

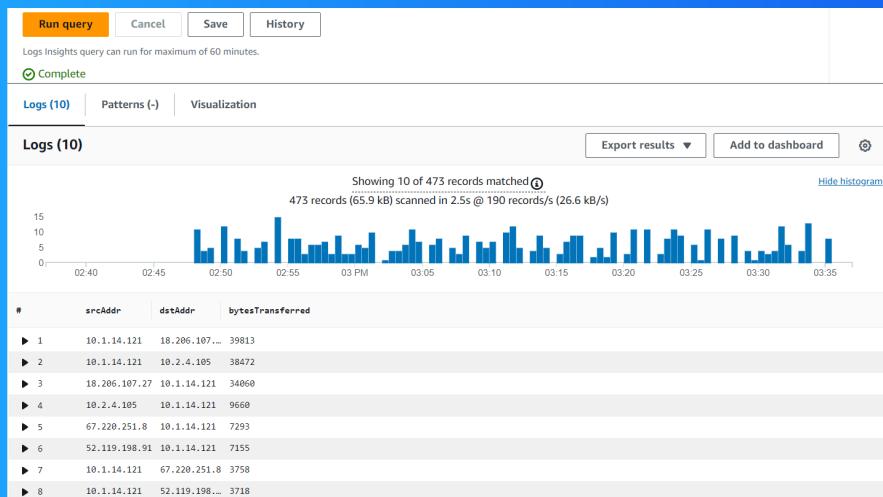


NextWork.org

VPC Monitoring with Flow Logs



Ivan Delgadillo Fernandez





Ivan Delgadillo Fernandez

NextWork Student

NextWork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon Virtual Private Cloud (Amazon VPC) gives you full control over your virtual networking environment, including resource placement, connectivity, and security.

How I used Amazon VPC in this project

Use Amazon VPC to launch AWS resources into a virtual network that is a logically isolated section of the AWS Cloud.

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

I didn't expect configure a Peering VPC

This project took me...

120 Minutes



Ivan Delgadillo Fernandez

NextWork Student

NextWork.org

In the first part of my project...

Step 1 - Set up VPCs

I use VPC wizard to create 2 VPC, that contain only public subnet with a internet gateway.

Step 2 - Launch EC2 instances

We need to create these EC2 instances so that they can send data to each other later in the project, which gives us network activity to monitor.

Step 3 - Set up Logs

Setup VPC Flow logs and cloud Watch

Step 4 - Set IAM permissions for Logs

Now that we know that logs are digital diaries that services keep, think of flow logs as a specific type of diary for VPCs. Flow logs capture traffic going to and from the network - noting down who's visiting your VPC and the specific network interfa



