A CLOUD GURU

# Viewing VPC Flow Logs



Steven Moran
TRAINING ARCHITECT

# VPC Flow Log Destinations

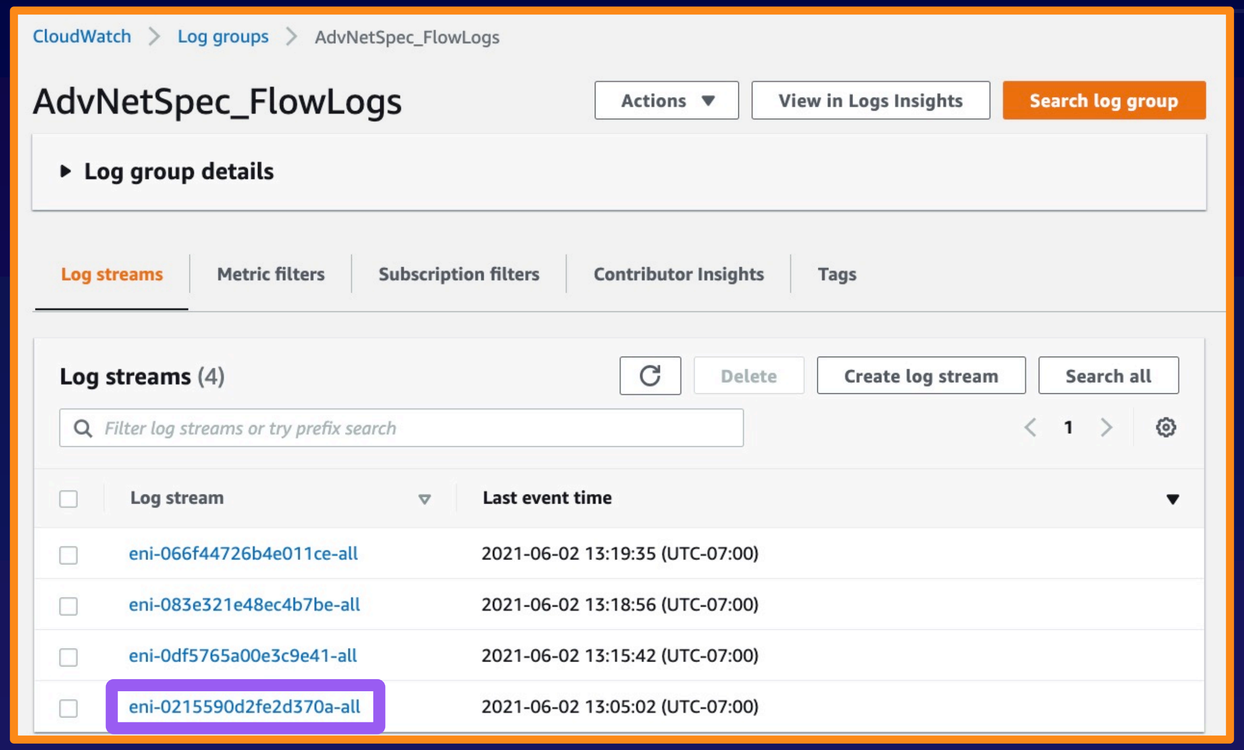


- CloudWatch log group

- S3 bucket

# Flow Logs in CloudWatch

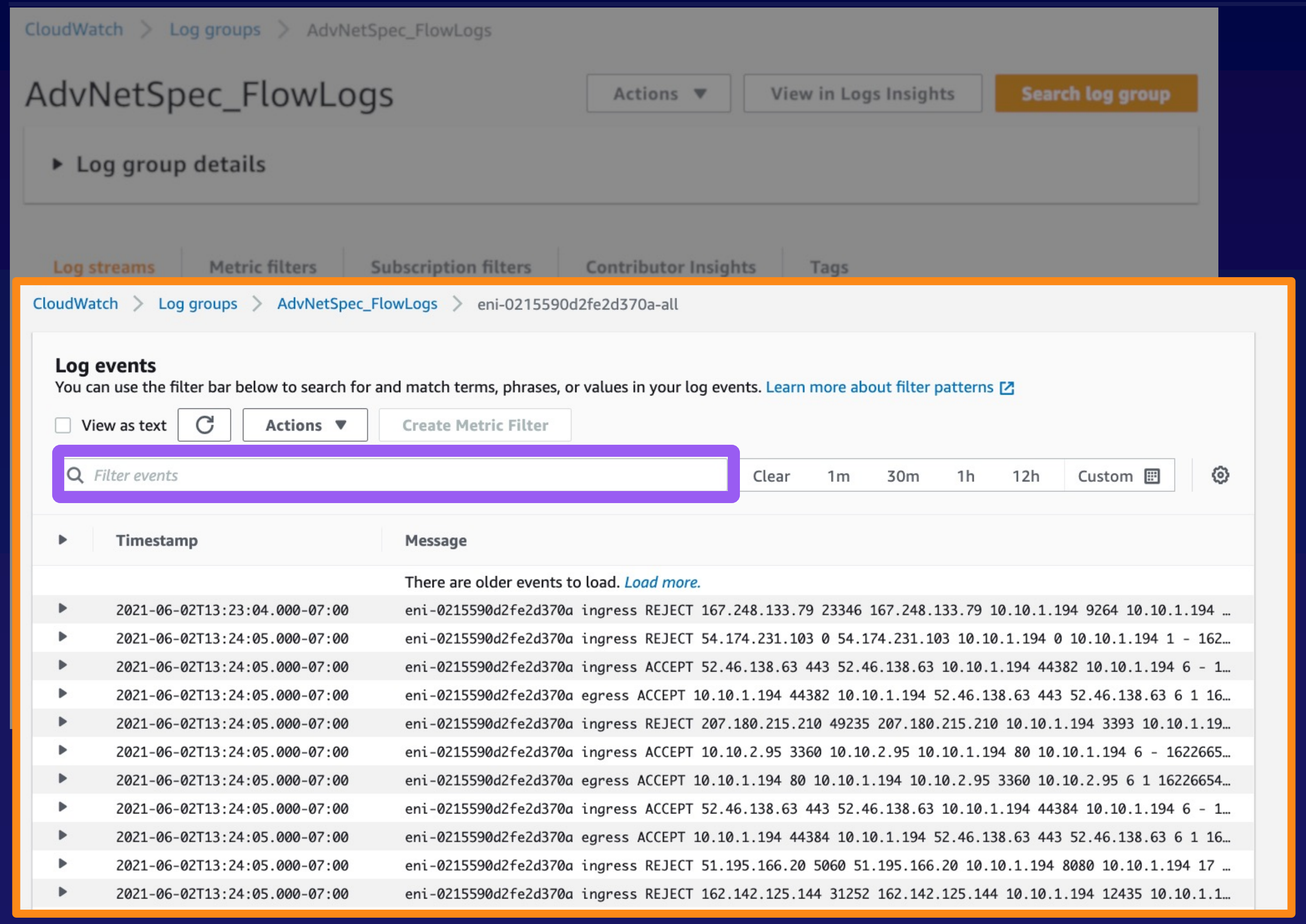
A CLOUD GURU




- One log stream per ENI

