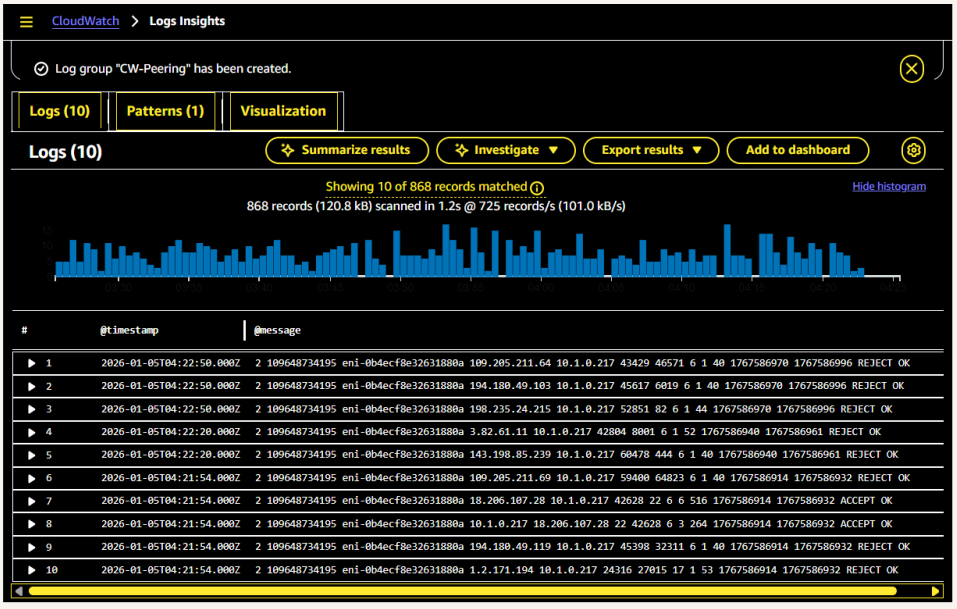
nextwork.org

VPC Monitoring with Flow Logs

Michael K.



Michael K.
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

What is Amazon VPC? Amazon VPC (Virtual Private Cloud) is a logicallyisolatedvirtualnetworkwithinAWS where i can launch and manage AWS resources(suchasEC2instances,RDS databases, and load balancers) using my owndefinedIPaddressrange,subnets, route tables, and network gateways.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create a peered network and monitor traffic between my peered VPCs (traffic in my network).

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

One thing I didn't expect in this project was its complexity and relationship between the different services used for monitory.

This project took me...

This project took me 3 hours.

Michael K.
NextWork Student

In the first part of my project...

Step 1 - Set up VPCs

In this step, I will Create two VPCs from scratch for VPC Peering.

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.

Step 3 - Set up Logs

In this step, I will set up a way to track all inbound and outbound network traffic and set up a space that stores all of these records.

Step 4 - Set IAM permissions for Logs

In this step, I will give VPC Flow Logs the permission to write logs and send them to CloudWatch (log group), and finish setting up my subnet's flow log.

Michael K.
NextWork Student

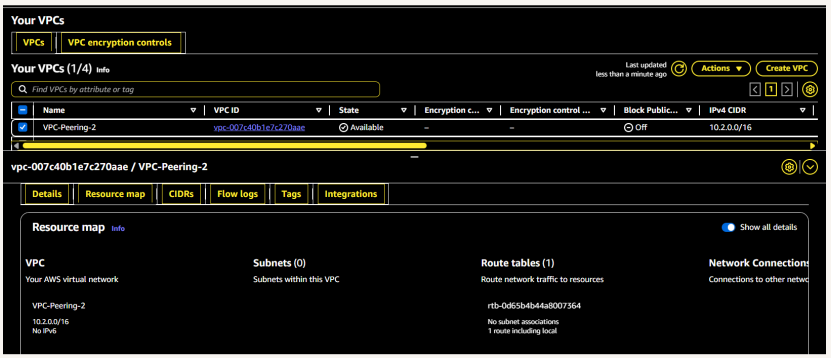
Multi-VPC Architecture

I started my project by launching 2 VPCs, 2 Subnets and their components.

