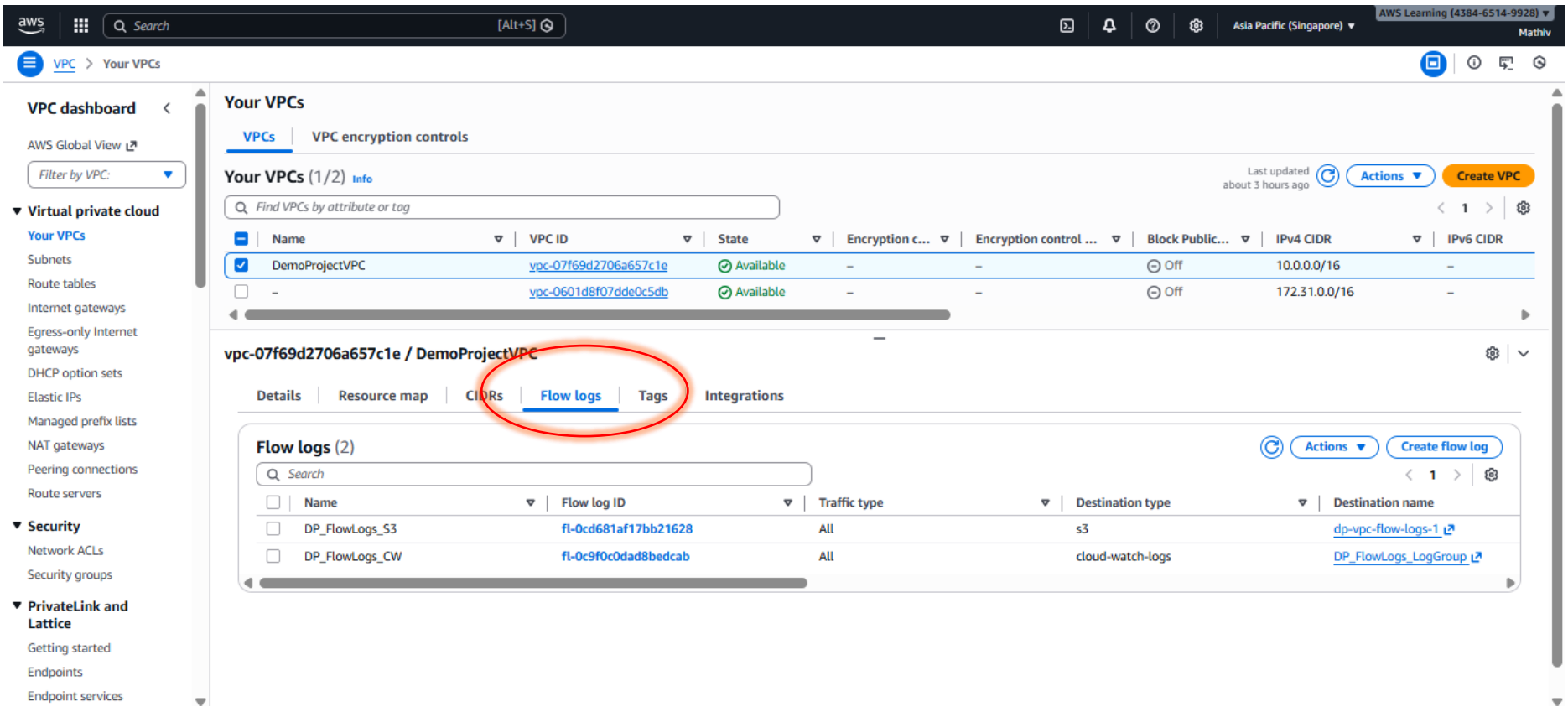
Setting up VPC Flow logs

With CloudWatch and S3+Athena



Short Summary:

Flow logs With S3+Athena

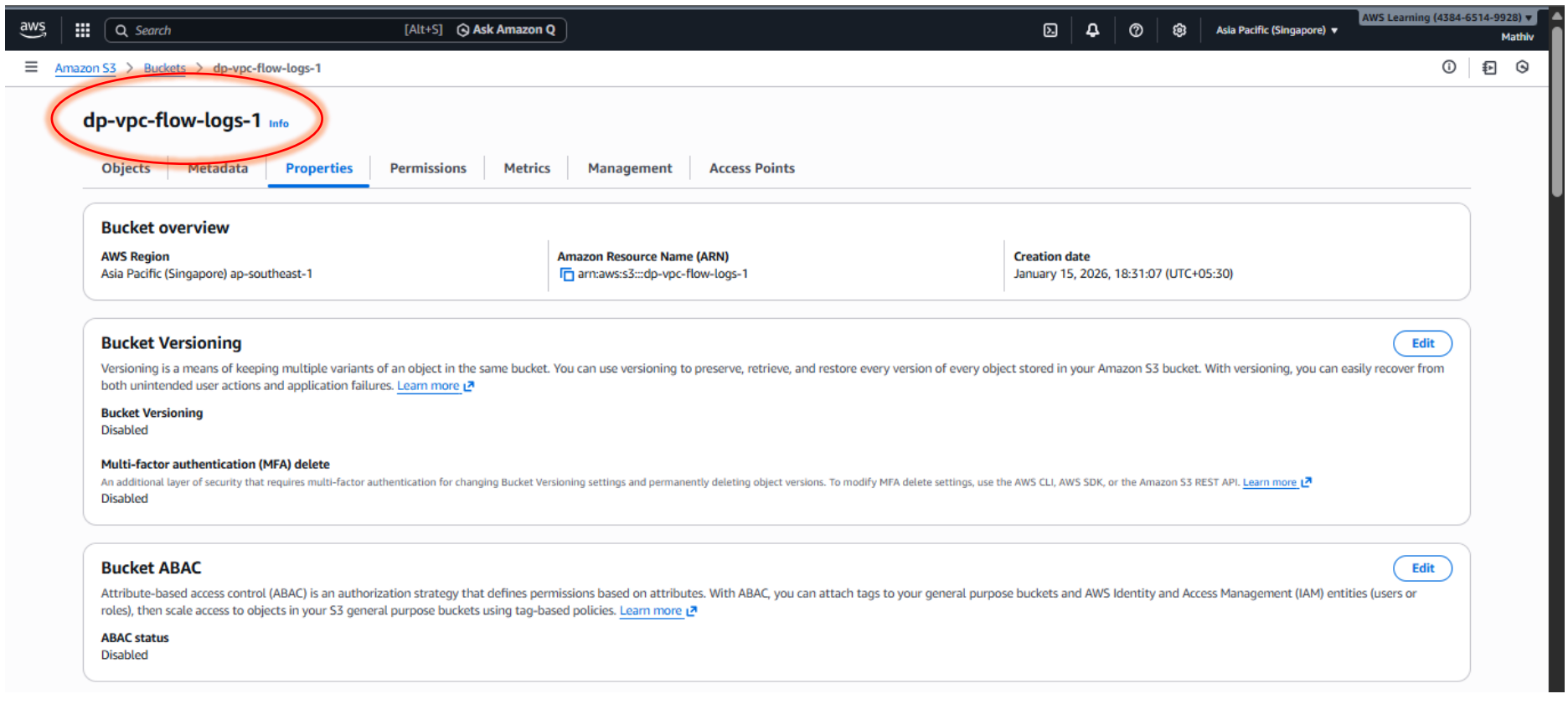
- To use with Athena, with this we can eliminate ETL(Extract, transform, load) pipelines, infrastructure setup, scaling, and ongoing management (but we still need to define a schema in Athena), which makes log analysis far simpler and faster because we can directly query flow logs without building heavy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

Flow logs With CloudWatch

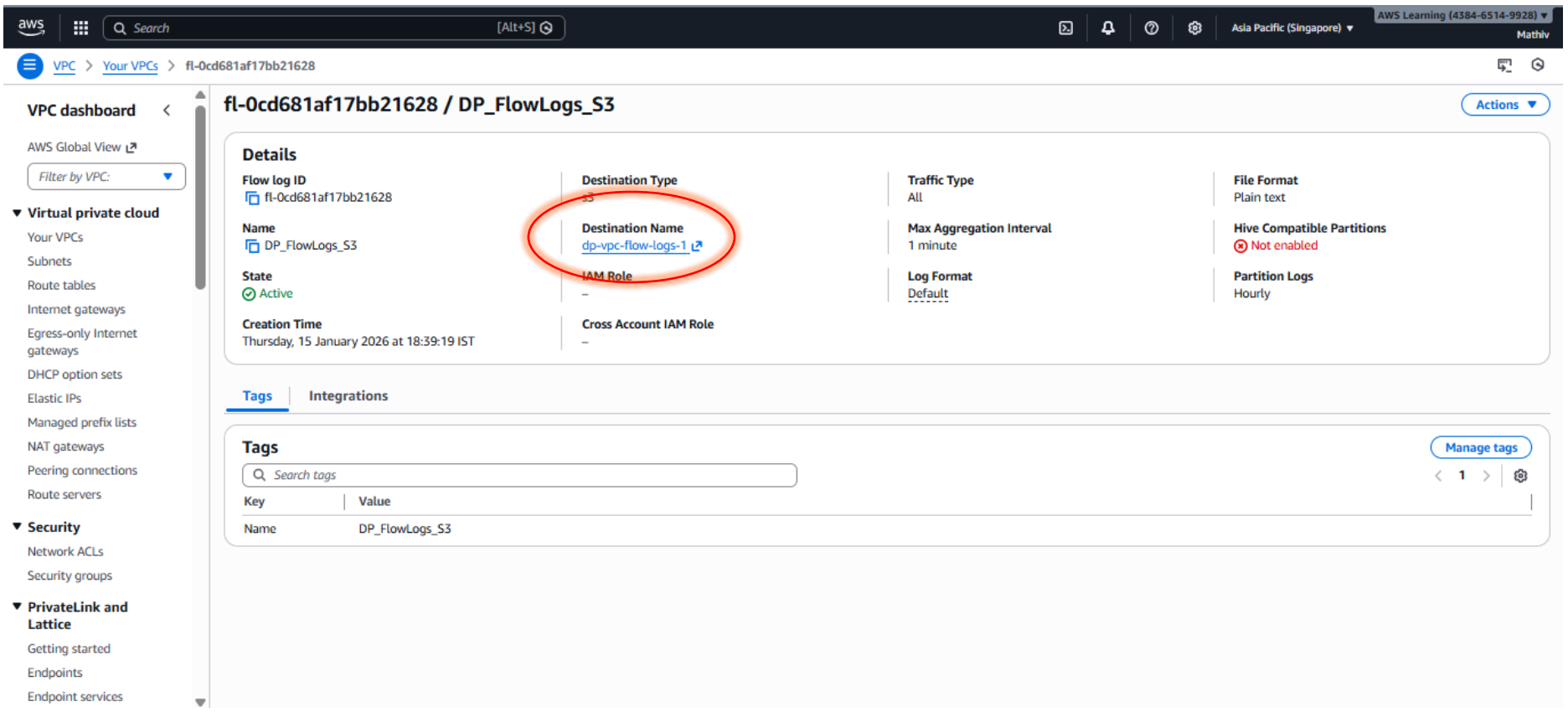
- For log analysis – Observability purpose
  Usecase: when you want **live monitoring and troubleshooting**.