# Flow Logs in CloudWatch

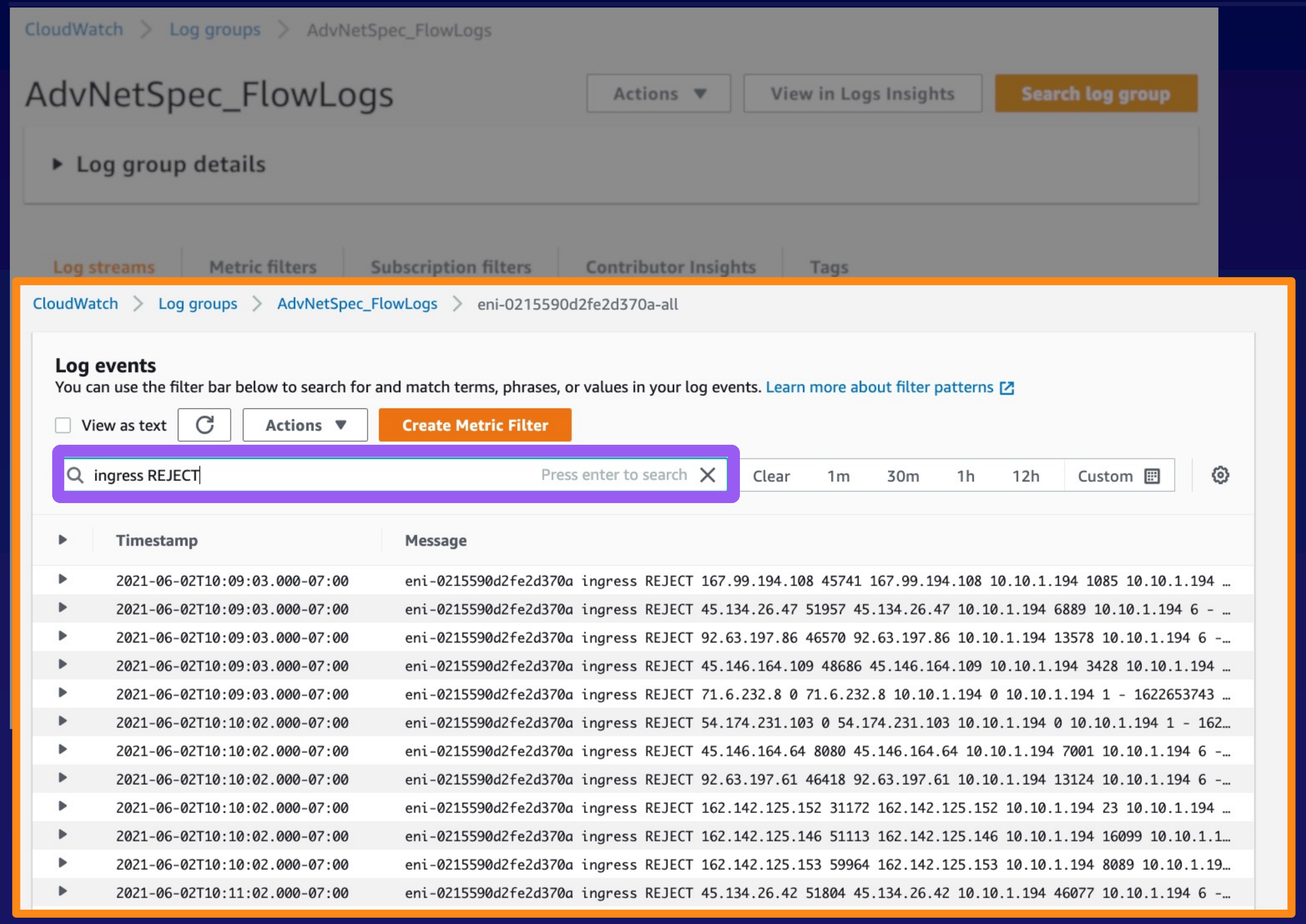
A CLOUD GURU




- One log stream per ENI
- Records may be filtered and exported.
  - Per-log stream

# Flow Logs in CloudWatch

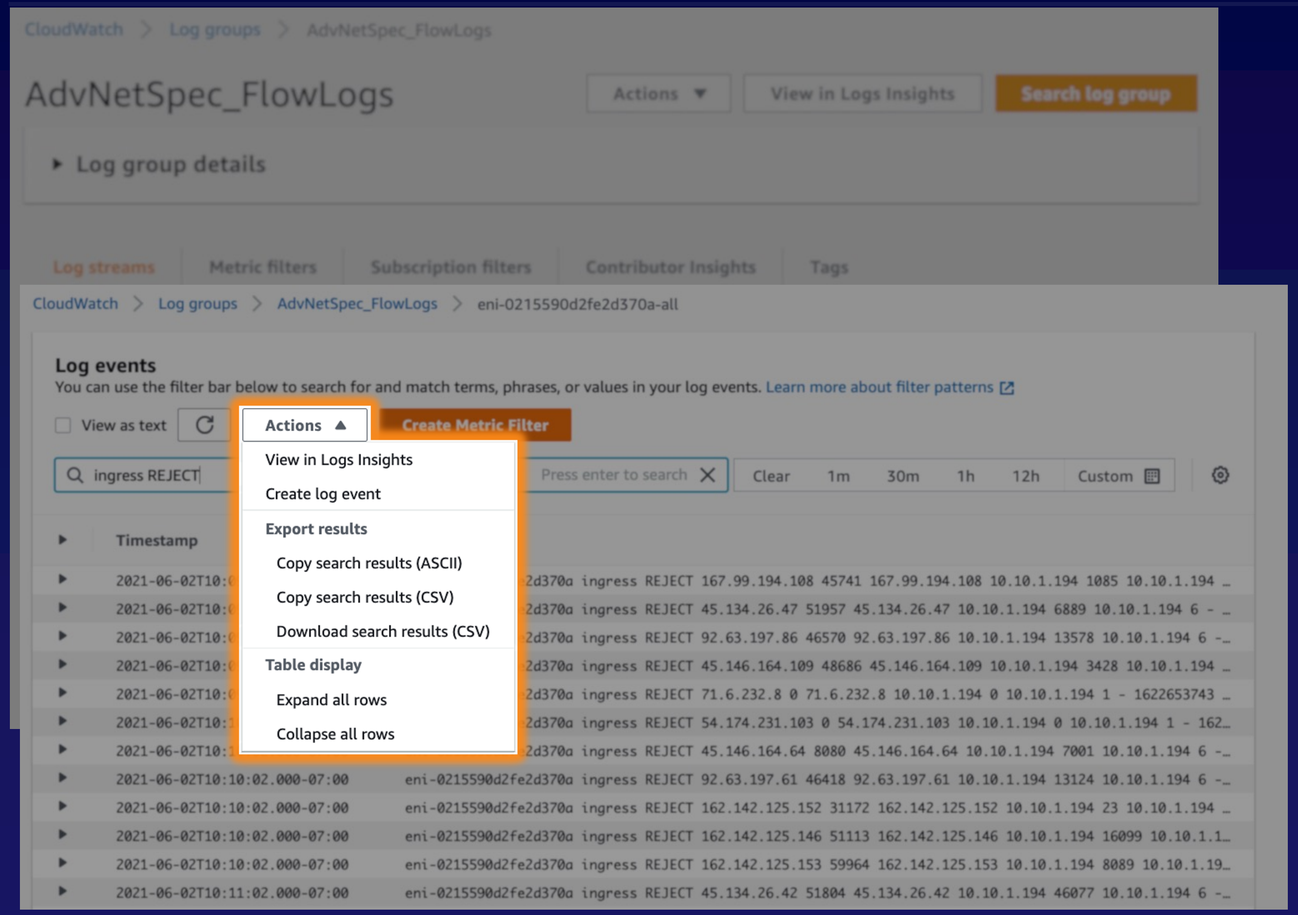
A CLOUD GURU




- One log stream per ENI
- Records may be filtered and exported.
  - Per-log stream

