



nextwork.org

VPC Monitoring with Flow Logs



saqibh49@gmail.com

The screenshot shows the AWS CloudWatch Logs Insights interface. At the top, there's a search bar and navigation links for 'Logs Insights QL', 'Query generator', 'Fields', 'Saved and sample queries', and 'Query commands'. Below that is a button for 'Run query' and a message indicating 'Completed. Query executed for 1 log group.' The main area has tabs for 'Logs (10)', 'Patterns (1)', and 'Visualization'. The 'Logs (10)' tab is selected, showing a histogram of log records over time (from 00:30 to 01:25) and a list of 529 matching records. The histogram shows a peak around 00:55. The log list table includes columns for '#', '@timestamp', and 'Message'. Each log entry starts with a right-pointing arrow and contains a timestamp, source IP, destination IP, port numbers, and a status like 'REJECT OK'. The bottom of the interface includes links for CloudShell, Feedback, and Console Mobile App, along with copyright information for 2026, Amazon Web Services, Inc. or its affiliates.

#	@timestamp	Message
1	2026-02-06T01:25:46.0...	2 510482603806 eni-07fe57effd32e861d 178.39.218.7 10.1.13.14 44319 8728 6 1 40 1770341146 1770341169 REJECT OK
2	2026-02-06T01:25:46.0...	2 510482603806 eni-07fe57effd32e861d 91.231.89.136 10.1.13.14 16348 5565 6 1 60 1770341146 1770341169 REJECT OK
3	2026-02-06T01:25:46.0...	2 510482603806 eni-07fe57effd32e861d 79.124.56.234 10.1.13.14 50684 11589 6 4 160 1770341146 1770341169 REJECT OK
4	2026-02-06T01:25:46.0...	2 510482603806 eni-07fe57effd32e861d 35.283.211.199 10.1.13.14 54839 47838 6 1 44 1770341146 1770341169 REJECT OK
5	2026-02-06T01:25:46.0...	2 510482603806 eni-07fe57effd32e861d 79.124.56.234 10.1.13.14 50684 10749 6 3 120 1770341146 1770341169 REJECT OK
6	2026-02-06T01:25:46.0...	2 510482603806 eni-07fe57effd32e861d 47.88.14.121 10.1.13.14 29290 11000 6 1 52 1770341146 1770341169 REJECT OK
7	2026-02-06T01:25:46.0...	2 510482603806 eni-07fe57effd32e861d 147.185.133.180 10.1.13.14 50684 48148 6 1 44 1770341146 1770341169 REJECT OK
8	2026-02-06T01:24:46.0...	2 510482603806 eni-07fe57effd32e861d 31.56.45.226 10.1.13.14 22 26708 6 1 40 1770341086 1770341113 REJECT OK
9	2026-02-06T01:24:46.0...	2 510482603806 eni-07fe57effd32e861d 71.6.135.131 10.1.13.14 29011 4567 6 1 44 1770341086 1770341113 REJECT OK
10	2026-02-06T01:24:46.0...	2 510482603806 eni-07fe57effd32e861d 162.216.150.116 10.1.13.14 54444 48917 6 1 44 1770341086 1770341113 REJECT OK

saqibh49@gmail.com

NextWork Student

nextwork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a sectioned off space within the large AWS cloud and it is useful because it provides secure spaces to users who need to store, share and access sensitive data within a network.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to test the connection between 2 VPCs and then explore the flow logs to better understand them.

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

One thing I didn't expect in this project was how complex the flow logs would be. They sent me into a bit of a downward spiral for a minute before I took a moment to understand the basics of them.

This project took me...

This project took me about an hour.

saqibh49@gmail.com

NextWork Student

nextwork.org

In the first part of my project...

Step 1 - Set up VPCs

In this step, I will set up my VPCs using the setup wizard because it is a much more efficient way of creating a VPC.

Step 2 - Launch EC2 instances

In this step, I will launch an EC2 instance in each of my VPCs because that will allow me to use Instance Connect to communicate between my VPCs later on.

