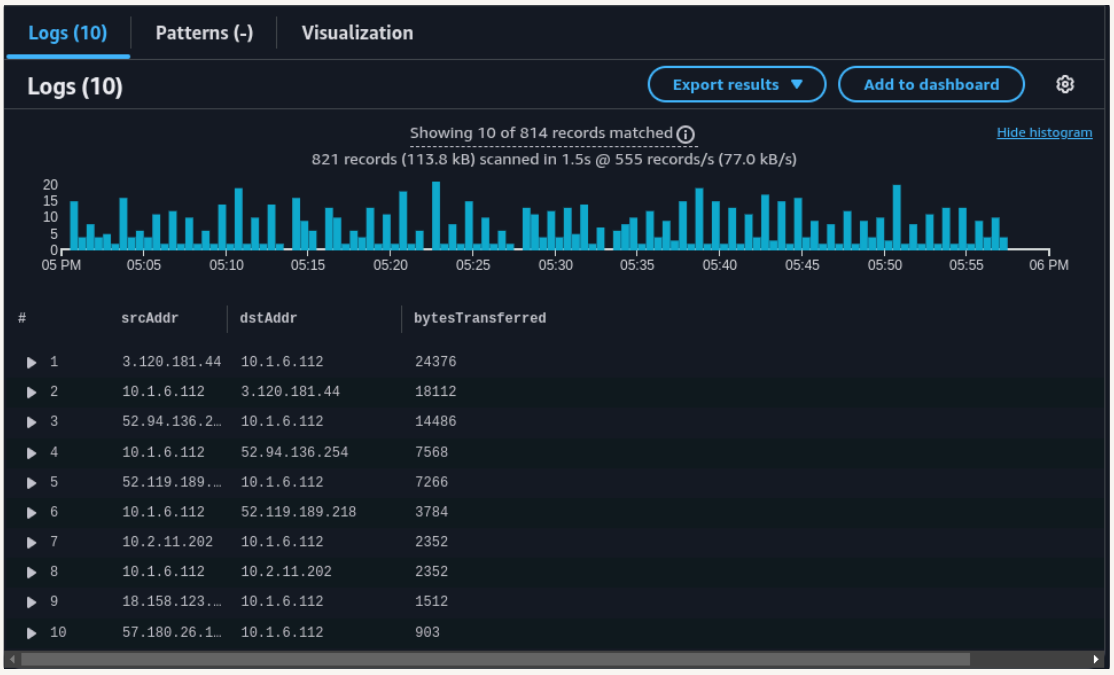
nextwork.org

VPC Monitoring with Flow Logs

Ivaylo Stoyanov



Ivaylo Stoyanov
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a service that lets you create a secure, isolated virtual network in AWS. It's useful for launching resources in a private, customizable environment with full control over IP ranges, subnets, and security.

How I used Amazon VPC in this project

I used Amazon VPC to create two VPCs, set up VPC peering, configured route tables, launched EC2 instances, tested connectivity with ping, and enabled VPC Flow Logs for monitoring traffic in CloudWatch.

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

One unexpected issue was the missing VPC peering connection. Initially, I thought Security Groups or NACLs were the problem, but the lack of a peering connection was the root cause. Fixing it resolved the connectivity issue.

Ivaylo Stoyanov
NextWork Student

This project took me...

This project took 4-6 hours: setting up VPCs, testing connectivity and troubleshooting with ping command.

Ivaylo Stoyanov
NextWork Student

In the first part of my project...

Step 1 - Set up VPCs

In this step, I'm going to create two VPCs from scratch.

Step 2 - Launch EC2 instances

In this phase of the project, I will launch EC2 instances in both VPCs. These instances will serve as resources that communicate across the VPC peering connection. By launching instances in each VPC, I can test and validate the connectivity.

Step 3 - Set up Logs

In this step, I will configure VPC Flow Logs to capture all inbound and outbound traffic within my VPC. The logs will be stored in Amazon CloudWatch, enabling real-time monitoring, analysis, and troubleshooting of network activity.

