Project 2

Configure VPC Flow Logs and Store Logs in S3 Using IAM Role

Batch

MCA 7 Feb 2025 &
DevOps 2 Jun 2025

Name

Suraj Molke

Name of the Mentor

Ravindra Bagle Sir
Swati Zampal Ma'am

Fortune Cloud Technologies

2nd Floor, Shirodkar House, Opposite To Amit Cafe, Congress House Road, Near Pune Municipal Corporation, Shivajinagar, Pune - 411005.

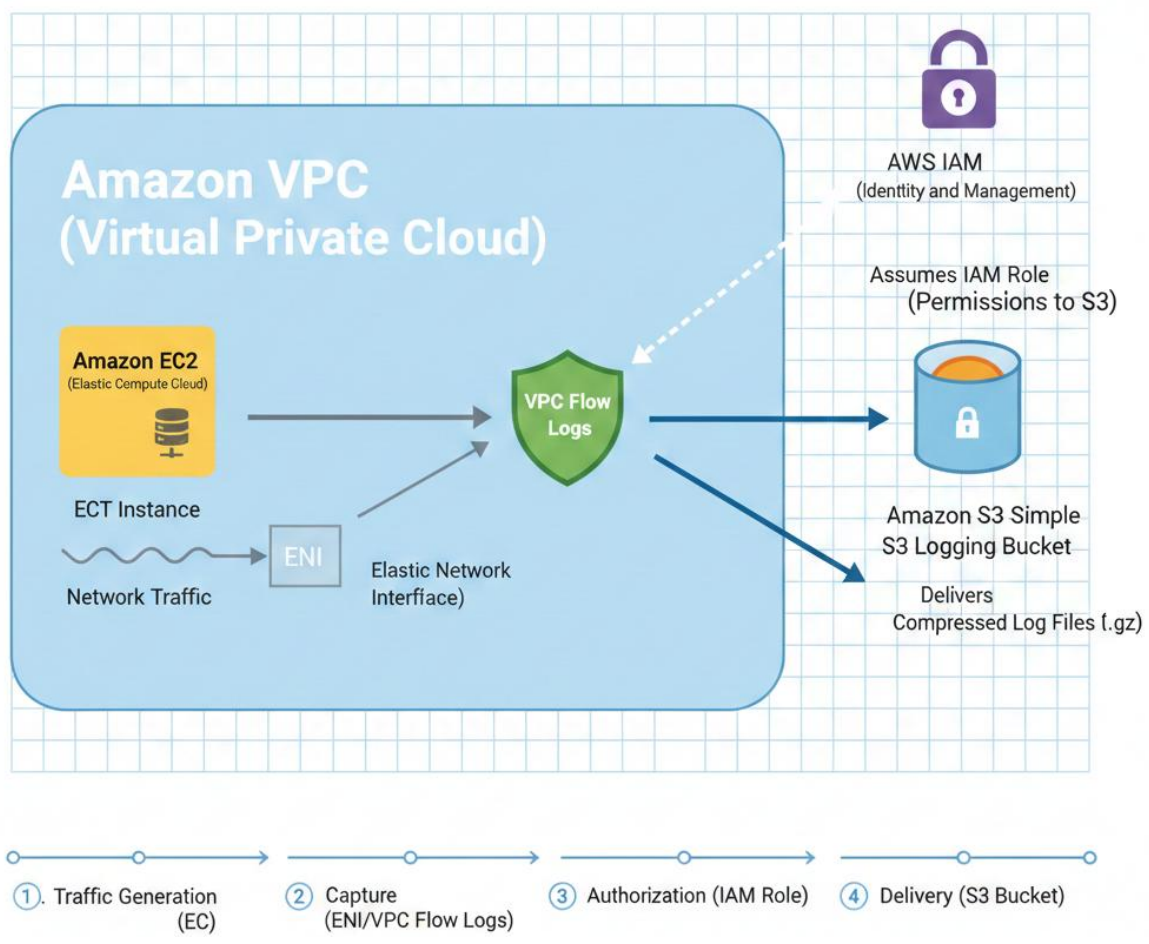
smolke9@gmail.com Suraj Molke Smolke9

Project Title: Configure VPC Flow Logs and Store Logs in S3Using IAM Role:

Objective:

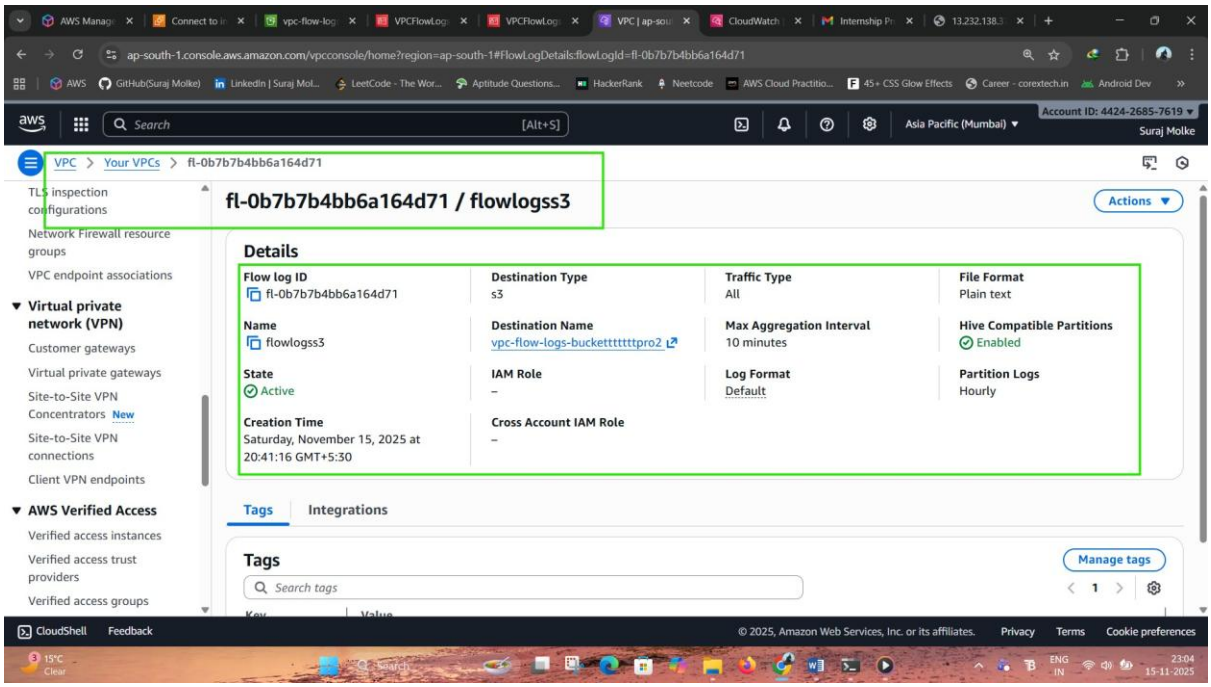
The goal of this project is to capture all the network traffic (incoming and outgoing) from a VPC using AWS
Flow Logs. These logs are stored in an S3 bucket using an IAM role. This setup helps monitor network activity
for security, auditing, or troubleshooting. It's helpful to know what kind of traffic is reaching your AWS
infrastructure. This project shows how to set that up from scratch using basic AWS services.