Ivan Delgadillo Fernandez

NextWork Student

NextWork.org

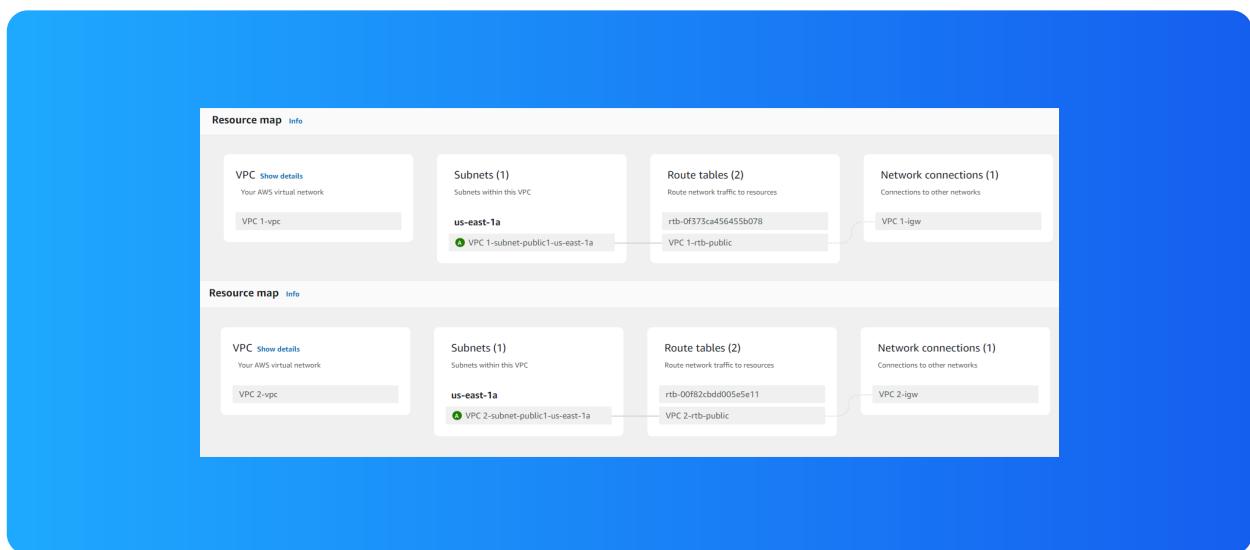
Multi-VPC Architecture

I stared my project by launching 2 VPCs using VPC wizard, I completed in 2 minutes.

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 you needed separate different workloads.

I also launched EC2 instances in each subnet

Security Groups allow access from a source with differents ports to access a Instances EC2 like a SSH, HTTP, ICMP.





Ivan Delgadillo Fernandez

NextWork Student

NextWork.org

Logs

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

Think of a log group as a big folder in AWS where you 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

I also set up a flow log for VPC 1

The screenshot shows the AWS VPC Flow Logs configuration page. At the top, a success message says "Successfully created flow log for vpc-038a5edba87f61848." Below this, the "Your VPCs (1/3) Info" section lists three VPCs:

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP
-	vpc-09e590b2738c761ee	Available	172.31.0.0/16	-	disabled
VPC 2-vpc	vpc-063702e3eb8f2889c	Available	10.2.0.0/16	-	disabled
VPC 1-vpc	vpc-038a5edba87f61848	Available	10.1.0.0/16	-	disabled

Below the VPC list, the "vpc-038a5edba87f61848 / VPC 1-vpc" section shows the "Flow logs (1) Info" table:

Name	Flow log ID	Filter	Destination type	Destination name
VPCFlowLog	f1-08f62e746bee9df2a	ALL	cloud-watch-logs	VPCFlowLogsGroup



Ivan Delgadillo Fernandez

NextWork Student

NextWork.org

IAM Policy and Roles

VPC Flow Logs by default don't have the permission to record logs and store them in your CloudWatch log group.

IAM roles made up of combinations of IAM policies

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.

The screenshot shows the 'Custom trust policy' creation interface in the AWS IAM console. The title bar says 'Custom trust policy'. Below it, a sub-header says 'Create a custom trust policy to enable others to perform actions in this account.' The main area contains a code editor with the following JSON policy:

```
1 Version: "2012-10-17",
2 Statement: [
3   {
4     Sid: "Statement1",
5     Effect: "Allow",
6     Principal: {
7       Service: "vpc-flow-logs.amazonaws.com"
8     },
9     Action: "sts:AssumeRole"
10   }
11 ]
12 ]
13 ]
```



Ivan Delgadillo Fernandez

NextWork Student

NextWork.org

In the second part of my project...

Step 5 - Ping testing and troubleshooting

Let's generate some network traffic and see whether our flow logs can pick up on them. We're going to generate network traffic by trying to get our instance in VPC 1 to send a message to our instance in VPC 2.

Step 6 - Set up a peering connection

Let's add that peering connection in this step to bridge our VPCs together! □

Step 7 - Update VPC route tables

Set up a way for traffic coming from VPC 1 to get to VPC 2. Set up a way for traffic coming from VPC 2 to get to VPC 1.

Step 8 - Analyze flow logs

Review the flow logs recorded about VPC 1's public subnet. Analyse the flow logs to get some tasty insights



Ivan Delgadillo Fernandez

NextWork Student

NextWork.org

Connectivity troubleshooting

My first ping test between my EC2 instances had no replies, which means there aren't connections between my VPCs

The screenshot shows a terminal window on an AWS Lambda function. The terminal output is as follows:

```
aws | Services | Search [Alt+S]
VPC Billing and Cost Management EC2

Amazon Linux 2
AL2 End of Life is 2025-06-30.
A newer version of Amazon Linux is available!
Amazon Linux 2023, GA and supported until 2028-03-15.
https://aws.amazon.com/linux/amazon-linux-2023/

[ec2-user@ip-10-1-14-121 ~]$ ping 10.2.4.105
PING 10.2.4.105 (10.2.4.105) 56(84) bytes of data.
```

I could receive ping replies if I ran the ping test using the other instance's public IP address



Ivan Delgadillo Fernandez

NextWork Student

NextWork.org

Connectivity troubleshooting

Looking at VPC 1's route table, I identified that the ping test with Instance 2's private address failed because the traffic is through the internet gateway i.e. traffic will travel through and be exposed to the public internet.

