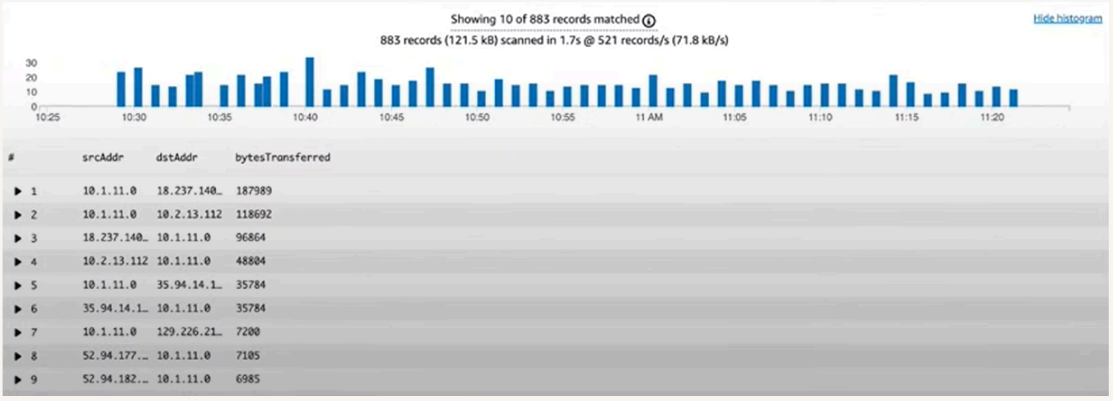
nextwork.org

VPC Monitoring with Flow Logs

LW lwazi995@outlook.com



LW
lwazi995@outlook.com
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPCs are basically cities that lets us control the underline network for our resources so we can control traffic flow and organize the resources through data packet and information.

How I used Amazon VPC in this project

In todays project we used Amazon VPC we achieved two big milestones we learnt to troubleshoot VPC peering connectivity issues. We learnt how to monitor Flow Logs using in our EC2 instances.

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

I didn't expect that the private subnet wouldn't troubleshoot in our EC2 without it being peer connected to both VPC1 and VPC2.

This project took me...

This project took me 3 hours to complete.

LW
lwazi995@outlook.com
NextWork Student

In the first part of my project...

Step 1 - Set up VPCs

I am about to Launch two VPCs, I will create two public subnets one public subnet in each VPC. With no private subnets.

Step 2 - Launch EC2 instances

We are launching two EC2 instance one in each VPC, so we can use them to test your VPC peering connection. Our EC2 instances will generate traffic that our VPC Flow Logs will 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 steps I am going to give VPC Flow Logs the permission to/create write logs and send them to CloudWatch. Also finishing the subnet flow log.

