

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.

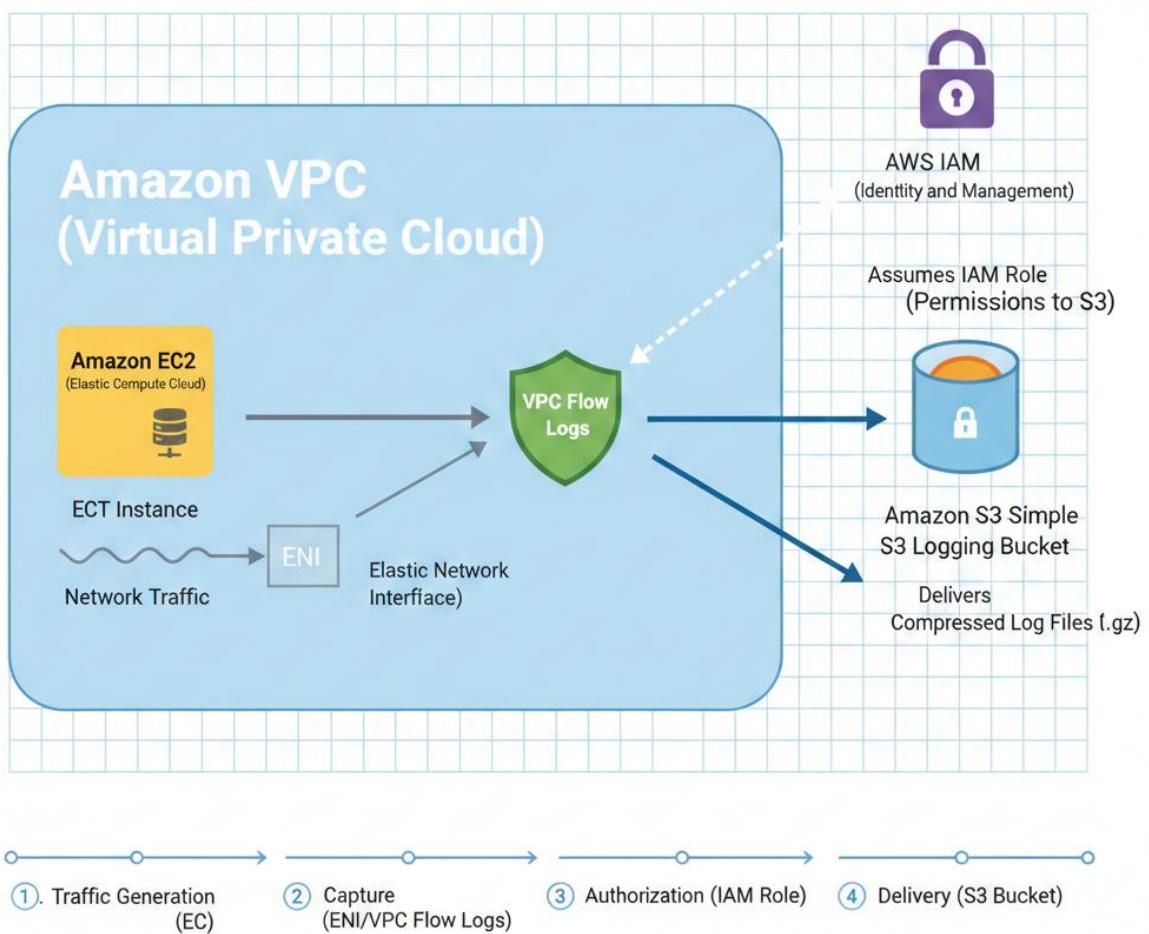
Project Title: Configure VPC Flow Logs and Store Logs in S3 Using IAM Role:

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

The screenshot shows the AWS VPC Flow Log configuration page. A green box highlights the 'fl-0b7b7b4bb6a164d71 / flowlogss3' log entry. The 'Details' section is expanded, showing the following configuration:

Flow log ID	Destination Type	Traffic Type	File Format
fl-0b7b7b4bb6a164d71	s3	All	Plain text
Name	Destination Name	Max Aggregation Interval	Hive Compatible Partitions
flowlogss3	vpc-flow-logs-bucketttttpro2	10 minutes	Enabled
State	IAM Role	Log Format	Partition Logs
Active	-	Default	Hourly
Creation Time	Cross Account IAM Role		
Saturday, November 15, 2025 at 20:41:16 GMT+5:30	-		

Below the details, there are tabs for 'Tags' and 'Integrations'. The 'Tags' tab has a search bar and a 'Manage tags' button. The 'Integrations' tab is currently inactive.