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

I also updated both VPCs' route tables so that both VPCs could PING to other VPC

	VPC 1-rtb-public	rtb-01f4075f4f9ef0855	subnet-07573335dc95e1...	-
<input type="checkbox"/>	VPC 2-rtb-public	rtb-0ddd7d42714518467	subnet-0a425cc69c57e3...	-
<input type="checkbox"/>	-	rtb-00r-281hhvrdar1f700	-	-

rtb-01f4075f4f9ef0855 / VPC 1-rtb-public				
Details	Routes	Subnet associations	Edge associations	Route propagation
Routes (3)				
<input type="text"/> Filter routes				
Destination	Target		Status	
0.0.0.0	igw-03fd1326d85d8c47d		Active	
10.1.0.0/16	local		Active	
10.2.0.0/16	pxx-0fe8418974674dec1		Active	



Ivan Delgadillo Fernandez

NextWork Student

NextWork.org

Connectivity troubleshooting

I received ping replies from Instance 2's private IP address! This means there are connection successful

```
aws | Services | Search [Alt+S]
VPC Billing and Cost Management EC2
64 bytes from 3.93.58.155: icmp_seq=1 ttl=254 time=1.02 ms
64 bytes from 3.93.58.155: icmp_seq=2 ttl=254 time=1.14 ms
64 bytes from 3.93.58.155: icmp_seq=3 ttl=254 time=0.989 ms
64 bytes from 3.93.58.155: icmp_seq=4 ttl=254 time=1.75 ms
64 bytes from 3.93.58.155: icmp_seq=5 ttl=254 time=1.24 ms
^C
--- 3.93.58.155 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 0.989/1.232/1.759/0.281 ms
[ec2-user@ip-10-1-14-121 ~]$ 
[ec2-user@ip-10-1-14-121 ~]$ 
[ec2-user@ip-10-1-14-121 ~]$ ping 10.2.4.105
PING 10.2.4.105 (10.2.4.105) 56(84) bytes of data.
64 bytes from 10.2.4.105: icmp_seq=1 ttl=255 time=2.59 ms
64 bytes from 10.2.4.105: icmp_seq=2 ttl=255 time=1.59 ms
64 bytes from 10.2.4.105: icmp_seq=3 ttl=255 time=1.70 ms
64 bytes from 10.2.4.105: icmp_seq=4 ttl=255 time=1.32 ms
64 bytes from 10.2.4.105: icmp_seq=5 ttl=255 time=0.687 ms
64 bytes from 10.2.4.105: icmp_seq=6 ttl=255 time=1.55 ms
64 bytes from 10.2.4.105: icmp_seq=7 ttl=255 time=1.00 ms
64 bytes from 10.2.4.105: icmp_seq=8 ttl=255 time=1.15 ms
64 bytes from 10.2.4.105: icmp_seq=9 ttl=255 time=1.13 ms
64 bytes from 10.2.4.105: icmp_seq=10 ttl=255 time=1.36 ms
64 bytes from 10.2.4.105: icmp_seq=11 ttl=255 time=0.937 ms
64 bytes from 10.2.4.105: icmp_seq=12 ttl=255 time=1.74 ms
64 bytes from 10.2.4.105: icmp_seq=13 ttl=255 time=1.88 ms
64 bytes from 10.2.4.105: icmp_seq=14 ttl=255 time=1.07 ms
64 bytes from 10.2.4.105: icmp_seq=15 ttl=255 time=1.13 ms
64 bytes from 10.2.4.105: icmp_seq=16 ttl=255 time=0.742 ms
```



Ivan Delgadillo Fernandez

NextWork Student

NextWork.org

Analyzing flow logs

This flow log shows 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").

For example, you might find one that says REJECT OK instead of ACCEPT OK at the end. These would represent the ping messages that failed to reach Instance 2!