Flow logs With S3

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

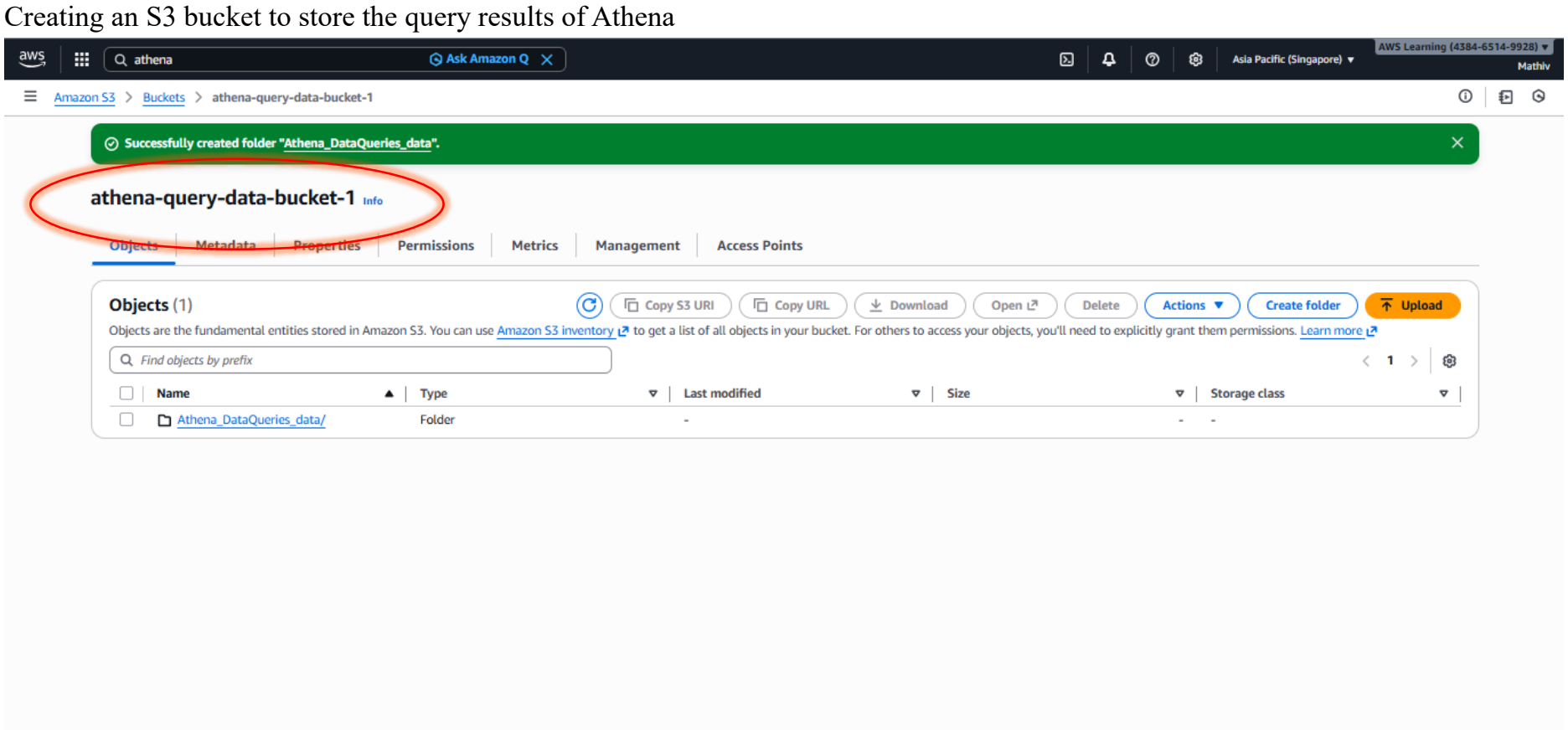


2. Create Flow logs from VPC
   Flow log created with destination: S3 Bucket

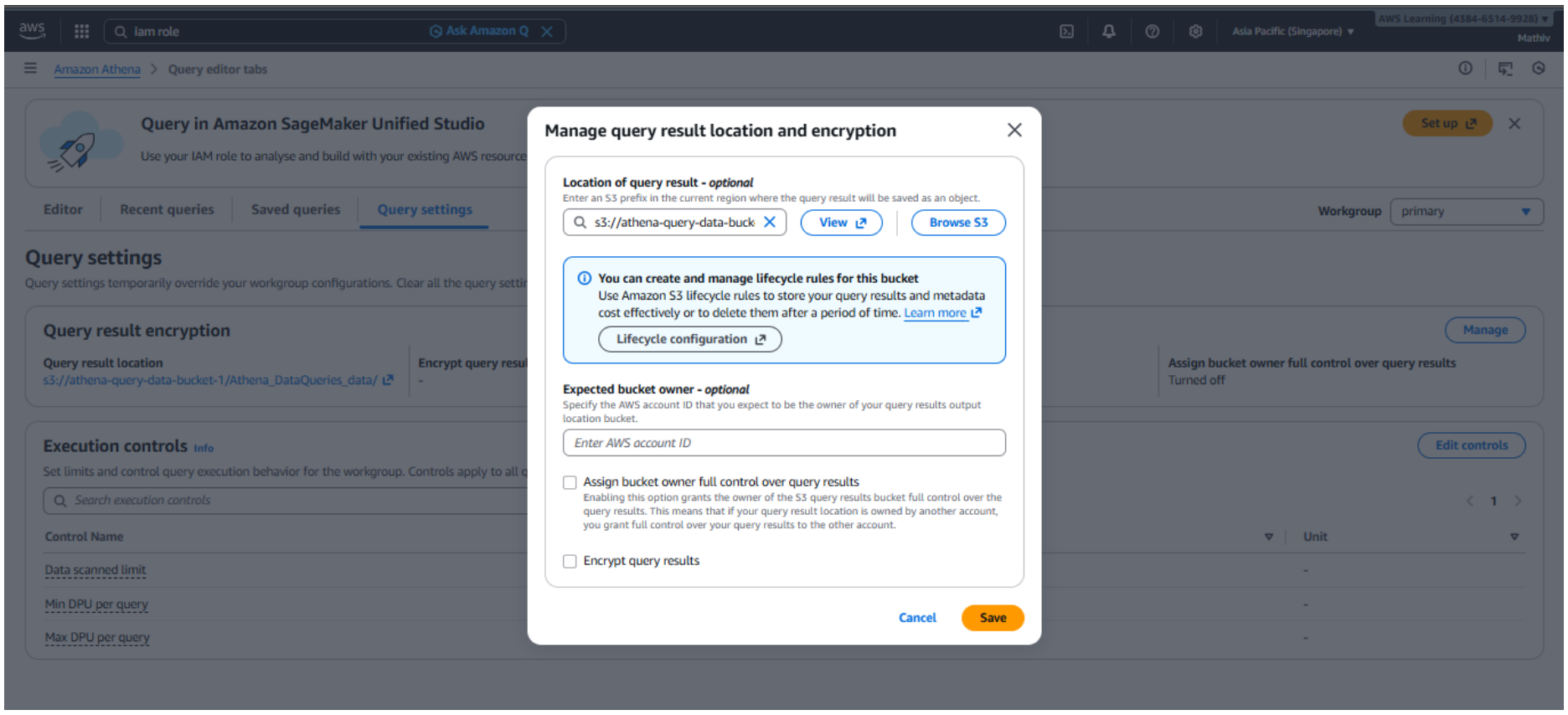