Step 3 - Set up Logs

In this step, I will set up VPC Flow Logs because this will allow me to track and manage the types of data in my VPCs.

Step 4 - Set IAM permissions for Logs

In this step, I will create an IAM policy for my flow logs because that is how I can give permission to my flow logs to store data and send it CloudWatch.

saqibh49@gmail.com

NextWork Student

nextwork.org

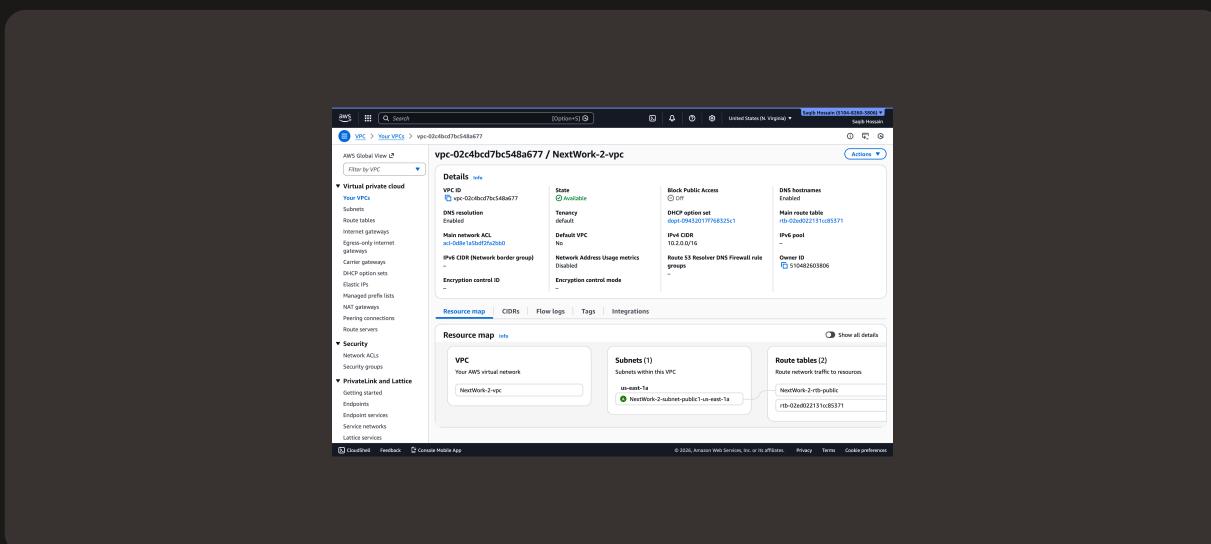
Multi-VPC Architecture

I started my project by launching 2 VPCs, each with 1 public subnet.

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 if resources in different connected VPC's have the same IP address, it can cause issues when accessing them.

I also launched EC2 instances in each subnet

My EC2 instances' security groups allow all ICMP traffic. This is because I will be using ICMP to communicate between my instances with Instance Connect.



