

# Viewing VPC Flow Logs



**Steven Moran**  
TRAINING ARCHITECT

- CloudWatch log group



- S3 bucket



# Flow Logs in CloudWatch

CloudWatch > Log groups > AdvNetSpec\_FlowLogs

AdvNetSpec\_FlowLogs Actions ▼ View in Logs Insights Search log group

► Log group details

**Log streams** | Metric filters | Subscription filters | Contributor Insights | Tags

Log streams (4) ↻ Delete Create log stream Search all

🔍 Filter log streams or try prefix search < 1 > ⚙️

| <input type="checkbox"/> | Log stream ▼                              | Last event time ▼               |
|--------------------------|---|---------------------------------|
| <input type="checkbox"/> | <a href="#">eni-066f44726b4e011ce-all</a> | 2021-06-02 13:19:35 (UTC-07:00) |
| <input type="checkbox"/> | <a href="#">eni-083e321e48ec4b7be-all</a> | 2021-06-02 13:18:56 (UTC-07:00) |
| <input type="checkbox"/> | <a href="#">eni-0df5765a00e3c9e41-all</a> | 2021-06-02 13:15:42 (UTC-07:00) |
| <input type="checkbox"/> | <a href="#">eni-0215590d2fe2d370a-all</a> | 2021-06-02 13:05:02 (UTC-07:00) |

- One log stream per ENI

# Flow Logs in CloudWatch

CloudWatch > Log groups > AdvNetSpec\_FlowLogs

AdvNetSpec\_FlowLogs

Actions View in Logs Insights Search log group

Log group details

Log streams Metric filters Subscription filters Contributor Insights Tags

CloudWatch > Log groups > AdvNetSpec\_FlowLogs > eni-0215590d2fe2d370a-all

**Log events**  
You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

View as text  Actions

Clear 1m 30m 1h 12h Custom

| Timestamp   | Message   |
|---|---|
| There are older events to load. <a href="#">Load more</a> . |   |
| 2021-06-02T13:23:04.000-07:00                               | eni-0215590d2fe2d370a ingress REJECT 167.248.133.79 23346 167.248.133.79 10.10.1.194 9264 10.10.1.194 ... |
| 2021-06-02T13:24:05.000-07:00                               | eni-0215590d2fe2d370a ingress REJECT 54.174.231.103 0 54.174.231.103 10.10.1.194 0 10.10.1.194 1 - 162... |
| 2021-06-02T13:24:05.000-07:00                               | eni-0215590d2fe2d370a ingress ACCEPT 52.46.138.63 443 52.46.138.63 10.10.1.194 44382 10.10.1.194 6 - 1... |
| 2021-06-02T13:24:05.000-07:00                               | eni-0215590d2fe2d370a egress ACCEPT 10.10.1.194 44382 10.10.1.194 52.46.138.63 443 52.46.138.63 6 1 16... |
| 2021-06-02T13:24:05.000-07:00                               | eni-0215590d2fe2d370a ingress REJECT 207.180.215.210 49235 207.180.215.210 10.10.1.194 3393 10.10.1.19... |
| 2021-06-02T13:24:05.000-07:00                               | eni-0215590d2fe2d370a ingress ACCEPT 10.10.2.95 3360 10.10.2.95 10.10.1.194 80 10.10.1.194 6 - 1622665... |
| 2021-06-02T13:24:05.000-07:00                               | eni-0215590d2fe2d370a egress ACCEPT 10.10.1.194 80 10.10.1.194 10.10.2.95 3360 10.10.2.95 6 1 16226654... |
| 2021-06-02T13:24:05.000-07:00                               | eni-0215590d2fe2d370a ingress ACCEPT 52.46.138.63 443 52.46.138.63 10.10.1.194 44384 10.10.1.194 6 - 1... |
| 2021-06-02T13:24:05.000-07:00                               | eni-0215590d2fe2d370a egress ACCEPT 10.10.1.194 44384 10.10.1.194 52.46.138.63 443 52.46.138.63 6 1 16... |
| 2021-06-02T13:24:05.000-07:00                               | eni-0215590d2fe2d370a ingress REJECT 51.195.166.20 5060 51.195.166.20 10.10.1.194 8080 10.10.1.194 17 ... |
| 2021-06-02T13:24:05.000-07:00                               | eni-0215590d2fe2d370a ingress REJECT 162.142.125.144 31252 162.142.125.144 10.10.1.194 12435 10.10.1.1... |