LW
lwazi995@outlook.com
NextWork Student

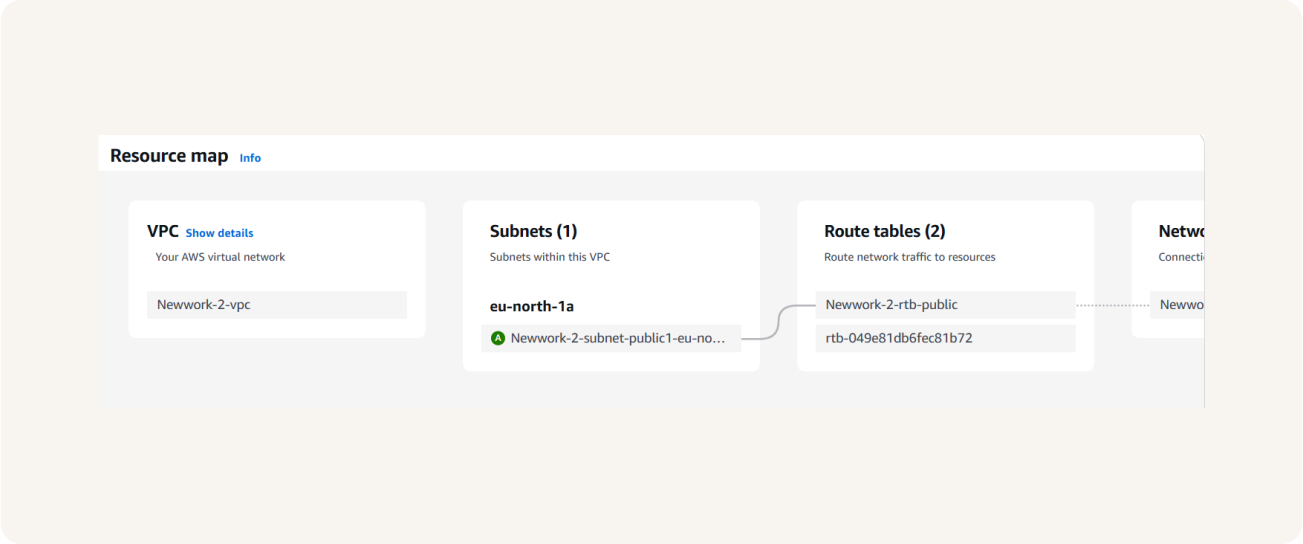
Multi-VPC Architecture

I started our project by launching two VPCs! I created two public subnets (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 respectively They have to be unique because having overlapping CIDR blocks will cause routing/traffic issues down the line when traffic is needed to go form one VPC to another.

I also launched EC2 instances in each subnet

My EC2 instances security groups allow SSH traffic and ICMP traffic type traffic. This is because EC2 instance connect will need to access our EC2 instances using SSH-type traffic, and because we need to allow ICMP type trafic for connectivity test.

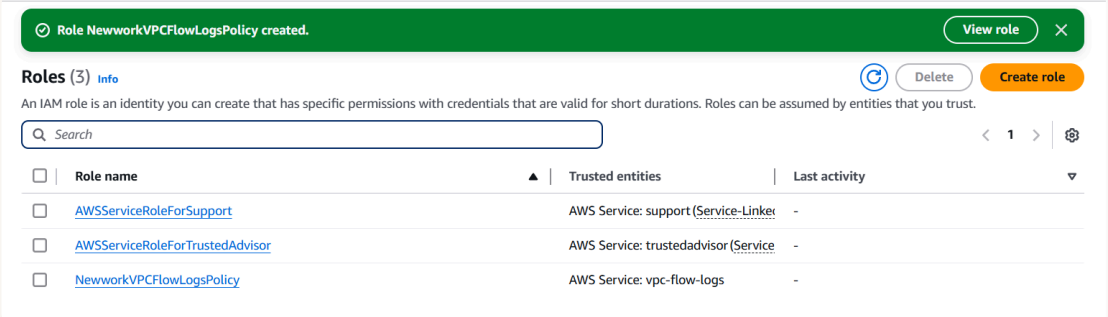


LW
lwazi995@outlook.com
NextWork Student

Logs

Logs are similar to a diary. They record everything that happens, from users logging in to errors popping up. It's the go to place to understand what is going on with your system.

This is a big folder where you keep the documentations/related of the logs together. Usually logs from the same source or application will be kept in the same log group. FYI Log data gets saved in the region it was created.



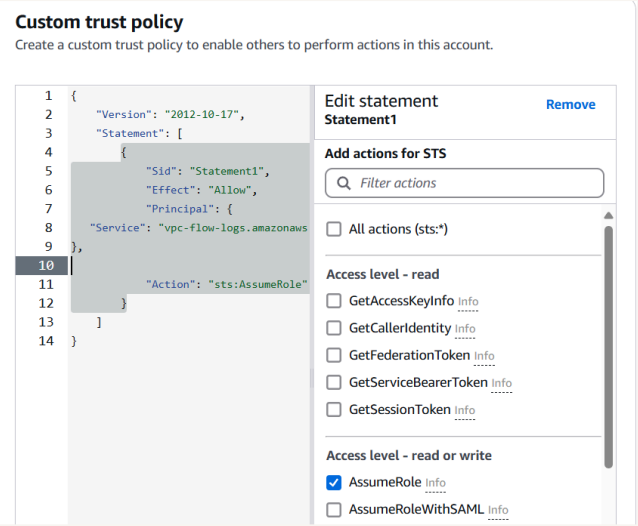
LW
lwazi995@outlook.com
NextWork Student

IAM Policy and Roles

This Policy to define the rules that allow policy holders example (VPC Flow Logs service) to be able to create log streams and upload them into the cloud watch to analyse them later.