# Flow Logs in CloudWatch

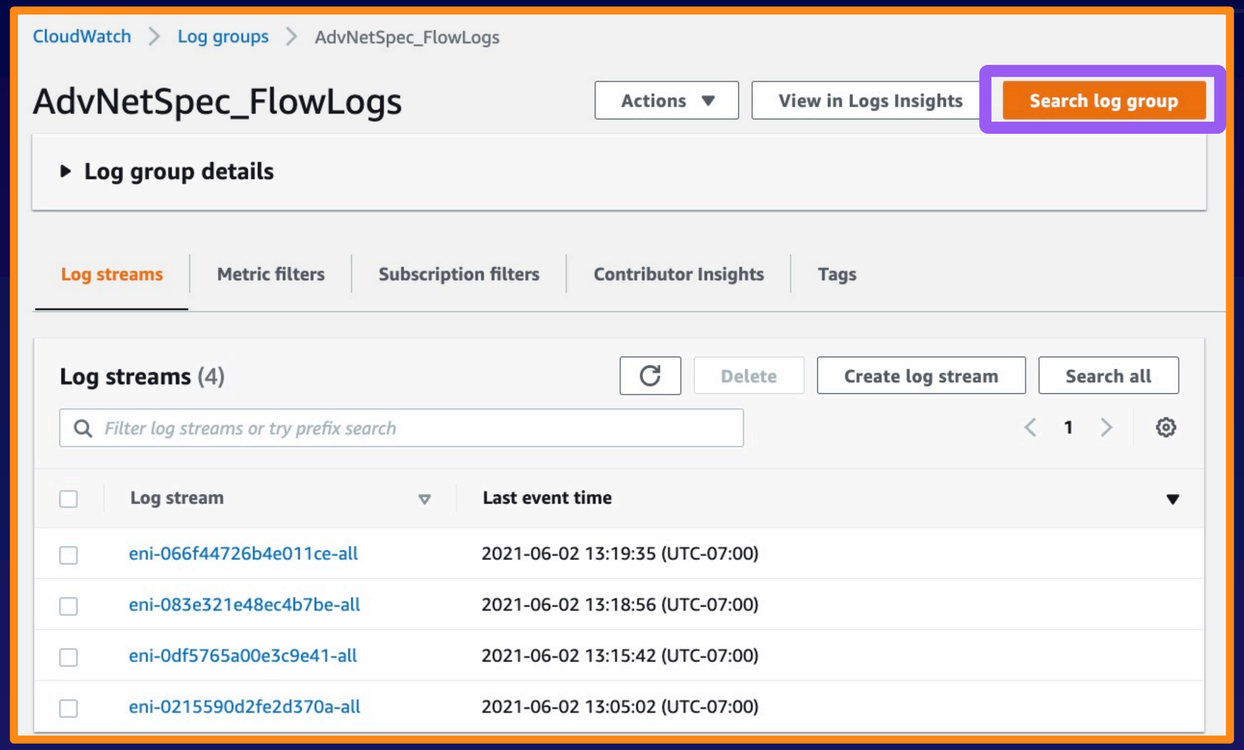
A CLOUD GURU




- One log stream per ENI
- Records may be filtered and exported.
  - Per-log stream

# Flow Logs in CloudWatch

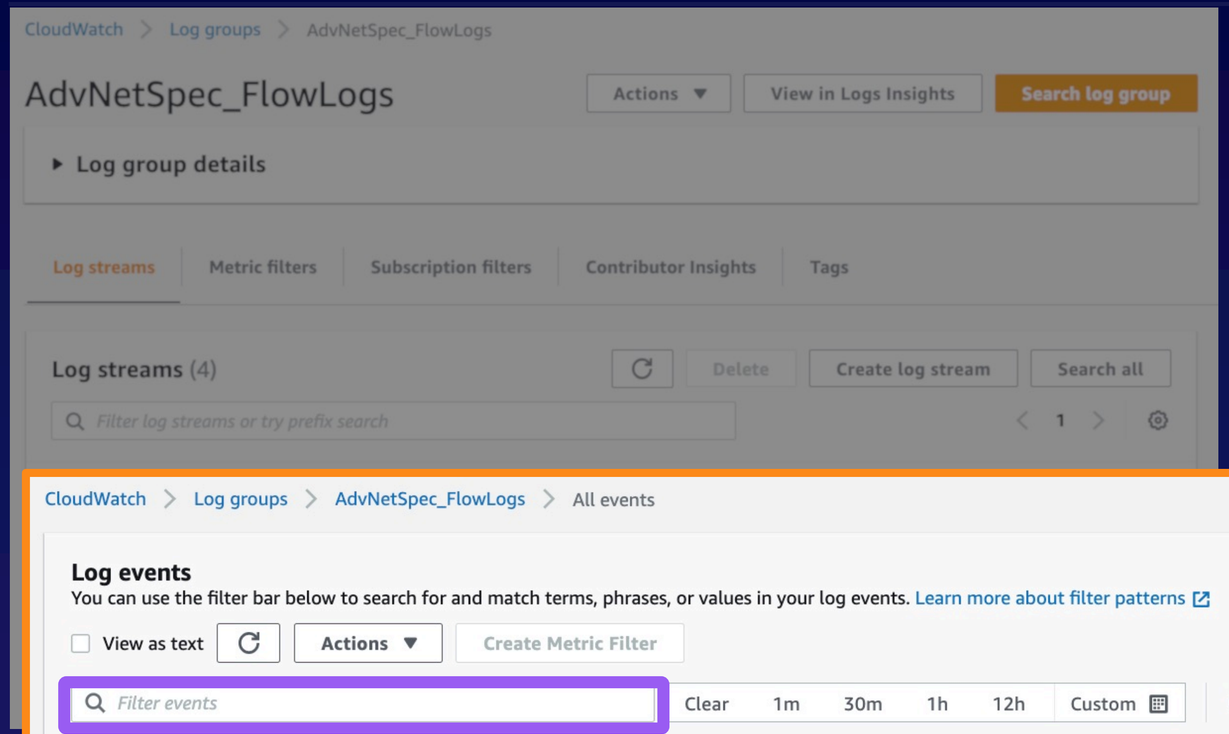
A CLOUD GURU

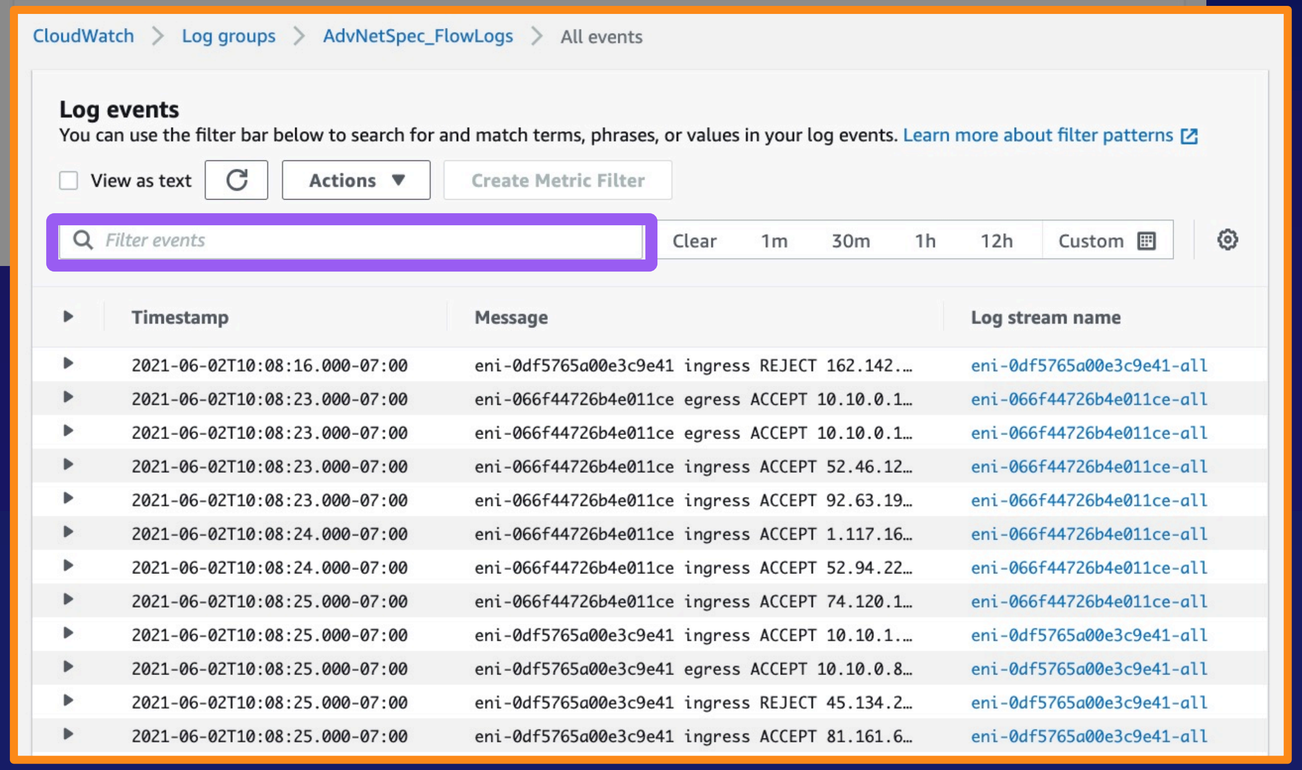



- One log stream per ENI
- Records may be filtered and exported.
  - Per-log stream
  - All streams in log group