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

# Flow Logs in CloudWatch

CloudWatch > Log groups > AdvNetSpec\_FlowLogs

AdvNetSpec\_FlowLogs Actions View in Logs Insights Search log group

▶ Log group details

Log streams Metric filters Subscription filters Contributor Insights Tags

CloudWatch > Log groups > AdvNetSpec\_FlowLogs > eni-0215590d2fe2d370a-all

**Log events**  
You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

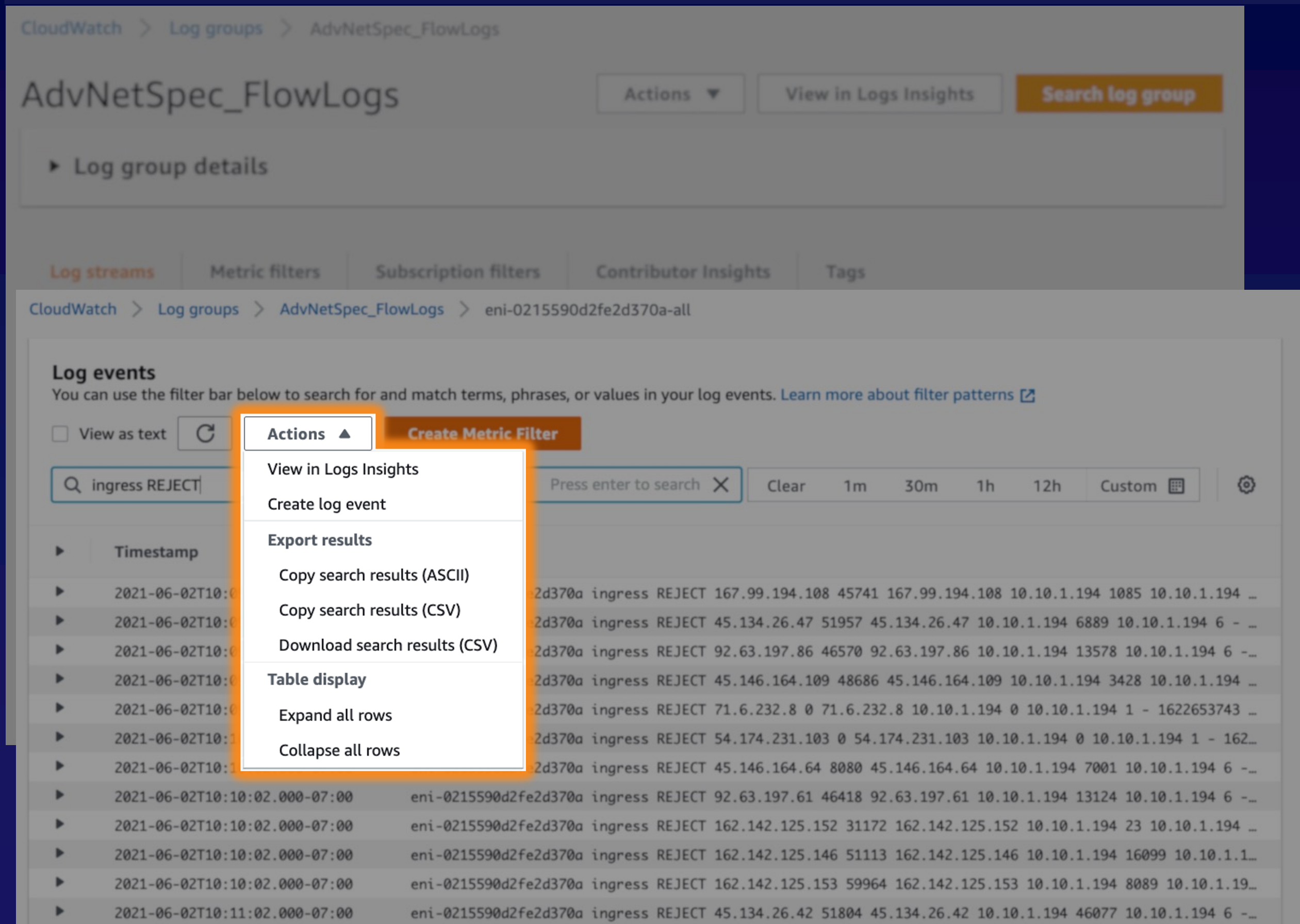
View as text ↻ Actions Create Metric Filter

Press enter to search ✕ Clear 1m 30m 1h 12h Custom ⌵ ⚙️

| ▶ | Timestamp                     | Message  |
|---|-------------------------------|--|
| ▶ | 2021-06-02T10:09:03.000-07:00 | eni-0215590d2fe2d370a ingress REJECT 167.99.194.108 45741 167.99.194.108 10.10.1.194 1085 10.10.1.194 ...  |
| ▶ | 2021-06-02T10:09:03.000-07:00 | eni-0215590d2fe2d370a ingress REJECT 45.134.26.47 51957 45.134.26.47 10.10.1.194 6889 10.10.1.194 6 - ...  |
| ▶ | 2021-06-02T10:09:03.000-07:00 | eni-0215590d2fe2d370a ingress REJECT 92.63.197.86 46570 92.63.197.86 10.10.1.194 13578 10.10.1.194 6 - ... |
| ▶ | 2021-06-02T10:09:03.000-07:00 | eni-0215590d2fe2d370a ingress REJECT 45.146.164.109 48686 45.146.164.109 10.10.1.194 3428 10.10.1.194 ...  |
| ▶ | 2021-06-02T10:09:03.000-07:00 | eni-0215590d2fe2d370a ingress REJECT 71.6.232.8 0 71.6.232.8 10.10.1.194 0 10.10.1.194 1 - 1622653743 ...  |
| ▶ | 2021-06-02T10:10:02.000-07:00 | eni-0215590d2fe2d370a ingress REJECT 54.174.231.103 0 54.174.231.103 10.10.1.194 0 10.10.1.194 1 - 162...  |
| ▶ | 2021-06-02T10:10:02.000-07:00 | eni-0215590d2fe2d370a ingress REJECT 45.146.164.64 8080 45.146.164.64 10.10.1.194 7001 10.10.1.194 6 - ... |
| ▶ | 2021-06-02T10:10:02.000-07:00 | eni-0215590d2fe2d370a ingress REJECT 92.63.197.61 46418 92.63.197.61 10.10.1.194 13124 10.10.1.194 6 - ... |
| ▶ | 2021-06-02T10:10:02.000-07:00 | eni-0215590d2fe2d370a ingress REJECT 162.142.125.152 31172 162.142.125.152 10.10.1.194 23 10.10.1.194 ...  |
| ▶ | 2021-06-02T10:10:02.000-07:00 | eni-0215590d2fe2d370a ingress REJECT 162.142.125.146 51113 162.142.125.146 10.10.1.194 16099 10.10.1.1...  |
| ▶ | 2021-06-02T10:10:02.000-07:00 | eni-0215590d2fe2d370a ingress REJECT 162.142.125.153 59964 162.142.125.153 10.10.1.194 8089 10.10.1.19...  |
| ▶ | 2021-06-02T10:11:02.000-07:00 | eni-0215590d2fe2d370a ingress REJECT 45.134.26.42 51804 45.134.26.42 10.10.1.194 46077 10.10.1.194 6 - ... |

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

# Flow Logs in CloudWatch



CloudWatch > Log groups > AdvNetSpec\_FlowLogs

AdvNetSpec\_FlowLogs

Log group details

Log streams | Metric filters | Subscription filters | Contributor Insights | Tags