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.

The screenshot shows the AWS S3 Bucket policy configuration page. A green box highlights the 'Bucket policy' section. The policy JSON is displayed:

```
{
  "Version": "2012-10-17",
  "Id": "AWSLogDeliveryWrite20150319",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryWrite1",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::vpc-flow-logs-bucketttttpro2/AWSLogs/442426857619/*"
    }
  ]
}
```

A 'Copy' button is located on the right side of the policy editor. The top navigation bar shows the URL as 'ap-south-1.console.amazon.com/s3/buckets/vpc-flow-logs-bucketttttpro2?region=ap-south-1&tab=permissions'.

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 1
Modify permissions in FlowLogsS3WritePolicy

Step 2
Review and save

Policy editor

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "AllowS3PutForFlowLogs",  
6       "Effect": "Allow",  
7       "Action": [  
8         "s3:PutObject",  
9         "s3:PutObjectAcl",  
10        "s3:AbortMultiPartUpload",  
11        "s3>ListMultipartUploadParts"  
12      ],  
13      "Resource": [  
14        "arn:aws:s3:::vpc-flow-logs-buckettttttpro2/442426857619/*"  
15      ]  
16    }  
17  ]  
18 }
```

Select a statement

+ Add new statement

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

Identity and Access Management (IAM)

Roles (27)

Role name	Trusted entities	Last activity
vpc-flow-logs.amazonaws.com	AWS Service: s3	-
VPCFlowLogsToS3Role	AWS Service: vpc-flow-logs	-

Access AWS from your non AWS workloads

X.509 Standard

Temporary credentials

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.

The screenshot shows the AWS IAM console with the path: IAM > Roles > VPCFlowLogsToS3Role > Edit policy. The 'Modify permissions in FlowLogsS3WritePolicy' page is displayed. A green box highlights the 'Policy editor' section containing the following JSON policy:

```

1 w {
2     "Version": "2012-10-17",
3     "Statement": [
4         {
5             "Sid": "AllowS3PutForFlowLogs",
6             "Effect": "Allow",
7             "Action": [
8                 "s3:PutObject",
9                 "s3:PutObjectAcl",
10                "s3:AbortMultipartUpload",
11                "s3>ListMultipartUploadParts"
12            ],
13            "Resource": [
14                "arn:aws:s3:::vpc-flow-logs-buckettttttpro2/44246857619/*"
15            ]
16        }
17    ]
18 }

```

The right side of the screen shows the 'Actions' tab selected, with a list of services including S3, AI Operations, AMP, API Gateway, and API Gateway V2. Below the actions is a 'Choose a service' search bar.

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

The screenshot shows an EC2 terminal window with the following command and output:

```
ssh -i "linux.pem" ec2-user@ec2-13-203-158-6.ap-south-1.compute.amazonaws.com
```

Output:

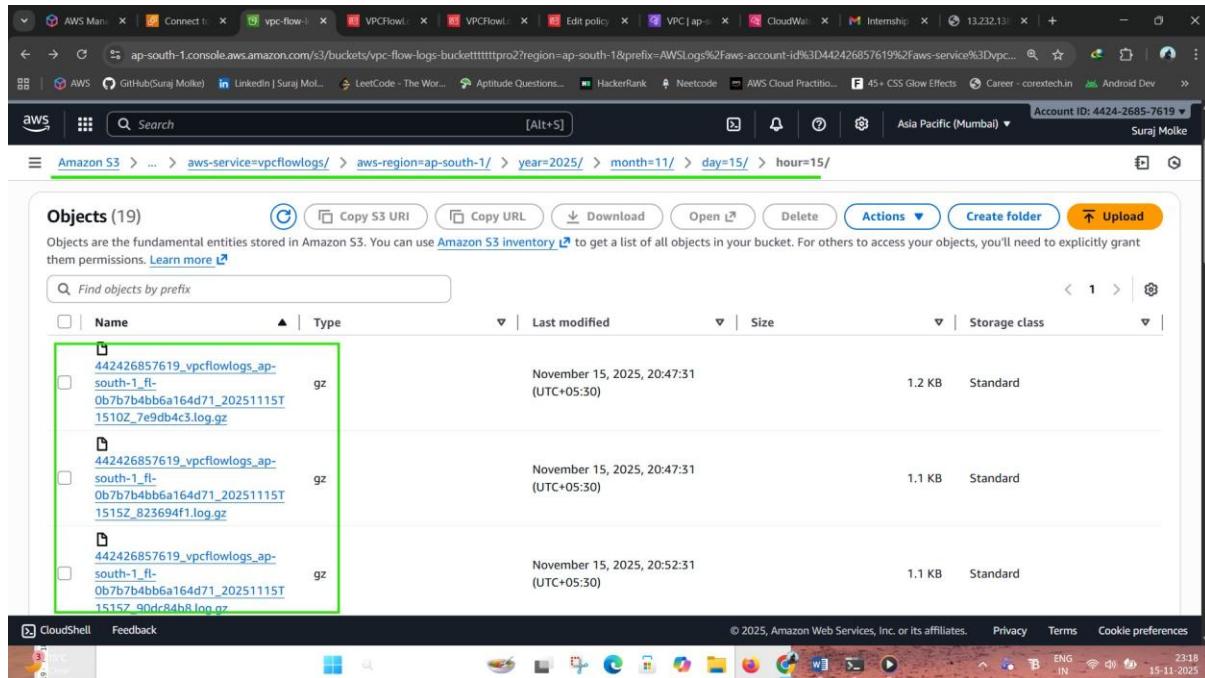
```

