Create VPC Flow Logs and Store in Amazon S3

Problem Statement

Create VPC Flow Logs to monitor incoming and outgoing traffic for your VPC and store the log files in an S3 bucket. This document captures the exact steps performed along with screenshots.

Outcome

• VPC Flow Log created for the target VPC • Destination configured as Amazon S3 • Logs successfully delivered to the bucket and verified

Prerequisites

- AWS Account with permissions for VPC, S3 and IAM.
- A VPC to monitor (default or custom).
- An S3 bucket to store logs (created in the same region).

Step 1 — Create an S3 bucket for logs

Create a bucket (example name used here: **vpc-flow-logs-samarth**) in the same region as your VPC (N. Virginia / us-east-1).

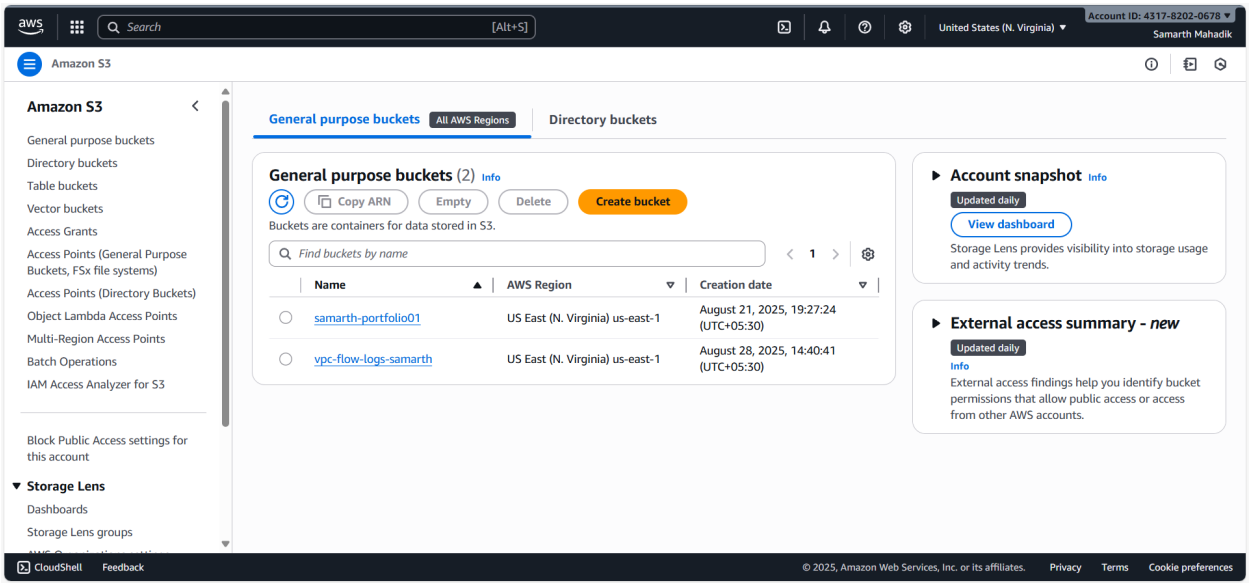

Figure: S3: Bucket list showing vpc-flow-logs-samarth.

Step 2 — Bucket policy used in this run

A bucket policy was attached to allow public read (GetObject) for demonstration. Note: For production, prefer a least-privilege policy that grants delivery to the AWS logs service only.

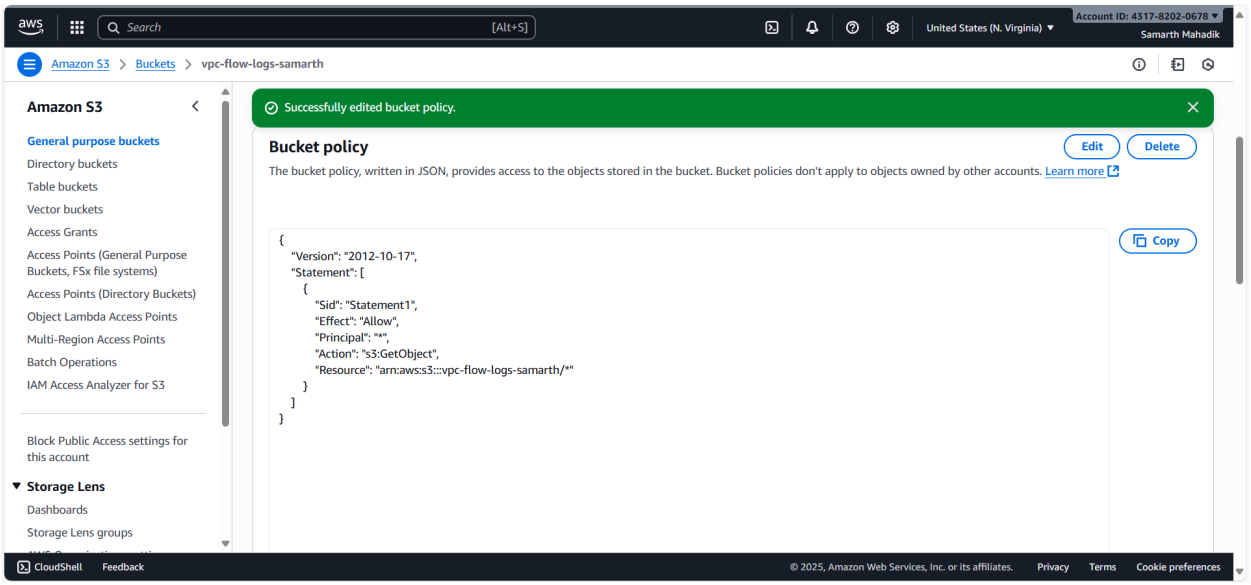

Figure: S3: Bucket policy attached during the task.