CloudWatch > Log groups > AdvNetSpec\_FlowLogs > eni-0215590d2fe2d370a-all

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

View as text

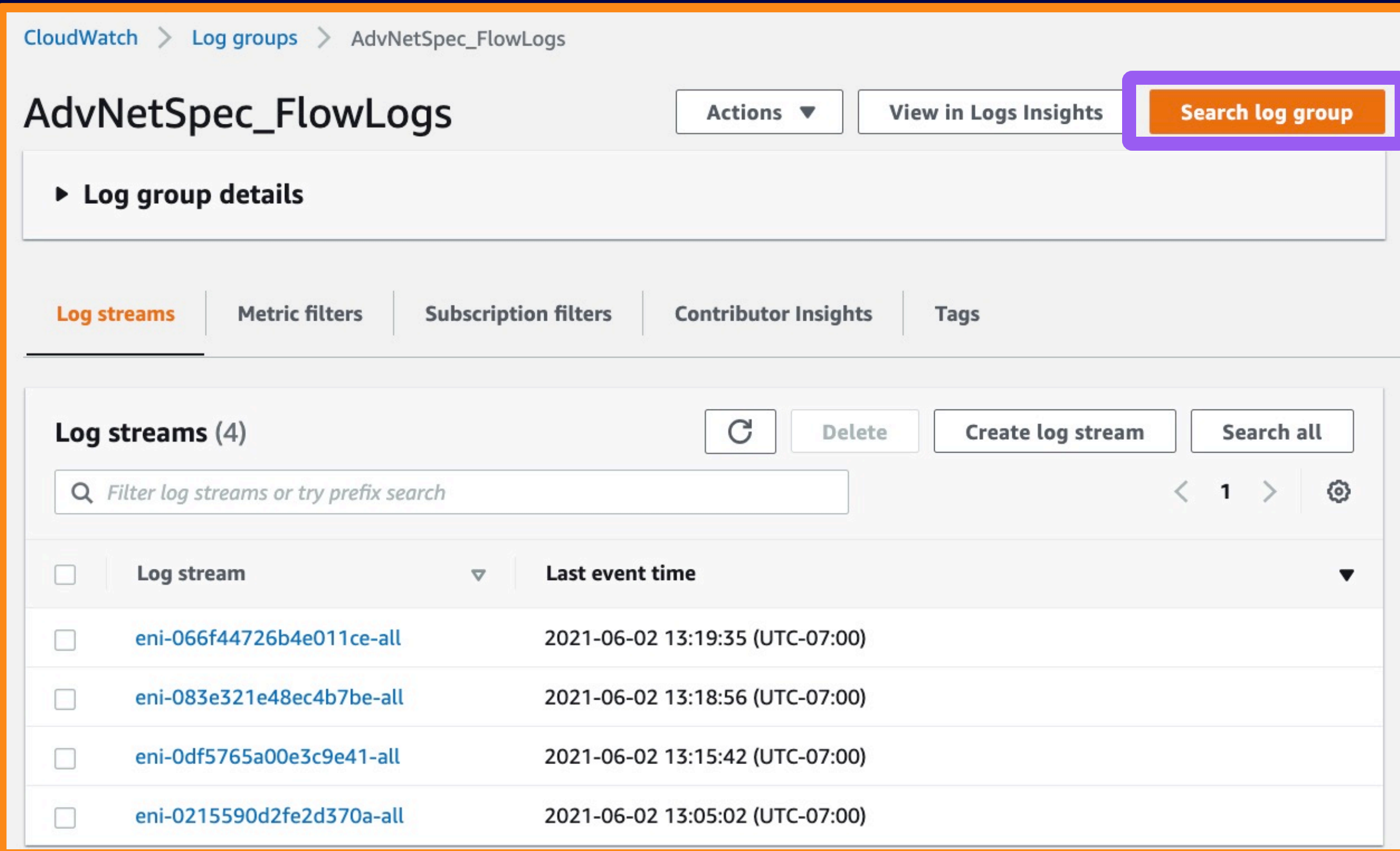
**Actions**

- View in Logs Insights
- Create log event
- Export results
  - Copy search results (ASCII)
  - Copy search results (CSV)
  - Download search results (CSV)
- Table display
  - Expand all rows
  - Collapse all rows

| Timestamp                     | Log event  |
|-------------------------------|--|
| 2021-06-02T10:00:00.000-07:00 | eni-0215590d2fe2d370a ingress REJECT 167.99.194.108 45741 167.99.194.108 10.10.1.194 1085 10.10.1.194 ...  |
| 2021-06-02T10:00:00.000-07:00 | eni-0215590d2fe2d370a ingress REJECT 45.134.26.47 51957 45.134.26.47 10.10.1.194 6889 10.10.1.194 6 - ...  |
| 2021-06-02T10:00:00.000-07:00 | eni-0215590d2fe2d370a ingress REJECT 92.63.197.86 46570 92.63.197.86 10.10.1.194 13578 10.10.1.194 6 - ... |
| 2021-06-02T10:00:00.000-07:00 | eni-0215590d2fe2d370a ingress REJECT 45.146.164.109 48686 45.146.164.109 10.10.1.194 3428 10.10.1.194 ...  |
| 2021-06-02T10:00:00.000-07:00 | eni-0215590d2fe2d370a ingress REJECT 71.6.232.8 0 71.6.232.8 10.10.1.194 0 10.10.1.194 1 - 1622653743 ...  |
| 2021-06-02T10:00:00.000-07:00 | eni-0215590d2fe2d370a ingress REJECT 54.174.231.103 0 54.174.231.103 10.10.1.194 0 10.10.1.194 1 - 162...  |
| 2021-06-02T10:00:00.000-07:00 | eni-0215590d2fe2d370a ingress REJECT 45.146.164.64 8080 45.146.164.64 10.10.1.194 7001 10.10.1.194 6 - ... |
| 2021-06-02T10:10:02.000-07:00 | eni-0215590d2fe2d370a ingress REJECT 92.63.197.61 46418 92.63.197.61 10.10.1.194 13124 10.10.1.194 6 - ... |
| 2021-06-02T10:10:02.000-07:00 | eni-0215590d2fe2d370a ingress REJECT 162.142.125.152 31172 162.142.125.152 10.10.1.194 23 10.10.1.194 ...  |
| 2021-06-02T10:10:02.000-07:00 | eni-0215590d2fe2d370a ingress REJECT 162.142.125.146 51113 162.142.125.146 10.10.1.194 16099 10.10.1.1...  |
| 2021-06-02T10:10:02.000-07:00 | eni-0215590d2fe2d370a ingress REJECT 162.142.125.153 59964 162.142.125.153 10.10.1.194 8089 10.10.1.19...  |
| 2021-06-02T10:11:02.000-07:00 | eni-0215590d2fe2d370a ingress REJECT 45.134.26.42 51804 45.134.26.42 10.10.1.194 46077 10.10.1.194 6 - ... |