# Flow Logs in CloudWatch



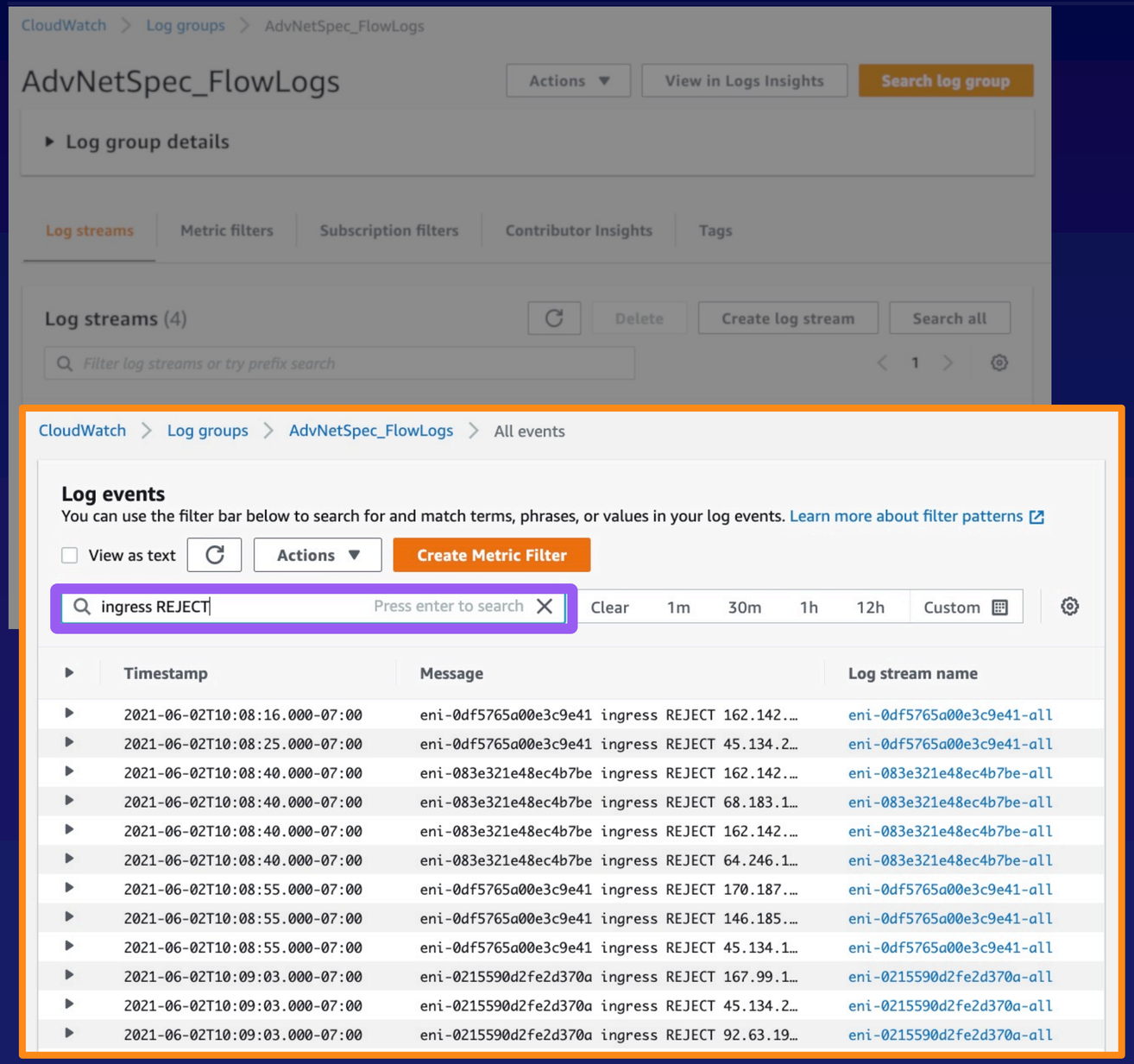



- One log stream per ENI
- Records may be filtered and exported.
  - Per-log stream
  - All streams in log group

# Flow Logs in CloudWatch



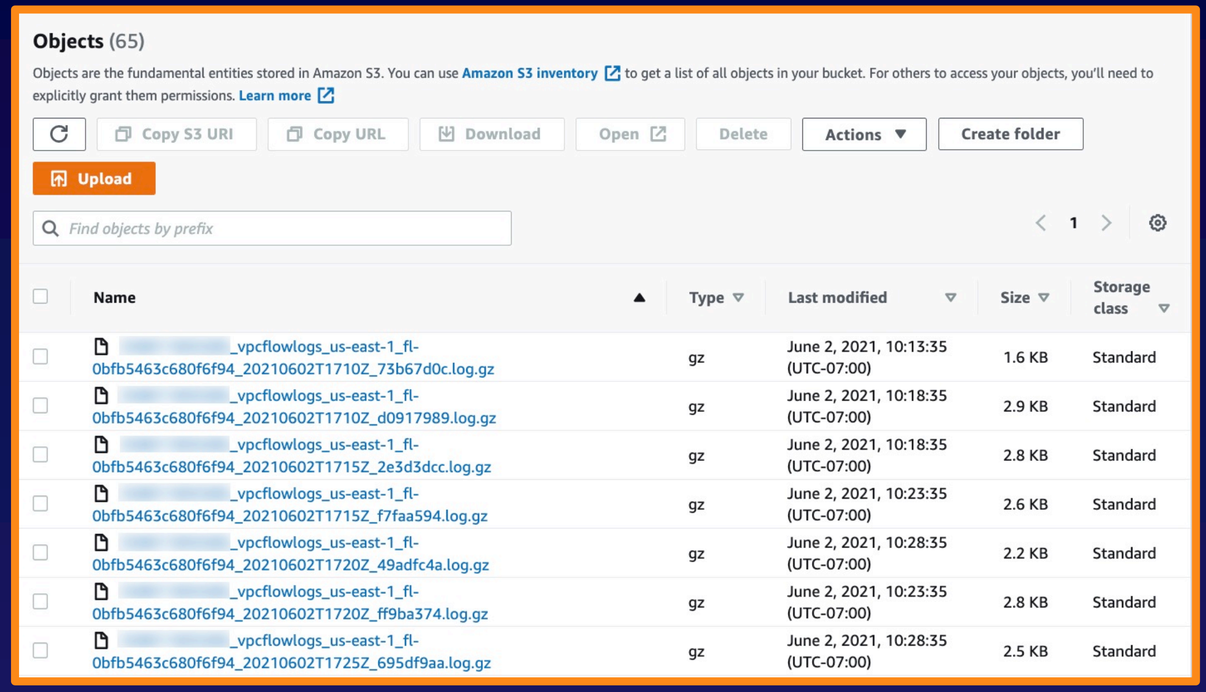



- One log stream per ENI
- Records may be filtered and exported.
  - Per-log stream
  - All streams in log group

# Flow Logs in S3



- Available data from all ENIs is collected into a single compressed file
  - Files published every 5 minutes or 75 MB




- Storage paths

```
bucket_ARN/optional_folder/AWSLogs/account#/vpcflowlogs/region/
yyyy/mm/dd/log_file_name.log.gz
```

```
aws_account_id_vpcflowlogs_region_flow_log_id_timestamp_hash.
log.gz
```

