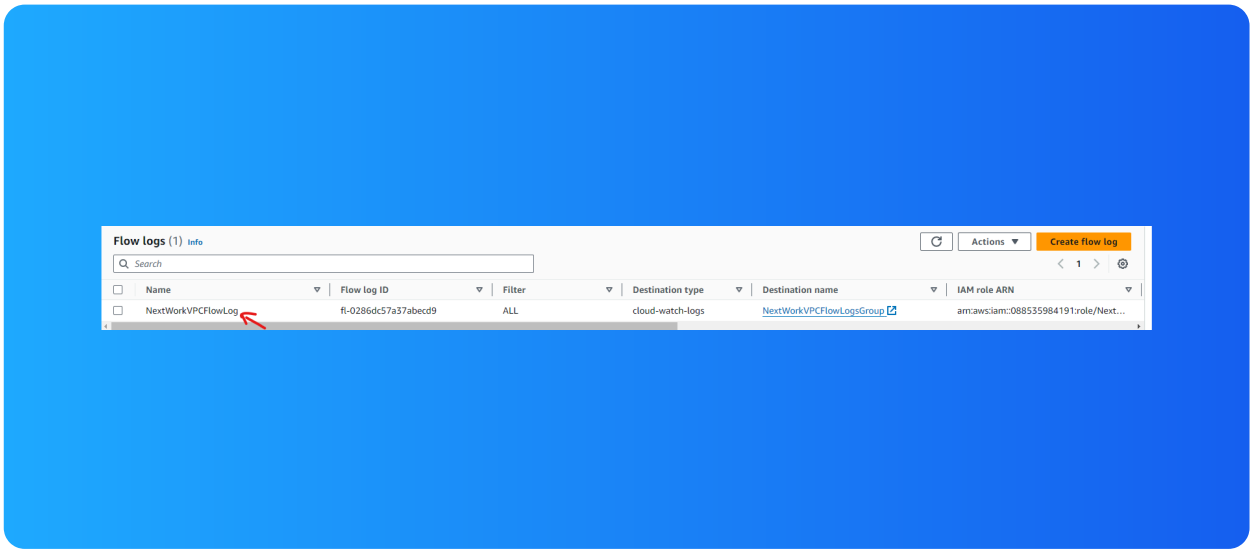
mmoorejr24@gmail.com
NextWork Student

Logs

Logs are like diary entries for my computer systems - they are detailed records of any kind of activity related to the traffic/resource/AWS service that the log is tracking.

Log groups are groupings of logs i.e. logs that belong to the project/application/source are often in a log group together!

I also set up a flow log for VPC 1



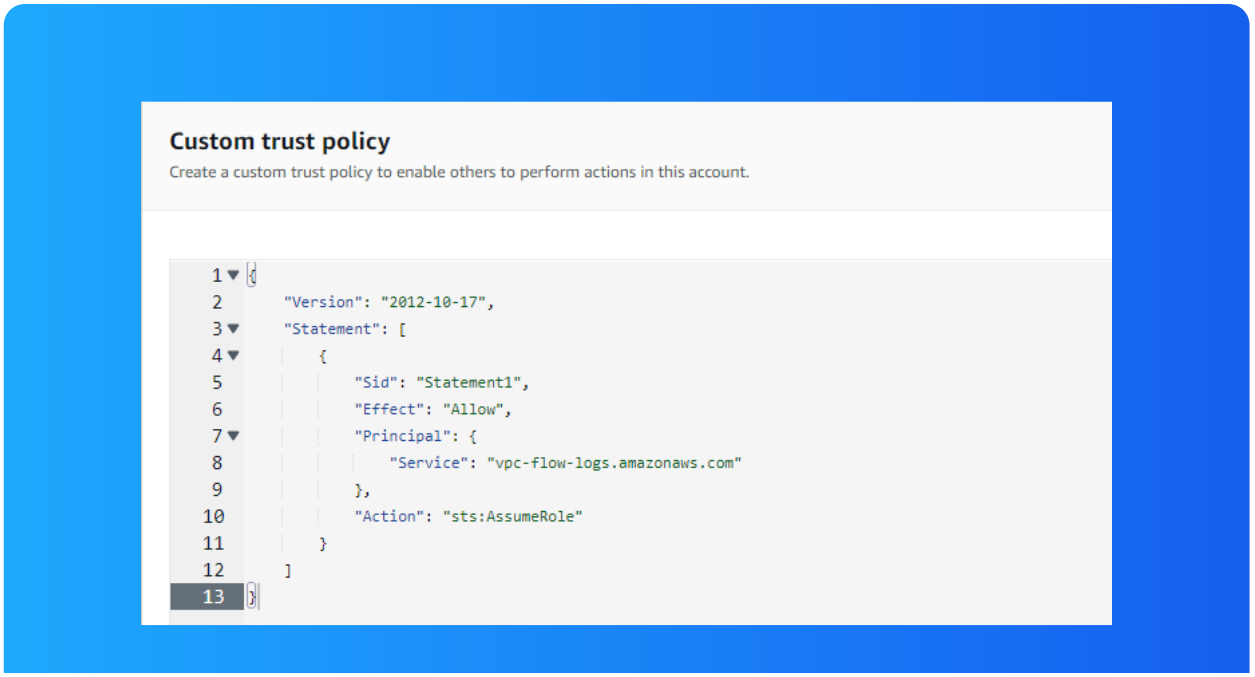
mmoorejr24@gmail.com
NextWork Student

IAM Policy and Roles

I created an IAM policy so that I can define a rule that allows policy holders e.g. our 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 Logs have to be associated with a role instead of JSON! Creating an IAM role will be necessary to give our VPC Logs the access it needs to record and upload logs.

