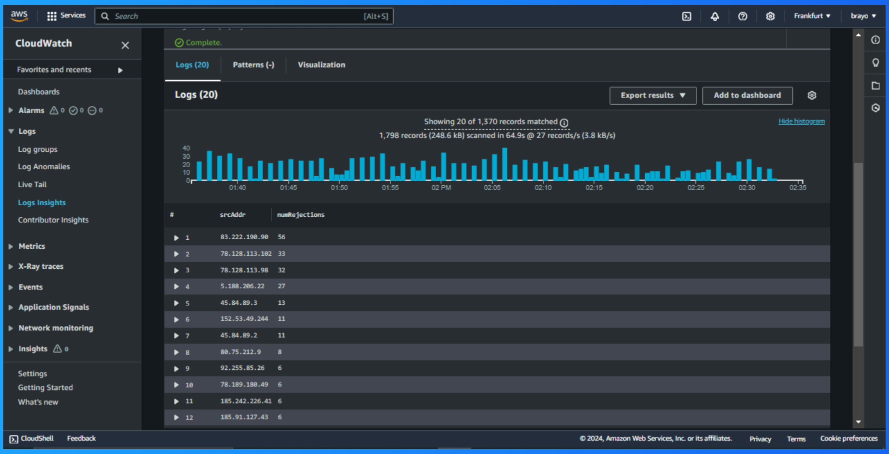
NextWork.org

VPC Monitoring with Flow Logs

Brian Kimemia N



Logs (20)

Showing 20 of 1,370 records matched
1,798 records (248.6 kB) scanned in 64.9s @ 27 records/s (3.8 kB/s)

#	srcAddr	numRejections
1	83.222.190.90	56
2	78.128.113.102	33
3	78.128.113.98	32
4	5.188.206.22	27
5	45.84.89.3	13
6	152.53.49.244	11
7	45.84.89.2	11
8	80.75.212.9	8
9	92.255.85.26	6
10	78.189.180.49	6
11	185.242.226.41	6
12	185.91.127.43	6

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) lets you create a private, isolated network in the AWS Cloud. It’s useful for controlling IP ranges, security, and access to resources, enabling secure and customized networking for your applications.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create two isolated networks with public subnets, set up a peering connection between them, and configured IAM,Cloudwatch and VPC Flow Logs to monitor network traffic and analyze connectivity issues.

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

One thing I didn't expect in this project was the level of insight VPC Flow Logs provided. Seeing detailed logs on network traffic rejections and byte transfers gave me a clearer understanding of network patterns and potential issues.

This project took me...

This project took me around 2. hours to complete. Setting up the VPCs, configuring flow logs, and analyzing data in CloudWatch Logs Insights required careful attention to detail, but it was manageable within that time frame.

In the first part of my project...

Step 1 - Set up VPCs

Create two VPCs

Step 2 - Launch EC2 instances

Launch an EC2 instance in each VPC, so we can use them to test your VPC peering connection later (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

Start monitoring VPC traffic. We're using a tool called VPC flow logs to do this. let's set them up . In this step, we're going to:. Set up a way to track all inbound and outbound network traffic.. Set up a space that stores all of these records.

Step 4 - Set IAM permissions for Logs

Give VPC Flow Logs the permission to write logs and send them to CloudWatch.. Finish setting up your subnet's flow log.

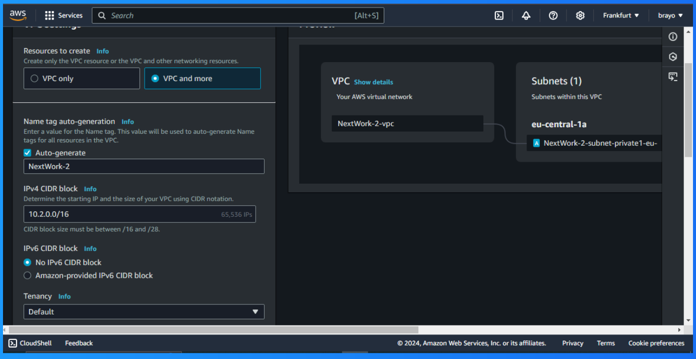
Multi-VPC Architecture

I started my project by launching two Amazon VPCs to set up isolated networks for testing. In each VPC, I created multiple subnets to distribute resources across availability zones, ensuring better network architecture and connectivity for peering.