# Flow Logs in S3 – Viewing Options

A CLOUD GURU

```
interface-id flow-direction action srcaddr srcport pkt-srcaddr dstaddr dstport pkt-dstaddr protocol traffic-path start end
eni-0df5765a00e3c9e41 ingress ACCEPT 10.10.1.194 80 10.10.1.194 10.10.0.81 24088 10.10.0.81 6 - 1622653852 1622653857
eni-0df5765a00e3c9e41 egress ACCEPT 10.10.0.81 24088 10.10.0.81 10.10.1.194 80 10.10.1.194 6 1 1622653852 1622653857
eni-0df5765a00e3c9e41 ingress REJECT 45.134.26.39 51747 45.134.26.39 10.10.0.81 58451 10.10.0.81 6 - 1622653852 1622653857
eni-066f44726b4e011ce ingress ACCEPT 10.10.1.194 42466 10.10.1.194 10.10.0.184 443 52.46.138.63 6 - 1622653849 1622653850
eni-066f44726b4e011ce egress ACCEPT 10.10.0.184 443 52.46.138.63 10.10.1.194 42466 10.10.1.194 6 1 1622653849 1622653850
eni-066f44726b4e011ce egress ACCEPT 10.10.0.184 11769 10.10.0.184 66.85.78.80 123 66.85.78.80 17 8 1622653856 1622653861
eni-066f44726b4e011ce ingress ACCEPT 185.156.73.67 48370 185.156.73.67 10.10.0.184 2082 10.10.0.184 6 - 1622653856 1622653861
eni-066f44726b4e011ce ingress ACCEPT 88.214.24.51 40560 88.214.24.51 10.10.0.184 3408 10.10.0.184 6 - 1622653838 1622653838
eni-066f44726b4e011ce egress ACCEPT 10.10.0.184 443 52.119.197.249 10.10.1.194 34944 10.10.1.194 6 1 1622653875 1622653876
eni-0df5765a00e3c9e41 ingress REJECT 162.142.125.157 16581 162.142.125.157 10.10.0.81 18019 10.10.0.81 6 - 1622653861 1622653872
eni-0df5765a00e3c9e41 ingress REJECT 170.187.156.71 53232 170.187.156.71 10.10.0.81 8028 10.10.0.81 6 - 1622653861 1622653872
eni-0df5765a00e3c9e41 ingress REJECT 45.134.26.45 51855 45.134.26.45 10.10.0.81 29142 10.10.0.81 6 - 1622653861 1622653872
eni-0df5765a00e3c9e41 ingress ACCEPT 10.10.1.194 80 10.10.1.194 10.10.0.81 24172 10.10.0.81 6 - 1622653861 1622653872
eni-0df5765a00e3c9e41 egress ACCEPT 10.10.0.81 24172 10.10.0.81 10.10.1.194 80 10.10.1.194 6 1 1622653861 1622653872
eni-066f44726b4e011ce ingress ACCEPT 10.10.1.194 37150 10.10.1.194 10.10.0.184 123 66.207.226.14 17 - 1622653838 1622653841
eni-066f44726b4e011ce egress ACCEPT 10.10.0.184 42724 10.10.0.184 66.207.226.14 123 66.207.226.14 17 8 1622653838 1622653841
eni-066f44726b4e011ce ingress ACCEPT 52.119.197.249 443 52.119.197.249 10.10.0.184 56549 10.10.0.184 6 - 1622653838 1622653841
eni-066f44726b4e011ce ingress ACCEPT 194.195.244.129 53291 194.195.244.129 10.10.0.184 8044 10.10.0.184 6 - 1622653841 1622653842
eni-066f44726b4e011ce ingress ACCEPT 10.10.1.194 39208 10.10.1.194 10.10.0.184 123 129.250.35.251 17 - 1622653841 1622653842
```

- Download and decompress

# Flow Logs in S3 – Viewing Options

A CLOUD GURU

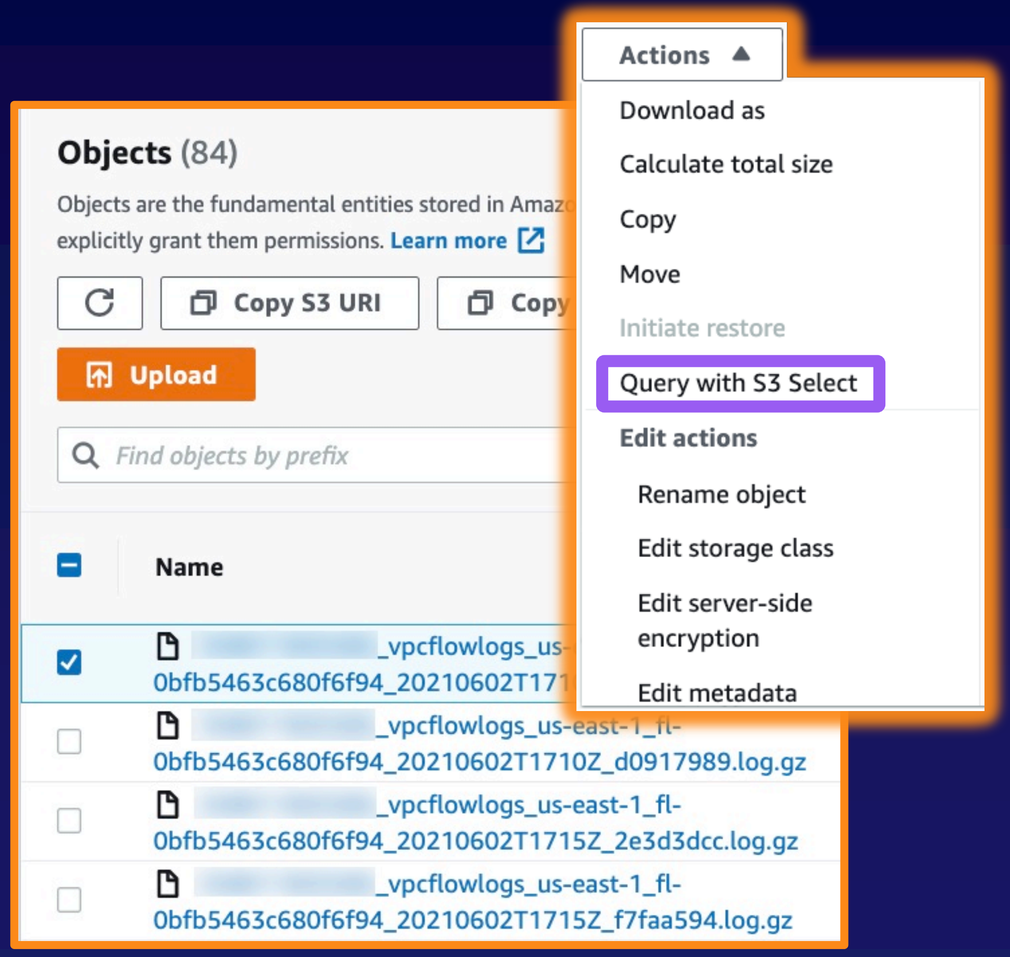
```
interface-id flow-direction action srcaddr srcport pkt-srcaddr dstaddr dstport pkt-dstaddr protocol traffic-path start end
eni-0df5765a00e3c9e41 ingress ACCEPT 10.10.1.194 80 10.10.1.194 10.10.0.81 24088 10.10.0.81 6 - 1622653852 1622653857
eni-0df5765a00e3c9e41 egress ACCEPT 10.10.0.81 24088 10.10.0.81 10.10.1.194 80 10.10.1.194 6 1 1622653852 1622653857
eni-0df5765a00e3c9e41 ingress REJECT 45.134.26.39 51747 45.134.26.39 10.10.0.81 58451 10.10.0.81 6 - 1622653852 1622653857
eni-066f44726b4e011ce ingress ACCEPT 10.10.1.194 42466 10.10.1.194 10.10.0.184 443 52.46.138.63 6 - 1622653849 1622653850
eni-066f44726b4e011ce egress ACCEPT 10.10.0.184 443 52.46.138.63 10.10.1.194 42466 10.10.1.194 6 1 1622653849 1622653850
eni-066f44726b4e011ce egress ACCEPT 10.10.0.184 11769 10.10.0.184 66.85.78.80 123 66.85.78.80 17 8 1622653856 1622653861
eni-066f44726b4e011ce ingress ACCEPT 185.156.73.67 48370 185.156.73.67 10.10.0.184 2082 10.10.0.184 6 - 1622653856 1622653861
eni-066f44726b4e011ce ingress ACCEPT 88.214.24.51 40560 88.214.24.51 10.10.0.184 3408 10.10.0.184 6 - 1622653838 1622653838
eni-066f44726b4e011ce egress ACCEPT 10.10.0.184 443 52.119.197.249 10.10.1.194 34944 10.10.1.194 6 1 1622653875 1622653876
eni-0df5765a00e3c9e41 ingress REJECT 162.142.125.157 16581 162.142.125.157 10.10.0.81 18019 10.10.0.81 6 - 1622653861 1622653872
eni-0df5765a00e3c9e41 ingress REJECT 170.187.156.71 53232 170.187.156.71 10.10.0.81 8028 10.10.0.81 6 - 1622653861 1622653872
```

