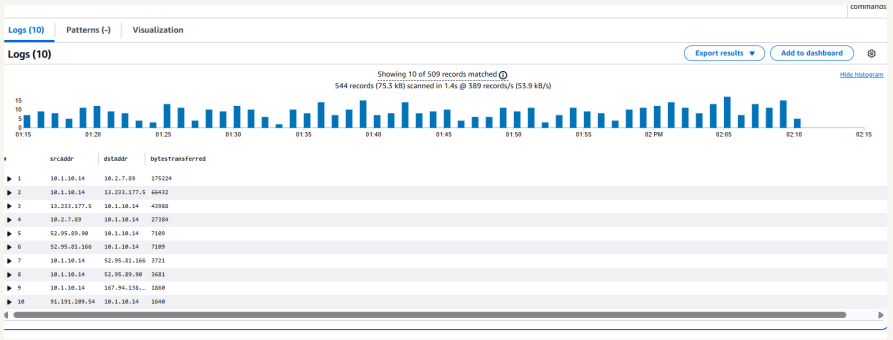
NextWork.org

VPC Monitoring with Flow Logs

DI dineshrajdhanapathy@gmail.com



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a service that allows you to create a private, isolated network within AWS. It provides control over IP addresses, subnets, and security, ensuring secure and scalable cloud resource management.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create isolated network environments, set up subnets, configure route tables, and establish VPC peering to enable secure communication between EC2 instances and learnt how to monitor traffic within our VPC.

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

One thing I didn’t expect in this project was the complexity of configuring the route tables and ensuring proper VPC peering for seamless communication. It required careful attention to detail for proper setup.

This project took me...

This project took me about 3-4 hours to complete. It involved setting up VPCs, configuring subnets, route tables, security groups, and testing the connectivity, which required some troubleshooting and adjustments.

In the first part of my project...

Step 1 - Set up VPCs

In this step, we are creating two VPCs from scratch to set up isolated network environments. This will allow us to configure peering connections and experiment with traffic flow and security between them.

Step 2 - Launch EC2 instances

In this step, we're launching an EC2 instance in each VPC to serve as test points. This allows us to verify the VPC peering connection by checking if the instances can communicate successfully.

Step 3 - Set up Logs

In this step, we're enabling VPC Flow Logs to track all inbound and outbound traffic. These logs are stored in CloudWatch or S3, helping monitor, troubleshoot, and analyze network activity securely.

Step 4 - Set IAM permissions for Logs

In this step, we're assigning permissions to VPC Flow Logs to write data to CloudWatch. Then, we configure the subnet's flow log to track and store traffic data for monitoring and troubleshooting purposes.

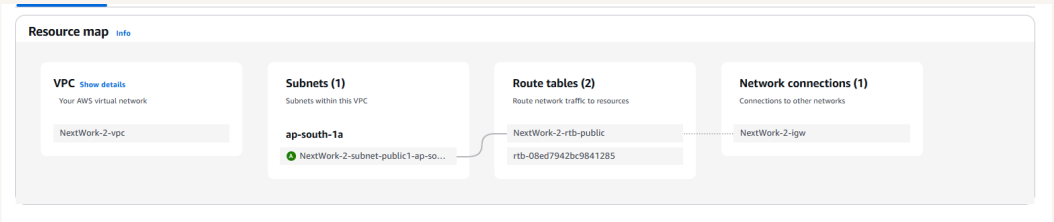
Multi-VPC Architecture

I started my project by launching a VPC with custom configurations. As part of this setup, I created one subnet: one public subnets for external access.

The CIDR blocks for VPCs 1 and 2 are unique(10.1.0.0/16 , 10.2.0.0/16) to avoid IP address conflicts. They have to be unique because overlapping IP ranges can disrupt routing, communication, and resource connectivity between VPCs.

I also launched EC2 instances in each subnet

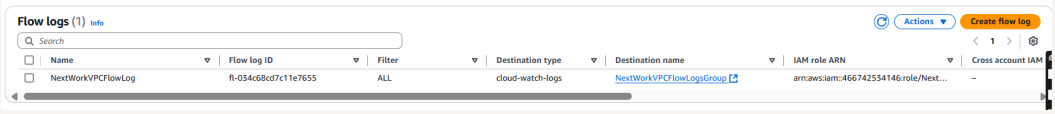
My EC2 instances' security groups allow inbound SSH (port 22) for management and ICMP for testing connectivity. This is because they enable secure access and help verify the VPC peering connection.



Logs

Logs are detailed records of events or activities generated by systems, applications, or networks. They provide insights into performance, errors, and security, helping in monitoring and troubleshooting.

Log groups are collections of related log streams in AWS CloudWatch. They organize logs from resources like EC2 instances, making it easier to manage, search, and analyze system or application activity.