The CIDR blocks for VPCs 1 and 2 are 10.0.0.0/16 and 192.168.0.0/16, respectively. They have to be unique because VPCs are isolated networks, and overlapping CIDR blocks would cause routing conflicts, preventing proper communication between the two.

I also launched EC2 instances in each subnet

My EC2 instances' security groups allow ICMP traffic from all IP addresses (0.0.0.0/0). This is because we need to perform a ping test, (requires ICMP traffic to be allowed from any IP address), ensuring connectivity between the instances in each VPC



Resources to create Info
Create only the VPC resource or the VPC and other networking resources.
VPC only [✓ VPC and more]

Name tag auto-generation Info
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.
✓ Auto-generate
NextWork-2

IPv4 CIDR block Info
Determine the starting IP and the size of your VPC using CIDR notation.
10.2.0.0/16 65,536 IPs
CIDR block size must be between /16 and /28.

IPv6 CIDR block Info
[✓ No IPv6 CIDR block]
Amazon-provided IPv6 CIDR block

Tenancy Info
Default

VPC Show details
Your AWS virtual network
NextWork-2-vpc

Subnets (1)
Subnets within this VPC
eu-central-1a
NextWork-2-subnet-private1-eu-

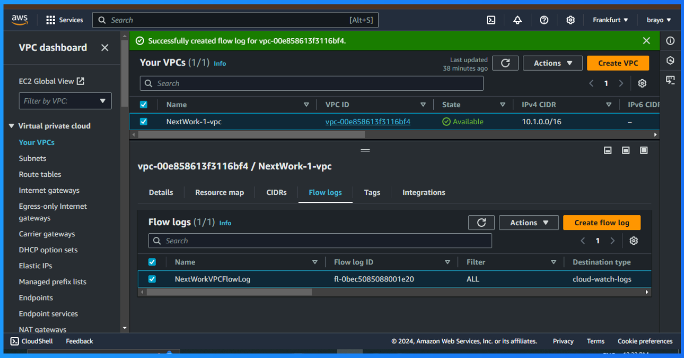
Brian Kimemia N
NextWork Student

Logs

Logs are records of events or activities in a system that help with monitoring, troubleshooting, and analyzing performance, providing valuable insights for diagnosing issues or auditing actions.

Log groups are containers in AWS CloudWatch that organize and store logs from different sources, such as EC2 instances or Lambda functions. They help manage and monitor logs more efficiently by grouping related log streams together.

I also set up a flow log for VPC 1



Successfully created flow log for vpc-00e858613f3116bf4.

Your VPCs (1/1) Info — Last updated 38 minutes ago

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
NextWork-1-vpc	vpc-00e858613f3116bf4	Available	10.1.0.0/16	–

vpc-00e858613f3116bf4 / NextWork-1-vpc

Flow logs (1/1) Info

Name	Flow log ID	Filter	Destination type
NextWorkVPCFlowLog	fl-0bec5085088001e20	ALL	cloud-watch-logs

© 2024, Amazon Web Services, Inc. or its affiliates.