| | A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | interface-id | flow-directio | action | srcaddr | srcport | pkt-srcaddr | dstaddr | dstport | pkt-dstaddr | protocol | traffic-path | start | end |
| 2 | eni-0df5765a00e3c9e41 | ingress | ACCEPT | 10.10.1.194 | 80 | 10.10.1.194 | 10.10.0.81 | 24088 | 10.10.0.81 | 6 | - | 1622653852 | 1622653857 |
| 3 | eni-0df5765a00e3c9e41 | egress | ACCEPT | 10.10.0.81 | 24088 | 10.10.0.81 | 10.10.1.194 | 80 | 10.10.1.194 | 6 | 1 | 1622653852 | 1622653857 |
| 4 | eni-0df5765a00e3c9e41 | ingress | REJECT | 45.134.26.39 | 51747 | 45.134.26.39 | 10.10.0.81 | 58451 | 10.10.0.81 | 6 | - | 1622653852 | 1622653857 |
| 5 | eni-066f44726b4e011ce | ingress | ACCEPT | 10.10.1.194 | 42466 | 10.10.1.194 | 10.10.0.184 | 443 | 52.46.138.63 | 6 | - | 1622653849 | 1622653850 |
| 6 | eni-066f44726b4e011ce | egress | ACCEPT | 10.10.0.184 | 443 | 52.46.138.63 | 10.10.1.194 | 42466 | 10.10.1.194 | 6 | 1 | 1622653849 | 1622653850 |
| 7 | eni-066f44726b4e011ce | egress | ACCEPT | 10.10.0.184 | 11769 | 10.10.0.184 | 66.85.78.80 | 123 | 66.85.78.80 | 17 | 8 | 1622653856 | 1622653861 |
| 8 | eni-066f44726b4e011ce | ingress | ACCEPT | 185.156.73.6 | 48370 | 185.156.73.6 | 10.10.0.184 | 2082 | 10.10.0.184 | 6 | - | 1622653856 | 1622653861 |
| 9 | eni-066f44726b4e011ce | ingress | ACCEPT | 88.214.24.51 | 40560 | 88.214.24.51 | 10.10.0.184 | 3408 | 10.10.0.184 | 6 | - | 1622653838 | 1622653838 |
| 10 | eni-066f44726b4e011ce | egress | ACCEPT | 10.10.0.184 | 443 | 52.119.197.2 | 10.10.1.194 | 34944 | 10.10.1.194 | 6 | 1 | 1622653875 | 1622653876 |
| 11 | eni-0df5765a00e3c9e41 | ingress | REJECT | 162.142.125. | 16581 | 162.142.125. | 10.10.0.81 | 18019 | 10.10.0.81 | 6 | - | 1622653861 | 1622653872 |
| 12 | eni-0df5765a00e3c9e41 | ingress | REJECT | 170.187.156. | 53232 | 170.187.156. | 10.10.0.81 | 8028 | 10.10.0.81 | 6 | - | 1622653861 | 1622653872 |
| 13 | eni-0df5765a00e3c9e41 | ingress | REJECT | 45.134.26.45 | 51855 | 45.134.26.45 | 10.10.0.81 | 29142 | 10.10.0.81 | 6 | - | 1622653861 | 1622653872 |
| 14 | eni-0df5765a00e3c9e41 | ingress | ACCEPT | 10.10.1.194 | 80 | 10.10.1.194 | 10.10.0.81 | 24172 | 10.10.0.81 | 6 | - | 1622653861 | 1622653872 |
| 15 | eni-0df5765a00e3c9e41 | egress | ACCEPT | 10.10.0.81 | 24172 | 10.10.0.81 | 10.10.1.194 | 80 | 10.10.1.194 | 6 | 1 | 1622653861 | 1622653872 |
| 16 | eni-066f44726b4e011ce | ingress | ACCEPT | 10.10.1.194 | 37150 | 10.10.1.194 | 10.10.0.184 | 123 | 66.207.226.1 | 17 | - | 1622653838 | 1622653841 |
| 17 | eni-066f44726b4e011ce | egress | ACCEPT | 10.10.0.184 | 42724 | 10.10.0.184 | 66.207.226.1 | 123 | 66.207.226.1 | 17 | 8 | 1622653838 | 1622653841 |
| 18 | eni-066f44726b4e011ce | ingress | ACCEPT | 52.119.197.2 | 443 | 52.119.197.2 | 10.10.0.184 | 56549 | 10.10.0.184 | 6 | - | 1622653838 | 1622653841 |
| 19 | eni-066f44726b4e011ce | ingress | ACCEPT | 194.195.244. | 53291 | 194.195.244. | 10.10.0.184 | 8044 | 10.10.0.184 | 6 | - | 1622653841 | 1622653842 |
| 20 | eni-066f44726b4e011ce | ingress | ACCEPT | 10.10.1.194 | 39208 | 10.10.1.194 | 10.10.0.184 | 123 | 129.250.35.2 | 17 | - | 1622653841 | 1622653842 |
| 21 | eni-066f44726b4e011ce | egress | ACCEPT | 10.10.0.184 | 56549 | 10.10.0.184 | 52.119.197.2 | 443 | 52.119.197.2 | 6 | 8 | 1622653858 | 1622653864 |
| 22 | eni-066f44726b4e011ce | ingress | ACCEPT | 10.10.1.194 | 34940 | 10.10.1.194 | 10.10.0.184 | 443 | 52.119.197.2 | 6 | - | 1622653858 | 1622653864 |
| 23 | eni-066f44726b4e011ce | ingress | ACCEPT | 34.96.130.13 | 64186 | 34.96.130.13 | 10.10.0.184 | 161 | 10.10.0.184 | 17 | - | 1622653852 | 1622653911 |
| 24 | eni-066f44726b4e011ce | ingress | ACCEPT | 10.10.1.194 | 34942 | 10.10.1.194 | 10.10.0.184 | 443 | 52.119.197.2 | 6 | - | 1622653852 | 1622653911 |
| 25 | eni-066f44726b4e011ce | egress | ACCEPT | 10.10.0.184 | 443 | 52.119.197.2 | 10.10.1.194 | 34942 | 10.10.1.194 | 6 | 1 | 1622653852 | 1622653911 |
| 26 | eni-066f44726b4e011ce | ingress | ACCEPT | 52.119.197.2 | 443 | 52.119.197.2 | 10.10.0.184 | 6143 | 10.10.0.184 | 6 | - | 1622653852 | 1622653911 |
| 27 | eni-066f44726b4e011ce | egress | ACCEPT | 10.10.0.184 | 6143 | 10.10.0.184 | 52.119.197.2 | 443 | 52.119.197.2 | 6 | 2 | 1622653852 | 1622653911 |
| 28 | eni-066f44726b4e011ce | ingress | ACCEPT | 52.46.141.15 | 443 | 52.46.141.15 | 10.10.0.184 | 2074 | 10.10.0.184 | 6 | - | 1622653852 | 1622653911 |
| 29 | eni-066f44726b4e011ce | egress | ACCEPT | 10.10.0.184 | 2074 | 10.10.0.184 | 52.46.141.15 | 443 | 52.46.141.15 | 6 | 2 | 1622653852 | 1622653911 |
| 30 | eni-066f44726b4e011ce | ingress | ACCEPT | 10.10.1.194 | 43616 | 10.10.1.194 | 10.10.0.184 | 443 | 52.46.128.12 | 6 | - | 1622653852 | 1622653911 |
| 31 | eni-066f44726b4e011ce | ingress | ACCEPT | 10.10.1.194 | 57990 | 10.10.1.194 | 10.10.0.184 | 443 | 52.46.141.15 | 6 | - | 1622653852 | 1622653911 |
| 32 | eni-066f44726b4e011ce | egress | ACCEPT | 10.10.0.184 | 443 | 52.46.141.15 | 10.10.1.194 | 57990 | 10.10.1.194 | 6 | 1 | 1622653852 | 1622653911 |
| 33 | eni-066f44726b4e011ce | egress | ACCEPT | 10.10.0.184 | 42390 | 10.10.0.184 | 52.46.128.12 | 443 | 52.46.128.12 | 6 | 2 | 1622653852 | 1622653911 |
| 34 | eni-066f44726b4e011ce | ingress | ACCEPT | 45.134.26.55 | 52089 | 45.134.26.55 | 10.10.0.184 | 55161 | 10.10.0.184 | 6 | - | 1622653879 | 1622653886 |
| 35 | eni-066f44726b4e011ce | ingress | ACCEPT | 10.10.1.194 | 53747 | 10.10.1.194 | 10.10.0.184 | 123 | 173.0.48.220 | 17 | - | 1622653879 | 1622653886 |
| 36 | eni-066f44726b4e011ce | ingress | ACCEPT | 52.119.197.2 | 443 | 52.119.197.2 | 10.10.0.184 | 15606 | 10.10.0.184 | 6 | - | 1622653879 | 1622653886 |
| 37 | eni-066f44726b4e011ce | ingress | ACCEPT | 162.142.125. | 16894 | 162.142.125. | 10.10.0.184 | 465 | 10.10.0.184 | 6 | - | 1622653869 | 1622653869 |
| 38 | eni-066f44726b4e011ce | ingress | ACCEPT | 173.0.48.220 | 123 | 173.0.48.220 | 10.10.0.184 | 51730 | 10.10.0.184 | 17 | - | 1622653869 | 1622653869 |
| 39 | eni-066f44726b4e011ce | egress | ACCEPT | 10.10.0.184 | 443 | 52.46.128.12 | 10.10.1.194 | 43616 | 10.10.1.194 | 6 | 1 | 1622653883 | 1622653891 |
| 40 | eni-066f44726b4e011ce | egress | ACCEPT | 10.10.0.184 | 443 | 52.119.197.2 | 10.10.1.194 | 34940 | 10.10.1.194 | 6 | 1 | 1622653883 | 1622653891 |
| 41 | eni-066f44726b4e011ce | ingress | ACCEPT | 52.46.128.12 | 443 | 52.46.128.12 | 10.10.0.184 | 42390 | 10.10.0.184 | 6 | - | 1622653883 | 1622653891 |
| 42 | eni-066f44726b4e011ce | egress | ACCEPT | 10.10.0.184 | 443 | 52.94.233.15 | 10.10.1.194 | 45514 | 10.10.1.194 | 6 | 1 | 1622653898 | 1622653898 |
| 43 | eni-066f44726b4e011ce | ingress | ACCEPT | 170.106.75.1 | 16949 | 170.106.75.1 | 10.10.0.184 | 445 | 10.10.0.184 | 6 | - | 1622653898 | 1622653898 |
| 44 | eni-066f44726b4e011ce | ingress | ACCEPT | 52.94.233.15 | 443 | 52.94.233.15 | 10.10.0.184 | 8360 | 10.10.0.184 | 6 | - | 1622653907 | 1622653920 |