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.




mmoorejr24@gmail.com
NextWork Student

In the second part of my project...

Step 5 - Ping testing and troubleshooting

In this step, I am generating network traffic! This becomes important when we are communicating to cloudworks/cloud networking/or cloud engineering.

Step 6 - Set up a peering connection

In this step, we are setting up a peering connection so that VPCs 1 and 2 can talk directly with each other.

Step 7 - Update VPC route tables

In this step, we are updating the route tables for our two VPCs so that traffic bound for the other VPC can be directed to the peering connection instead of the public internet.

Step 8 - Analyze flow logs

In this step, we are tracking the network data that's been collected on our VPCs, and then analyze that data to extract insights.

mmoorejr24@gmail.com
NextWork Student

Connectivity troubleshooting

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

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

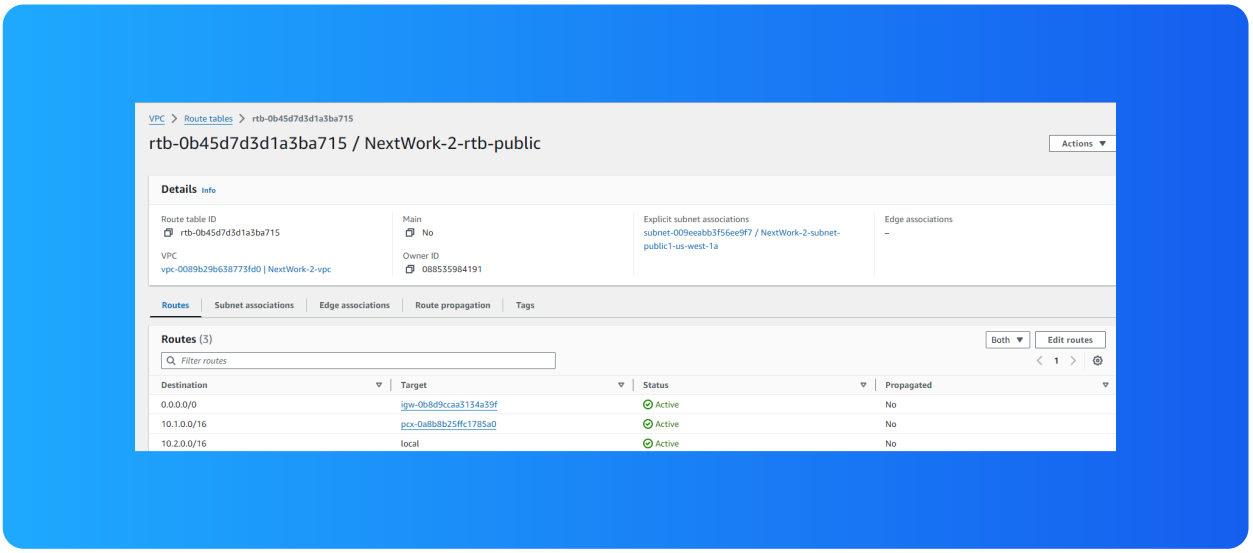
mmoorejr24@gmail.com
NextWork Student

Connectivity troubleshooting

Looking at VPC 1's route table, I identified that the ping test with Instance 2's private address failed because we do not have a route in our VPCs' route tables 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 be directed to go through the peer connection instead of the public internet.



mmoorejr24@gmail.com
NextWork Student

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 solve the connectivity error of our VPCs' traffic not being able to navigate from one VPC to another.