saqibh49@gmail.com

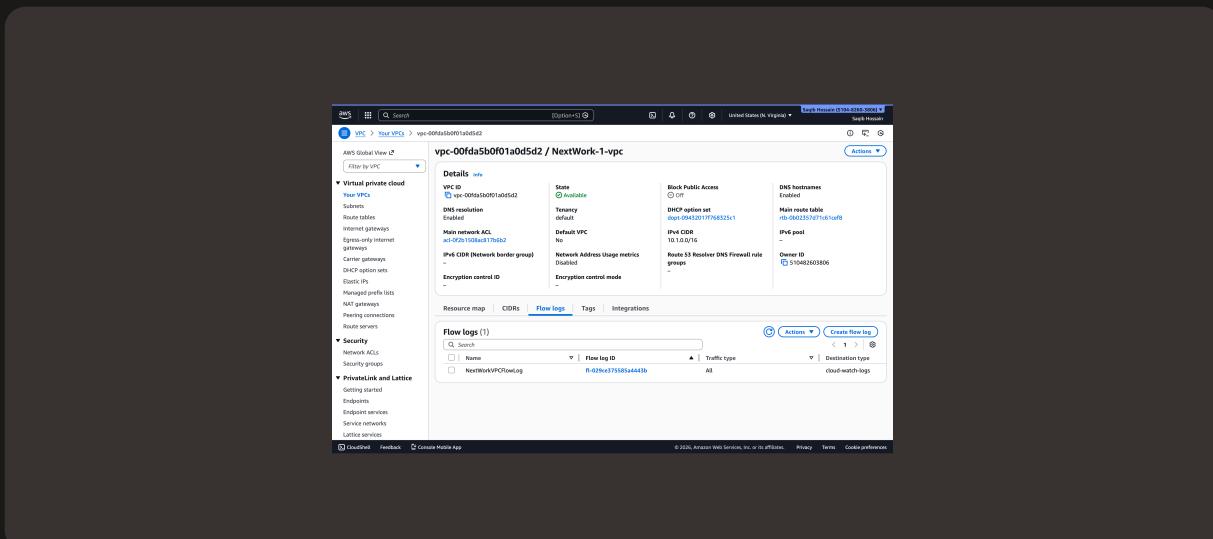
NextWork Student

nextwork.org

Logs

Logs are essentially notes on what is going on in the VPC. For example, if someone tries to login, that will show in the logs, if there's an error somewhere, that too will be in the logs, so on and so forth.

Log groups are folders for storing logs of the same category in one place.



saqibh49@gmail.com

NextWork Student

nextwork.org

IAM Policy and Roles

I created an IAM policy because this will allow my log flow to log data and send it wherever it needs to go.

I also created an IAM role because this role gives me the ability to create a rule that only allows the flow logs service to use my IAM policy's allowances.

A custom trust policy is essentially a rule within a role that tells AWS which service or services can access a role.

The screenshot shows the AWS IAM 'Create a new role' wizard. The current step is 'Configure permissions'. On the left, there is a 'Custom trust policy' section containing the following JSON code:

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

On the right, there are several configuration panels:

- Edit statement Statement1**: A link to edit the current trust policy statement.
- Add actions for STS**: A search bar and a checkbox for "All actions (sts:*)".
- Access level - read**: A list of checkboxes for various STS actions, none of which are checked.
- Access level - read or write**: A list of checkboxes for various STS actions, with the "AssumeRole" checkbox checked.
- Add a principal**: A button to add a principal to the role.
- Add a condition (optional)**: A button to add a condition to the role.

At the bottom of the page, there are links for CloudShell, Feedback, and Console Mobile App, along with copyright information for Amazon Web Services, Inc. and links for Privacy, Terms, and Cookie preferences.

saqibh49@gmail.com

NextWork Student

nextwork.org

In the second part of my project...

Step 5 - Ping testing and troubleshooting

In this step, I will send a message between my 2 instances because that will create traffic that my flow logs will pickup on, allowing me to test not only my flow logs, but also my VPC connection.

Step 6 - Set up a peering connection

In this step, I will set up a peering connection because this will provide a secure way for my 2 instances to communicate that doesn't send sensitive data over the open internet.

Step 7 - Analyze flow logs

In this step, I will review the flow logs because this will show me exactly what traffic came into my instances.