- Download and decompress
  - Analyze with local applications.

# Flow Logs in S3 – Viewing Options

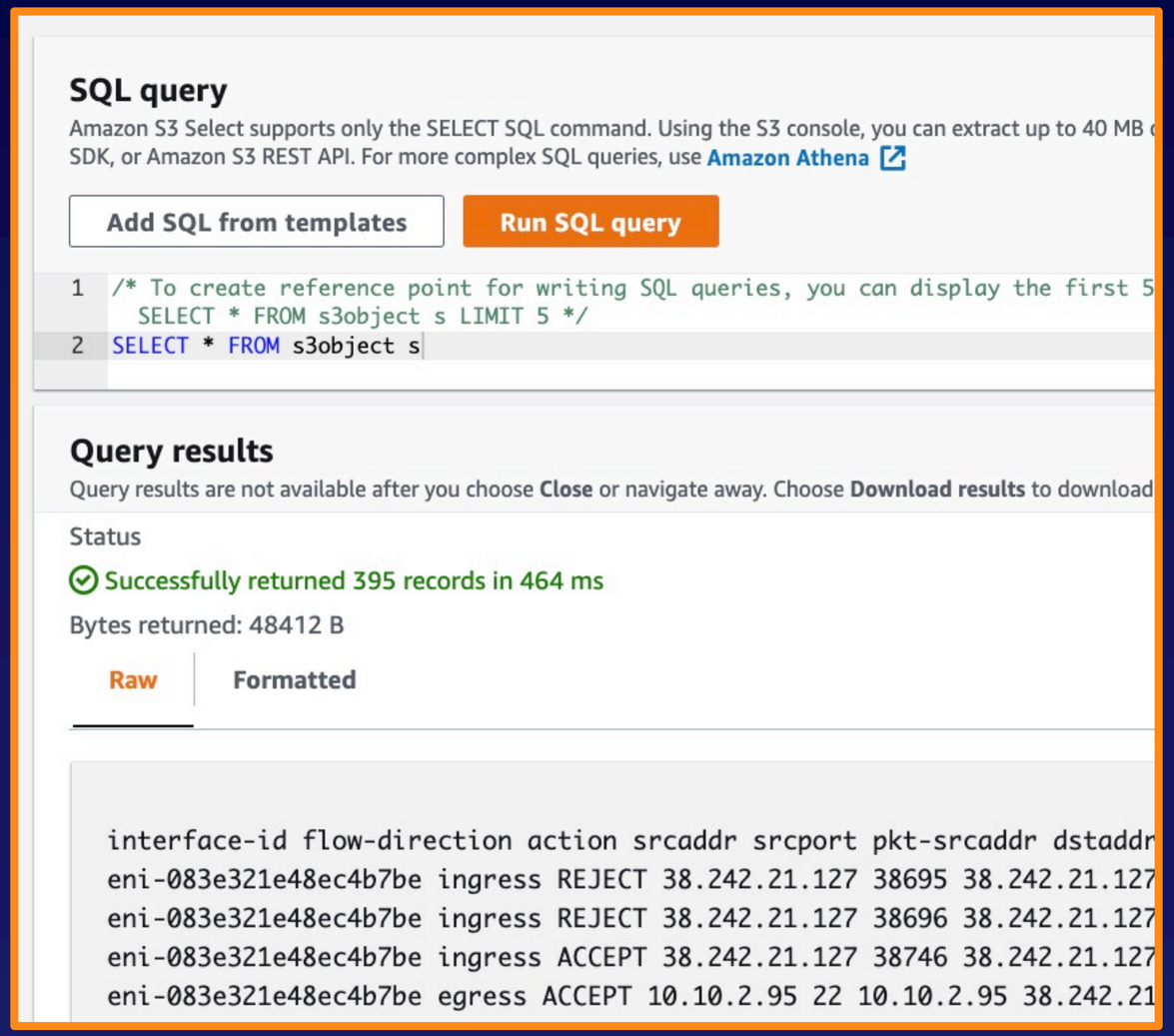





- Download and decompress
  - Analyze with local applications.
- Query with S3 Select

# Flow Logs in S3 – Viewing Options






- Download and decompress
  - Analyze with local applications.
- Query with S3 Select

# Flow Logs in S3 – Viewing Options

A CLOUD GURU

```
1  /* To create reference point for writing S
2  SELECT _1, _2, _3 FROM s3object s
3
```

```
interface-id    flow-direction  action
eni-083e321e48ec4b7be   ingress REJECT
eni-083e321e48ec4b7be   ingress REJECT
eni-083e321e48ec4b7be   ingress ACCEPT
eni-083e321e48ec4b7be   egress  ACCEPT
eni-083e321e48ec4b7be   ingress REJECT
eni-083e321e48ec4b7be   ingress REJECT
eni-083e321e48ec4b7be   ingress ACCEPT
```