Step 4 - Set IAM permissions for Logs

In this step I will grant VPC Flow Logs the necessary permissions to write logs and send them to Amazon CloudWatch. This involves creating an IAM role with the appropriate policies.

I
Ivaylo Stoyanov
NextWork Student

Multi-VPC Architecture

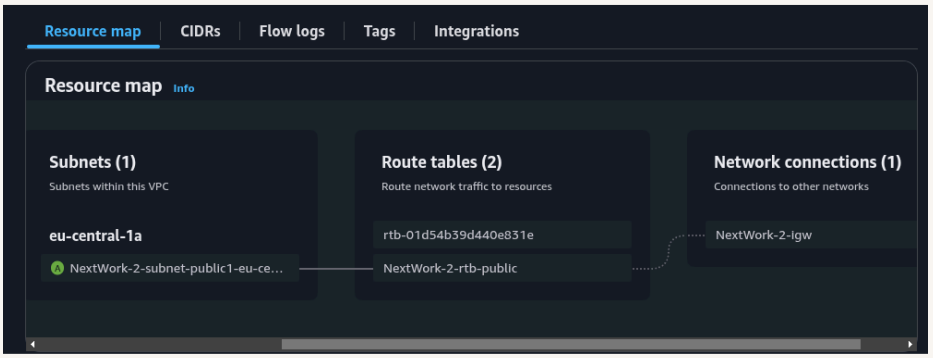
I began my project by navigating to the VPC Dashboard in the AWS Management Console and selecting Your VPCs. From there, I clicked Create VPC and chose the VPC and more option to streamline the setup process. For this project, I created two subnets.

The CIDR blocks for VPC 1 and VPC 2 are 10.1.0.0/16 and 10.2.0.0/16, respectively. It is crucial that these CIDR blocks are unique and non-overlapping because overlapping IP address ranges can lead to routing conflicts and connectivity issues.

I also launched EC2 instances in each subnet

The security group rules for my EC2 instances were configured to ensure secure and controlled access.

Ivaylo Stoyanov
NextWork Student

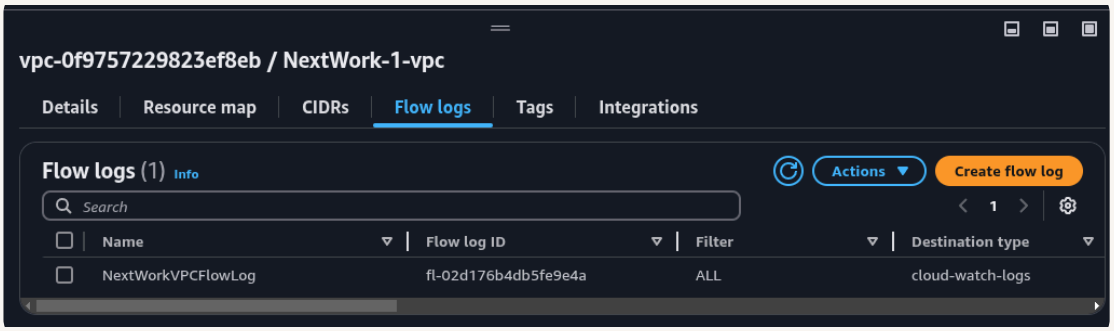


Ivaylo Stoyanov
NextWork Student

Logs

Logs are records of events or activities generated by systems, applications, or networks. They provide valuable insights for monitoring, troubleshooting, and auditing.