Last login: Sat Nov 15 14:02:08 2025 from 223.228.141.154
[ec2-user@ip-172-31-12-12 ~]$ sudo yum install httpd-tools -y
Last metadata expiration check: 0:52:10 ago on Sat Nov 15 14:01:41 2025.
Package httpd-tools-2.4.65-1.amzn2023.0.2.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[ec2-user@ip-172-31-12-12 ~]$ sudo apt install apache2-utils -y
sudo: apt: command not found
[ec2-user@ip-172-31-12-12 ~]$ curl google.com
<HTML><HEAD><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A href="http://www.google.com/">here</A>.
</BODY></HTML>
[ec2-user@ip-172-31-12-12 ~]$ ping google.com
PING google.com (172.217.174.238) 56(84) bytes of data.
64 bytes from bom12s03-in-f14.1e100.net (172.217.174.238): icmp_seq=1 ttl=117 time=2.20 ms
64 bytes from bom12s03-in-f14.1e100.net (172.217.174.238): icmp_seq=2 ttl=117 time=2.23 ms
64 bytes from bom12s03-in-f14.1e100.net (172.217.174.238): icmp_seq=3 ttl=117 time=2.45 ms
64 bytes from bom12s03-in-f14.1e100.net (172.217.174.238): icmp_seq=4 ttl=117 time=2.42 ms
64 bytes from bom12s03-in-f14.1e100.net (172.217.174.238): icmp_seq=5 ttl=117 time=2.48 ms
64 bytes from bom12s03-in-f14.1e100.net (172.217.174.238): icmp_seq=6 ttl=117 time=2.34 ms
64 bytes from bom12s03-in-f14.1e100.net (172.217.174.238): icmp_seq=7 ttl=117 time=2.37 ms
64 bytes from bom12s03-in-f14.1e100.net (172.217.174.238): icmp_seq=8 ttl=117 time=2.44 ms
64 bytes from bom12s03-in-f14.1e100.net (172.217.174.238): icmp_seq=9 ttl=117 time=2.91 ms
64 bytes from bom12s03-in-f14.1e100.net (172.217.174.238): icmp_seq=10 ttl=117 time=2.58 ms
64 bytes from bom12s03-in-f14.1e100.net (172.217.174.238): icmp_seq=11 ttl=117 time=2.19 ms
^C

```

The terminal also shows the IP address as 172.217.174.238 and the destination IP as External IP.

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.



The screenshot shows the AWS S3 console interface. The URL in the address bar is: `Amazon S3 > ... > aws-service=vpcflowlogs/ > aws-region=ap-south-1/ > year=2025/ > month=11/ > day=15/ > hour=15/`. The main area displays a list of objects (log files) under the heading "Objects (19)". The first three files are highlighted with a green box. The details for these files are as follows:

Name	Type	Last modified	Size	Storage class
442426857619_vpcflowlogs_ap-south-1_fl-0b7b7b4bb6a164d71_20251115T1510Z_7e9db4c3.log.gz	gz	November 15, 2025, 20:47:31 (UTC+05:30)	1.2 KB	Standard
442426857619_vpcflowlogs_ap-south-1_fl-0b7b7b4bb6a164d71_20251115T1515Z_823694f1.log.gz	gz	November 15, 2025, 20:47:31 (UTC+05:30)	1.1 KB	Standard
442426857619_vpcflowlogs_ap-south-1_fl-0b7b7b4bb6a164d71_20251115T1515Z_9ndr84bh.log.gz	gz	November 15, 2025, 20:52:31 (UTC+05:30)	1.1 KB	Standard

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.