Raw | Formatted

```
interface-id flow-direction action srcaddr srcport pkt-srcaddr dstaddr
eni-083e321e48ec4b7be ingress REJECT 38.242.21.127 38695 38.242.21.127
eni-083e321e48ec4b7be ingress REJECT 38.242.21.127 38696 38.242.21.127
eni-083e321e48ec4b7be ingress ACCEPT 38.242.21.127 38746 38.242.21.127
eni-083e321e48ec4b7be egress ACCEPT 10.10.2.95 22 10.10.2.95 38.242.21
```

- Download and decompress
  - Analyze with local applications.
- Query with S3 Select

# Flow Logs in S3 – Viewing Options

A CLOUD GURU

```
1  /* To create reference point for writing S
2  SELECT _1, _2, _3 FROM s3object s
3
```

```
interface-id    flow-direction  action
eni-083e321e48ec4b7be   ingress REJECT
eni-083e321e48ec4b7be   ingress REJECT
eni-083e321e48ec4b7be   ingress REJECT
```

```
1  /* To create reference point for writing SQL queries,
2  SELECT _1, _2, _3 FROM s3object s where _3 = 'REJECT'
3
```

```
eni-083e321e48ec4b7be   ingress REJECT
eni-083e321e48ec4b7be   ingress REJECT
eni-083e321e48ec4b7be   ingress REJECT
eni-083e321e48ec4b7be   ingress REJECT
eni-083e321e48ec4b7be   ingress REJECT
eni-083e321e48ec4b7be   ingress REJECT
eni-083e321e48ec4b7be   ingress REJECT
eni-083e321e48ec4b7be   ingress REJECT
eni-083e321e48ec4b7be   ingress REJECT
```

- Download and decompress
  - Analyze with local applications.
- Query with S3 Select
  - Queries limited to selected log file

# Flow Logs in S3 – Viewing Options



- Download and decompress
  - Analyze with local applications.
- Query with S3 Select
  - Queries limited to selected log file
- AWS Athena

# Flow Logs in S3 – Viewing Options

A CLOUD GURU

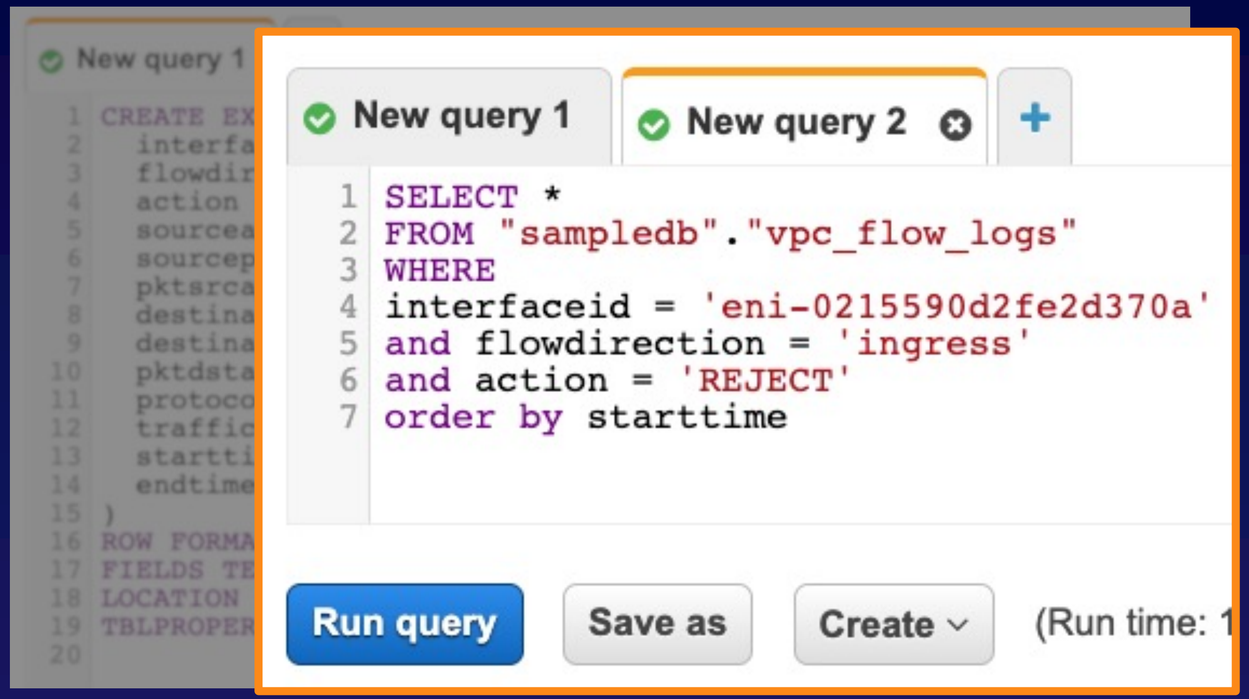
New query 1

```
CREATE EXTERNAL TABLE IF NOT EXISTS vpc_flow_logs (
  interfaceid string,
  flowdirection string,
  action string,
  sourceaddress string,
  sourceport int,
  pktsrcaddr string,
  destinationaddress string,
  destinationport int,
  pktdstaddr string,
  protocol int,
  trafficpath string,
  starttime int,
  endtime int
)
ROW FORMAT DELIMITED
FIELDS TERMINATED BY ' '
LOCATION 's3://advnetspec-vpcflowlogsdemo/AWSLogs/                /
TBLPROPERTIES ("skip.header.line.count"="1");
```

- Download and decompress
  - Analyze with local applications.
- Query with S3 Select
  - Queries limited to selected log file
- AWS Athena
  - Create table linked to S3 flow log path

# Flow Logs in S3 – Viewing Options






Results

| | interfaceid | flowdirection | action | sourceaddress | sourceport | pktsrcaddr | destinationaddress | destinationport |
|---|---|---|---|---|---|---|---|---|
| 1 | eni-0215590d2fe2d370a | ingress | REJECT | 162.142.125.158 | 17812 | 162.142.125.158 | 10.10.1.194 | 4444 |
| 2 | eni-0215590d2fe2d370a | ingress | REJECT | 45.134.26.33 | 51605 | 45.134.26.33 | 10.10.1.194 | 46043 |
| 3 | eni-0215590d2fe2d370a | ingress | REJECT | 162.142.125.144 | 44085 | 162.142.125.144 | 10.10.1.194 | 12084 |
| 4 | eni-0215590d2fe2d370a | ingress | REJECT | 45.134.26.42 | 51804 | 45.134.26.42 | 10.10.1.194 | 46077 |
| 5 | eni-0215590d2fe2d370a | ingress | REJECT | 45.134.26.41 | 51781 | 45.134.26.41 | 10.10.1.194 | 25024 |
| 6 | eni-0215590d2fe2d370a | ingress | REJECT | 129.82.138.44 | 0 | 129.82.138.44 | 10.10.1.194 | 0 |
| 7 | eni-0215590d2fe2d370a | ingress | REJECT | 118.178.121.209 | 53950 | 118.178.121.209 | 10.10.1.194 | 2375 |
| 8 | eni-0215590d2fe2d370a | ingress | REJECT | 180.76.98.133 | 53683 | 180.76.98.133 | 10.10.1.194 | 2376 |
| 9 | eni-0215590d2fe2d370a | ingress | REJECT | 54.174.231.103 | 0 | 54.174.231.103 | 10.10.1.194 | 0 |
| 10 | eni-0215590d2fe2d370a | ingress | REJECT | 162.142.125.147 | 57554 | 162.142.125.147 | 10.10.1.194 | 9170 |

- Download and decompress
  - Analyze with local applications.
- Query with S3 Select
  - Queries limited to selected log file
- AWS Athena
  - Create table linked to S3 flow log path
  - Queries read all applicable log files

# Other Options



- CloudWatch Insights
  - Generates graphs based on log data

- Amazon Redshift
  - Query larger data sets
  - Query data in S3

- Kinesis
  - Move data to other storage or analysis tools

# Fast Takeaways



Log viewing methods vary by storage destination.

Many different analysis tools and services are available.

All flow log activities incur charges.