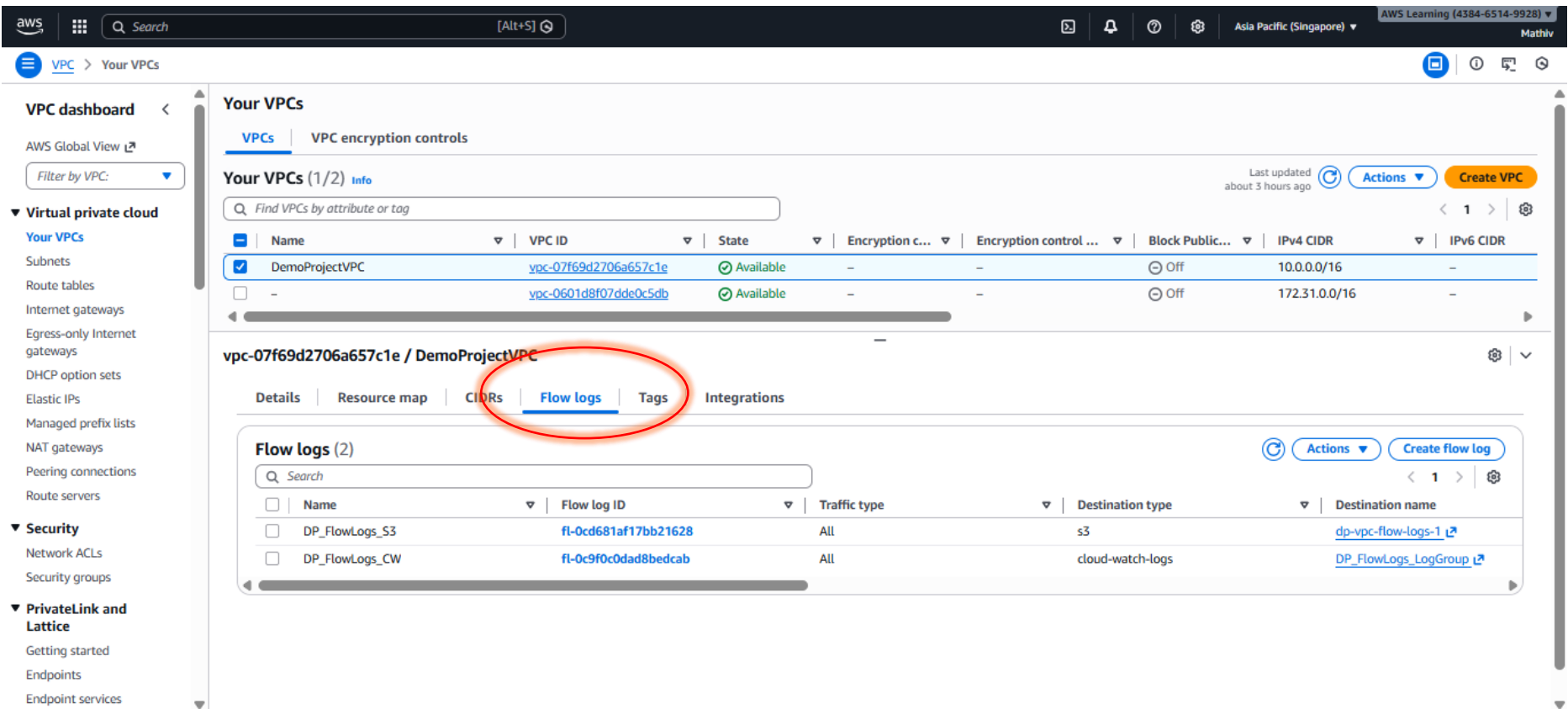


Setting up VPC Flow logs

With CloudWatch and S3+Athena



Short Summary:

Flow logs With S3+Athena

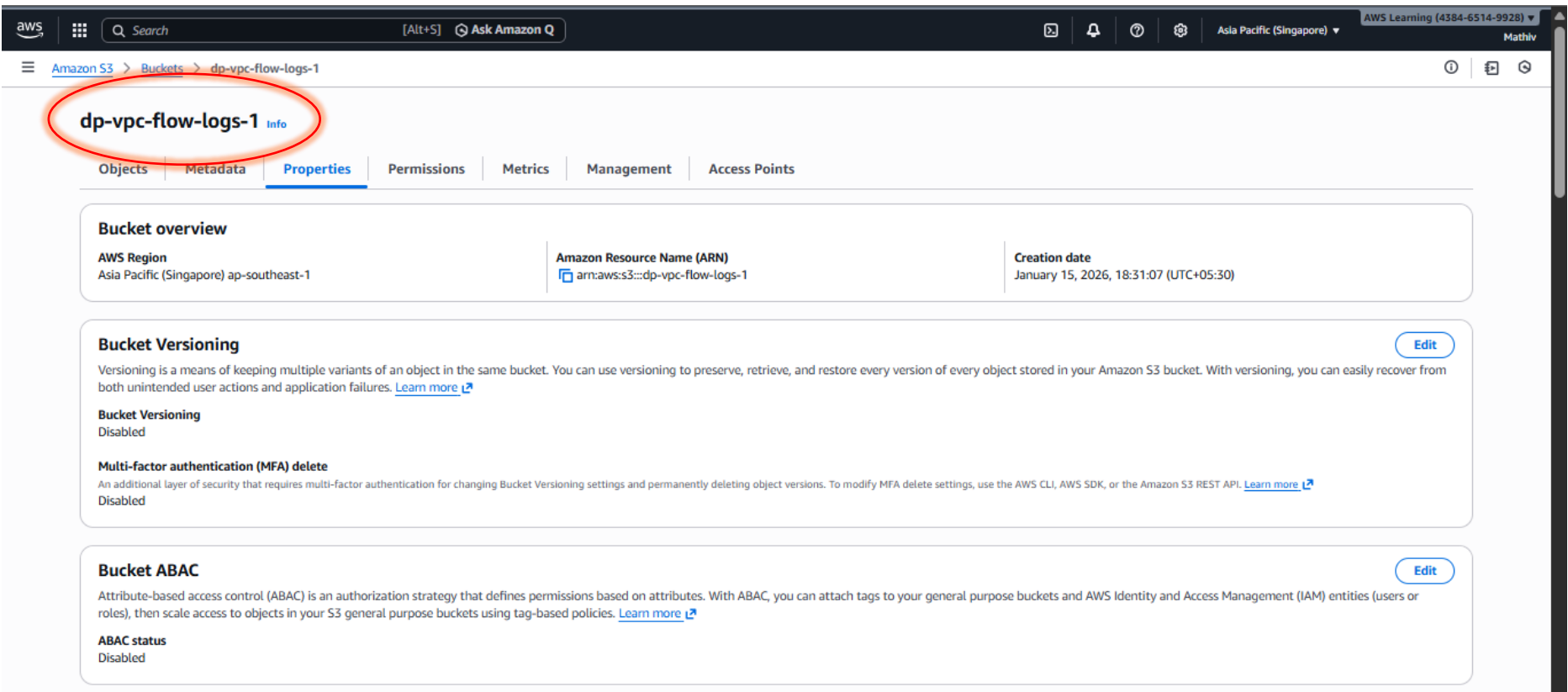
- To use with Athena, with this we can eliminate ETL(Extract, transform, load) pipelines, infrastructure setup, scaling, and ongoing management (but we still need to define a schema in Athena), which makes log analysis far simpler and faster because we can directly query flow logs without building heavy data pipelines.
Usecase: when you want **deep analysis, reporting, and trend insights** over time.

Flow logs With CloudWatch

- For log analysis – Observability purpose
Usecase: when you want **live monitoring and troubleshooting**.

Flow logs With S3

1. Create an S3 bucket in the Same region as VPC



2. Create Flow logs from VPC
- Flow log created with destination: S3 Bucket

aws

Search

[Alt+S]

Asia Pacific (Singapore)

AWS Learning (4384-6514-9928)

Mathiv

VPC > Your VPCs > fl-0cd681af17bb21628

VPC dashboard

AWS Global View

Filter by VPC:

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only Internet gateways

DHCP option sets

Elastic IPs

Managed prefix lists

NAT gateways

Peering connections

Route servers

Security

Network ACLs

Security groups

PrivateLink and Lattice

Getting started

Endpoints

Endpoint services

fl-0cd681af17bb21628 / DP_FlowLogs_S3

Actions

Details

Flow log ID

fl-0cd681af17bb21628

Destination Type

S3

Traffic Type

All

File Format

Plain text

Name

DP_FlowLogs_S3

Destination Name

dp-vpc-flow-logs-1

Max Aggregation Interval

1 minute

Hive Compatible Partitions

Not enabled

State

Active

IAM Role

-

Log Format

Default

Partition Logs

Hourly

Creation Time

Thursday, 15 January 2026 at 18:39:19 IST

Cross Account IAM Role

-

Tags

Integrations

Tags

Search tags

Manage tags

1

Using Athena with the logs stored in S3

1. Creating an S3 bucket to store the query results of Athena

aws

athena

Ask Amazon Q

Asia Pacific (Singapore)

AWS Learning (4384-6514-9928)

Mathiv

Amazon S3 > Buckets > athena-query-data-bucket-1

Successfully created folder "Athena_DataQueries_data".

athena-query-data-bucket-1

Info

Objects

Metadata

Properties

Permissions

Metrics

Management

Access Points

Objects (1)