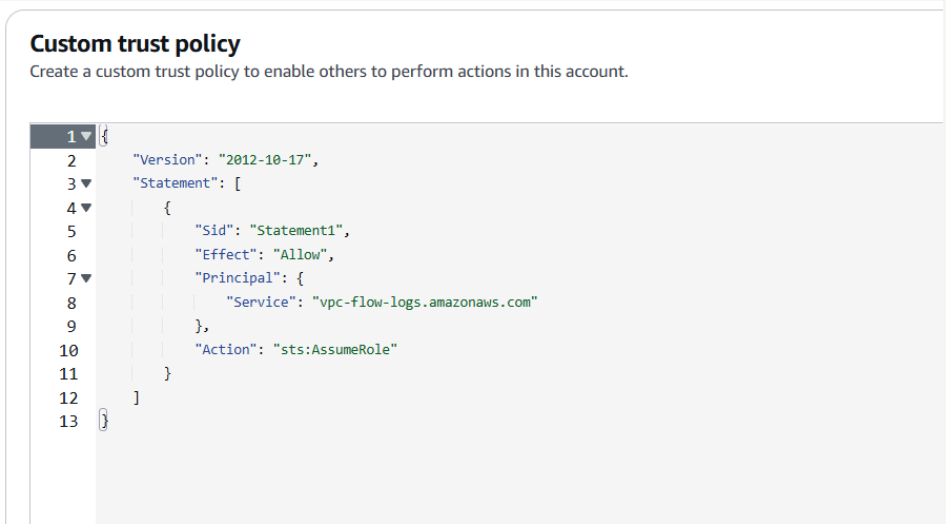


IAM Policy and Roles

I created an IAM policy because it defines the permissions needed for VPC Flow Logs to write log data to CloudWatch. This ensures secure and controlled access to manage and store log information.

I also created an IAM role because it allows VPC Flow Logs to assume the necessary permissions defined in the IAM policy, enabling it to write log data securely to CloudWatch or S3 on my behalf.

A custom trust policy is a JSON document that specifies which AWS services or accounts can assume a role. It defines trusted entities, ensuring secure role delegation for specific tasks or permissions.



In the second part of my project...

Step 5 - Ping testing and troubleshooting

In this step, we're sending test messages from Instance 1 to Instance 2 to verify the VPC peering connection. This ensures that communication between the instances across VPCs is functioning correctly.

Step 6 - Set up a peering connection

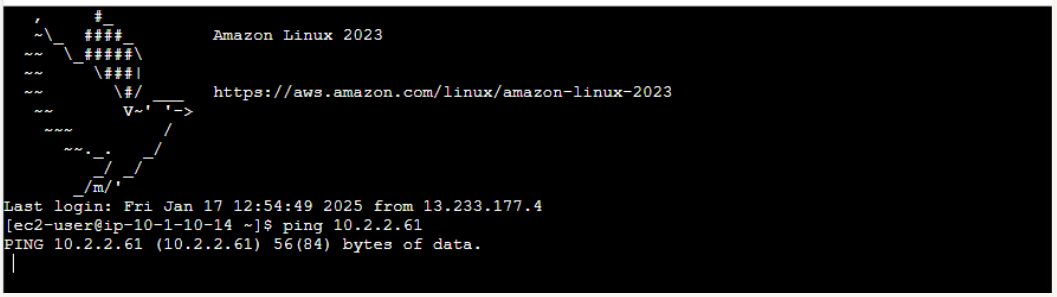
In this step, we're setting up a VPC peering connection between our VPCs to enable communication between them. This ensures that resources in different VPCs can interact using private IP addresses for better security and efficiency.

Step 7 - Analyze flow logs

In this step, we're reviewing the flow logs for VPC 1's public subnet to analyze inbound and outbound traffic. This helps us identify any issues, monitor performance, and ensure security policies are working effectively.

Connectivity troubleshooting

My first ping test between my EC2 instances had no replies, which means the network connection between the instances might be blocked or misconfigured, possibly due to security groups or routing issues.



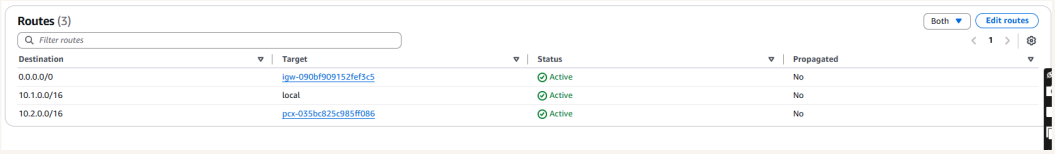
I could receive ping replies if I ran the ping test using the other instance's public IP address, which means the instances are reachable over the internet, but there might be an issue with private IP communication.