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

# Flow Logs in CloudWatch



CloudWatch > Log groups > AdvNetSpec\_FlowLogs

AdvNetSpec\_FlowLogs

Actions View in Logs Insights **Search log group**

► Log group details

Log streams Metric filters Subscription filters Contributor Insights Tags

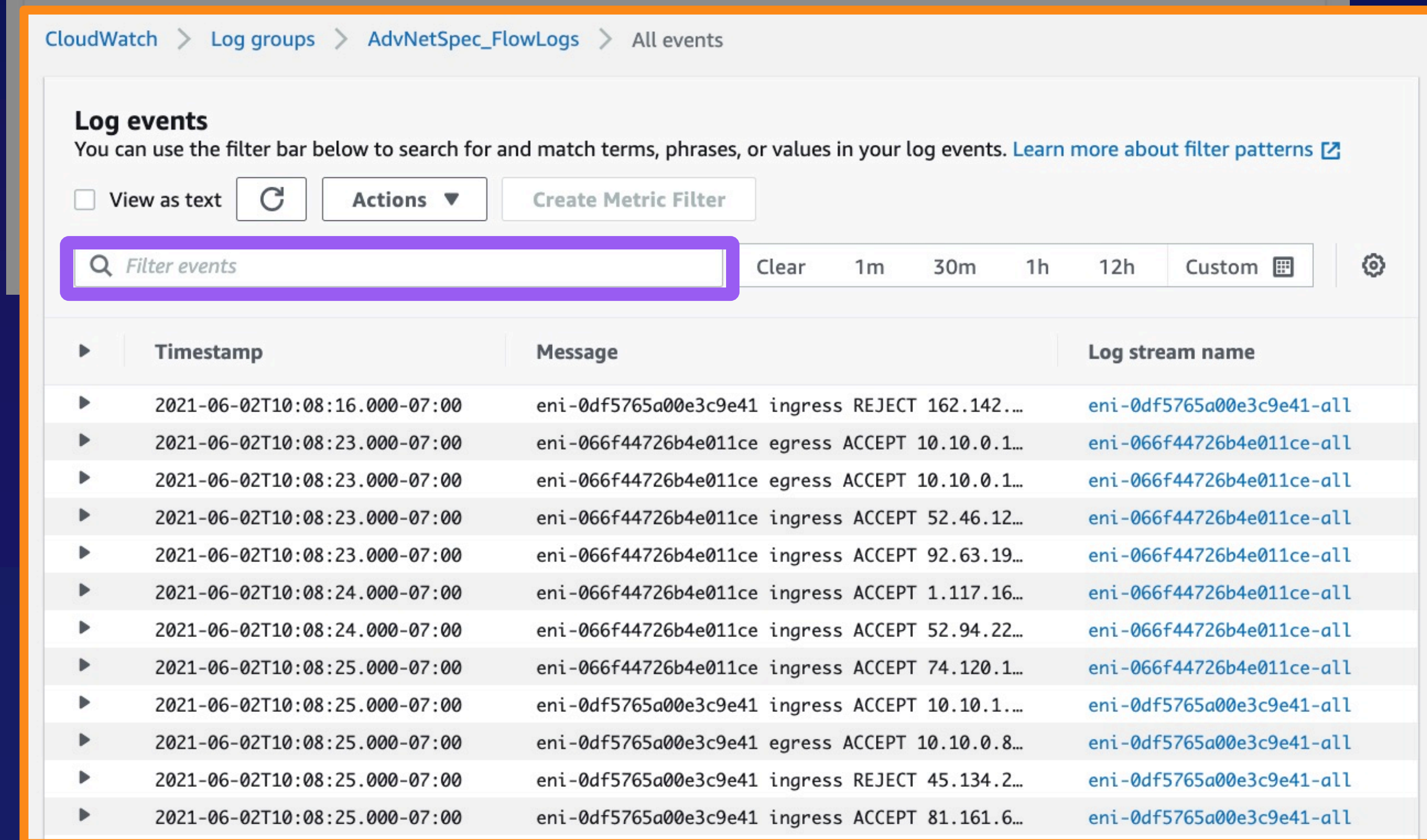
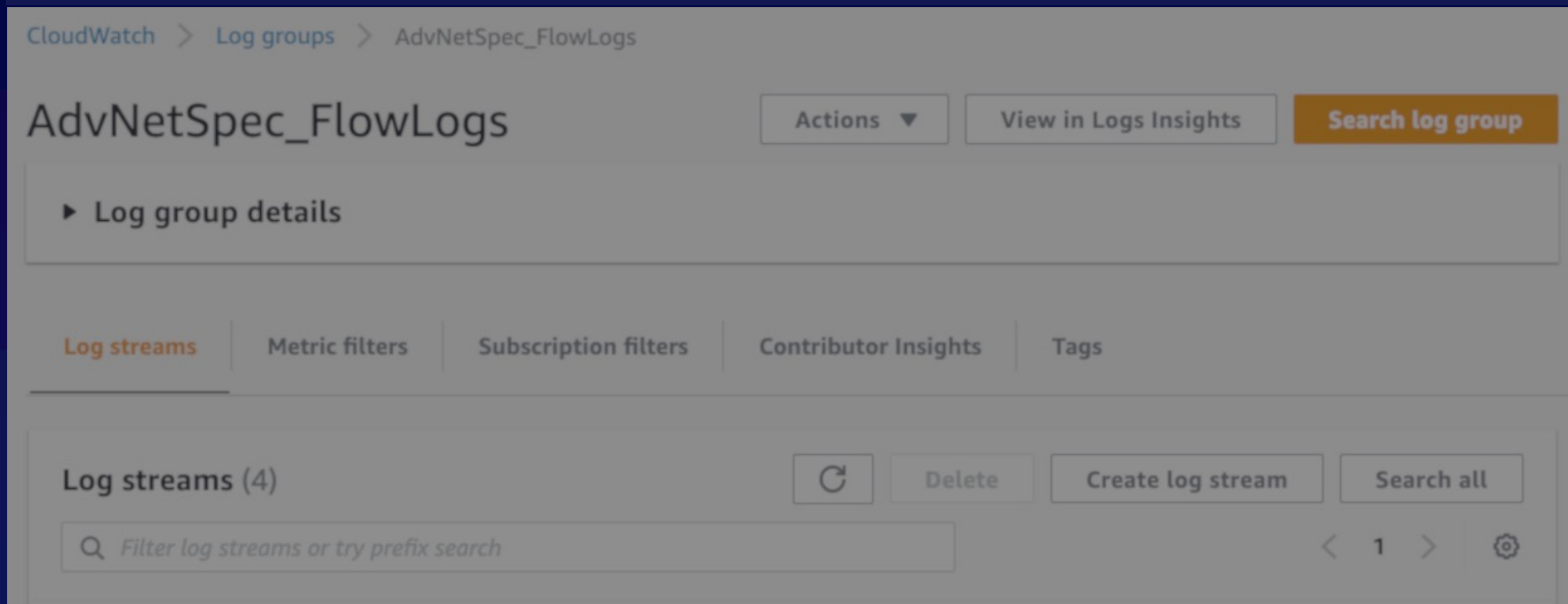
Log streams (4)