Log groups are containers for log streams in Amazon CloudWatch. They organize and store logs from the same source (e.g., an application or system), making it easier to manage, monitor, and analyze log data centrally



Ivaylo Stoyanov
NextWork Student

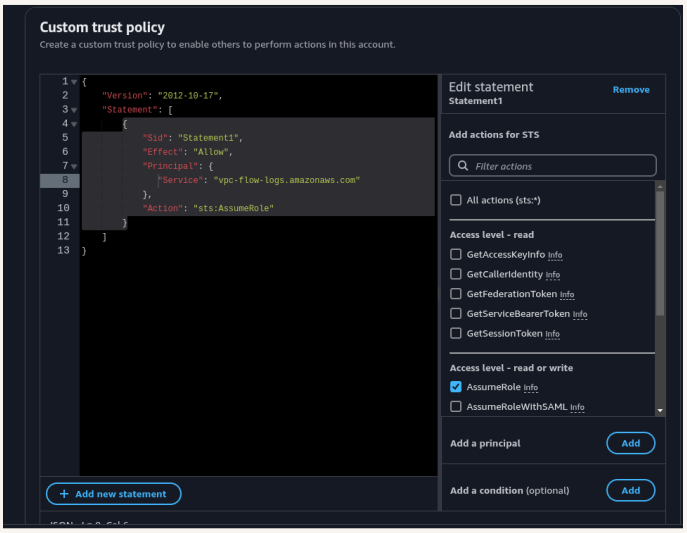
IAM Policy and Roles

I created an IAM policy because it defines the permissions required for VPC Flow Logs to write logs to Amazon CloudWatch. This policy ensures that the necessary actions, such as logs:CreateLogGroup and logs:CreateLogStream, are allowed.

I also created an IAM role because it provides a secure way to delegate permissions to VPC Flow Logs. By attaching the IAM policy to this role, I ensured that Flow Logs has the necessary permissions to write logs to Amazon CloudWatch.

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

Ivaylo Stoyanov
NextWork Student



In the second part of my project...

Step 5 - Ping testing and troubleshooting

In this phase, I will generate network traffic by sending a message from the VPC 1 to VPC 2. This test will validate the VPC peering connection and confirm whether the flow logs successfully capture the traffic.

Step 6 - Set up a peering connection

In this step of the project, I will use the VPC peering connection to bridge our VPCs together, enabling secure and private communication between resources in different VPCs using private IP addresses.

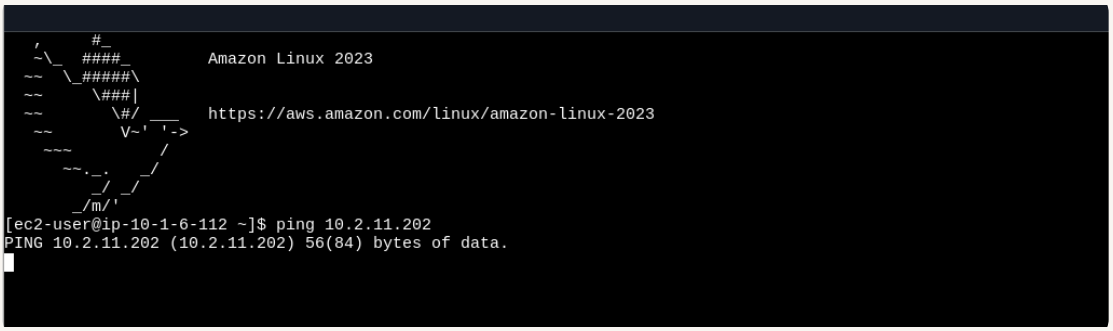
Step 7 - Analyze flow logs

In this step, I will review the flow logs recorded for VPC 1's public subnet and analyze them to gain valuable insights into network traffic patterns, security, and performance. These insights will help optimize and secure the VPC configuration.

Ivaylo Stoyanov
NextWork Student

Connectivity troubleshooting

My first ping test between my EC2 instances had no replies, which means there was no successful communication between them. This indicates a potential issue with the VPC peering connection, route tables, security groups, or network ACLs.



I could receive ping replies by running the test using the other instance's public IP address, which means the traffic is routed over the public internet.