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Find objects by prefix

1

Name

Type

Last modified

Size

Storage class

Athena_DataQueries_data/

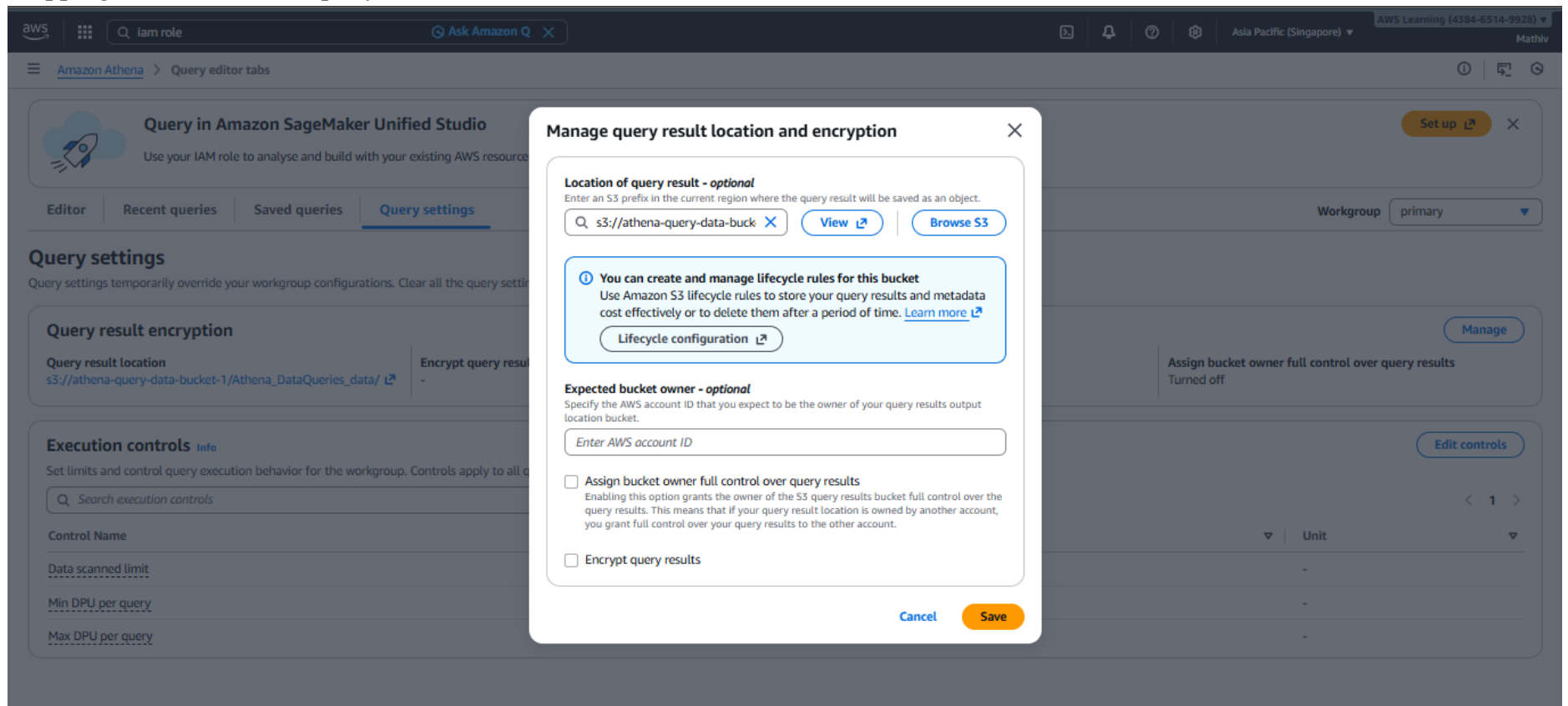
Folder

-

-

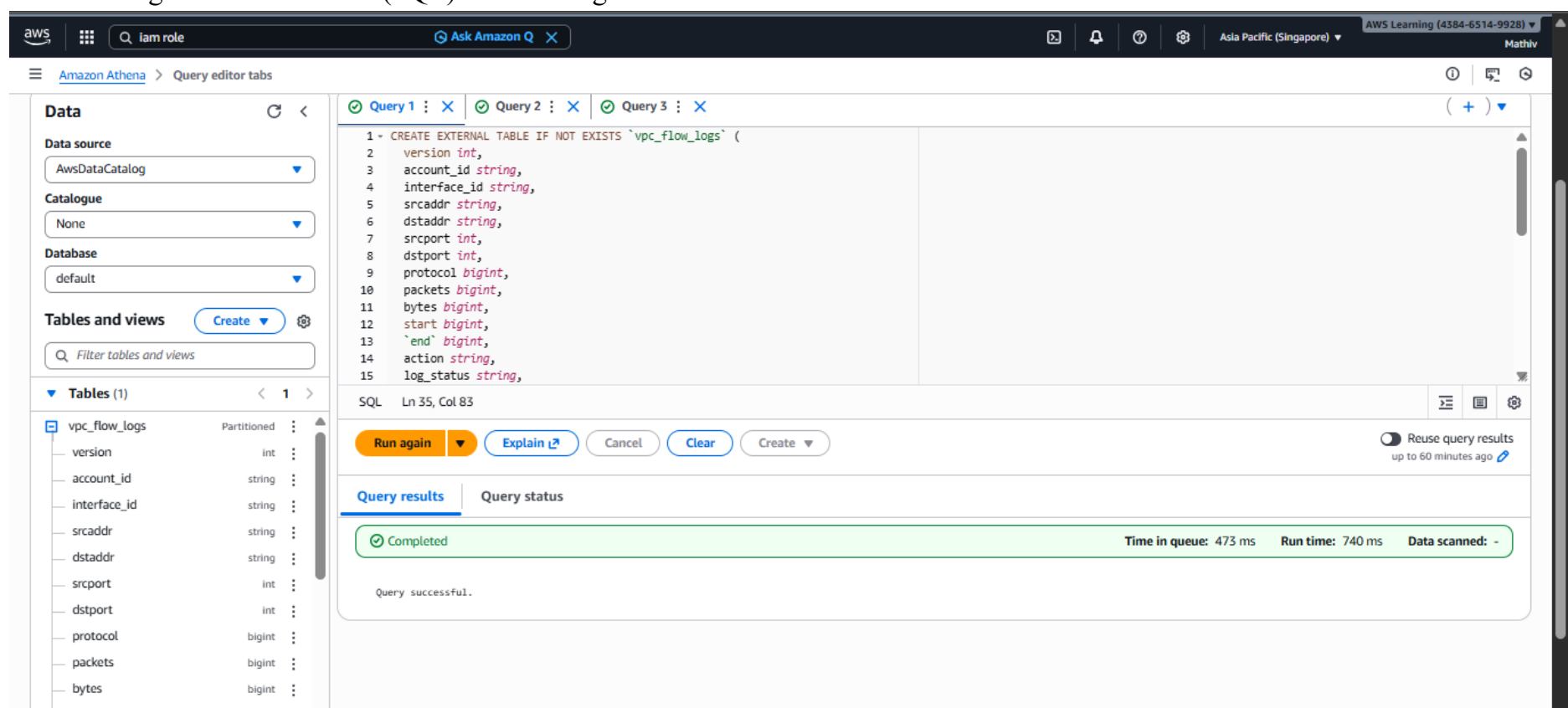
-

2. Mapping S3 bucket in the query location of Athena