Filter log streams or try prefix search

| Log stream                | Last event time                 |
|---------------------------|---------------------------------|
| eni-066f44726b4e011ce-all | 2021-06-02 13:19:35 (UTC-07:00) |
| eni-083e321e48ec4b7be-all | 2021-06-02 13:18:56 (UTC-07:00) |
| eni-0df5765a00e3c9e41-all | 2021-06-02 13:15:42 (UTC-07:00) |
| eni-0215590d2fe2d370a-all | 2021-06-02 13:05:02 (UTC-07:00) |

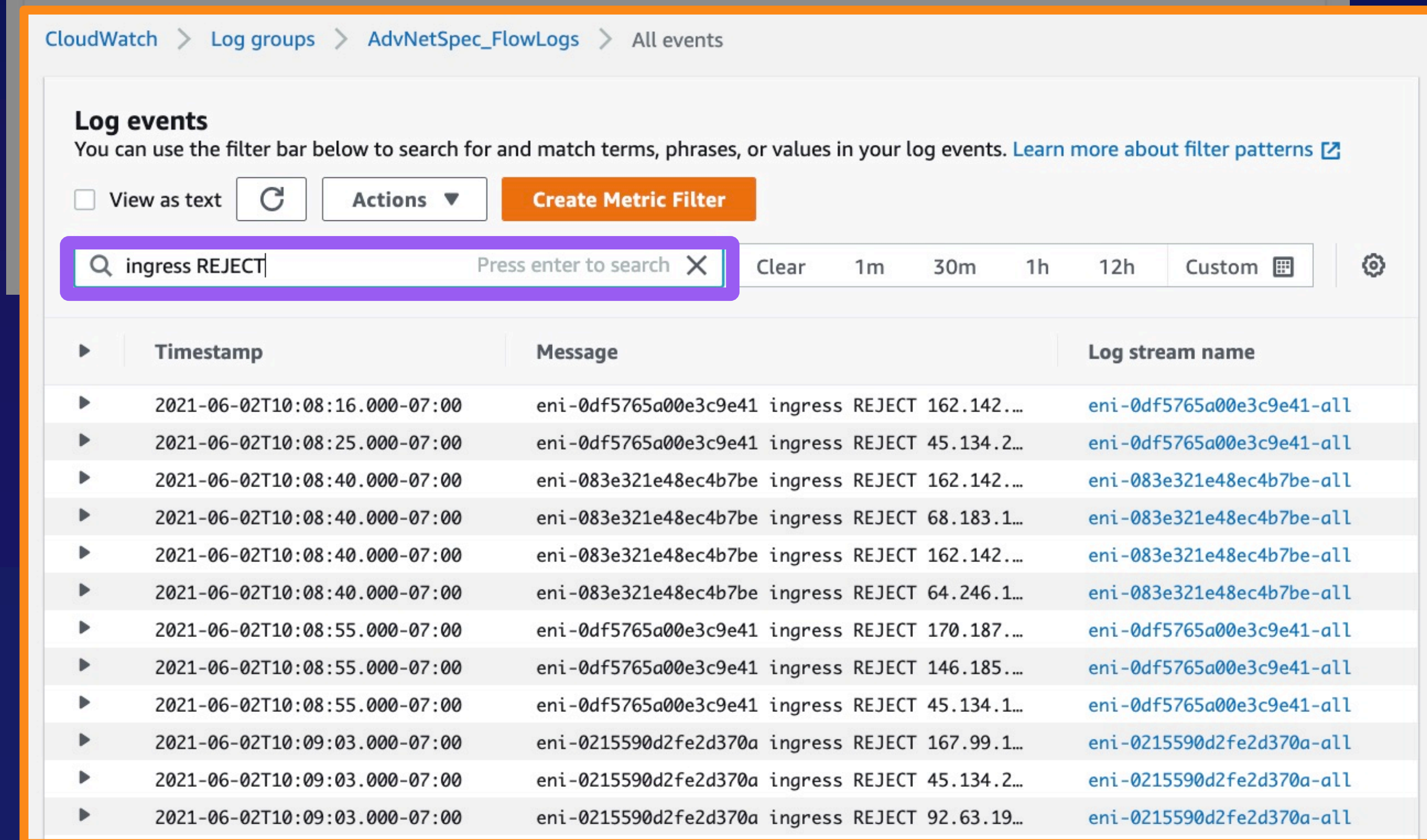
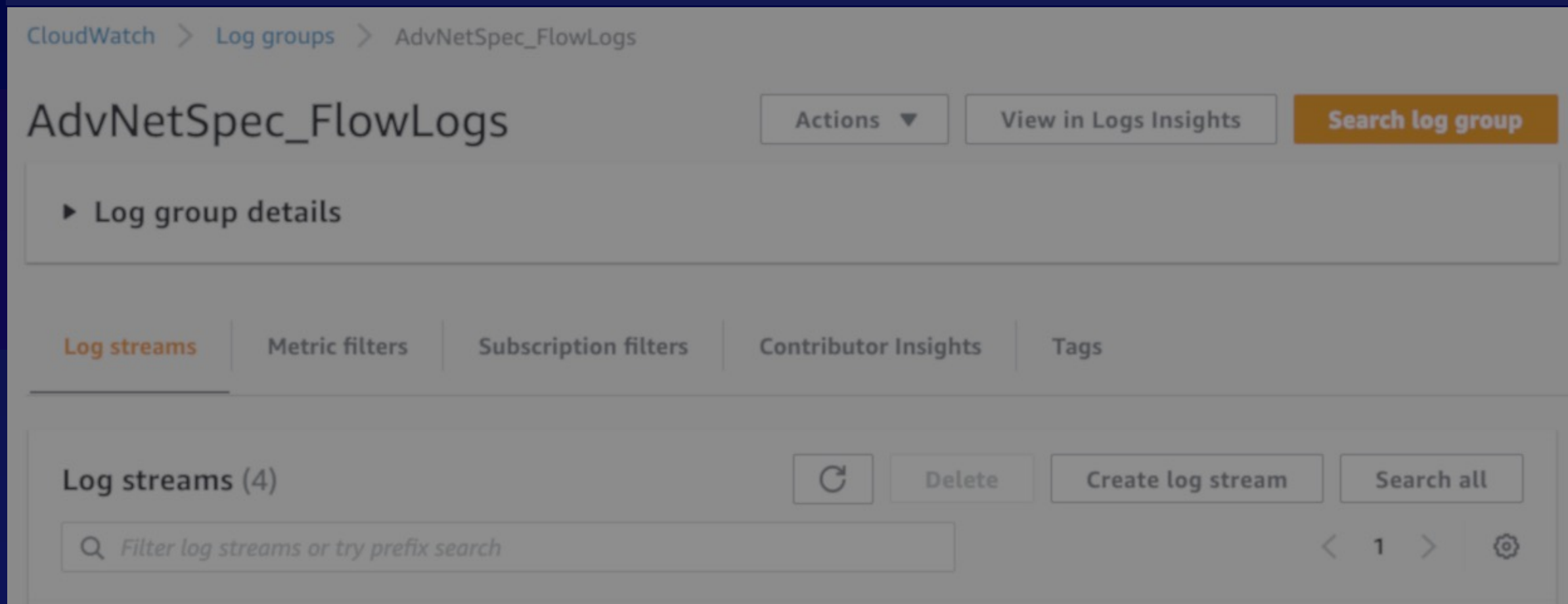
- One log stream per ENI
- Records may be filtered and exported.
  - Per-log stream
  - All streams in log group