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 inorder to avoids IP Adresse overlap.

I also launched EC2 instances in each subnet

My EC2 instances' security groups allow traffic in and out of my EC2 Instances. The Inbound rules for the first Instance security group were : SSH, and All ICMP IPv4 from the second VPC. The Outbound rules wer : All Traffic to anywhere. The Inbound rules for the second Instance security group were : All ICMP IPv4 from the first VPC. The Outbound rules wer : All Traffic to anywhere.

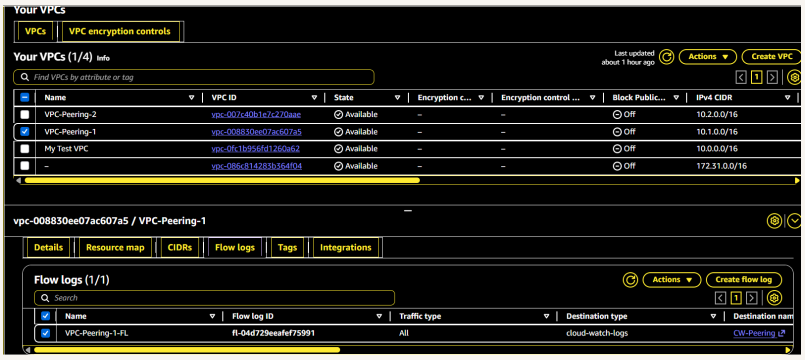


Michael K.
NextWork Student

Logs

Logs are like a diary which record everything that happens in my region, from users logging in to errors popping up. It's the go-to place to understand what's going on with my systems, troubleshoot problems, and keep an eye on who’s doing what.

Log groups are like big folders in AWS where i 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.



Michael K.
NextWork Student

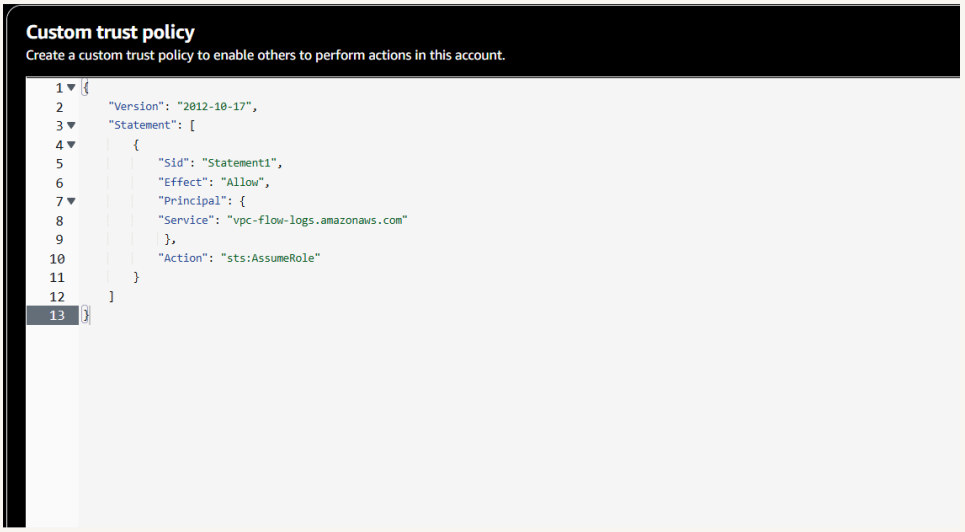
IAM Policy and Roles

I created an IAM policy to give VPC Flow Logs the permission to record traffic and store them in my CloudWatch. This policy makes sure that my VPC Flow log can now send log data to my log group!

I also created an IAM role permission can't be directly attached to AWS services to perfom some actions on AWS resources. Only roles containing these Policies (permissions) can.

A custom trust policy is a specific type of policy! While IAM policies help me define the actions a user/service can or cannot do, custom trust policies are used to very narrowly define who can use a role.

Michael K.
NextWork Student



Michael K.
NextWork Student

In the second part of my project...

Step 5 - Ping testing and troubleshooting

In this step, I will get Instance 1 to send test messages to Instance 2 to test my VPC Peering.

Step 6 - Set up a peering connection

In this step, I will set up a connection link between your VPCs.