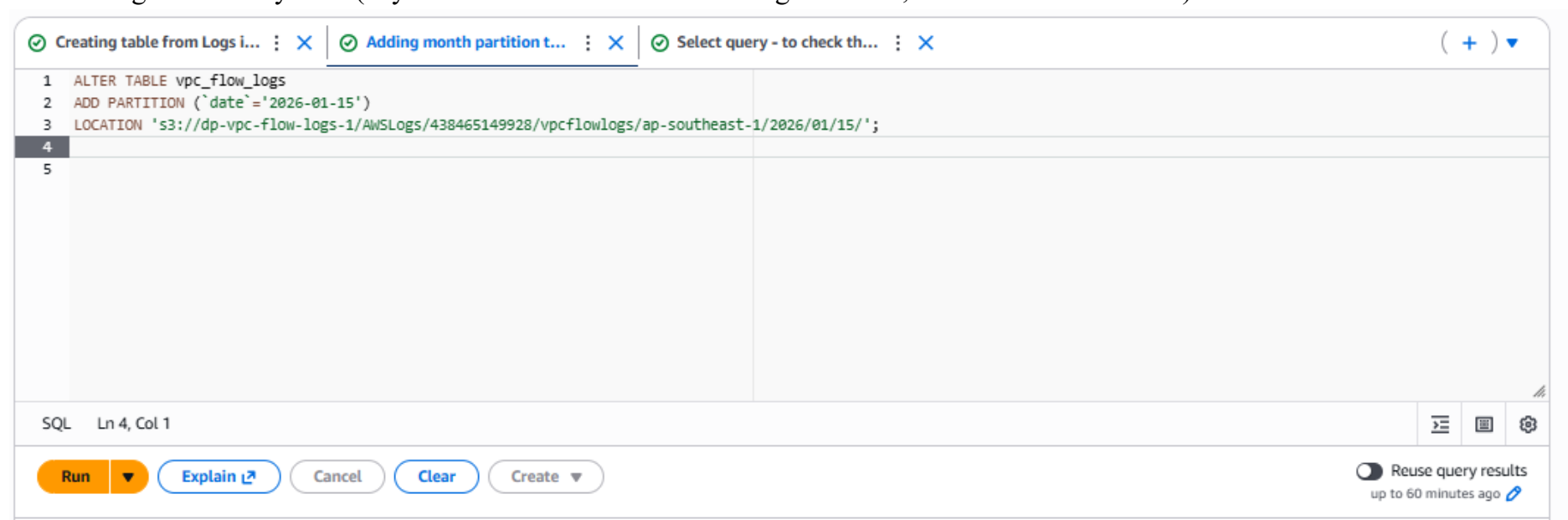


3. Querying logs from S3 with Athena | Querylink: [Create a table for Amazon VPC flow logs and query it - Amazon Athena](#)

a. First creating a Structured Table(SQL) from the logs stored in S3



b. Partitioning the table by time (day or hour is recommended for large datasets, month is fine for demo)