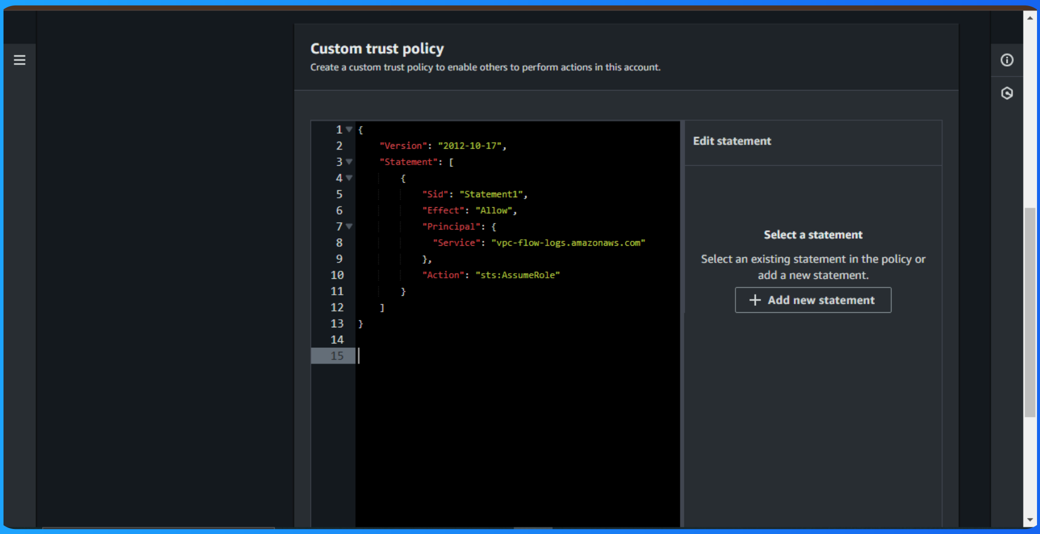
Brian Kimemia N
NextWork Student

IAM Policy and Roles

I created an IAM policy because it allows me to define specific permissions for accessing and managing CloudWatch logs. This ensures that only authorized users or services can read, write, or modify log data

I also created an IAM role because it allows VPC Flow Logs to assume specific permissions to write logs to CloudWatch,hence,I ensuring VPC Flow Logs service can securely deliver flow log data to my CloudWatch log group for monitoring and analysis.

A custom trust policy is a set of permissions in IAM that specifies which AWS services or accounts are allowed to assume a particular IAM role, enabling secure cross-service and cross-account access.



Custom trust policy

Create a custom trust policy to enable others to perform actions in this account.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Principal": {
              "Service": "vpc-flow-logs.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}

```

Edit statement
Select a statement
Select an existing statement in the policy or add a new statement.
Add new statement

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, testing our VPC peering setup

Step 6 - Set up a peering connection

Create a Peering Connection and Configure Route Tables.Let's add that peering connection in this step to bridge our VPCs together! ▯

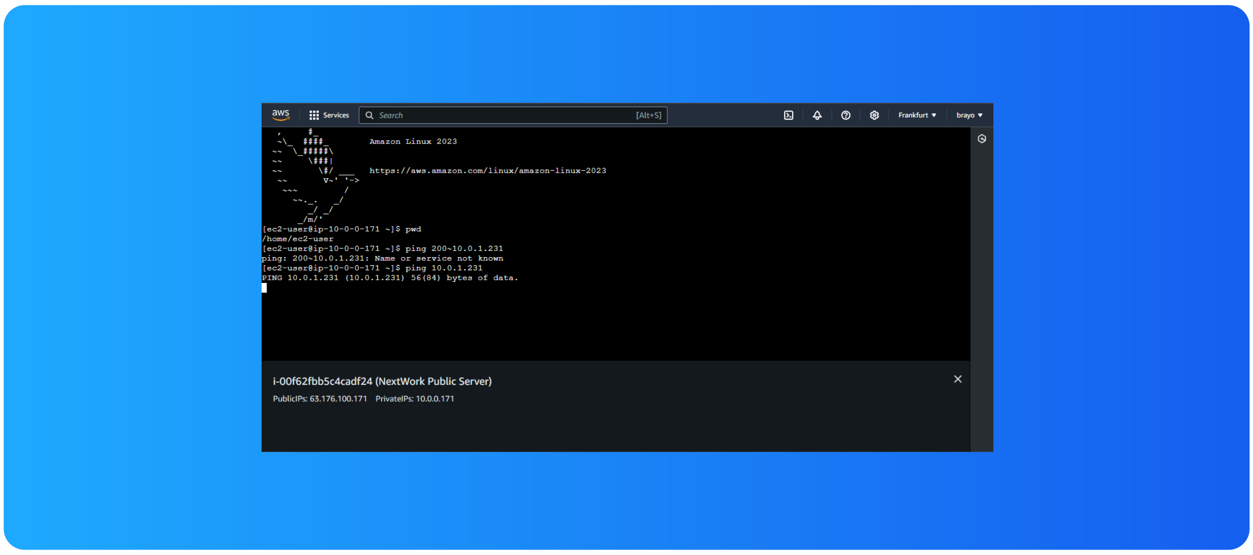
Step 7 - Analyze flow logs

check out what VPC Flow Logs has recorded about our network's activity!It's monitoring time 😎▯ We're going to: Review the flow logs recorded aboout VPC 1's public subnet.. Analyse the flow logs to get some tasty insights ▯

Brian Kimemia N
NextWork Student

Connectivity troubleshooting

My first ping test between my EC2 instances had no replies, which means there was likely a connectivity issue between them. This could be due to incorrect security group settings, missing VPC peering, or misconfigured route tables