Architectural diagram

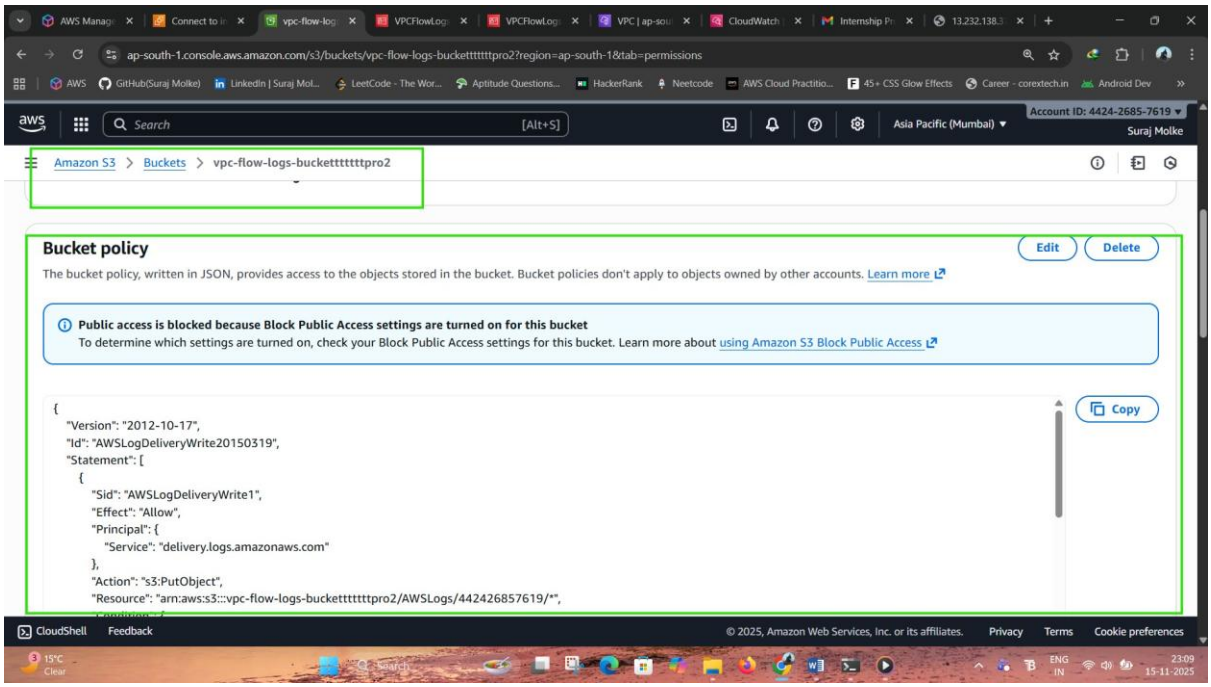


Step 1 : You need a private network (VPC) where AWS resources like EC2 will run. This is where traffic will be logged. Go to VPC in AWS Console. Click

Create VPC → Choose VPC only → Give a name → Keep default settings → Create



Step 2: Create an S3 Bucket with Versioning: We need a place to store the logs. S3 is like cloud storage. Versioning helps keep track of any changes. Go to S3 → Click Create bucket. Give a unique name and choose the same region as your VPC. Enable bucket versioning → Create bucket.

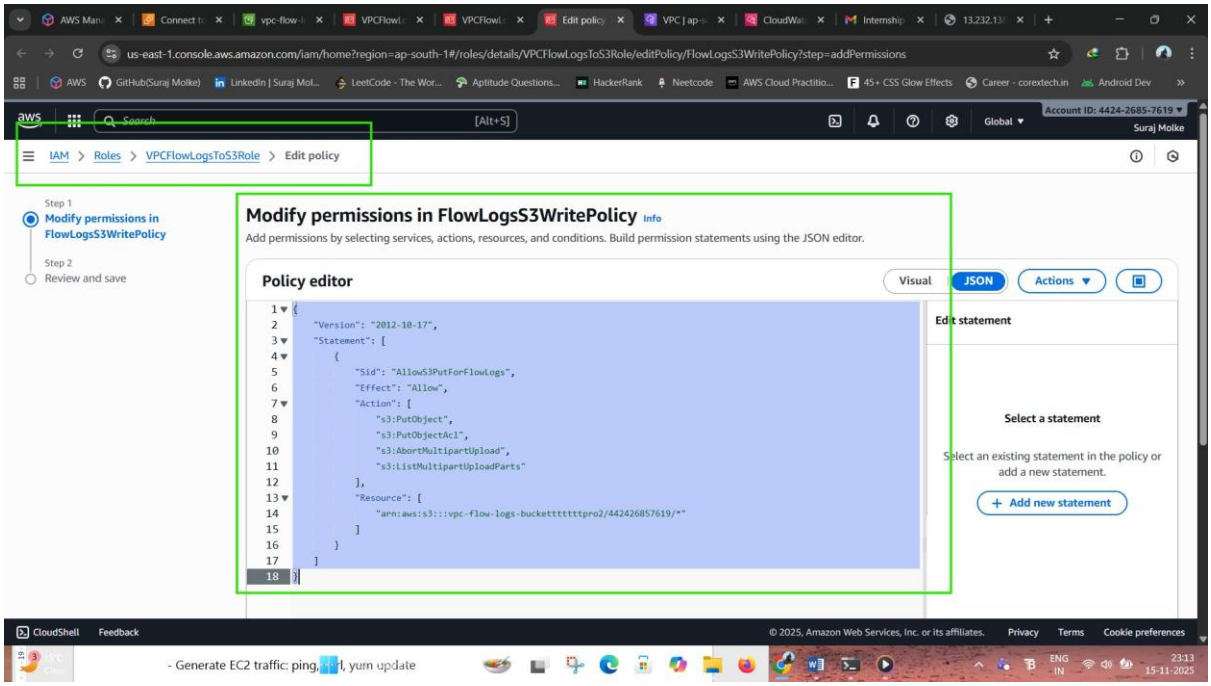


Step 3: Add a Bucket Policy:

We must allow the VPC Flow Logs service to write logs to the bucket.