Result:

Tables (1)			< 1 >
instance_id	string	:	
tcp_flags	int	:	
type	string	:	
pkt_srcaddr	string	:	
pkt_dstaddr	string	:	
region	string	:	
az_id	string	:	
sublocation_type	string	:	
sublocation_id	string	:	
pkt_src_aws_service	string	:	
pkt_dst_aws_service	string	:	
flow_direction	string	:	
traffic_path	int	:	
date	date (Partitioned)	:	
Views (0)			< 1 >

c. Checking the logs with accepted action

aws

iam role

Ask Amazon Q

Asia Pacific (Singapore)

AWS Learning (4384-6514-9928)

Mathiv

Amazon Athena > Query editor tabs

Data

Data source

AwsDataCatalog

Catalogue

None

Database

default

Tables and views

Create

Filter tables and views

Tables (1)

< 1 >

vpc_flow_logs

Partitioned

int

string

string

string

int

int

int

bigint

bigint

bigint

Creating table from Logs i...

Adding month partition t...

Select query - to check th...

1 SELECT day_of_week(date) AS

2 day,

3 date,

4 interface_id,

5 srcaddr,

6 action,

7 protocol

8 FROM vpc_flow_logs

9 WHERE action = 'ACCEPT' AND protocol = 6

10 LIMIT 100;

SQL Ln 10, Col 11

Run again Explain Cancel Clear Create

Reuse query results up to 60 minutes ago

Query results

Query status

Completed

Time in queue: 57 ms Run time: 656 ms Data scanned: 17.04 KB

Copy Download results CSV

Results (100)

Search rows

#	day	date	interface_id	srcaddr	action	protocol
1	4	2026-01-15	eni-05f05e980dd47e002	10.0.0.97	ACCEPT	6

Results (100)