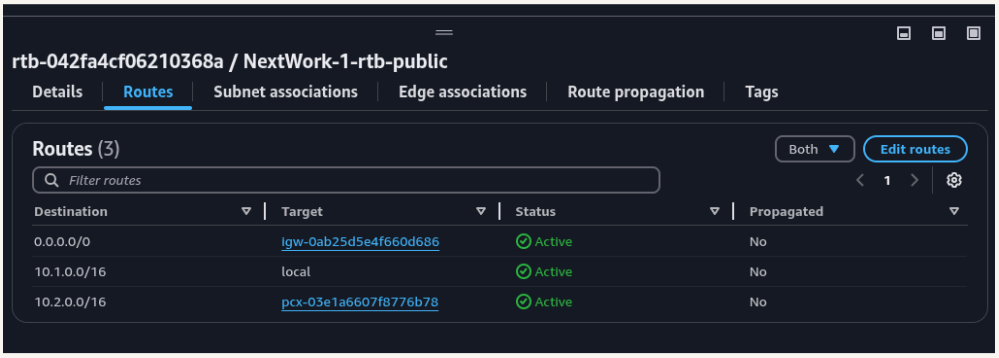
Ivaylo Stoyanov
NextWork Student

Connectivity troubleshooting

After reviewing VPC 1's route table, I identified that the ping test using Instance 2's private IP address failed because there was no route directing traffic to the VPC peering connection. Without this route, VPC 1 cannot communicate with VPC 2.

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

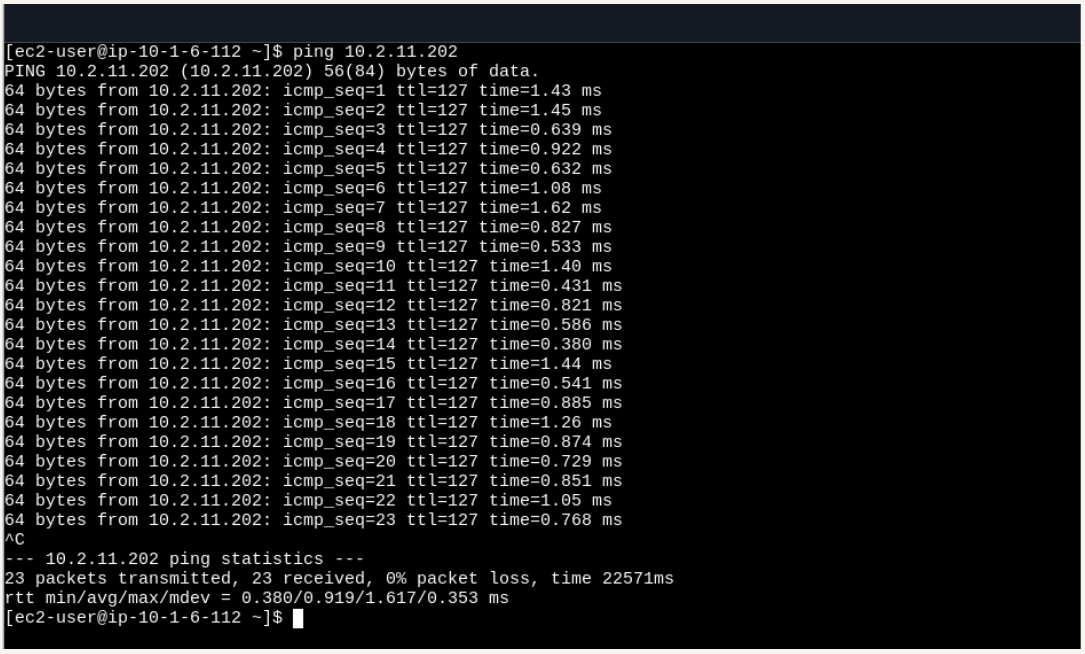
I also updated both VPCs' route tables to include routes directing traffic between the VPCs through the peering connection. This ensures that instances in one VPC can communicate with instances in the other VPC using private IP addresses.