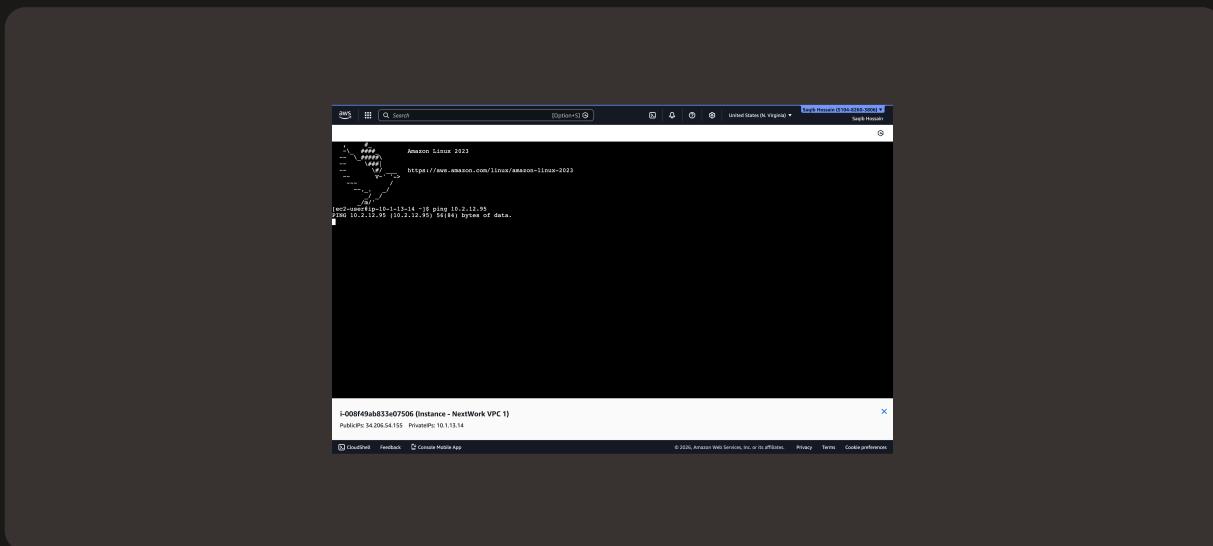
saqibh49@gmail.com

NextWork Student

nextwork.org

Connectivity troubleshooting

My first ping test between my EC2 instances had no replies, which means the message was sent, but no reply was received from the other instance, meaning its not getting my message.



I could receive ping replies if I ran the ping test using the other instance's public IP address, which means the other instance is able to receive traffic from the open internet, but I need to configure it to be able to receive traffic from server 1 without going through the open internet.

saqibh49@gmail.com

NextWork Student

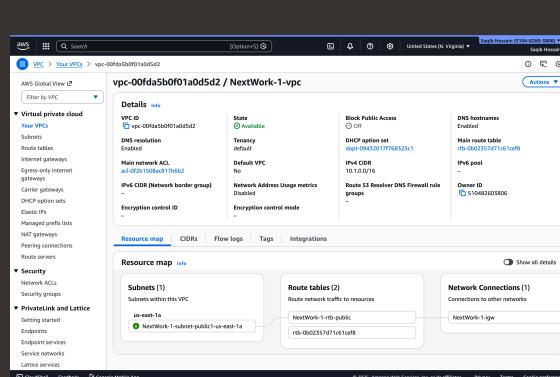
nextwork.org

Connectivity troubleshooting

Looking at VPC 1's route table, I identified that the ping test with Instance 2's private address failed because it doesn't have a direct link set up to the other instance.

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

I also updated both VPCs' route tables so that a new route connecting the 2 instances directly was added to each subnet.



saqibh49@gmail.com

NextWork Student

nextwork.org

Connectivity troubleshooting

I received ping replies from Instance 2's private IP address! This means that both instances are connected over a secure route that doesn't have to go through the open internet.