Using Athena with the logs stored in S3

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

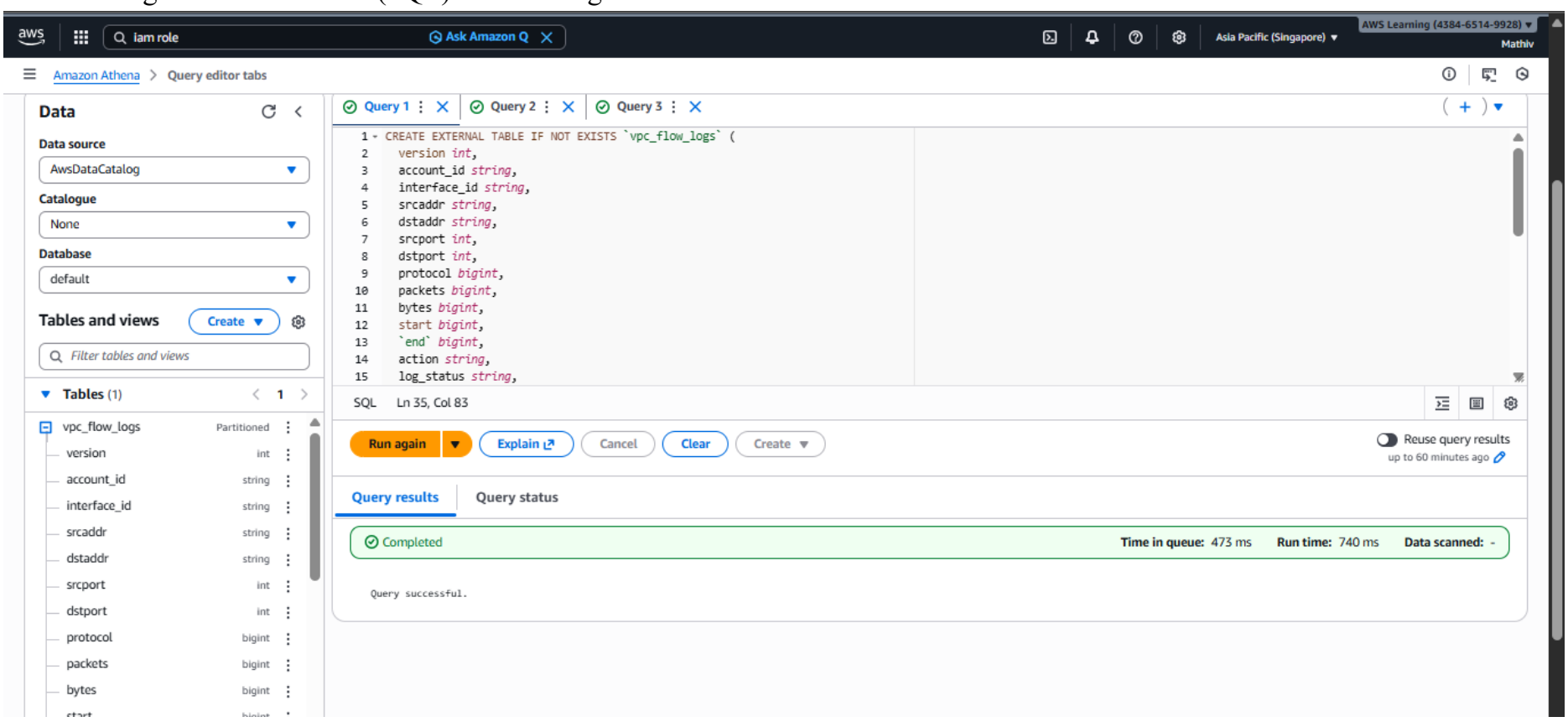


2. Mapping S3 bucket in the query location of Athena

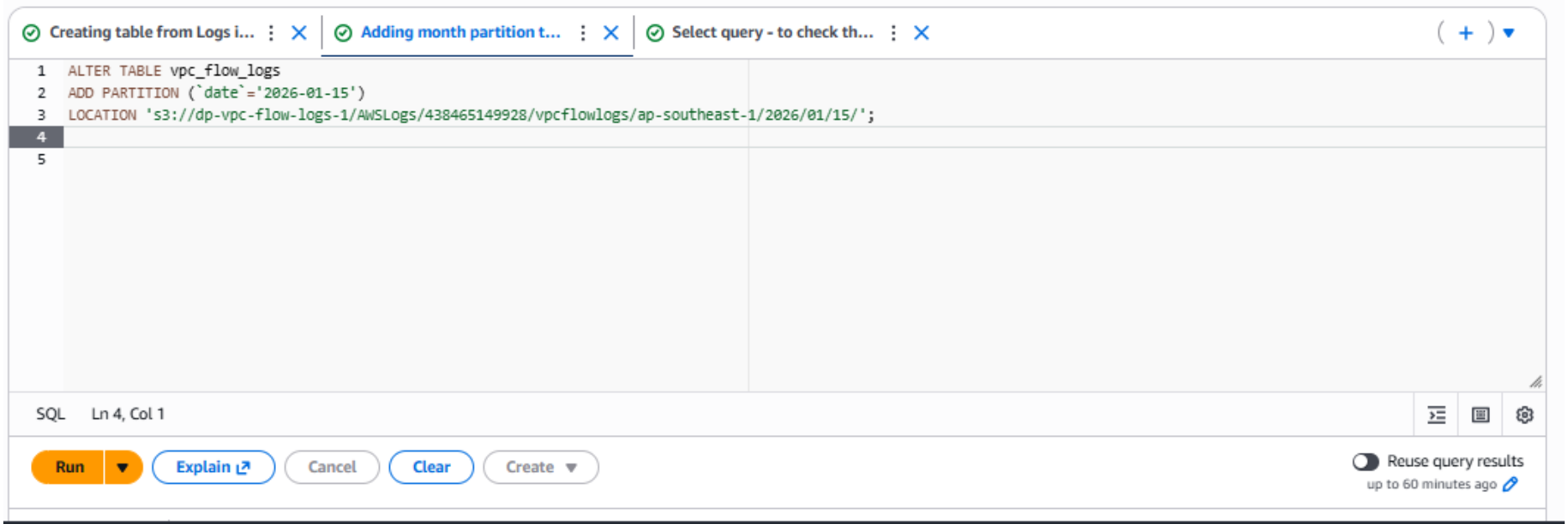