```
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-10-0-0-171 ~]$ pwd
/home/ec2-user
[ec2-user@ip-10-0-0-171 ~]$ ping 200~10.0.1.231
ping: 200~10.0.1.231: Name or service not known
[ec2-user@ip-10-0-0-171 ~]$ ping 10.0.1.231
PING 10.0.1.231 (10.0.1.231) 56(84) bytes of data.
```

i-00f62fbb5c4cadf24 (NextWork Public Server)
PublicIPs: 63.176.100.171 PrivateIPs: 10.0.0.171

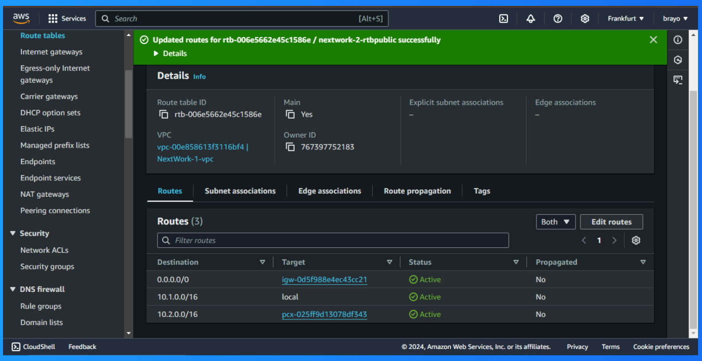
I could receive ping replies if I ran the ping test using the other instance's public IP address, which means the network connectivity between the two instances is working, and the security groups are correctly configured to allow ICMP traffic.

Connectivity troubleshooting

Looking at VPC 1's route table, I identified that the ping test with Instance 2's private address failed because there was no route configured to direct traffic from VPC 1 to VPC 2's private IP addresses.

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

I also updated both VPCs' route tables so that traffic could be correctly routed between the two VPCs over the peering connection. This allowed instances in each VPC to communicate with each other using their private IP addresses.



Updated routes for rtb-006e5662e45c1586e / nextwork-2-rtbpublic successfully

Details Info

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-006e5662e45c1586e	Yes	–	–

VPC: vpc-00e858613f3116bf4 \| NextWork-1-vpc
Owner ID: 767397752183

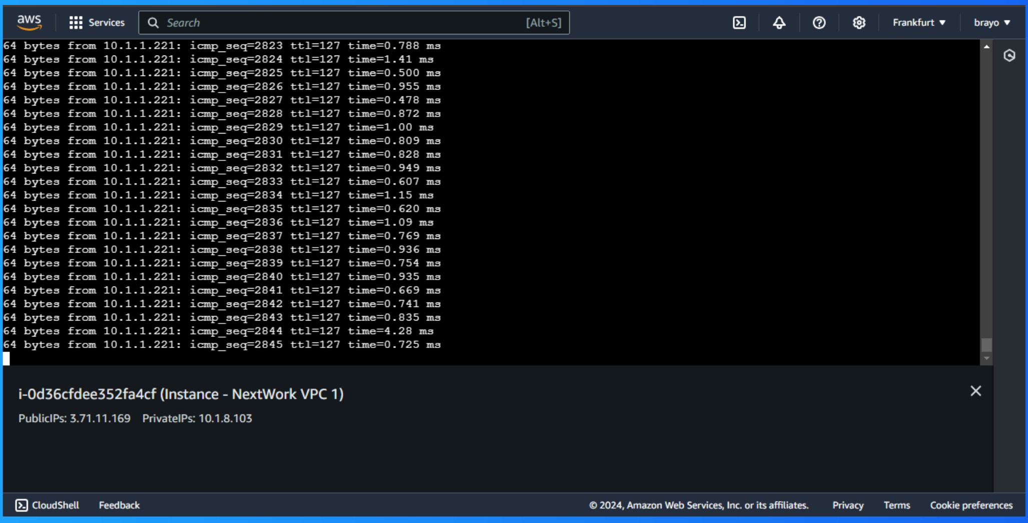
Routes (3)

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0d5f988e4ec43cc21	Active	No
10.1.0.0/16	local	Active	No
10.2.0.0/16	pcx-025ff9d13078df343	Active	No

© 2024, Amazon Web Services, Inc. or its affiliates.

Connectivity troubleshooting

I received ping replies from Instance 2's private IP address! This means the VPC peering connection is working correctly, and traffic between the two instances in different VPCs is being routed successfully through their private IP addresses.