Copy

Download results CSV

Search rows

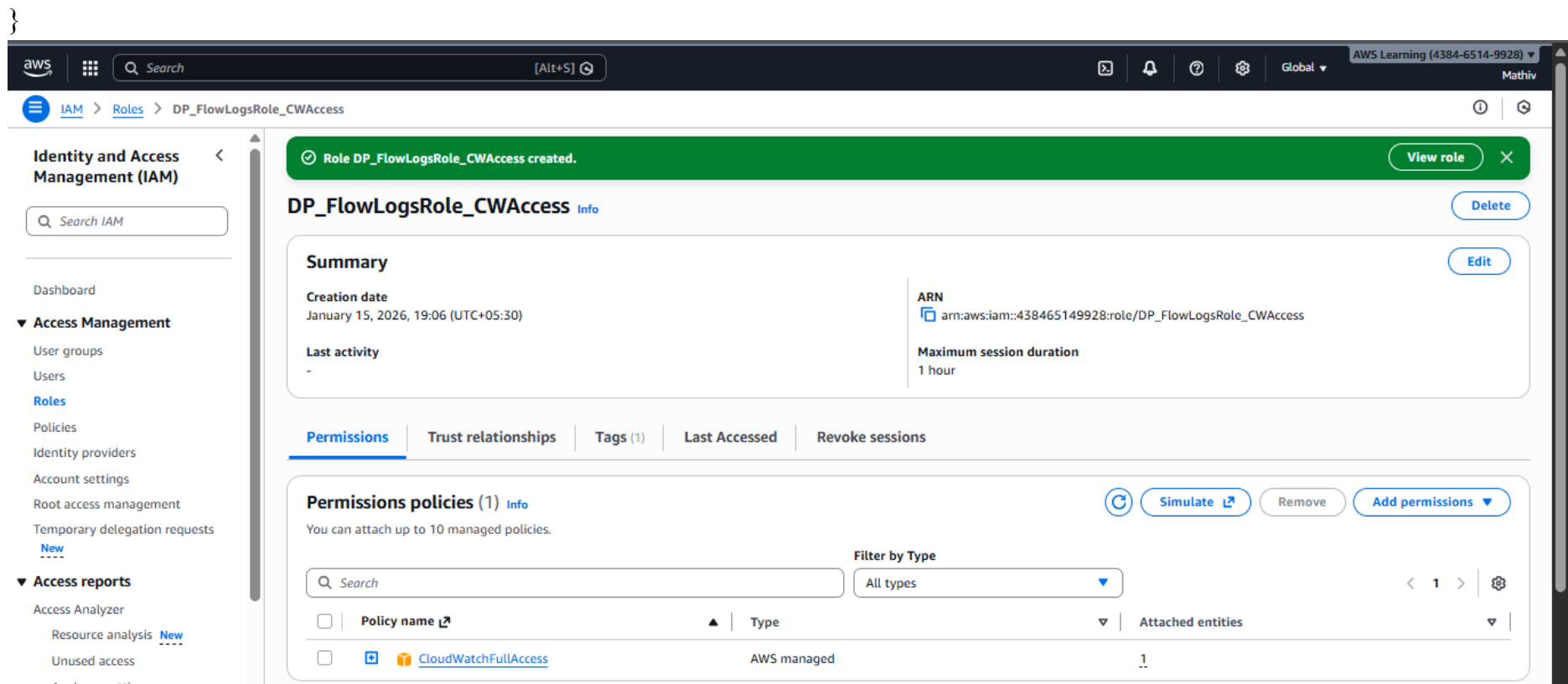
#	▼	day	▼	date	▼	interface_id	▼	srcaddr	▼	action	▼	protocol	▼
1		4		2026-01-15		eni-05f05e980dd47e002		10.0.0.97		ACCEPT		6	
2		4		2026-01-15		eni-05f05e980dd47e002		45.78.219.190		ACCEPT		6	
3		4		2026-01-15		eni-05f05e980dd47e002		10.0.0.97		ACCEPT		6	
4		4		2026-01-15		eni-05f05e980dd47e002		10.0.0.97		ACCEPT		6	
5		4		2026-01-15		eni-05f05e980dd47e002		61.222.211.114		ACCEPT		6	
6		4		2026-01-15		eni-05f05e980dd47e002		10.0.0.97		ACCEPT		6	
7		4		2026-01-15		eni-05f05e980dd47e002		47.128.4.216		ACCEPT		6	
8		4		2026-01-15		eni-05f05e980dd47e002		10.0.0.97		ACCEPT		6	
9		4		2026-01-15		eni-05f05e980dd47e002		91.224.92.74		ACCEPT		6	
10		4		2026-01-15		eni-05f05e980dd47e002		10.0.0.97		ACCEPT		6	
11		4		2026-01-15		eni-05f05e980dd47e002		209.38.84.119		ACCEPT		6	
12		4		2026-01-15		eni-05f05e980dd47e002		10.0.0.97		ACCEPT		6	
13		4		2026-01-15		eni-015eed3c53e08adf8		10.0.2.181		ACCEPT		6	
14		4		2026-01-15		eni-015eed3c53e08adf8		10.0.2.181		ACCEPT		6	
15		4		2026-01-15		eni-015eed3c53e08adf8		10.0.2.181		ACCEPT		6	

Flowlogs With CloudWatch

1. Create an IAM role with Custom policy(When delivering flow logs to CloudWatch, we must explicitly create and attach an IAM role that VPC Flow Logs can assume.) and “[CloudWatchFullAccess](#)”

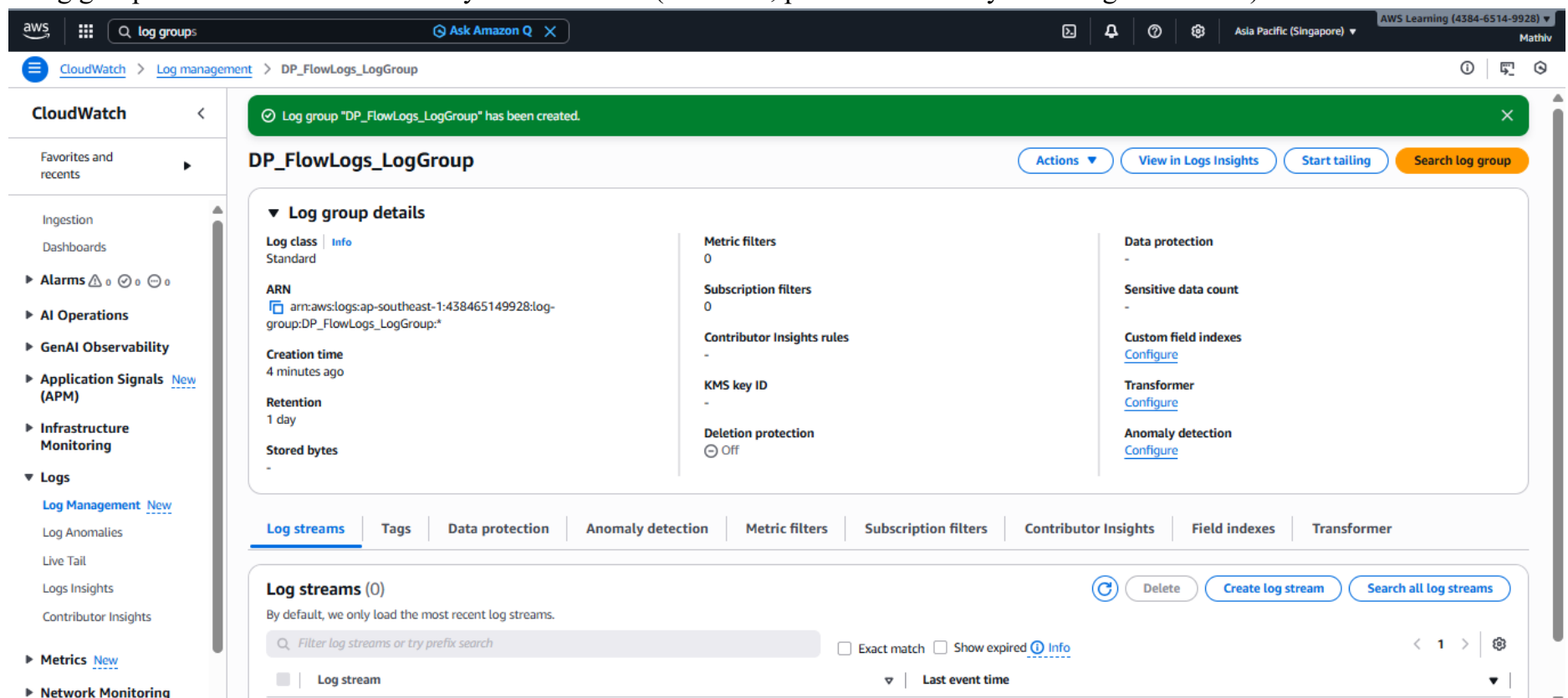
Custom Trust policy:

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



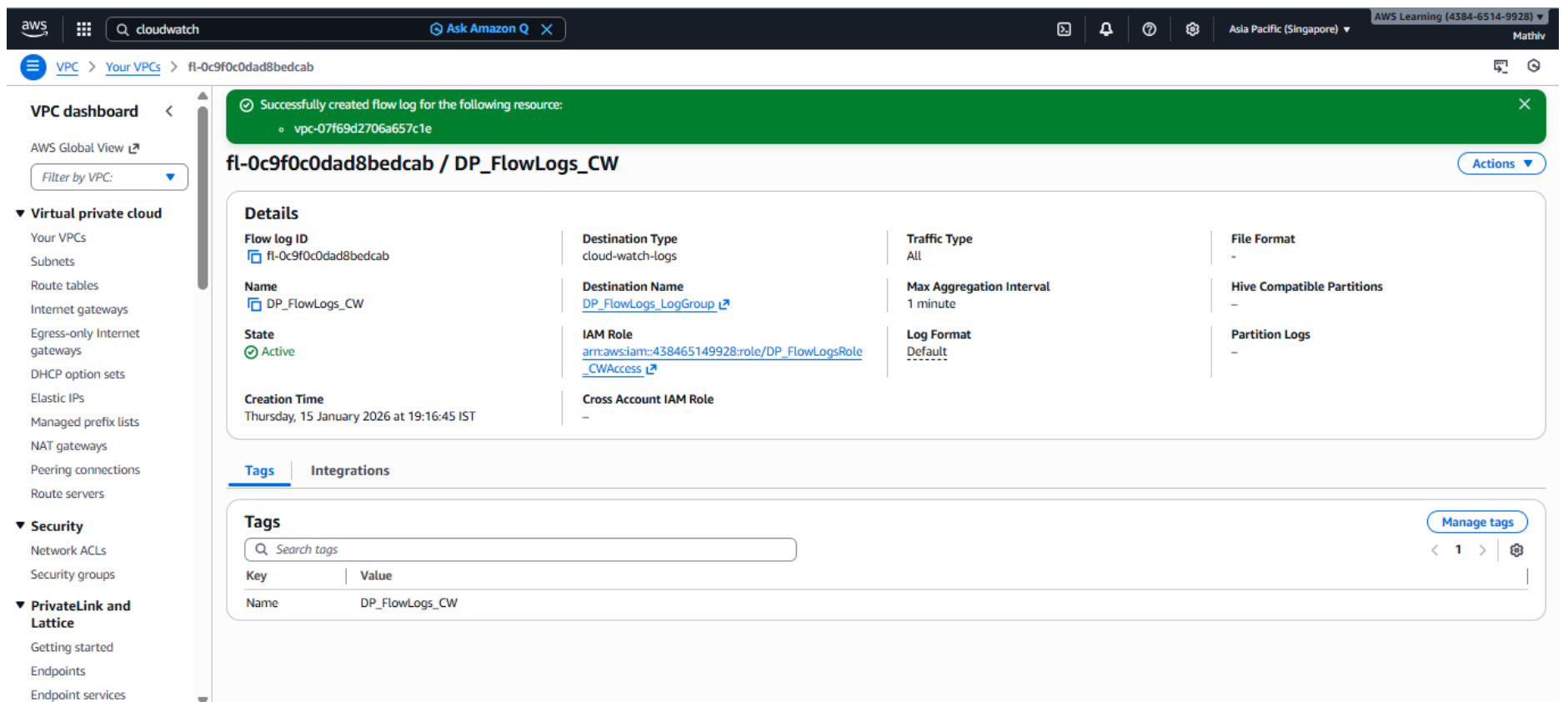
2. Create log group

A log group has been created with 1-day retention time (for demo; production usually uses longer retention)