The screenshot shows a list of log events for EC2 log events. The columns are 'Timestamp' and 'Message'. The 'Message' column contains detailed network flow information. Most entries show successful connections ('ACCEPT OK') while some show failed ones ('REJECT OK'). The log entries are as follows:

Timestamp	Message
2024-09-26T15:11:58.000Z	2 600627346491 en1-0459e5ba20b05419 18.237.140.165 10.1.14.121 31403 22 6 4 344 1727363518 1727363549 ACCEPT OK
2024-09-26T15:11:58.000Z	2 600627346491 en1-0459e5ba20b05419 10.1.14.121 10.206.107.27 22 31403 6 2 176 1727363518 1727363549 ACCEPT OK
2024-09-26T15:11:58.000Z	2 600627346491 en1-0459e5ba20b05419 99.214.27.14 10.1.14.121 42386 8881 6 1 44 1727363518 1727363549 REJECT OK
2024-09-26T15:11:58.000Z	2 600627346491 en1-0459e5ba20b05419 181.10.144.116 10.1.14.121 25319 23 6 1 48 1727363518 1727363549 REJECT OK
2024-09-26T15:11:58.000Z	2 600627346491 en1-0459e5ba20b05419 185.242.226.50 10.1.14.121 52381 7620 6 1 44 1727363518 1727363549 REJECT OK
2024-09-26T15:11:58.000Z	2 600627346491 en1-0459e5ba20b05419 165.154.51.90 10.1.14.121 44925 6160 6 1 60 1727363518 1727363549 REJECT OK
2024-09-26T15:11:58.000Z	2 600627346491 en1-0459e5ba20b05419 193.3.53.6 10.1.14.121 41492 47888 6 1 40 1727363518 1727363549 REJECT OK
2024-09-26T15:11:58.000Z	2 600627346491 en1-0459e5ba20b05419 164.52.0.9 10.1.14.121 58174 3333 6 1 44 1727363518 1727363549 REJECT OK
2024-09-26T15:11:58.000Z	2 600627346491 en1-0459e5ba20b05419 164.52.0.91 10.1.14.121 58176 3333 6 1 44 1727363518 1727363549 REJECT OK
2024-09-26T15:11:58.000Z	2 600627346491 en1-0459e5ba20b05419 45.84.89.3 10.1.14.121 63235 61616 6 1 52 1727363518 1727363549 REJECT OK



Ivan Delgadillo Fernandez

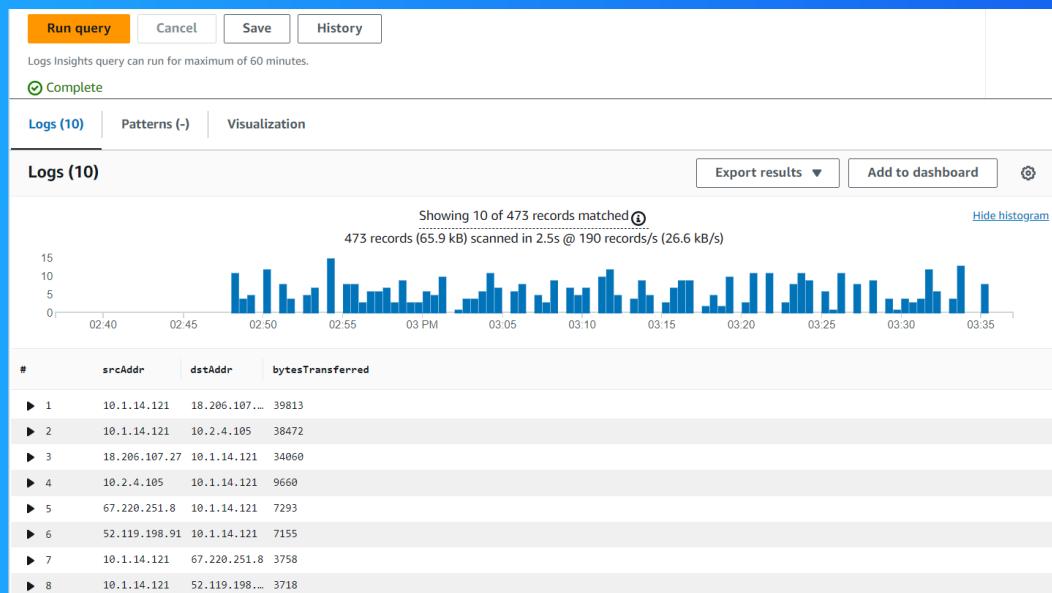
NextWork Student

NextWork.org

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!

Queries are like commands you run to analyze your logs! You can use queries to filter logs, group data, and perform calculations like sums and averages.





NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for
more projects