I
Ivaylo Stoyanov
NextWork Student

Connectivity troubleshooting

I successfully received ping replies from Instance 2's private IP address! This means the VPC peering connection is functioning correctly, and the route tables, security groups, and network ACLs are properly configured to allow private communication.

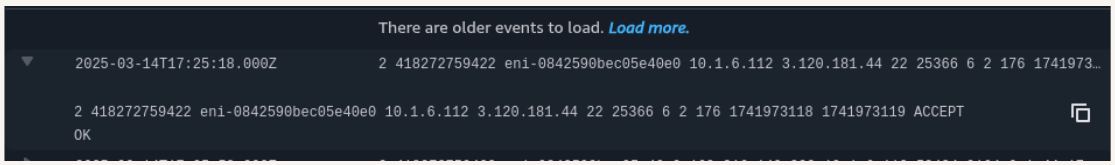

[ec2-user@ip-10-1-6-112 ~]$ ping 10.2.11.202
PING 10.2.11.202 (10.2.11.202) 56(84) bytes of data.
64 bytes from 10.2.11.202: icmp_seq=1 ttl=127 time=1.43 ms
64 bytes from 10.2.11.202: icmp_seq=2 ttl=127 time=1.45 ms
64 bytes from 10.2.11.202: icmp_seq=3 ttl=127 time=0.639 ms
64 bytes from 10.2.11.202: icmp_seq=4 ttl=127 time=0.922 ms
64 bytes from 10.2.11.202: icmp_seq=5 ttl=127 time=0.632 ms
64 bytes from 10.2.11.202: icmp_seq=6 ttl=127 time=1.08 ms
64 bytes from 10.2.11.202: icmp_seq=7 ttl=127 time=1.62 ms
64 bytes from 10.2.11.202: icmp_seq=8 ttl=127 time=0.827 ms
64 bytes from 10.2.11.202: icmp_seq=9 ttl=127 time=0.533 ms
64 bytes from 10.2.11.202: icmp_seq=10 ttl=127 time=1.40 ms
64 bytes from 10.2.11.202: icmp_seq=11 ttl=127 time=0.431 ms
64 bytes from 10.2.11.202: icmp_seq=12 ttl=127 time=0.821 ms
64 bytes from 10.2.11.202: icmp_seq=13 ttl=127 time=0.586 ms
64 bytes from 10.2.11.202: icmp_seq=14 ttl=127 time=0.380 ms
64 bytes from 10.2.11.202: icmp_seq=15 ttl=127 time=1.44 ms
64 bytes from 10.2.11.202: icmp_seq=16 ttl=127 time=0.541 ms
64 bytes from 10.2.11.202: icmp_seq=17 ttl=127 time=0.885 ms
64 bytes from 10.2.11.202: icmp_seq=18 ttl=127 time=1.26 ms
64 bytes from 10.2.11.202: icmp_seq=19 ttl=127 time=0.874 ms
64 bytes from 10.2.11.202: icmp_seq=20 ttl=127 time=0.729 ms
64 bytes from 10.2.11.202: icmp_seq=21 ttl=127 time=0.851 ms
64 bytes from 10.2.11.202: icmp_seq=22 ttl=127 time=1.05 ms
64 bytes from 10.2.11.202: icmp_seq=23 ttl=127 time=0.768 ms
^C
--- 10.2.11.202 ping statistics ---
23 packets transmitted, 23 received, 0% packet loss, time 22571ms
rtt min/avg/max/mdev = 0.380/0.919/1.617/0.353 ms
[ec2-user@ip-10-1-6-112 ~]$

Ivaylo Stoyanov
NextWork Student

Analyzing flow logs

Flow logs provide detailed information about the IP traffic flowing through your VPC, including source and destination IPs, ports, protocols, and traffic status (accepted or rejected).

For example, the flow log I captured reveals details such as the source and destination IP addresses, ports, protocols, and whether the traffic was accepted.