The screenshot shows a terminal window in the AWS CloudShell interface. The user has run a ping command from their local machine (IP 10.1.13.14) to an instance in a VPC (IP 13.222.113.154). The output shows 142 packets transmitted, 142 received, with 0% packet loss and a total time of 146616ms. The ping results are as follows:

```
64 bytes from 13.222.113.154: icmp_seq=1 ttl=126 time=0.292 ms
64 bytes from 13.222.113.154: icmp_seq=2 ttl=126 time=0.312 ms
64 bytes from 13.222.113.154: icmp_seq=3 ttl=126 time=0.311 ms
64 bytes from 13.222.113.154: icmp_seq=4 ttl=126 time=0.316 ms
64 bytes from 13.222.113.154: icmp_seq=5 ttl=126 time=0.316 ms
64 bytes from 13.222.113.154: icmp_seq=6 ttl=126 time=0.353 ms
64 bytes from 13.222.113.154: icmp_seq=7 ttl=126 time=0.353 ms
64 bytes from 13.222.113.154: icmp_seq=8 ttl=126 time=0.299 ms
64 bytes from 13.222.113.154: icmp_seq=9 ttl=126 time=0.316 ms
64 bytes from 13.222.113.154: icmp_seq=10 ttl=126 time=0.289 ms
64 bytes from 13.222.113.154: icmp_seq=11 ttl=126 time=0.311 ms
64 bytes from 13.222.113.154: icmp_seq=12 ttl=126 time=0.285 ms
64 bytes from 13.222.113.154: icmp_seq=13 ttl=126 time=0.267 ms
64 bytes from 13.222.113.154: icmp_seq=14 ttl=126 time=0.376 ms
64 bytes from 13.222.113.154: icmp_seq=15 ttl=126 time=0.367 ms
64 bytes from 13.222.113.154: icmp_seq=16 ttl=126 time=0.369 ms
64 bytes from 13.222.113.154: icmp_seq=17 ttl=126 time=0.290 ms
64 bytes from 13.222.113.154: icmp_seq=18 ttl=126 time=0.293 ms
64 bytes from 13.222.113.154: icmp_seq=19 ttl=126 time=0.296 ms
64 bytes from 13.222.113.154: icmp_seq=20 ttl=126 time=0.333 ms
64 bytes from 13.222.113.154: icmp_seq=21 ttl=126 time=0.331 ms
64 bytes from 13.222.113.154: icmp_seq=22 ttl=126 time=0.347 ms
^C
--- 13.222.113.154 ping statistics ---
142 packets transmitted, 142 received, 0% packet loss, time 146616ms
rtt min/avg/max/mdev = 0.267/0.316/0.353/0.079ms
[ec2-13-222-113-15-14-15] ping to 13.222.113.154
PING 13.222.113.154 (13.222.113.154) 56(84) bytes of data.
64 bytes from 13.222.113.154: icmp_seq=1 ttl=126 time=0.239 ms
64 bytes from 13.222.113.154: icmp_seq=2 ttl=126 time=0.278 ms
64 bytes from 13.222.113.154: icmp_seq=3 ttl=126 time=0.311 ms
64 bytes from 13.222.113.154: icmp_seq=4 ttl=126 time=0.397 ms
64 bytes from 13.222.113.154: icmp_seq=5 ttl=126 time=0.306 ms
64 bytes from 13.222.113.154: icmp_seq=6 ttl=126 time=0.313 ms
64 bytes from 13.222.113.154: icmp_seq=7 ttl=126 time=0.314 ms
64 bytes from 13.222.113.154: icmp_seq=8 ttl=126 time=0.273 ms
64 bytes from 13.222.113.154: icmp_seq=9 ttl=126 time=0.301 ms
64 bytes from 13.222.113.154: icmp_seq=10 ttl=126 time=0.291 ms
64 bytes from 13.222.113.154: icmp_seq=11 ttl=126 time=0.285 ms
64 bytes from 13.222.113.154: icmp_seq=12 ttl=126 time=0.270 ms
64 bytes from 13.222.113.154: icmp_seq=13 ttl=126 time=0.298 ms

```

i-008f49ab833e07506 (Instance - NextWork VPC 1)

Public IPs: 34.206.54.155 Private IPs: 10.1.13.14

CloudShell Feedback Console Mobile App

© 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

saqibh49@gmail.com

NextWork Student

nextwork.org

Analyzing flow logs

Flow logs tell us the amount of data that was sent from which IP address to which IP address, from which port, how many packets it contained, and whether it was allowed or rejected.

For example, the flow log I've captured tells us that the data was sent from 35.203.210.53 to 10.1.13.14, it was received at port 6 and it was only 1 packet. Finally, it says that it was rejected but the data was logged successfully, as marked by the OK.