# 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



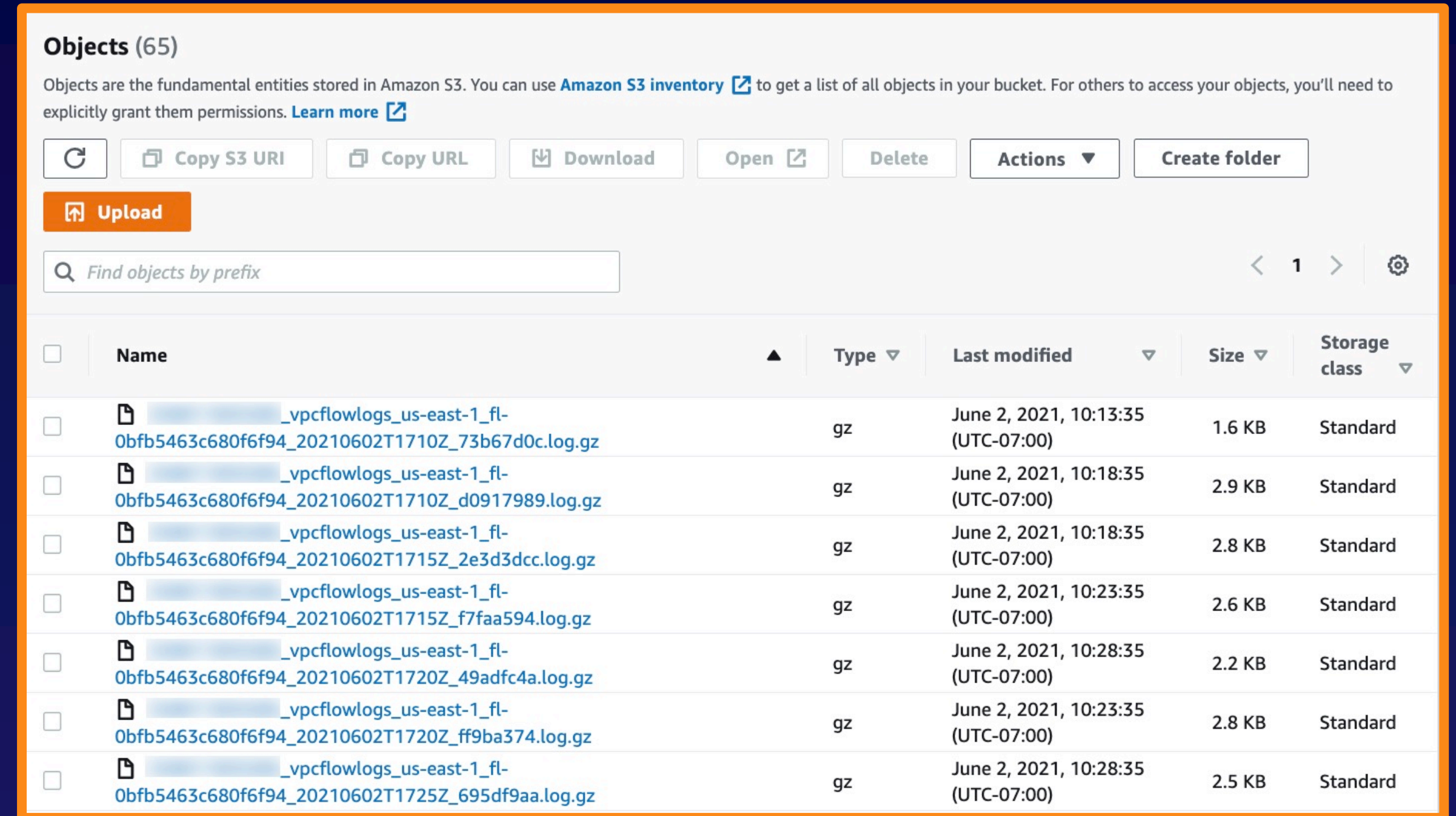
- One log stream per ENI
- Records may be filtered and exported.
  - Per-log stream
  - All streams in log group

# 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`



**Objects (65)**

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

| <input type="checkbox"/> | Name   | Type | Last modified                      | Size   | Storage class |
|--------------------------|--|------|------------------------------------|--------|---------------|
| <input type="checkbox"/> | <a href="#">_vpcflowlogs_us-east-1_fl-0bfb5463c680f6f94_20210602T1710Z_73b67d0c.log.gz</a> | gz   | June 2, 2021, 10:13:35 (UTC-07:00) | 1.6 KB | Standard      |
| <input type="checkbox"/> | <a href="#">_vpcflowlogs_us-east-1_fl-0bfb5463c680f6f94_20210602T1710Z_d0917989.log.gz</a> | gz   | June 2, 2021, 10:18:35 (UTC-07:00) | 2.9 KB | Standard      |
| <input type="checkbox"/> | <a href="#">_vpcflowlogs_us-east-1_fl-0bfb5463c680f6f94_20210602T1715Z_2e3d3dcc.log.gz</a> | gz   | June 2, 2021, 10:18:35 (UTC-07:00) | 2.8 KB | Standard      |
| <input type="checkbox"/> | <a href="#">_vpcflowlogs_us-east-1_fl-0bfb5463c680f6f94_20210602T1715Z_f7faa594.log.gz</a> | gz   | June 2, 2021, 10:23:35 (UTC-07:00) | 2.6 KB | Standard      |
| <input type="checkbox"/> | <a href="#">_vpcflowlogs_us-east-1_fl-0bfb5463c680f6f94_20210602T1720Z_49adfc4a.log.gz</a> | gz   | June 2, 2021, 10:28:35 (UTC-07:00) | 2.2 KB | Standard      |
| <input type="checkbox"/> | <a href="#">_vpcflowlogs_us-east-1_fl-0bfb5463c680f6f94_20210602T1720Z_ff9ba374.log.gz</a> | gz   | June 2, 2021, 10:23:35 (UTC-07:00) | 2.8 KB | Standard      |
| <input type="checkbox"/> | <a href="#">_vpcflowlogs_us-east-1_fl-0bfb5463c680f6f94_20210602T1725Z_695df9aa.log.gz</a> | gz   | June 2, 2021, 10:28:35 (UTC-07:00) | 2.5 KB | Standard      |