Step 3 — Create the VPC Flow Log

From VPC Console → Your VPCs → Select the VPC → Flow logs tab → Create flow log. Use these settings: • Destination: S3 • Traffic type: ALL • Max aggregation interval: 1 minute • Log format: Default • Partition logs: Hourly

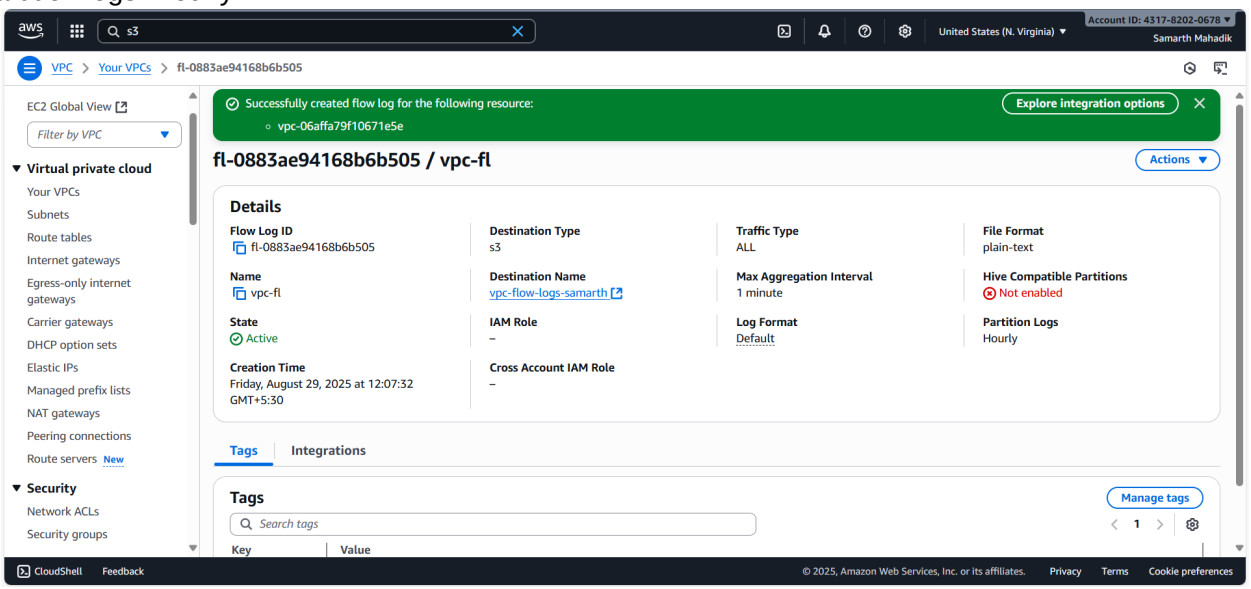

Figure: VPC: Flow Log created and Active, writing to S3 bucket.

Step 4 — Verify delivery in S3

Open the S3 bucket. You should see the **AWSLogs/** prefix and folders by account, region, service and date. This confirms delivery is working.