```
64 bytes from 10.1.1.221: icmp_seq=2823 ttl=127 time=0.788 ms
64 bytes from 10.1.1.221: icmp_seq=2824 ttl=127 time=1.41 ms
64 bytes from 10.1.1.221: icmp_seq=2825 ttl=127 time=0.500 ms
64 bytes from 10.1.1.221: icmp_seq=2826 ttl=127 time=0.955 ms
64 bytes from 10.1.1.221: icmp_seq=2827 ttl=127 time=0.478 ms
64 bytes from 10.1.1.221: icmp_seq=2828 ttl=127 time=0.872 ms
64 bytes from 10.1.1.221: icmp_seq=2829 ttl=127 time=1.00 ms
64 bytes from 10.1.1.221: icmp_seq=2830 ttl=127 time=0.809 ms
64 bytes from 10.1.1.221: icmp_seq=2831 ttl=127 time=0.828 ms
64 bytes from 10.1.1.221: icmp_seq=2832 ttl=127 time=0.949 ms
64 bytes from 10.1.1.221: icmp_seq=2833 ttl=127 time=0.607 ms
64 bytes from 10.1.1.221: icmp_seq=2834 ttl=127 time=1.15 ms
64 bytes from 10.1.1.221: icmp_seq=2835 ttl=127 time=0.620 ms
64 bytes from 10.1.1.221: icmp_seq=2836 ttl=127 time=1.09 ms
64 bytes from 10.1.1.221: icmp_seq=2837 ttl=127 time=0.769 ms
64 bytes from 10.1.1.221: icmp_seq=2838 ttl=127 time=0.936 ms
64 bytes from 10.1.1.221: icmp_seq=2839 ttl=127 time=0.754 ms
64 bytes from 10.1.1.221: icmp_seq=2840 ttl=127 time=0.935 ms
64 bytes from 10.1.1.221: icmp_seq=2841 ttl=127 time=0.669 ms
64 bytes from 10.1.1.221: icmp_seq=2842 ttl=127 time=0.741 ms
64 bytes from 10.1.1.221: icmp_seq=2843 ttl=127 time=0.835 ms
64 bytes from 10.1.1.221: icmp_seq=2844 ttl=127 time=4.28 ms
64 bytes from 10.1.1.221: icmp_seq=2845 ttl=127 time=0.725 ms
```

i-0d36cfdee352fa4cf (Instance - NextWork VPC 1)

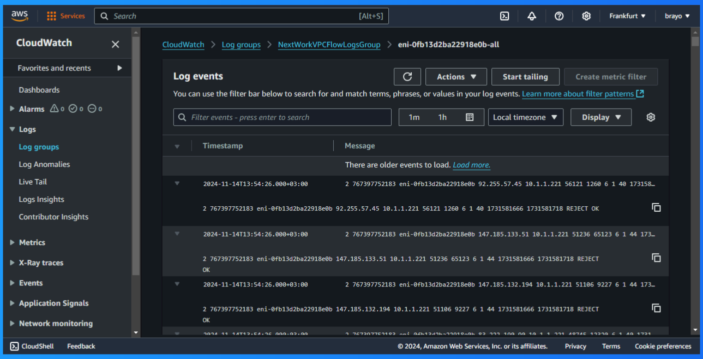
PublicIPs: 3.71.11.169 PrivateIPs: 10.1.8.103

Brian Kimemia N
NextWork Student

Analyzing flow logs

Flow logs tell us about network traffic, including the timestamp, source and destination IPs, ports, protocol, number of packets and bytes, action (accept/reject), and the status of the log.

For example, the flow log I've captured tells us that a network request from the source IP 92.255.57.45 to the destination IP 10.1.1.221 was rejected. The request was on port 56121 using the TCP protocol, and it involved 1260 bytes of data.