# Flow Logs in S3 – Viewing Options

```

1 |interface-id flow-direction 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 185.156.73.67 48370 185.156.73.67 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 52.119.197.249 10.10.1.194 34944 10.10.1.194 6 1 1622653875 1622653876
11 |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
12 |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
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 66.207.226.14 17 - 1622653838 1622653841
17 |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
18 |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
19 |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
20 |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

```

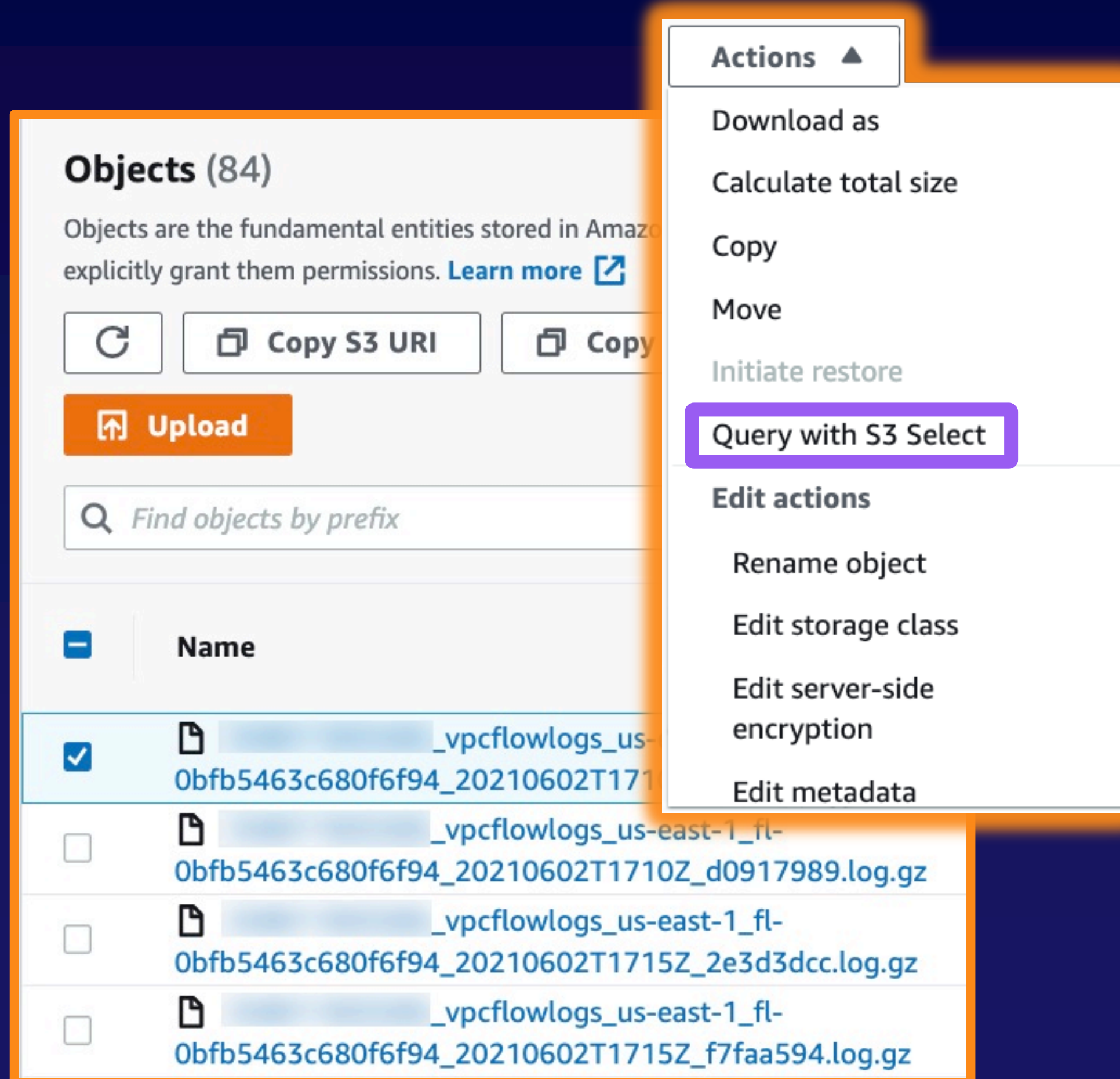
1 interface-id flow-direction action srcaddr srcport pkt-srcaddr dstaddr dstport pkt-dstaddr protocol traffic-path start end
2 eni-0df5765a00e3c9e41 ingress ACCEPT 10.10.1.194 80 10.10.1.194 10.10.0.81 24088 10.10.0.81 6 - 1622653852 1622653857
3 eni-0df5765a00e3c9e41 egress ACCEPT 10.10.0.81 24088 10.10.0.81 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 185.156.73.67 48370 185.156.73.67 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 52.119.197.249 10.10.1.194 34944 10.10.1.194 6 1 1622653875 1622653876
11 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
12 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
13 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

```





- Download and decompress
- Analyze with local applications.

|    | A                     | B              | C      | D             | E       | F             | G            | H       | I            | J        | K            | L          | M          |
|----|-----------------------|----------------|--------|---------------|---------|---------------|--------------|---------|--------------|----------|--------------|------------|------------|
| 1  | interface-id          | flow-direction | 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 | 185.156.73.67 | 48370   | 185.156.73.67 | 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 |

# Flow Logs in S3 – Viewing Options



**Objects (84)**  
Objects are the fundamental entities stored in Amazon S3. You can explicitly grant them permissions. [Learn more](#)

| <input type="checkbox"/>            | Name   |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> |  <a href="#">[redacted]_vpcflowlogs_us-east-1_fl-0bfb5463c680f6f94_20210602T1710Z_d0917989.log.gz</a> |
| <input type="checkbox"/>            |  <a href="#">[redacted]_vpcflowlogs_us-east-1_fl-0bfb5463c680f6f94_20210602T1710Z_d0917989.log.gz</a> |
| <input type="checkbox"/>            |  <a href="#">[redacted]_vpcflowlogs_us-east-1_fl-0bfb5463c680f6f94_20210602T1715Z_2e3d3dcc.log.gz</a> |
| <input type="checkbox"/>            |  <a href="#">[redacted]_vpcflowlogs_us-east-1_fl-0bfb5463c680f6f94_20210602T1715Z_f7faa594.log.gz</a> |

**Actions** ▲

- Download as
- Calculate total size
- Copy
- Move
- Initiate restore
- Query with S3 Select**
- Edit actions**
- Rename object
- Edit storage class
- Edit server-side encryption
- Edit metadata

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

# Flow Logs in S3 – Viewing Options

## SQL query

Amazon S3 Select supports only the SELECT SQL command. Using the S3 console, you can extract up to 40 MB of data using the AWS CLI, AWS SDK, or Amazon S3 REST API. For more complex SQL queries, use [Amazon Athena](#).

Add SQL from templates

Run SQL query