3. Querying logs from S3 with Athena | Querylink: [Create a table for Amazon VPC flow logs and query it - Amazon Athena]

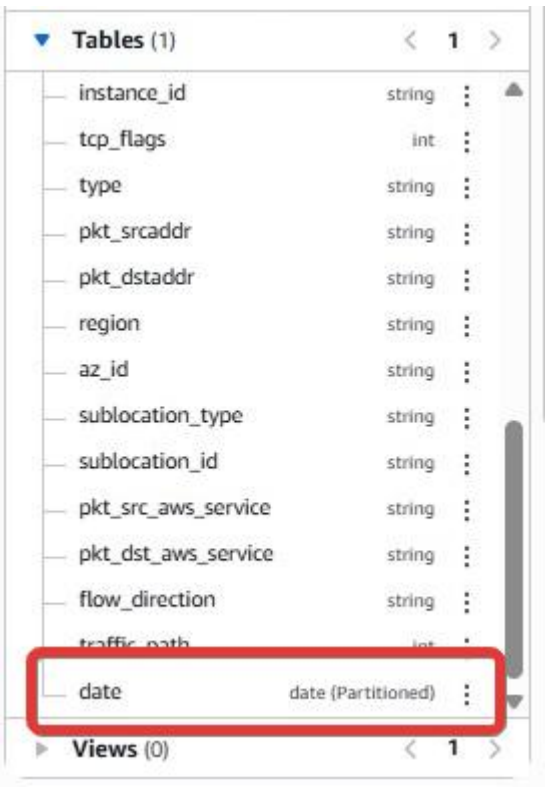
   a. First creating a Structured Table(SQL) from the logs stored in S3