CloudWatch > Log groups > NextWorkVPCFlowLogsGroup > eni-0fb13d2ba22918e0b-all

Log events

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

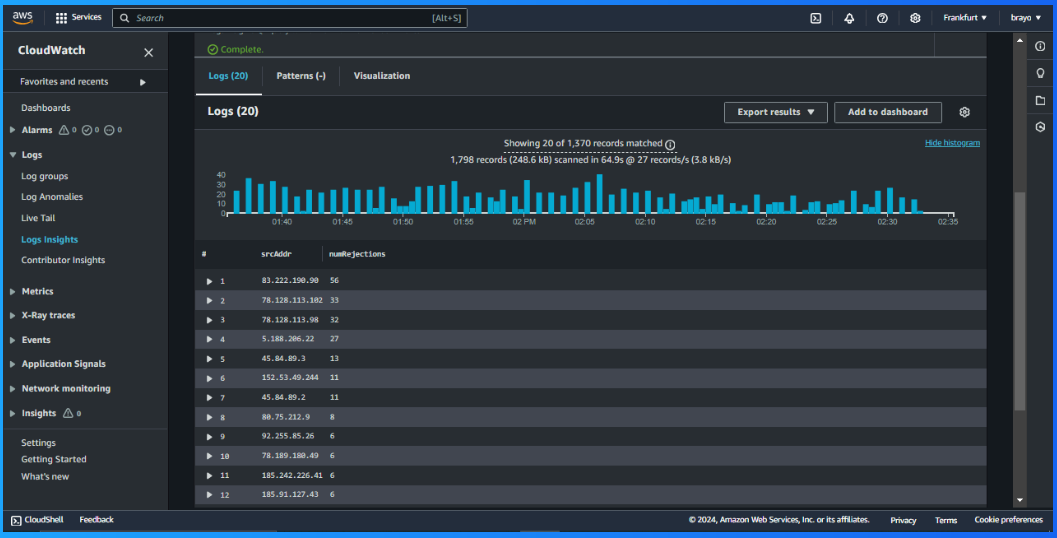
```
Timestamp                       Message
                                There are older events to load. Load more.
2024-11-14T13:54:26.000+03:00   2 767397752183 eni-0fb13d2ba22918e0b 92.255.57.45 10.1.1.221 56121 1260 6 1 40 173158…
2 767397752183 eni-0fb13d2ba22918e0b 92.255.57.45 10.1.1.221 56121 1260 6 1 40 1731581666 1731581718 REJECT OK
2024-11-14T13:54:26.000+03:00   2 767397752183 eni-0fb13d2ba22918e0b 147.185.133.51 10.1.1.221 51236 65123 6 1 44 173…
2 767397752183 eni-0fb13d2ba22918e0b 147.185.133.51 10.1.1.221 51236 65123 6 1 44 1731581666 1731581718 REJECT
OK
2024-11-14T13:54:26.000+03:00   2 767397752183 eni-0fb13d2ba22918e0b 147.185.132.194 10.1.1.221 51106 9227 6 1 44 173…
2 767397752183 eni-0fb13d2ba22918e0b 147.185.132.194 10.1.1.221 51106 9227 6 1 44 1731581666 1731581718 REJECT
OK
```

Brian Kimemia N
NextWork Student

Logs Insights

Logs Insights is a powerful tool within Amazon CloudWatch that allows you to run queries on log data, helping to analyze, filter, and extract insights from logs in real-time.

I ran the query filter action="REJECT" | stats count(*) as numRejections by srcAddr | sort numRejections desc | limit 20. This query analyzes rejected network connections, showing the top 20 source IPs with the most rejections



Logs (20)

Showing 20 of 1,370 records matched
1,798 records (248.6 kB) scanned in 64.9s @ 27 records/s (3.8 kB/s)

#	srcAddr	numRejections
1	83.222.190.90	56
2	78.128.113.102	33
3	78.128.113.98	32
4	5.188.206.22	27
5	45.84.89.3	13
6	152.53.49.244	11
7	45.84.89.2	11
8	80.75.212.9	8
9	92.255.85.26	6
10	78.189.180.49	6
11	185.242.226.41	6
12	185.91.127.43	6