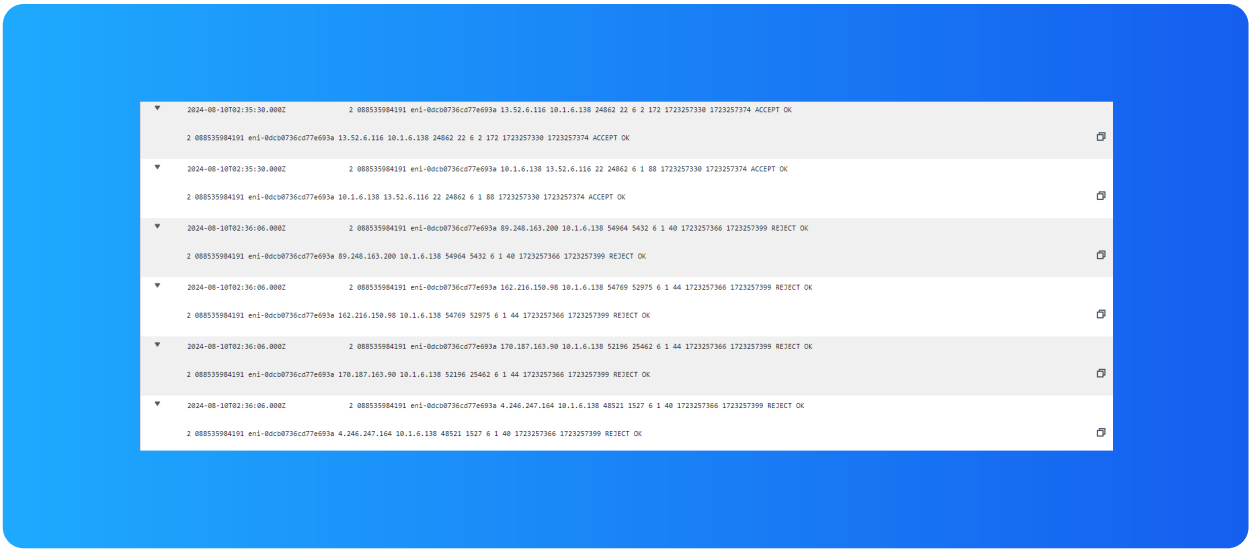
```
64 bytes from 3.101.190.41: icmp_seq=4 ttl=126 time=0.911 ms
64 bytes from 3.101.190.41: icmp_seq=5 ttl=126 time=0.741 ms
64 bytes from 3.101.190.41: icmp_seq=6 ttl=126 time=1.23 ms
^C
--- 3.101.190.41 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5192ms
rtt min/avg/max/mdev = 0.461/0.821/1.226/0.244 ms
[ec2-user@ip-10-1-6-138 ~]$ ping 10.2.8.174
PING 10.2.8.174 (10.2.8.174) 56(84) bytes of data.
64 bytes from 10.2.8.174: icmp_seq=1 ttl=127 time=1.41 ms
64 bytes from 10.2.8.174: icmp_seq=2 ttl=127 time=1.14 ms
64 bytes from 10.2.8.174: icmp_seq=3 ttl=127 time=0.915 ms
64 bytes from 10.2.8.174: icmp_seq=4 ttl=127 time=0.708 ms
64 bytes from 10.2.8.174: icmp_seq=5 ttl=127 time=0.567 ms
64 bytes from 10.2.8.174: icmp_seq=6 ttl=127 time=1.11 ms
64 bytes from 10.2.8.174: icmp_seq=7 ttl=127 time=0.985 ms
64 bytes from 10.2.8.174: icmp_seq=8 ttl=127 time=0.637 ms
64 bytes from 10.2.8.174: icmp_seq=9 ttl=127 time=1.11 ms
64 bytes from 10.2.8.174: icmp_seq=10 ttl=127 time=0.492 ms
64 bytes from 10.2.8.174: icmp_seq=11 ttl=127 time=0.730 ms
64 bytes from 10.2.8.174: icmp_seq=12 ttl=127 time=0.740 ms
64 bytes from 10.2.8.174: icmp_seq=13 ttl=127 time=0.579 ms
64 bytes from 10.2.8.174: icmp_seq=14 ttl=127 time=0.722 ms
64 bytes from 10.2.8.174: icmp_seq=15 ttl=127 time=0.870 ms
64 bytes from 10.2.8.174: icmp_seq=16 ttl=127 time=0.463 ms
64 bytes from 10.2.8.174: icmp_seq=17 ttl=127 time=0.694 ms
64 bytes from 10.2.8.174: icmp_seq=18 ttl=127 time=0.642 ms
64 bytes from 10.2.8.174: icmp_seq=19 ttl=127 time=0.849 ms
64 bytes from 10.2.8.174: icmp_seq=20 ttl=127 time=0.716 ms
64 bytes from 10.2.8.174: icmp_seq=21 ttl=127 time=0.691 ms
^C
--- 10.2.8.174 ping statistics ---
21 packets transmitted, 21 received, 0% packet loss, time 20567ms
rtt min/avg/max/mdev = 0.463/0.798/1.410/0.234 ms
[ec2-user@ip-10-1-6-138 ~]$ ping 3.101.190.41
PING 3.101.190.41 (3.101.190.41) 56(84) bytes of data.
64 bytes from 3.101.190.41: icmp_seq=1 ttl=126 time=0.472 ms
64 bytes from 3.101.190.41: icmp_seq=2 ttl=126 time=0.672 ms
64 bytes from 3.101.190.41: icmp_seq=3 ttl=126 time=0.738 ms
64 bytes from 3.101.190.41: icmp_seq=4 ttl=126 time=1.16 ms
```

mmoorejr24@gmail.com
NextWork Student

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 is being rejected or accepted.

For example, the flow log I've captured tells us that traffic went from one address to another. We can also extract that the traffic was accepted by the security groups and network ACLs of my VPC.



mmoorejr24@gmail.com
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 top 10 biggest data transfers between IP addresses in your network!

Everyone should be in a job they love.

Check out nextwork.org for more projects