The screenshot shows the AWS CloudWatch Log Management interface. The left sidebar has a 'Log Management' tree view with nodes like 'CloudWatch', 'Favorites and recent', 'Logs', and 'Metrics'. Under 'Logs', 'Log Management Tree' is selected. The main area is titled 'Log events' and shows a list of log entries. A search bar at the top says 'You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns.' Below the search bar are buttons for 'Actions', 'Start tailing', 'Create metric filter', and 'Display' (set to '1m'). The log entries are timestamped and show various network traffic details, including source and destination IP addresses, ports, and actions like 'REJECT OK'.

Timestamp	Message
2020-02-07T01:08:16,000Z	2.53M42080000.eni-0f767a4f052d8481.35.203.210.53.18.1.13.14.55C7B.50806.6.1.44.3798339616.3798339645.RL
2020-02-07T01:08:16,000Z	2.53M42080000.eni-0f767a4f052d8481.35.203.210.53.18.1.13.14.55C7B.50806.6.1.44.3798339616.3798339645.REJECT OK
2020-02-07T01:08:16,000Z	2.53M42080000.eni-0f767a4f052d8481.162.216.149.232.18.1.13.14.5995.2897.6.1.44.3798339616.3798339645.RL
2020-02-07T01:08:16,000Z	2.53M42080000.eni-0f767a4f052d8481.136.299.179.32.18.1.13.14.5995.68.6.1.49.3798339616.3798339645.RL
2020-02-07T01:08:16,000Z	2.53M42080000.eni-0f767a4f052d8481.162.216.149.232.18.1.13.14.5995.68.6.1.49.3798339616.3798339645.RL
2020-02-07T01:08:16,000Z	2.53M42080000.eni-0f767a4f052d8481.35.283.201.154.18.1.13.14.5995.68.6.1.49.3798339616.3798339645.RL
2020-02-07T01:08:16,000Z	2.53M42080000.eni-0f767a4f052d8481.154.283.201.154.18.1.13.14.5995.68.6.1.49.3798339616.3798339645.RL
2020-02-07T01:08:16,000Z	2.53M42080000.eni-0f767a4f052d8481.154.283.201.154.18.1.13.14.5995.68.6.1.49.3798339616.3798339645.RL
2020-02-07T01:08:16,000Z	2.53M42080000.eni-0f767a4f052d8481.154.283.201.154.18.1.13.14.5995.68.6.1.49.3798339616.3798339645.RL
2020-02-07T01:08:16,000Z	2.53M42080000.eni-0f767a4f052d8481.15.221.155.155.18.1.13.14.5995.68.6.1.49.3798339616.3798339645.RL
2020-02-07T01:08:16,000Z	2.53M42080000.eni-0f767a4f052d8481.13.221.155.155.18.1.13.14.5995.68.6.1.49.3798339616.3798339645.RL
2020-02-07T01:08:16,000Z	2.53M42080000.eni-0f767a4f052d8481.13.221.155.155.18.1.13.14.5995.68.6.1.49.3798339616.3798339645.ACCEPT
2020-02-07T01:08:16,000Z	2.53M42080000.eni-0f767a4f052d8481.18.1.13.14.5995.68.6.1.50.3798339616.3798339645.ACCEPT
2020-02-07T01:08:16,000Z	2.53M42080000.eni-0f767a4f052d8481.147.181.155.49.18.1.13.14.5995.69.6.1.44.3798339644.3798339645.RL
2020-02-07T01:08:16,000Z	2.53M42080000.eni-0f767a4f052d8481.136.289.179.181.18.1.13.14.5995.68.6.1.49.3798339644.3798339645.RL
2020-02-07T01:08:16,000Z	2.53M42080000.eni-0f767a4f052d8481.205.238.21.27.18.1.13.14.53873.508.6.1.44.3798339644.3798339645.RL
2020-02-07T01:08:16,000Z	2.53M42080000.eni-0f767a4f052d8481.162.216.149.232.18.1.13.14.5995.69.6.1.49.3798339644.3798339645.RL
2020-02-07T01:08:16,000Z	7.176A000000.eni-0f767a4f052d8481.162.216.149.232.18.1.13.14.5995.69.6.1.49.3798339644.3798339645.RL