I also created an IAM role because I assigned permission to the user attached to the policies this will be necessary to give our VPC Flow Logs the access it needs to record and upload logs.

A custom trust policy is a type of policy used to design who or what is allowed access to the IAM role.



LW
lwazi995@outlook.com
NextWork Student

In the second part of my project...

Step 5 - Ping testing and troubleshooting

In this step we are generating network traffic, this becomes important when we are communicating about cloud networks, cloud engineering and cloud works.

Step 6 - Set up a peering connection

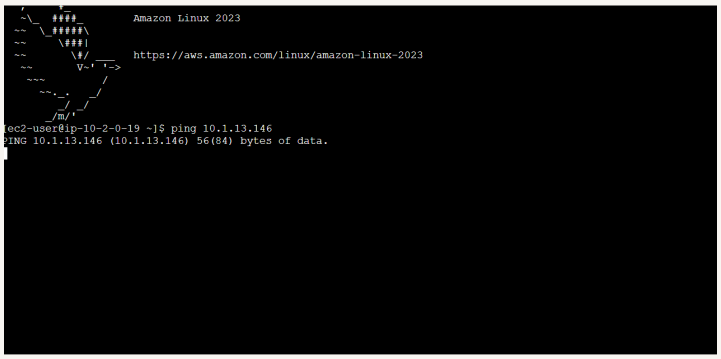
In this step we are setting up a peering connection so that VPCs 1 and 2 can communicate together.

Step 7 - Analyze flow logs

In this step, I am going to review the flow logs recorded about the VPC 1's public subnet also to get some tasty insights.

Connectivity troubleshooting

My first ping test between my EC2 instance had no replies, which means that the ICMP traffic could be blocked by the security groups or ACLs. Also our traffic is being routed to a wrong path which is causing miscommunicaton.



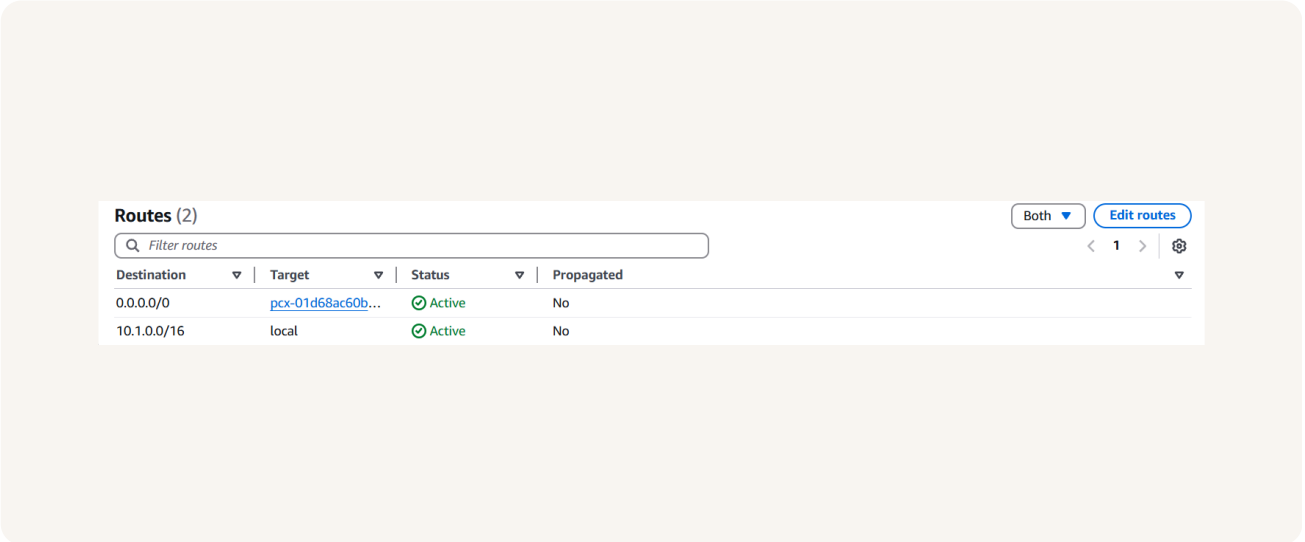
I could receive ping replies if I ran the ping test using the other instance's public IP address, which means our second instant is allow ICMP traffic.