Connectivity troubleshooting

Looking at VPC 1's route table, I identified that the ping test with Instance 2's private address failed because the route for VPC peering was not properly configured, preventing communication between the VPCs.

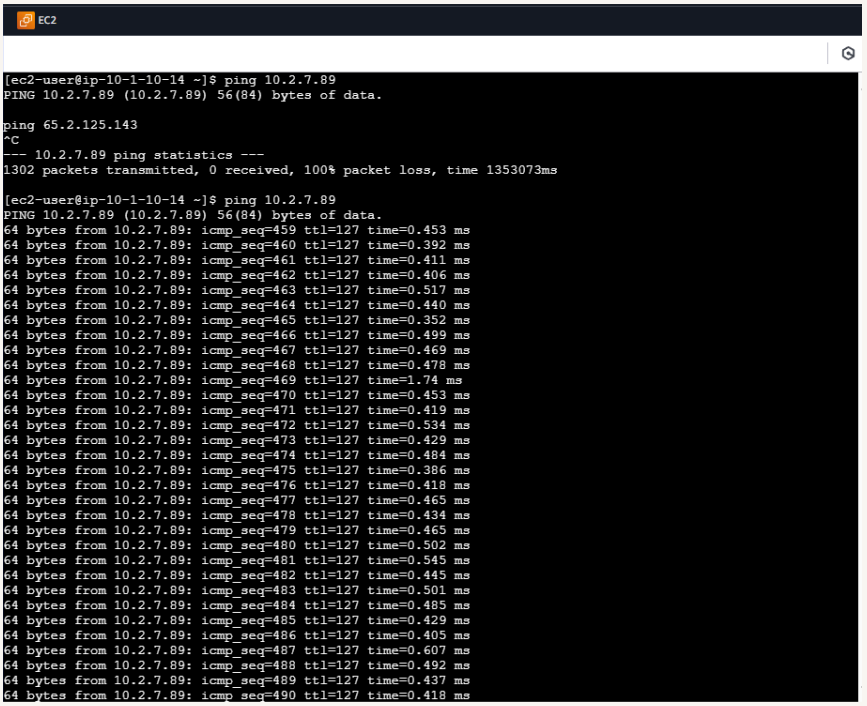
To solve this, I set up a peering connection between my VPCs

I also updated both VPCs' route tables so that traffic could flow between the VPCs via the peering connection. This ensures proper routing of requests between instances in different VPCs using private IPs.



Connectivity troubleshooting

I received ping replies from Instance 2's private IP address! This means the VPC peering connection and route table configurations are correct, allowing successful communication between instances in different VPCs.



Analyzing flow logs

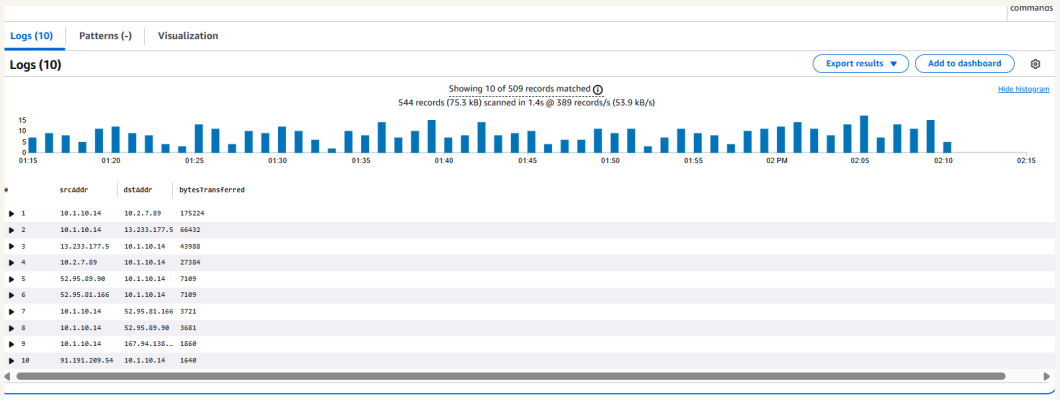
Flow logs tell us about various network traffic details, including the source and destination IP addresses, ports, protocol, traffic direction, action (allow or deny), and the number of bytes transferred during communication.

For example, the flow log I've captured tells us that traffic from a specific source IP was allowed to reach a destination IP on a particular port. It also shows the protocol used and the amount of data transferred.

Logs Insights

Logs Insights is a powerful tool within AWS CloudWatch that allows you to query and analyze log data. It helps you gain insights into performance, troubleshoot issues, and monitor applications through custom queries.

I ran the query fields "stats sum(bytes) as bytesTransferred by srcAddr, dstAddr | sort bytesTransferred desc | limit 10". This query analyzes the logs for executed log groups successfully.



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for more projects