```
1 /* To create reference point for writing SQL queries, you can display the first 5
   SELECT * FROM s3object s LIMIT 5 */
2 SELECT * FROM s3object s
```

## Query results

Query results are not available after you choose **Close** or navigate away. Choose **Download results** to download results.

Status

✔ Successfully returned 395 records in 464 ms

Bytes returned: 48412 B

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

```
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

```
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
```

```
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
```

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

# Flow Logs in S3 – Viewing Options



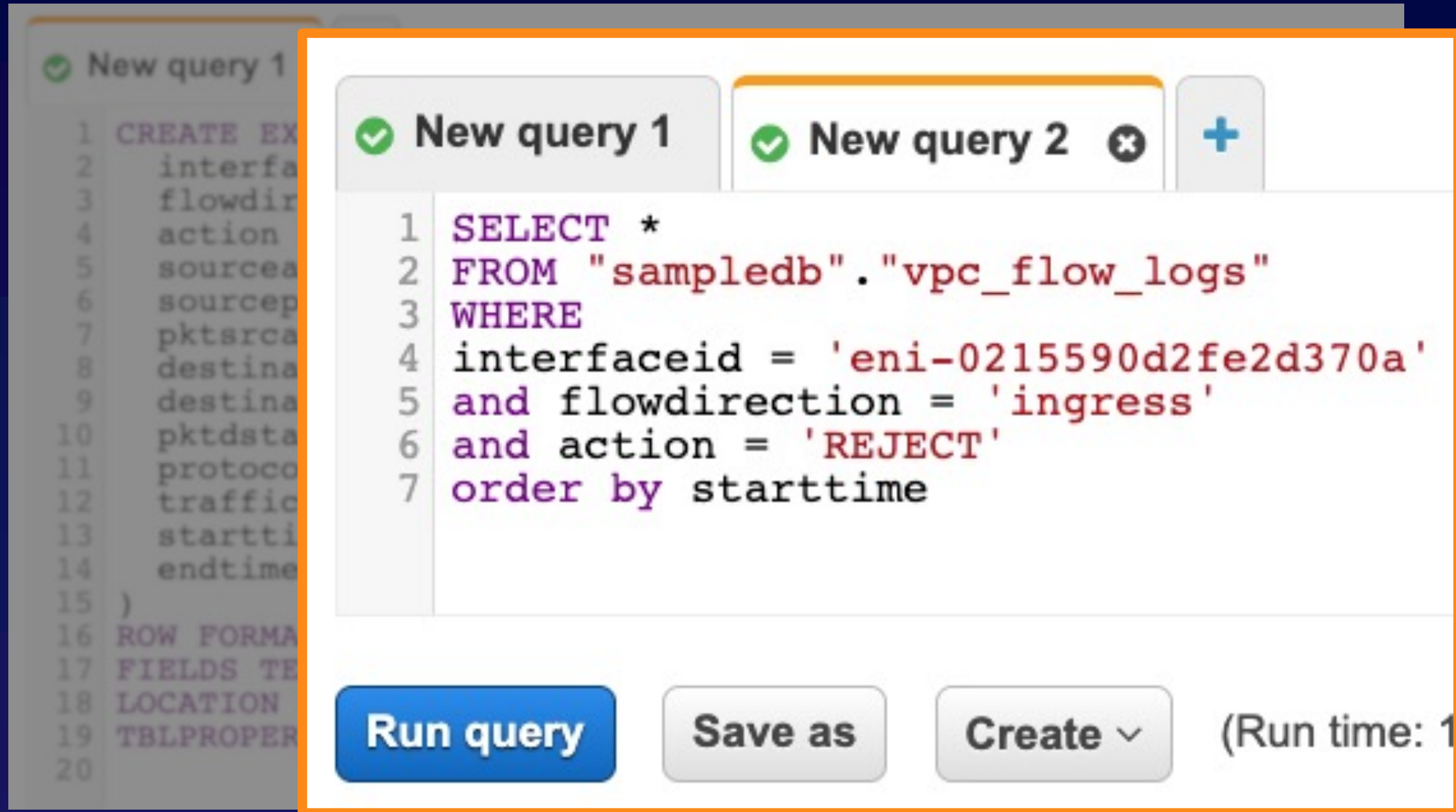
- Download and decompress
  - Analyze with local applications.
- Query with S3 Select
  - Queries limited to selected log file
- AWS Athena

# Flow Logs in S3 – Viewing Options

```
✓ New query 1 +
1 CREATE EXTERNAL TABLE IF NOT EXISTS vpc_flow_logs (
2   interfaceid string,
3   flowdirection string,
4   action string,
5   sourceaddress string,
6   sourceport int,
7   pktsrcaddr string,
8   destinationaddress string,
9   destinationport int,
10  pktdstaddr string,
11  protocol int,
12  trafficpath string,
13  starttime int,
14  endtime int
15 )
16 ROW FORMAT DELIMITED
17 FIELDS TERMINATED BY ' '
18 LOCATION 's3://advnetspec-vpcflowlogsdemo/AWSLogs/'
19 TBLPROPERTIES ("skip.header.line.count"="1");
20
```

- 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



```

1 SELECT *
2 FROM "sampledb"."vpc_flow_logs"
3 WHERE
4 interfaceid = 'eni-0215590d2fe2d370a'
5 and flowdirection = 'ingress'
6 and action = 'REJECT'
7 order by starttime

```

Run query Save as Create (Run time: 1)

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



Log viewing methods vary by storage destination.

---

Many different analysis tools and services are available.

---

All flow log activities incur charges.