Step 7 - Analyze flow logs

In this step, I will review the flow logs recorded about VPC 1's public subnet and analyse the flow logs to get some insights.

Michael K.
NextWork Student

Connectivity troubleshooting

My first ping test between my EC2 instances had no replies, which means the connection to the second server was not reachable. but i solved the problem and it worked.,

I could receive ping replies if I ran the ping test using the other instance's public IP address, which means it is publicly reachable.

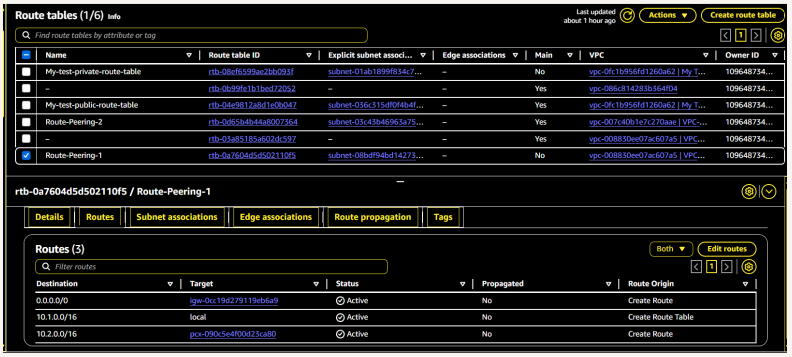
Michael K.
NextWork Student

Connectivity troubleshooting

Looking at VPC 1's route table, I identified that the ping test with Instance 2's private address failed because the ICMP rule was not setup at the security group level. Also, the peering rule was not setup at the Network ACL level for both Instances.

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

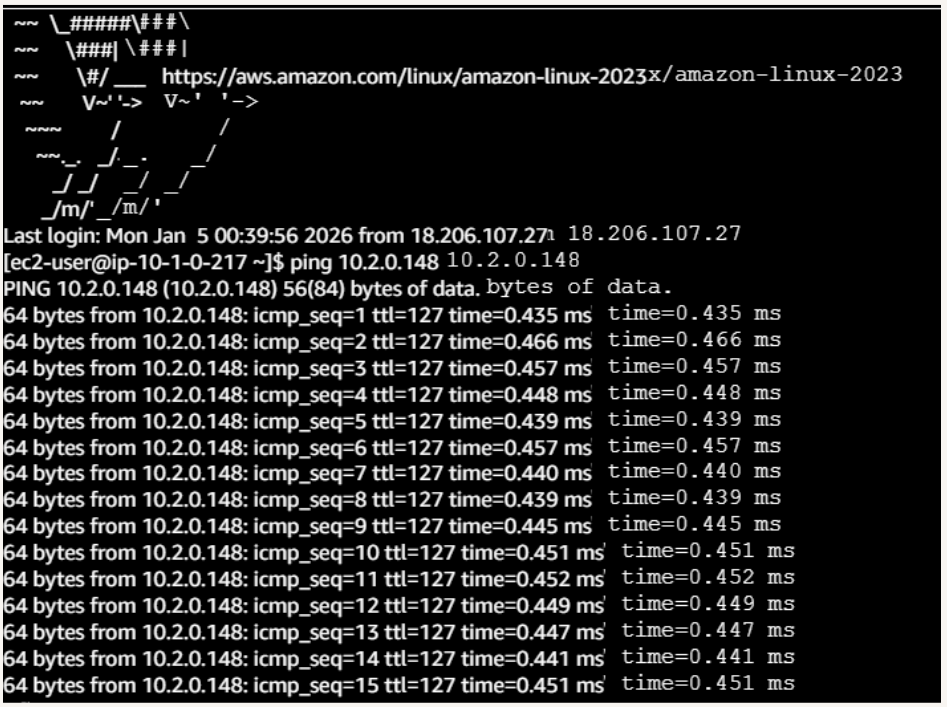
I also updated both VPCs' route tables so that it can have the peering route for the connection with each other.



Michael K.
NextWork Student

Connectivity troubleshooting

I received ping replies from Instance 2's private IP address! This means that the Peering was succesful.