Go to S3 → Your Bucket → Permissions tab → Bucket policy.

Click Edit and paste the provided JSON policy → Save.

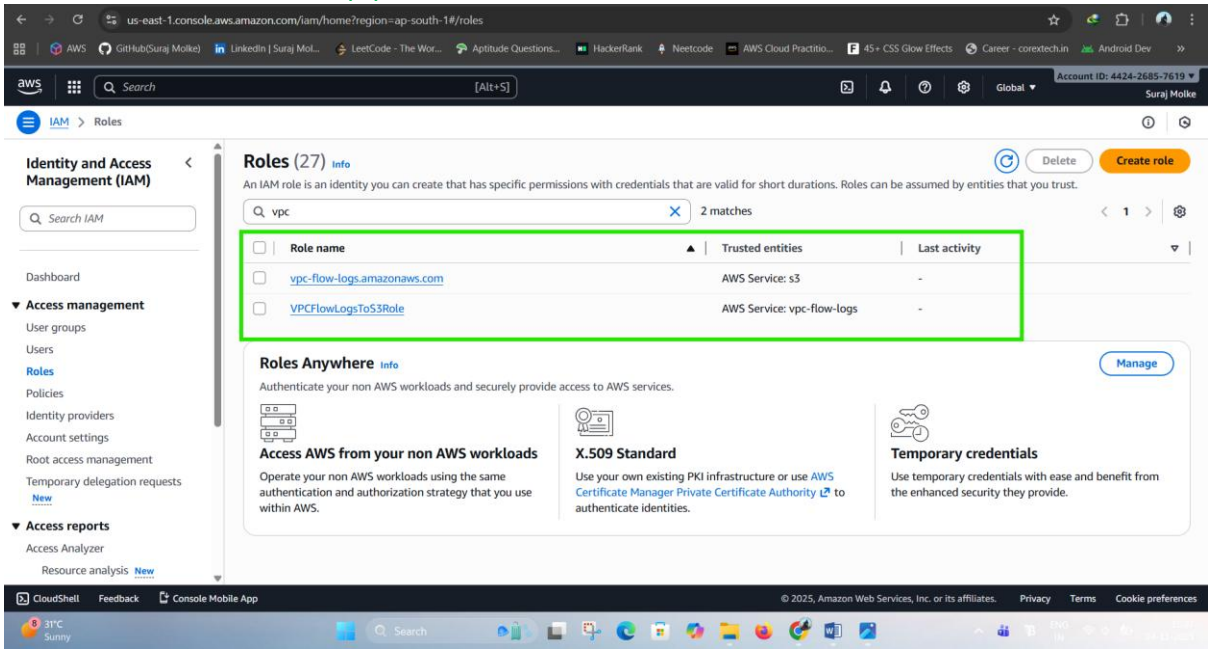


Step 4: Create an IAM Role with Trust Policy:

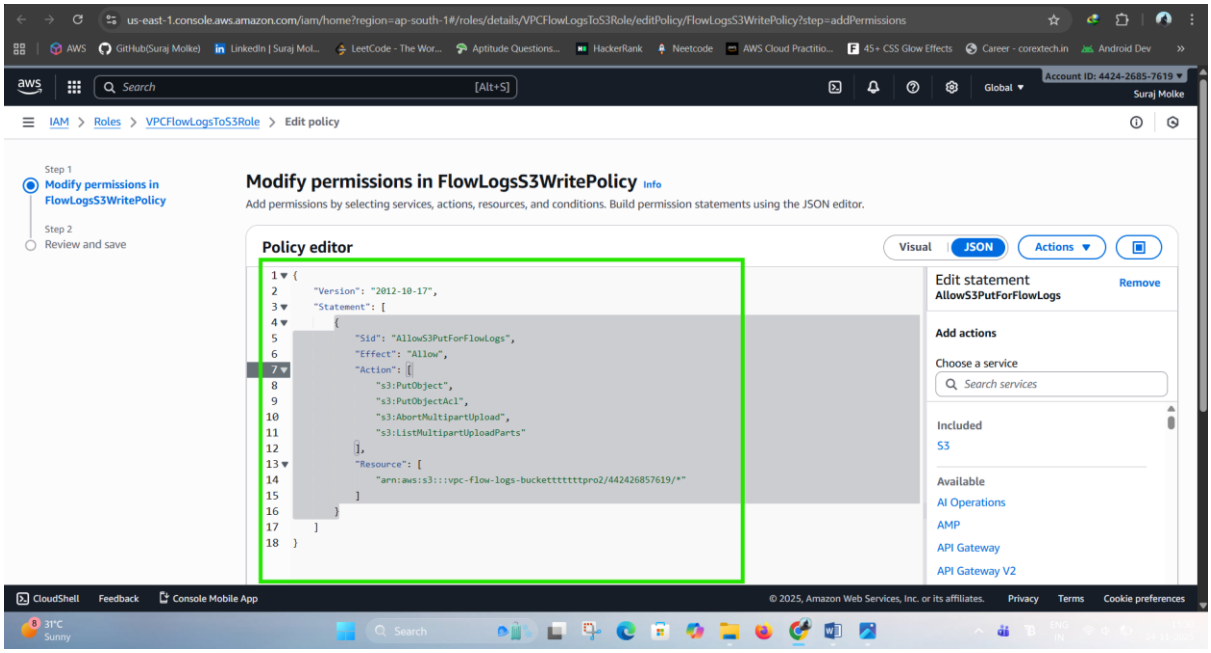
This role lets the VPC Flow Logs service act on your behalf to store logs in S3.

Go to IAM → Roles → Create Role → Custom Trust Policy.

Paste the trust JSON → Skip permissions → Give a name → Create role



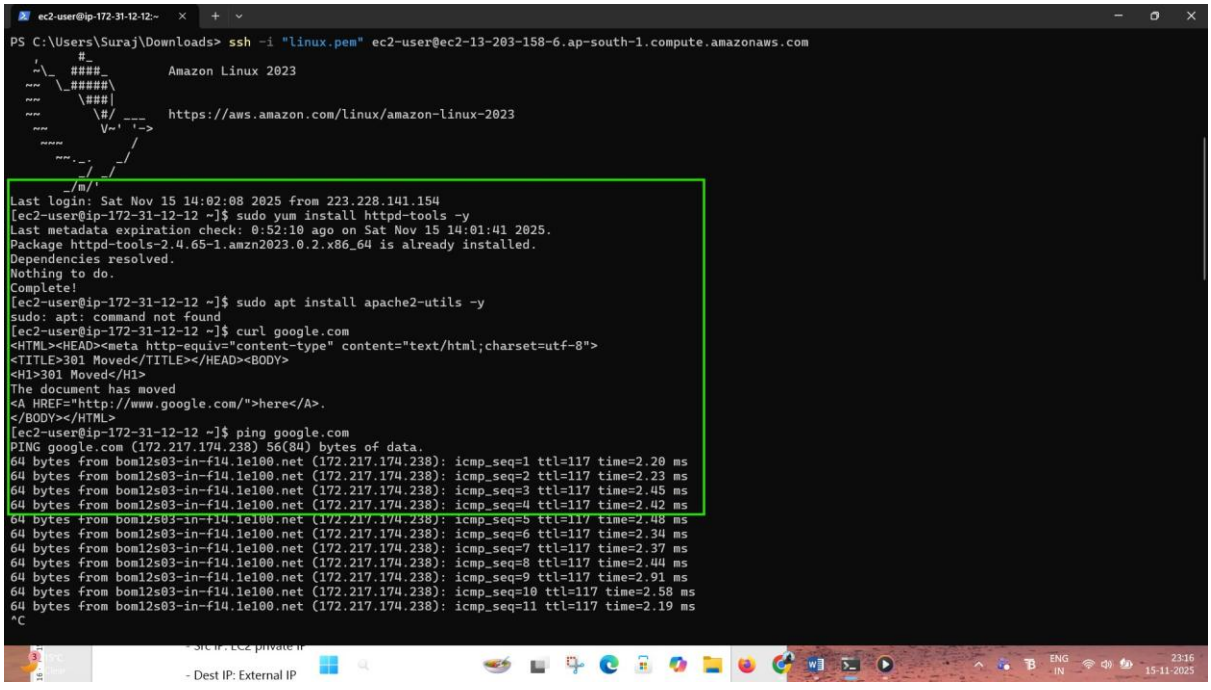
Step 5 : Attach a Permission Policy to the Role: This allows the role to put logs into the S3 bucket. Go to IAM → Your Role → Permissions tab → Add inline policy. Choose JSON tab, paste the policy, save it with a name.