Connectivity troubleshooting

Looking at VPC 1's route table, I identified that the ping test with Instance 2's private address failed because we didn't set up a route in our VPC Route tables that directs traffic from that peering connection that directly connects our VPCs.

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

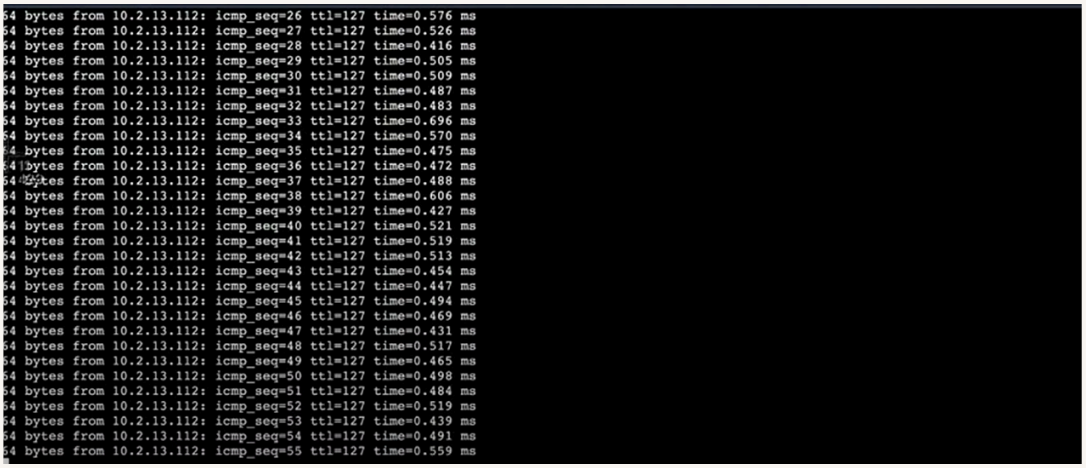
I also updated both VPCs' route tables, so traffic from 1 of the VPC can get directed and heading to the other VPC that they can have a peering connection instead of the public internet.



LW
lwazi995@outlook.com
NextWork Student
NextWork.org

Connectivity troubleshooting

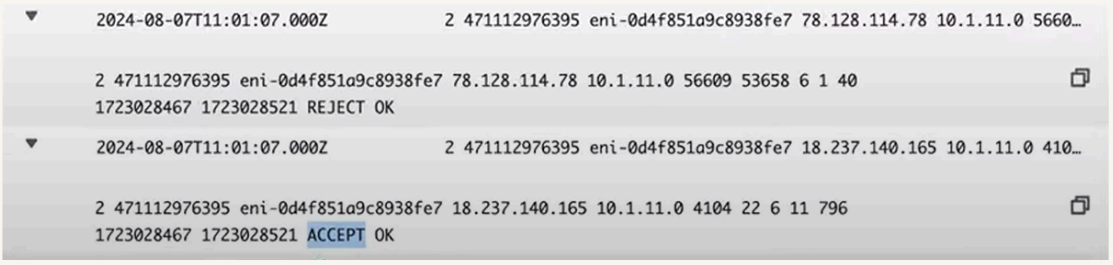
I received ping replies from Instance 2's private IP address! This means setting up the peering connection and then the route table to connect VPC 1 and VPC 2 traffic to navigate from one VPC to the other.