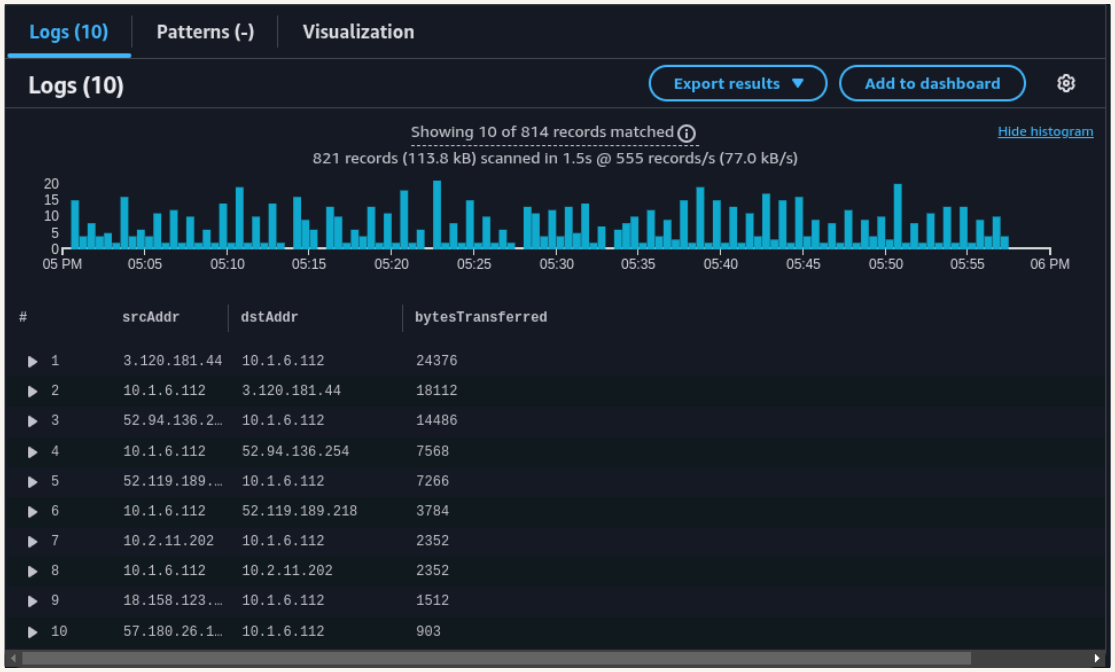


I
Ivaylo Stoyanov
NextWork Student

Logs Insights

Logs Insights is a powerful feature of Amazon CloudWatch that allows me to interactively search and analyze log data. It enables me to run queries, visualize trends, and gain actionable insights from your logs.

I ran the query 'Top 10 byte transfers by source and destination IP addresses'. This query analyzes the log data to identify the top 10 traffic flows based on the volume of data transferred, helping pinpoint the most active communication patterns.


Logs (10)
Patterns (-)
Visualization
Logs (10)
Export results
Add to dashboard
Showing 10 of 814 records matched
Hide histogram
821 records (113.8 kB) scanned in 1.5s @ 555 records/s (77.0 kB/s)
20
15
10
5
0
05 PM
05:05
05:10
05:15
05:20
05:25
05:30
05:35
05:40
05:45
05:50
05:55
06 PM
srcAddr dstAddr bytesTransferred
1 3.120.181.44 10.1.6.112 24376
2 10.1.6.112 3.120.181.44 18112
3 52.94.136.2… 10.1.6.112 14486
4 10.1.6.112 52.94.136.254 7568
5 52.119.189.… 10.1.6.112 7266
6 10.1.6.112 52.119.189.218 3784
7 10.2.11.202 10.1.6.112 2352
8 10.1.6.112 10.2.11.202 2352
9 18.158.123.… 10.1.6.112 1512
10 57.180.26.1… 10.1.6.112 903

NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for more projects