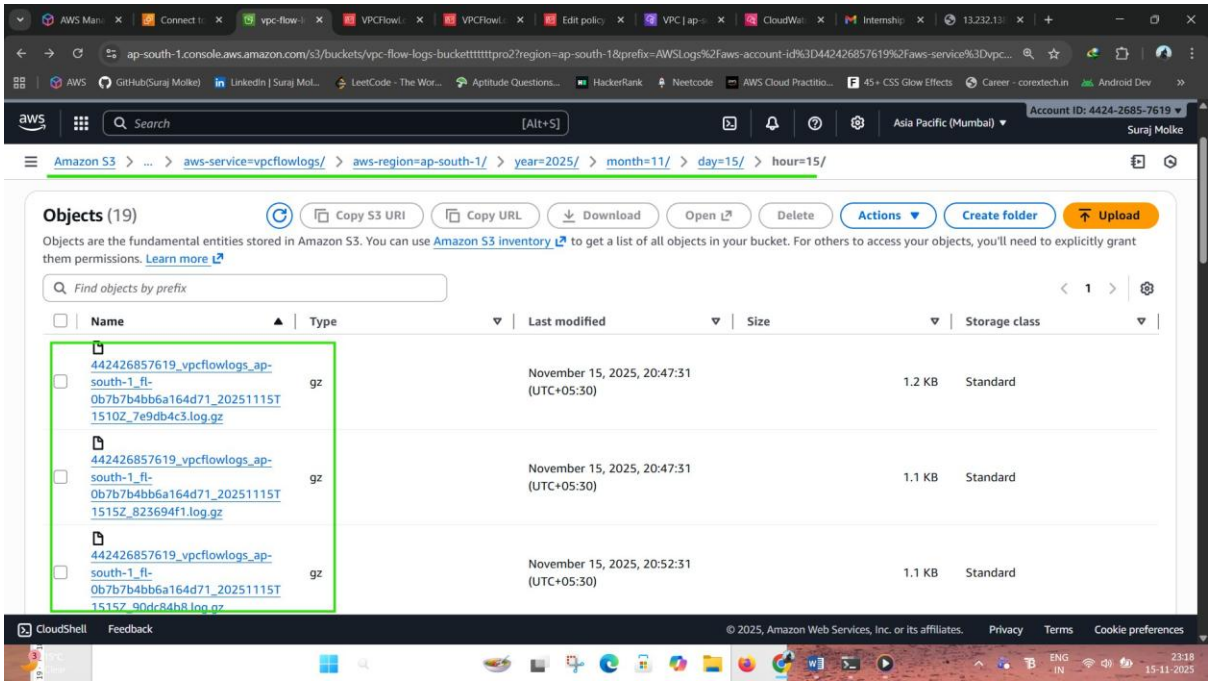
Step 6: Enable VPC Flow Logs: This captures traffic logs for your VPC and sends them to the S3 bucket using the role.

Go to VPC → Your VPC → Flow Logs tab → Create Flow Log. Choose All traffic, Send to S3, select the IAM role, and provide the S3 bucket ARN.

Step 7: Generate Traffic Using EC2: We test if logs are working by sending traffic (like pinging a website). SSH into EC2 → Run this command: ping google.com



Step 8 : Check Logs in S3: To confirm that traffic logs are being captured and saved in the bucket. Go to S3 → Your bucket → AWSLogs folder Open folders by account ID → region → date → Download log file and open.



Conclusion:

This project successfully established a secure and centralized logging system on AWS. By creating a dedicated VPC, configuring an S3 bucket for log storage, and implementing an IAM Role for secure permissions, the environment was properly prepared for traffic monitoring. Enabling VPC Flow Logs and testing with an EC2 instance confirmed that network activity was being captured and stored reliably. Overall, the setup provides an efficient and scalable foundation for monitoring and analysing AWS network traffic, improving both security visibility and operational awareness.