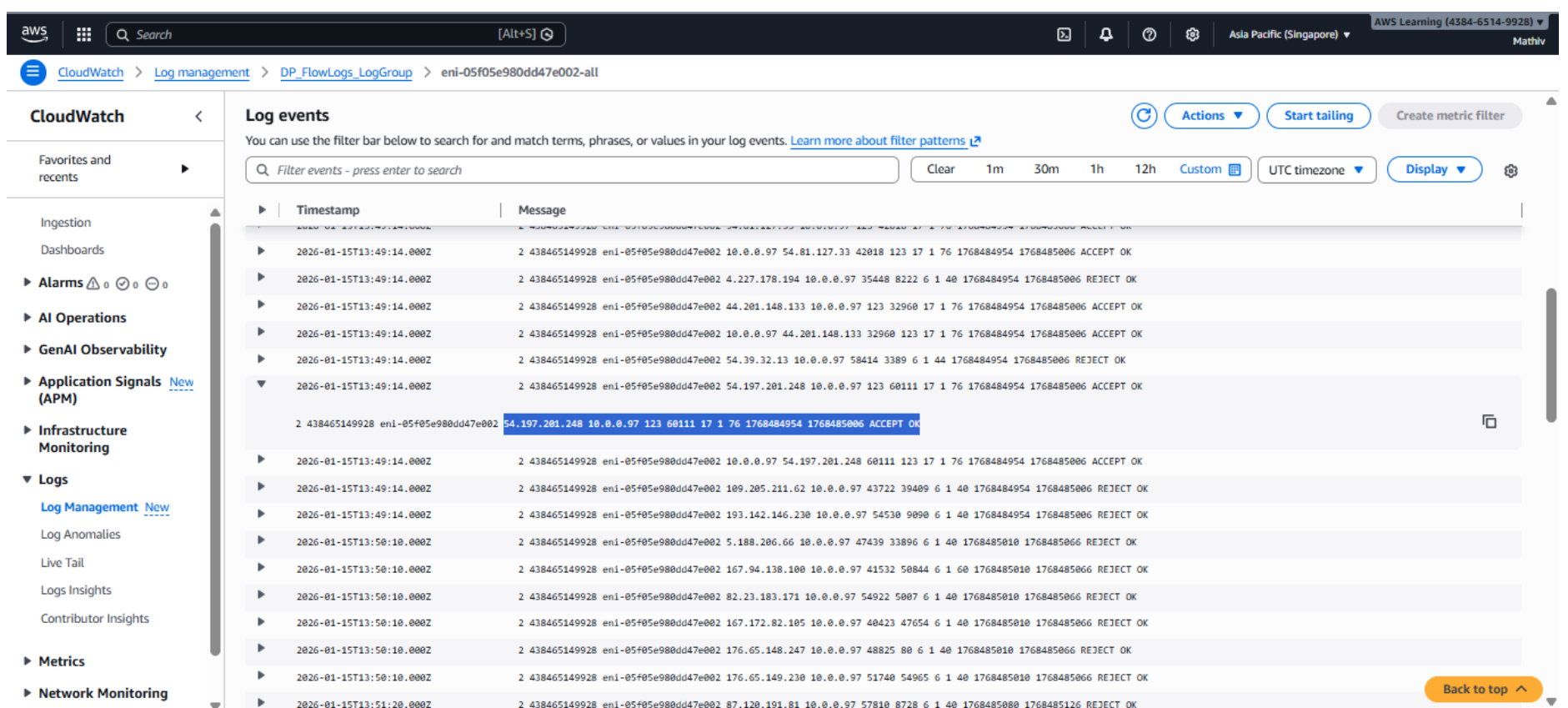


3. Flow log created with destination: CloudWatch

- attaching the created IAM role provides access to CloudWatch



Once the flow log has been set up with cloud watch, we could see the server activities are logging in the CloudWatch log group:



Note:

We could see many requests to our servers being rejected—these are unsolicited requests (bots, scanners, crawlers) blocked by security groups/NACLs, as intended

The accepted requests are from AWS – we could confirm that by checking the IP address

Whois IP 54.197.201.248

```
OrgName:      Amazon Technologies Inc.
OrgId:        AT-88-Z
Address:      410 Terry Ave N.
City:         Seattle
StateProv:    WA
PostalCode:   98109
Country:      US
RegDate:      2011-12-08
Updated:      2024-01-24
Comment:      All abuse reports MUST include:
Comment:      * src IP
```