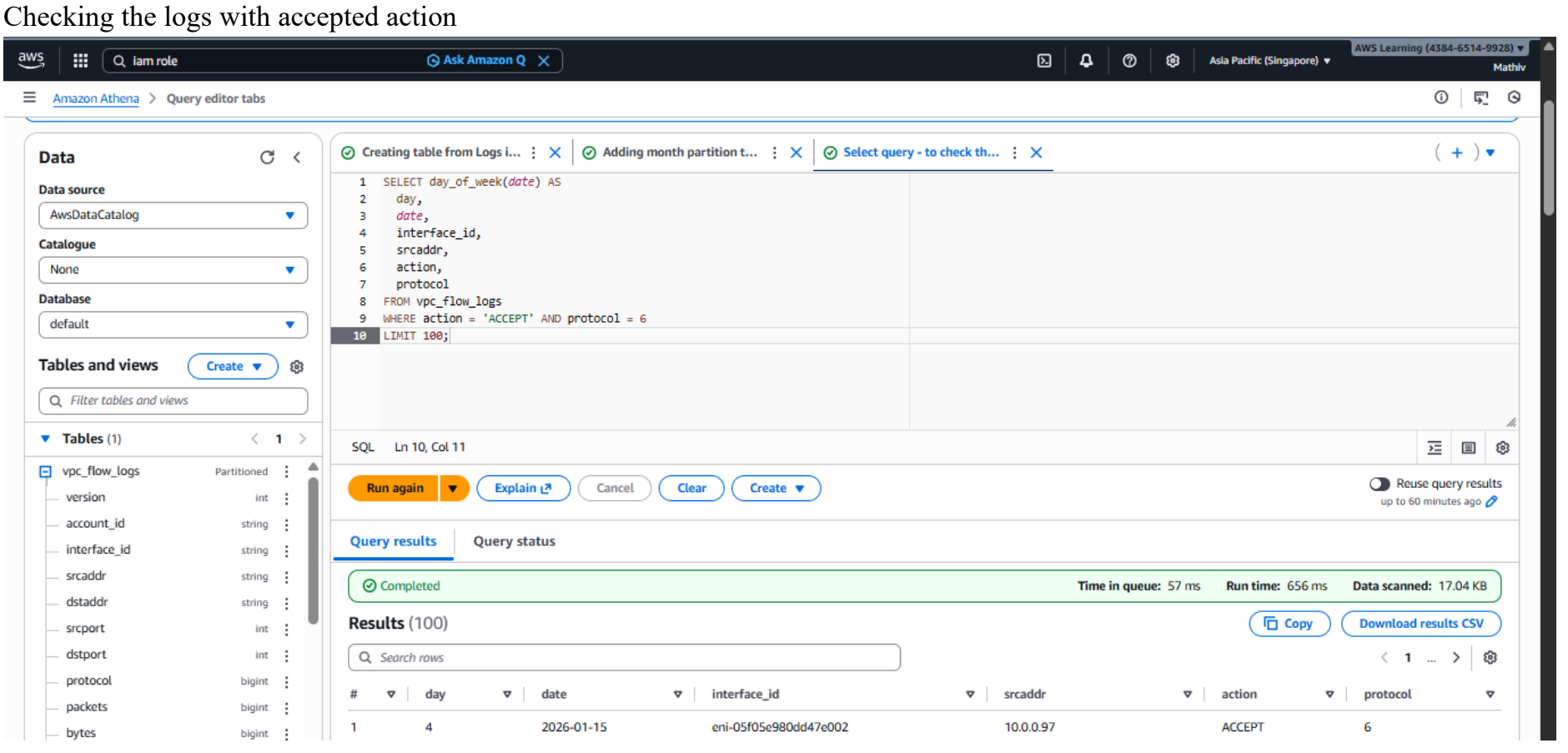
   b. Partitioning the table by time (day or hour is recommended for large datasets, month is fine for demo)



Result:



c. Checking the logs with accepted action



Results (100)

Copy | Download results CSV

Search rows

1 ...

