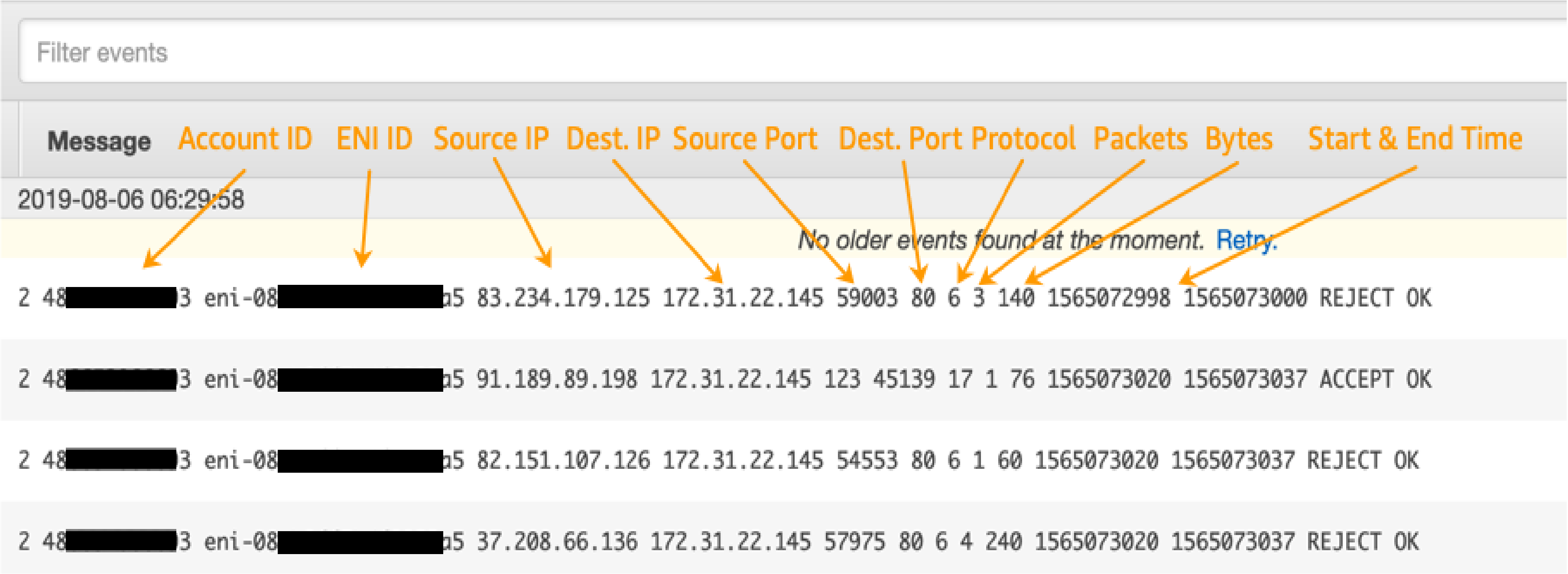
Amazon Web Services

Flow logs

ankitnarula1991@gmail.com

Flow logs

- VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to Amazon CloudWatch Logs or Amazon S3.
- **Flow Logs Syntax**



Filter events

Message

2019-08-06 06:29:58

No older events found at the moment. Retry.

```
2 48[redacted]3 eni-08[redacted]5 83.234.179.125 172.31.22.145 59003 80 6 3 140 1565072998 1565073000 REJECT OK

2 48[redacted]3 eni-08[redacted]5 91.189.89.198 172.31.22.145 123 45139 17 1 76 1565073020 1565073037 ACCEPT OK

2 48[redacted]3 eni-08[redacted]5 82.151.107.126 172.31.22.145 54553 80 6 1 60 1565073020 1565073037 REJECT OK

2 48[redacted]3 eni-08[redacted]5 37.208.66.136 172.31.22.145 57975 80 6 4 240 1565073020 1565073037 REJECT OK
```

Flow logs

- Create VPC
- Create Public Subnet
- Create Internet gateway
- Attach Internet gateway with VPC
- Create Route table
- Attach Subnet with route table

Flow logs

- Attach Internet Gateway with route table
- Create Linux EC2 Machine
- Enter Bootstrap Script: Click Here
- Create Security group
- Enable SSH & HTTP port
- Now check the public IP

Flow logs – S3

- Create S3 Bucket & Don’t give public Access
- Create VPC Flow Logs in S3
- Select VPC & go to Flow logs tab
- Click on Create Flow logs
- Enter the name
- Select filter as ALL

Flow logs – S3

- Copy S3 Bucket ARN
- Paste the ARN In the flow logs
- Click on Create Flow log
- Open all folders in the bucket

Flow logs – Cloud Watch

- Create New Flow Logs
- Enter Name
- Select filter as All
- Select Maximum aggregation interval & Select Cloud Watch Logs
- To do setups we need IAM Role & Cloud Watch Group

Flow logs – Cloud Watch

- Create IAM Role
- Click on Setup Permissions
- Click on policies
- Click on create policy
- Select the service as **CloudWatch Logs**
- Select actions
- In list Select (DescribeLogGroups, DescribeLogStreams)

Flow logs – Cloud Watch

- In Write Select (CreateLogGroup, CreateLogStream, PutLogEvents)
- Select resource as all resources
- Click on Next tags
- Click on Next: Review
- Enter the Name & Description
- Click on create policy

Flow logs – Cloud Watch

- **Create Role**
- Click on create role
- Select custom trust policy
- Code: **Click Here**
- Click on Next
- Select the policy which we have created
- Enter the role name & description
- Click on create role
- Now select the role in VPC Flow logs role in VPC

Flow logs – Cloud Watch

- Now we need to create destination log group
- Go to Cloud Watch
- Click on log groups
- Click on Create Log Group
- Enter the Log Group Name
- Select retention Settings
- Click on Create

Flow logs – Cloud Watch

- Select the log group In VPC Flow log
- Click on Create flow log
- Go to Cloud Watch
- Click on Log Group
- Open our log group
- Click on Log Streams tab
- Click on log stream file

ankitnarula1991@gmail.com