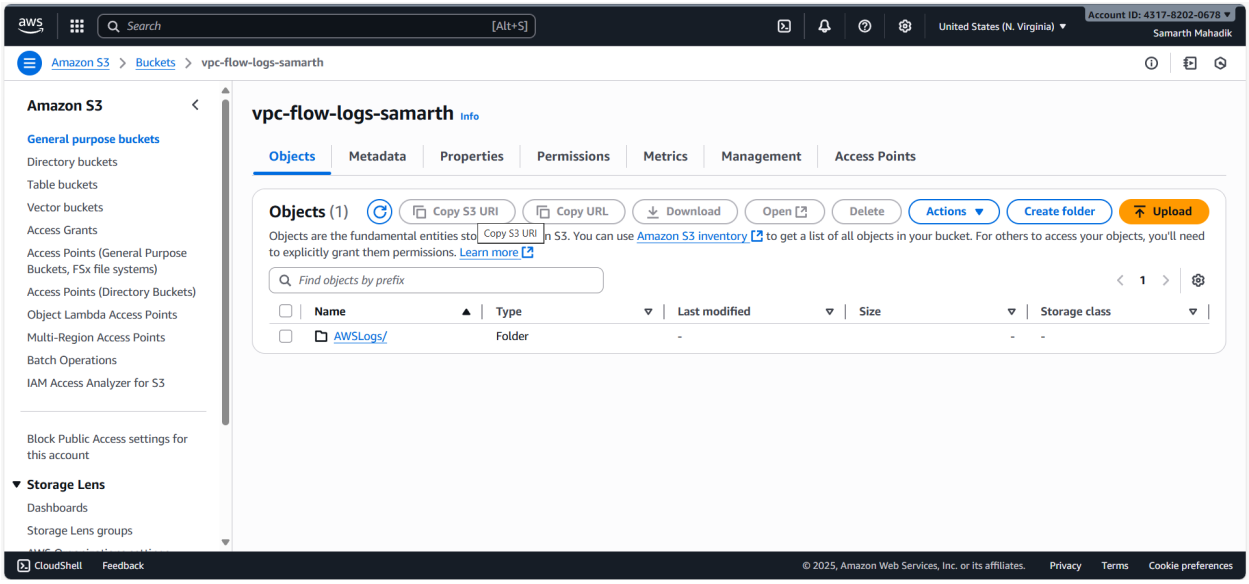

Figure: S3: Logs landing in AWSLogs/ for the bucket.

Step 5 — Review a sample log file

Download any log file and open it to see records. Each line is space-delimited. The header typically is:

version account-id interface-id srcaddr dstaddr srcport dstport protocol packets bytes start end action log-status

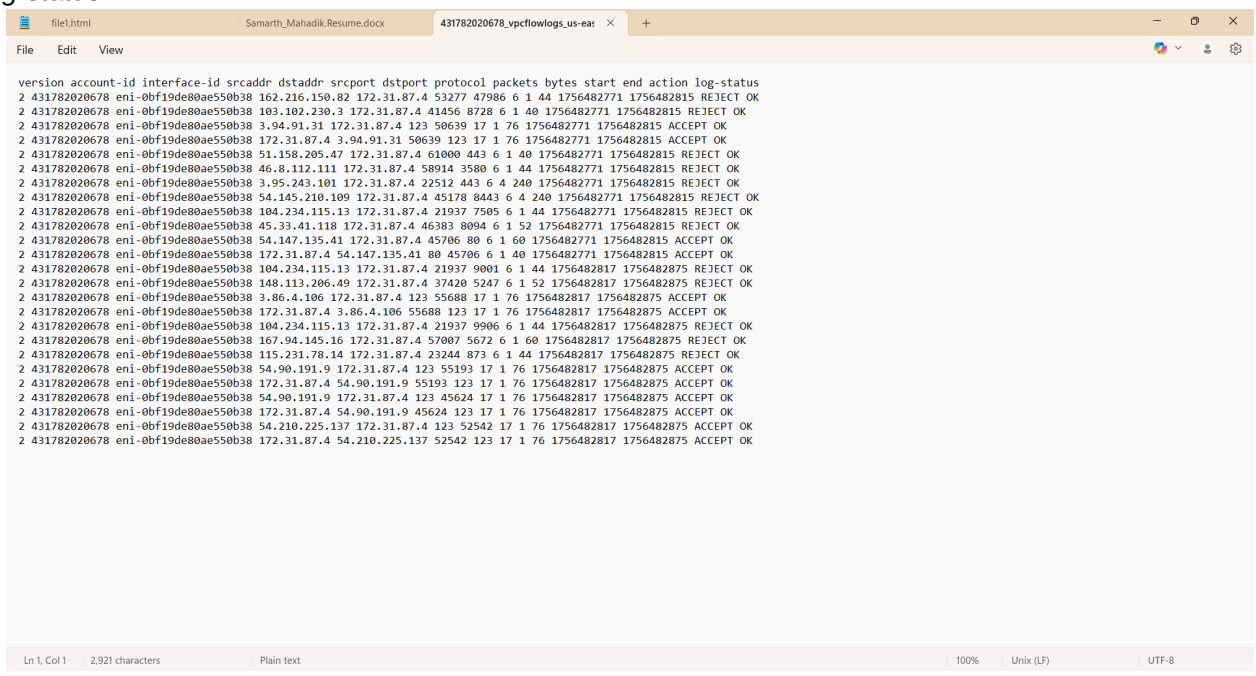

Figure: Example log lines (REJECT/ACCEPT events).

Field Quick Reference

Field	Meaning / Notes
version	Flow log version (e.g., 2).
account-id	AWS account ID where the flow log was captured.
interface-id	ENI where traffic was observed.

srcaddr / dstaddr	Source / destination IP addresses.
srcport / dstport	Source / destination port numbers.
protocol	IANA protocol number (6=TCP, 17=UDP, 1=ICMP, etc.).
packets / bytes	Number of packets and bytes in the aggregation window.
start / end	Unix epoch seconds for the aggregation window start/end.
action	ACCEPT or REJECT based on security group/NACL outcome.
log-status	Whether the record was logged OK or if there was an issue.

Notes & Best Practices

- Keep the S3 bucket private. Grant only required service principals to write logs.
- Consider lifecycle rules to transition/expire older logs to control cost.
- If you need to query logs, enable Hive-compatible partitions or use Athena with a proper table definition.