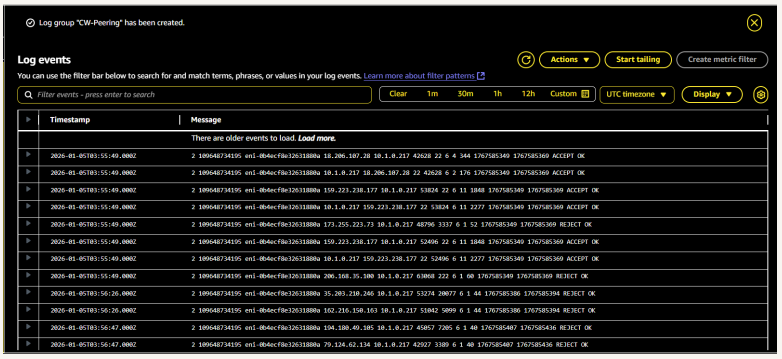


Michael K.
NextWork Student

Analyzing flow logs

Flow logs tell me about the number of data that were sent successfully from one IP address (e.g 18.237.140.165) to another, the protocol and port used, the number of packets transferred and if the traffic was allowed ("ACCEPT") or not ("REJECT").

For example, the flow log I've captured tells me that 344 bytes of data were sent successfully from the IP address 18.237.140.165 to 10.1.5.112 using TCP protocol on port 22, with 4 packets transferred and the traffic was allowed ("ACCEPT").

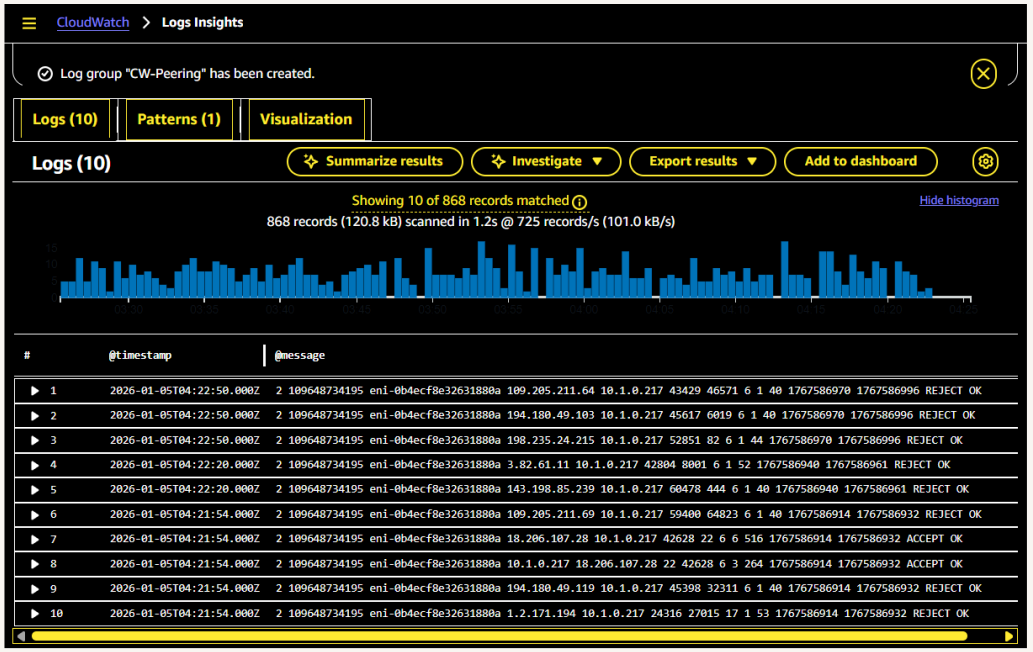


Michael K.
NextWork Student

Logs Insights

Logs Insights is a CloudWatch feature that analyzes logs. In Log Insights, i use queries to filter, process and combine data to troubleshoot problems or better understand my network traffic!

I ran the query : fields @timestamp, @message | sort @timestamp desc | limit 10 This query analyzes "Top 10 byte transfers by source and destination IP addresses" and is all about discovering the top 10 biggest data transfers between IP addresses in my network!



The place to learn & showcase your skills

Check out nextwork.org for more projects