#	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

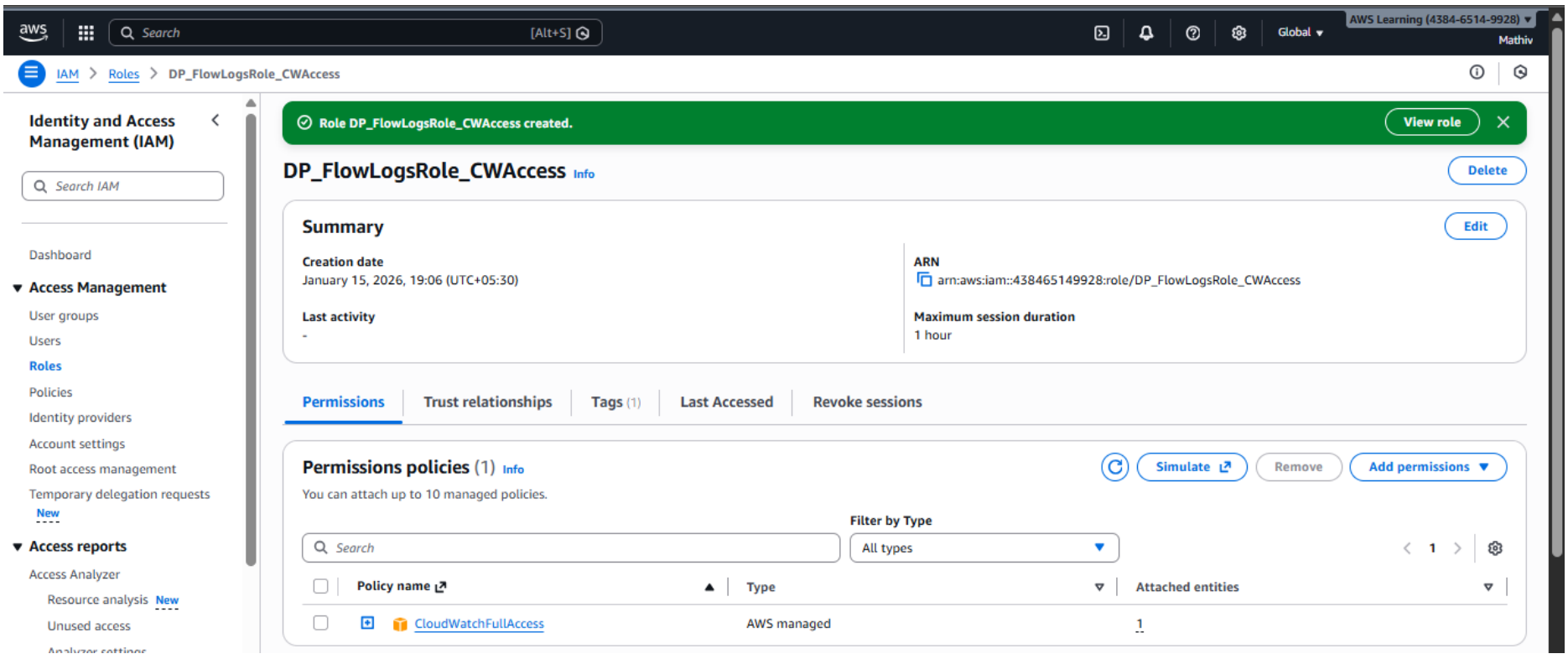
Flowlogs With CloudWatch

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"

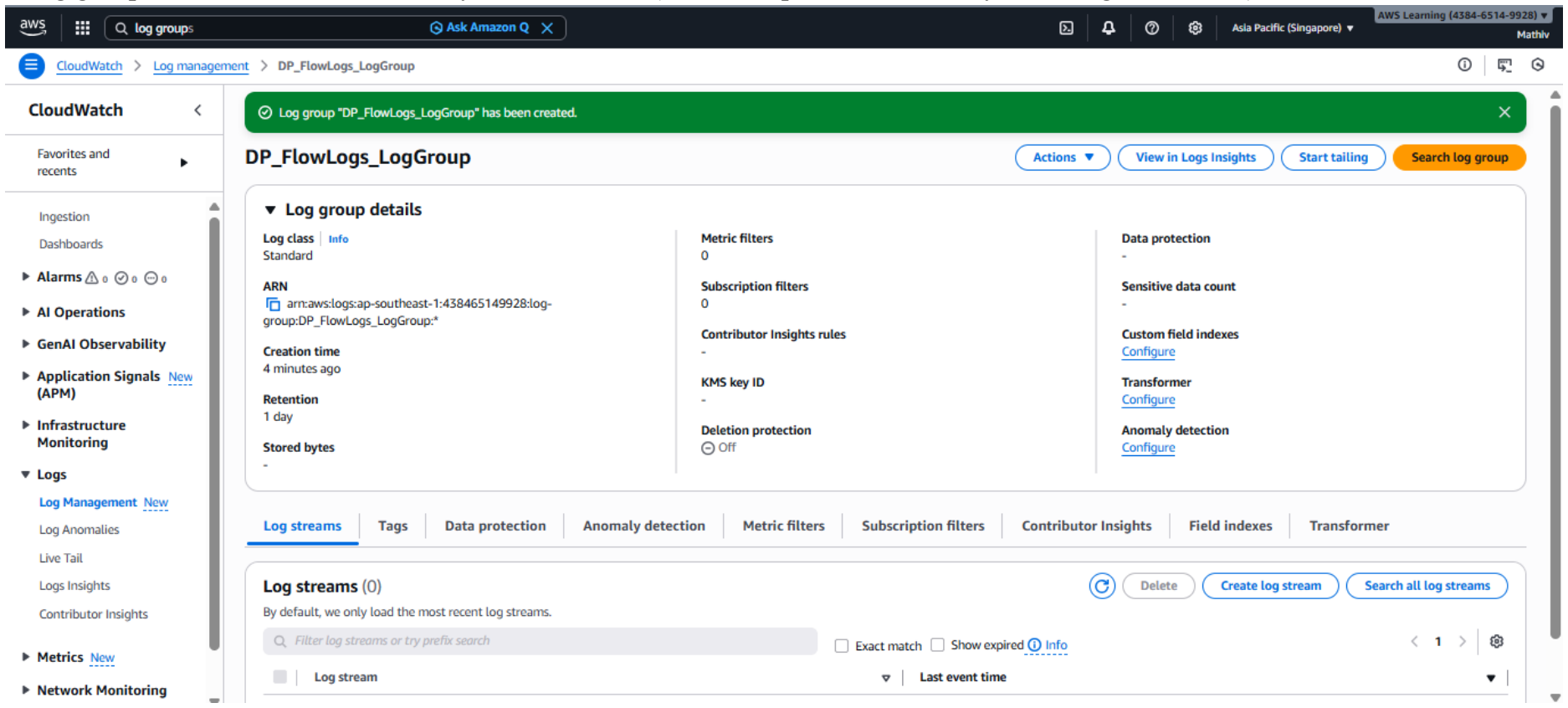
Custom Trust policy:

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

}

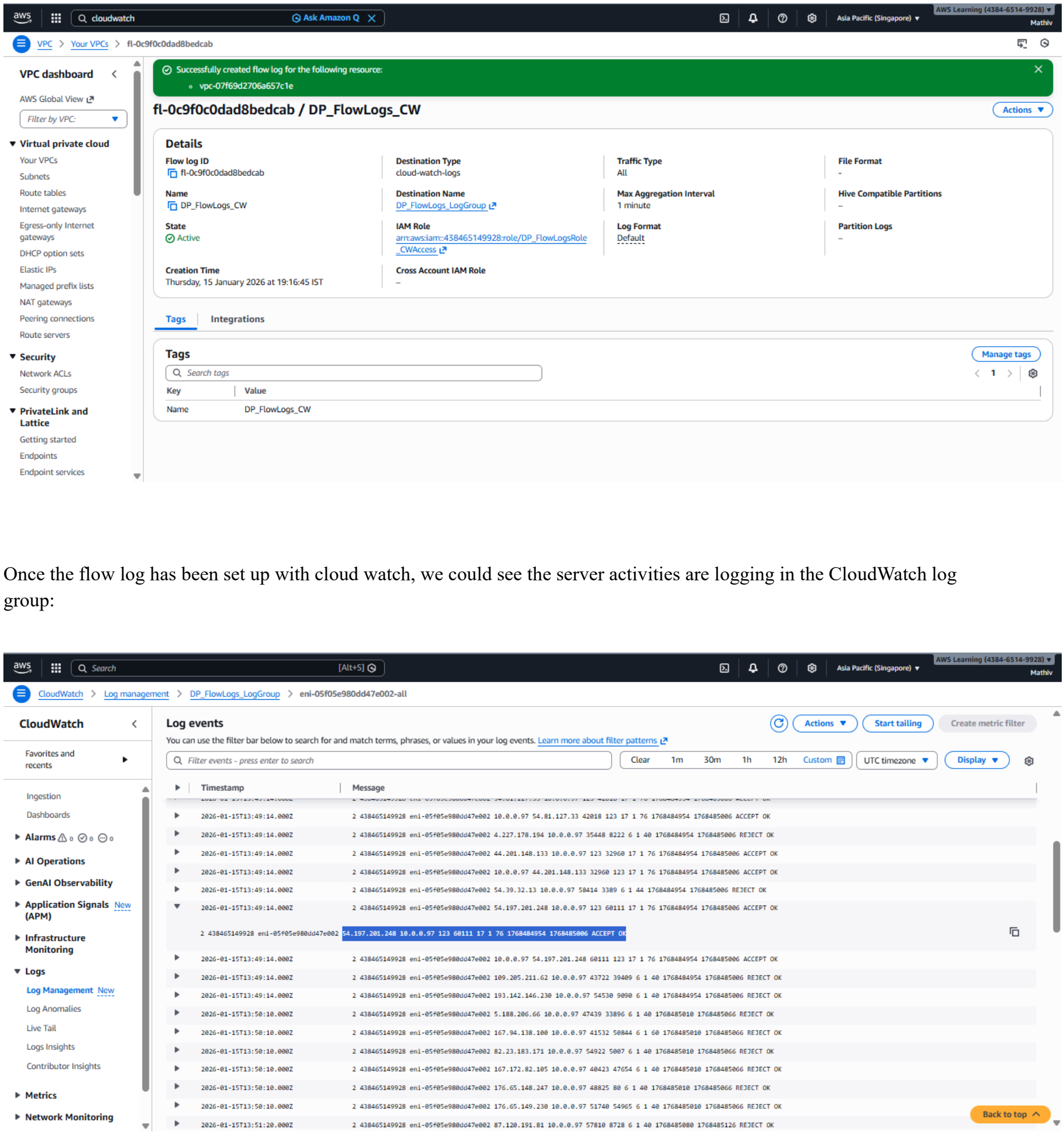


2. Create log group
A log group has been created with 1-day retention time (for demo; production usually uses longer retention)



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


```
# start

NetRange:       54.144.0.0 - 54.221.255.255
CIDR:           54.160.0.0/11, 54.216.0.0/14, 54.144.0.0/12, 54.208.0.0/13, 54
NetName:        AMAZON
NetHandle:      NET-54-144-0-0-1
Parent:         NET54 (NET-54-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Amazon Technologies Inc. (AT-88-Z)
RegDate:        2014-10-23
Updated:        2021-02-10
Ref:            https://rdap.arin.net/registry/ip/54.144.0.0
```



```
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
```