saqibh49@gmail.com

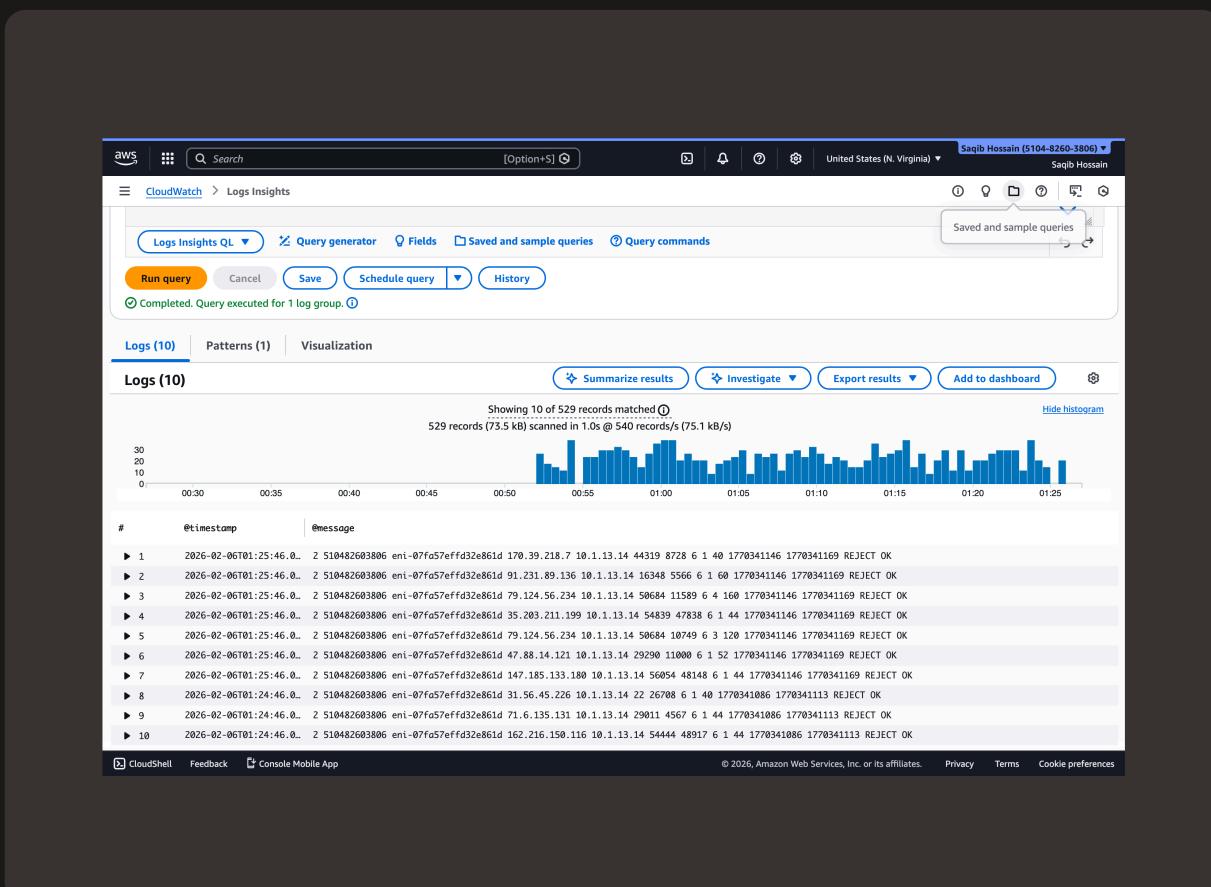
NextWork Student

nextwork.org

Logs Insights

Logs Insights is a way to search through logs using queries.

I ran the query: fields @timestamp, @message | sort @timestamp desc | limit 10
This query analyzes 10 of the most recent logs.





nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects

