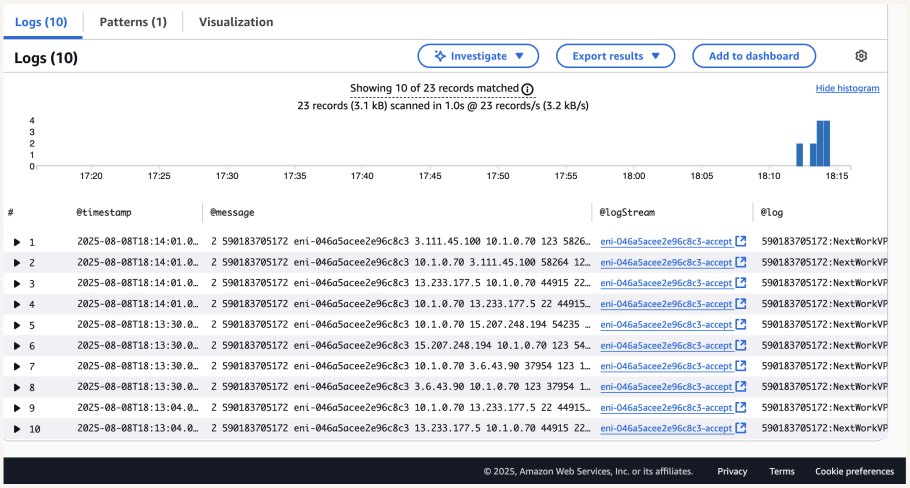
nextwork.org

# VPC Monitoring with Flow Logs

Gaurav Balpande



**Gaurav Balpande**
NextWork Student



# Introducing Today's Project!

## What is Amazon VPC?

Amazon VPC is the fundamental networking tool which is used for creation of private space within the AWS region. It is needed for security and to easily manage the resources.

## How I used Amazon VPC in this project

in today's project i had perform various monitoring tool which include cloudwatch and flow logs.

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

One thing I never expected is that we can easily create diagram for queries of logs with insight feature..

## This project took me...

it took near to 2.30 hr and it slightly hard.

# In the first part of my project...

## Step 1 - Set up VPCs

In this step,we are going to build the infrastructure by building two VPC with one public subnet in each and also some security tool we would apply.

## Step 2 - Launch EC2 instances

In this step we are going to launch Ec2 instance in each VPC so that we will be able to send data from one VPC to other.

## Step 3 - Set up Logs

In this step, we are going to add the monitoring tool AWS FLOW LOGS. It is a place where all the logs will be stored and we can make decison based on it.

## Step 4 - Set IAM permissions for Logs

In this step,we are going to build IAM role as it would not be possible for flow logs to send information to Amazon cloudwatch and also for storing and loging we would need IAM role.

**Gaurav Balpande**
NextWork Student



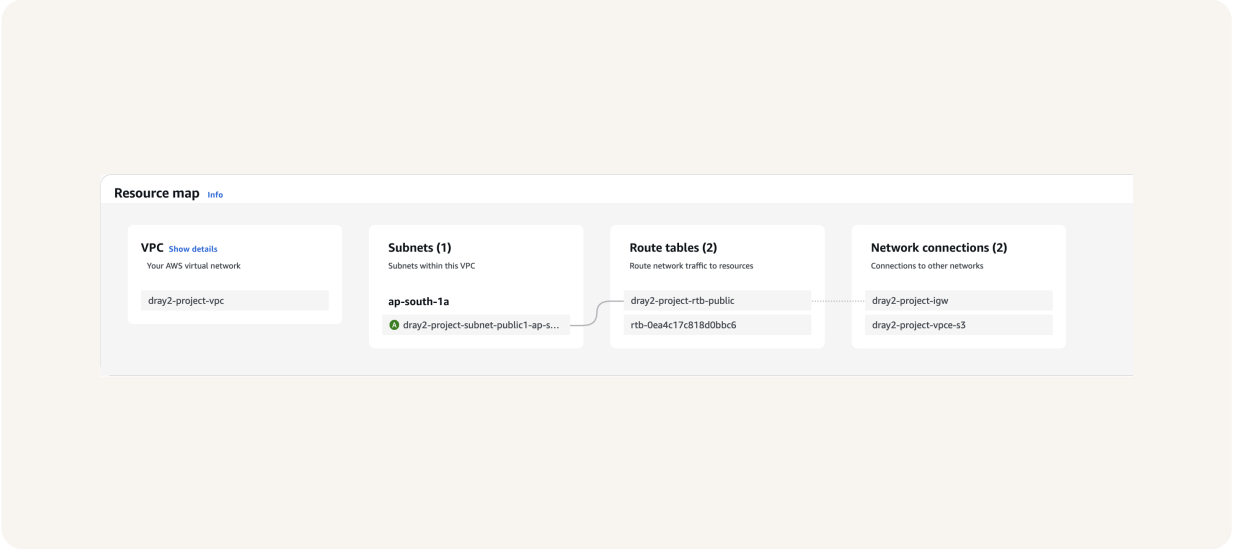
# Multi-VPC Architecture

I started my project by launching two VPC with one public subnet in each.

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 we are going to peer and peering can create a conflict.

## I also launched EC2 instances in each subnet

My EC2 instances' security groups allow all ICMP traffic This is because for sending data from one VPC to other we need to have ICMP messages be able to send.



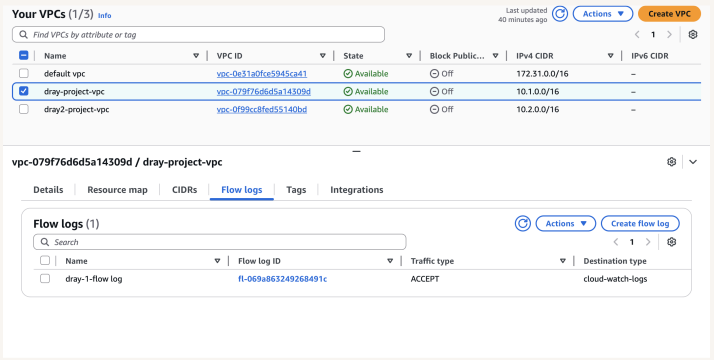
**Gaurav Balpande**
NextWork Student



# Logs

Logs are like a diary which store all the information related to a topic.

Log groups are like a folder which contain information related to a specific type and can be used for debigging and finding solution.



**Gaurav Balpande**
NextWork Student

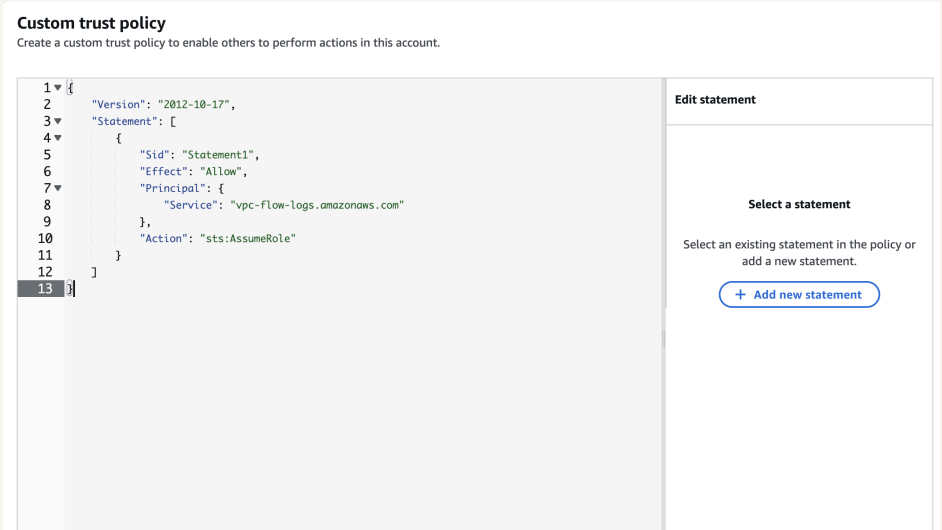


# IAM Policy and Roles

I created an IAM policy because for various task like creation and descrption of log group,log stream in cloudwatch we would need IAM role.

I also created an IAM role because for various task like creation and description of log group and log stream rewuired IAM roles.

A custom trust policy is to very narowly assign policy to specufic resource.



# In the second part of my project...

## Step 5 - Ping testing and troubleshooting

In this step for checking the flow log we will send message from one instance to other instance and that too in different VPC. So we will create instance in two VPC and send data from one to other.

## Step 6 - Set up a peering connection

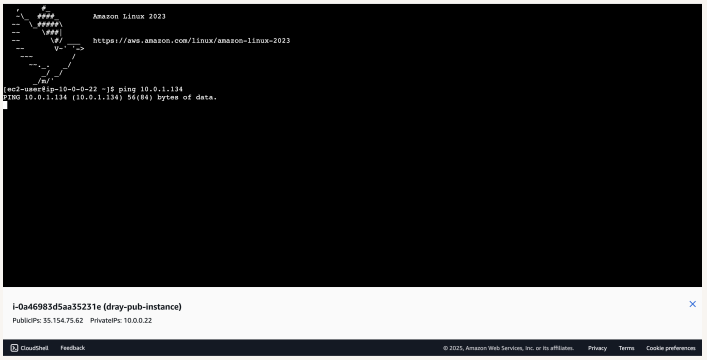
In this step,we are going to create a VPC peering between the two VPC so that there is a private connection between the two.

## Step 7 - Analyze flow logs

In this step,we are finally going to observe and anlysis the logs on cloudwatch and will analyse the insights.

# Connectivity troubleshooting

My first ping test between my EC2 instances had no replies, which means there is no VPC peering.




I could receive ping replies if I ran the ping test using the other instance's public IP address, which means that the public ip can be ping from any instance.

**Gaurav Balpande**
NextWork Student

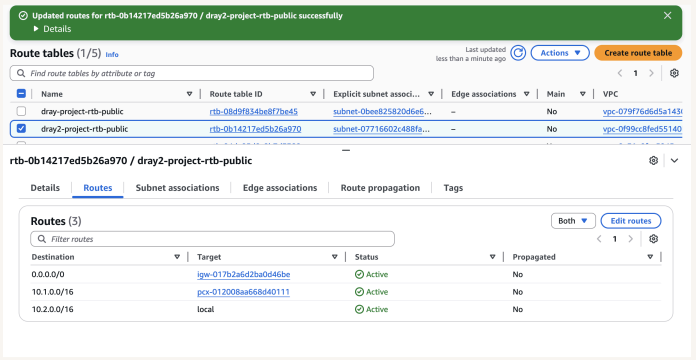


# Connectivity troubleshooting

Looking at VPC 1's route table, I identified that the ping test with Instance 2's private address failed because there is no route table for VPC peering.

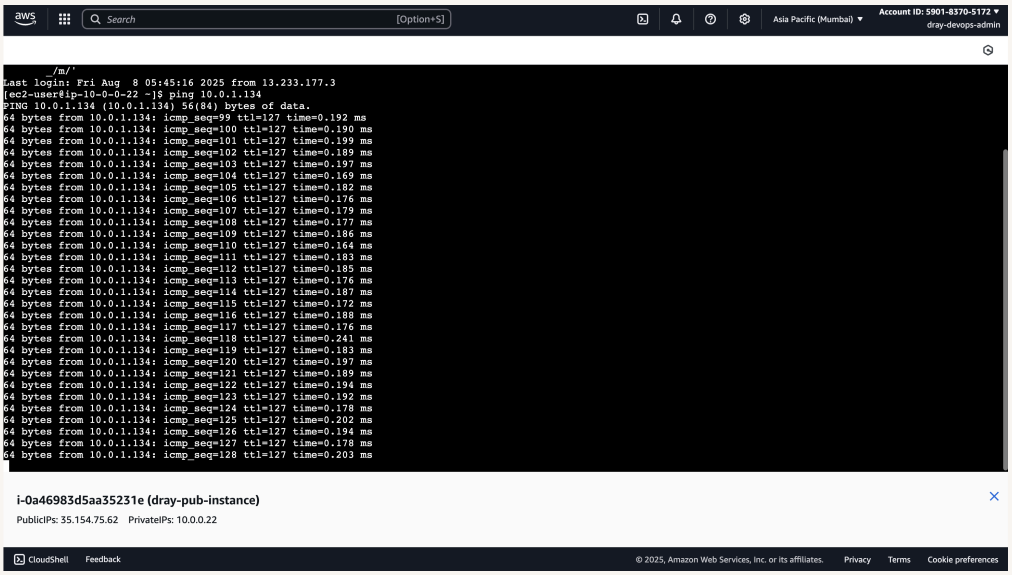
## To solve this, I set up a peering connection between my VPCs

I also updated both VPCs' route tables so that there is peering connection between the two instances.



# Connectivity troubleshooting

I received ping replies from Instance 2's private IP address! This means that the peering connection is set successfully.



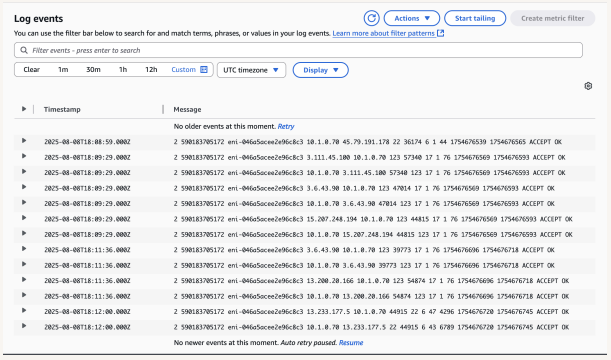
**Gaurav Balpande**
NextWork Student



# Analyzing flow logs

Flow logs tell us about all the necessary information like source port,destination port,entry time,completion time,id,ENI id,etc

For example, the flow log I've captured tells us 2025-08-08T18:08:59.000Z 2 590183705172 eni-046a5acee2e96c8c3 10.1.0.70 45.79.191.178 22 36174 6 1 44 1754676539 1754676565 ACCEPT OK 2025-08-08T18:09:29.000Z 2 590183705172 eni-046a5acee2e96c8c3 3.111



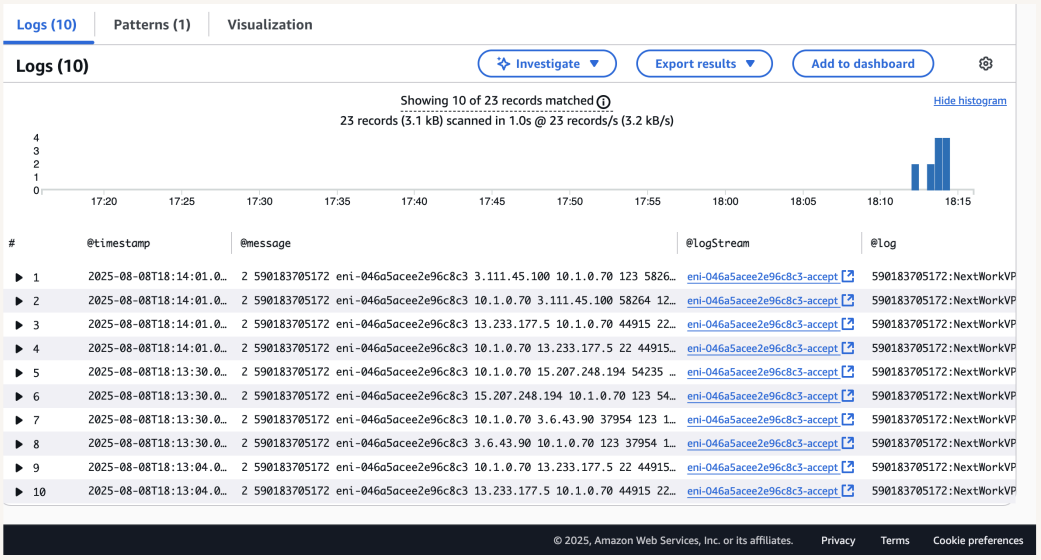
**Gaurav Balpande**
NextWork Student



# Logs Insights

Logs Insights is a tool in aws which helps us in understanding the logs by providing the feature of queries and diagram.

I ran the query Top 10 byte transfers by source and destination IP addresses This query analyzes the top 10 address with highest traffic.



# The place to learn & showcase your skills

Check out nextwork.org for more projects