64 bytes from 10.2.13.112: icmp_seq=26 ttl=127 time=0.576 ms
64 bytes from 10.2.13.112: icmp_seq=27 ttl=127 time=0.526 ms
64 bytes from 10.2.13.112: icmp_seq=28 ttl=127 time=0.416 ms
64 bytes from 10.2.13.112: icmp_seq=29 ttl=127 time=0.505 ms
64 bytes from 10.2.13.112: icmp_seq=30 ttl=127 time=0.509 ms
64 bytes from 10.2.13.112: icmp_seq=31 ttl=127 time=0.487 ms
64 bytes from 10.2.13.112: icmp_seq=32 ttl=127 time=0.483 ms
64 bytes from 10.2.13.112: icmp_seq=33 ttl=127 time=0.696 ms
64 bytes from 10.2.13.112: icmp_seq=34 ttl=127 time=0.570 ms
64 bytes from 10.2.13.112: icmp_seq=35 ttl=127 time=0.475 ms
64 bytes from 10.2.13.112: icmp_seq=36 ttl=127 time=0.472 ms
64 bytes from 10.2.13.112: icmp_seq=37 ttl=127 time=0.488 ms
64 bytes from 10.2.13.112: icmp_seq=38 ttl=127 time=0.606 ms
64 bytes from 10.2.13.112: icmp_seq=39 ttl=127 time=0.427 ms
64 bytes from 10.2.13.112: icmp_seq=40 ttl=127 time=0.521 ms
64 bytes from 10.2.13.112: icmp_seq=41 ttl=127 time=0.519 ms
64 bytes from 10.2.13.112: icmp_seq=42 ttl=127 time=0.513 ms
64 bytes from 10.2.13.112: icmp_seq=43 ttl=127 time=0.454 ms
64 bytes from 10.2.13.112: icmp_seq=44 ttl=127 time=0.447 ms
64 bytes from 10.2.13.112: icmp_seq=45 ttl=127 time=0.494 ms
64 bytes from 10.2.13.112: icmp_seq=46 ttl=127 time=0.469 ms
64 bytes from 10.2.13.112: icmp_seq=47 ttl=127 time=0.431 ms
64 bytes from 10.2.13.112: icmp_seq=48 ttl=127 time=0.517 ms
64 bytes from 10.2.13.112: icmp_seq=49 ttl=127 time=0.465 ms
64 bytes from 10.2.13.112: icmp_seq=50 ttl=127 time=0.498 ms
64 bytes from 10.2.13.112: icmp_seq=51 ttl=127 time=0.484 ms
64 bytes from 10.2.13.112: icmp_seq=52 ttl=127 time=0.519 ms
64 bytes from 10.2.13.112: icmp_seq=53 ttl=127 time=0.439 ms
64 bytes from 10.2.13.112: icmp_seq=54 ttl=127 time=0.491 ms
64 bytes from 10.2.13.112: icmp_seq=55 ttl=127 time=0.559 ms

Analyzing flow logs

Flow logs tell us about the source of the IP address how long it took the destination, the amount of data that is being transferred. The protocol it uses as well as weither the traffic was accepted or rejected

For example, the flow log I've captured tells us that traffic went from this IP address 18.237.140.165 to 10.1.11.0. It also tells us that it was accepted by our security groups and network ACLs of the VPC.

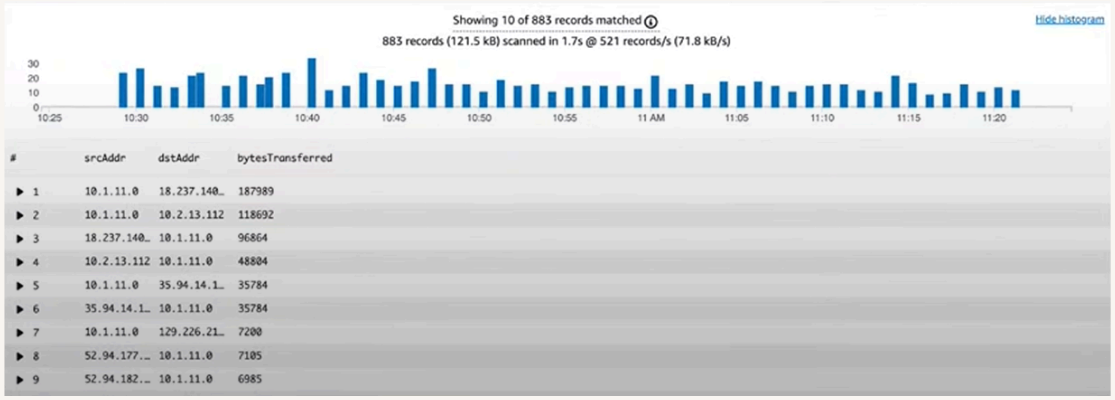


LW
lwazi995@outlook.com
NextWork Student

Logs Insights

Logs Insights is a special tool within Amazon CloudWatch helps with analysing logs and creating visual graphs and charts through queries.

I ran the query return the top 10 byte transfers by source and destination IP addresses This query analyzes flow logs collected on EC2 instance 1, and it will return the top ten pairs of IP based on the amount of data transfered between them.



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for more projects