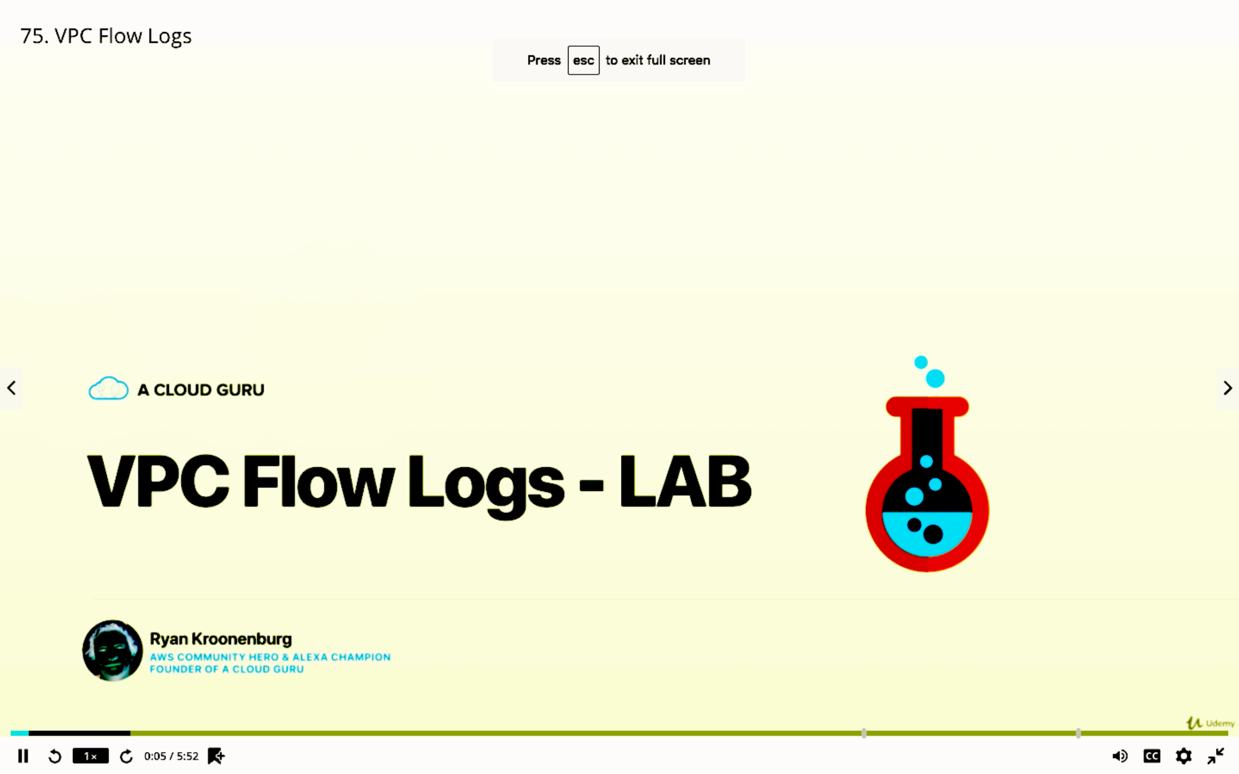
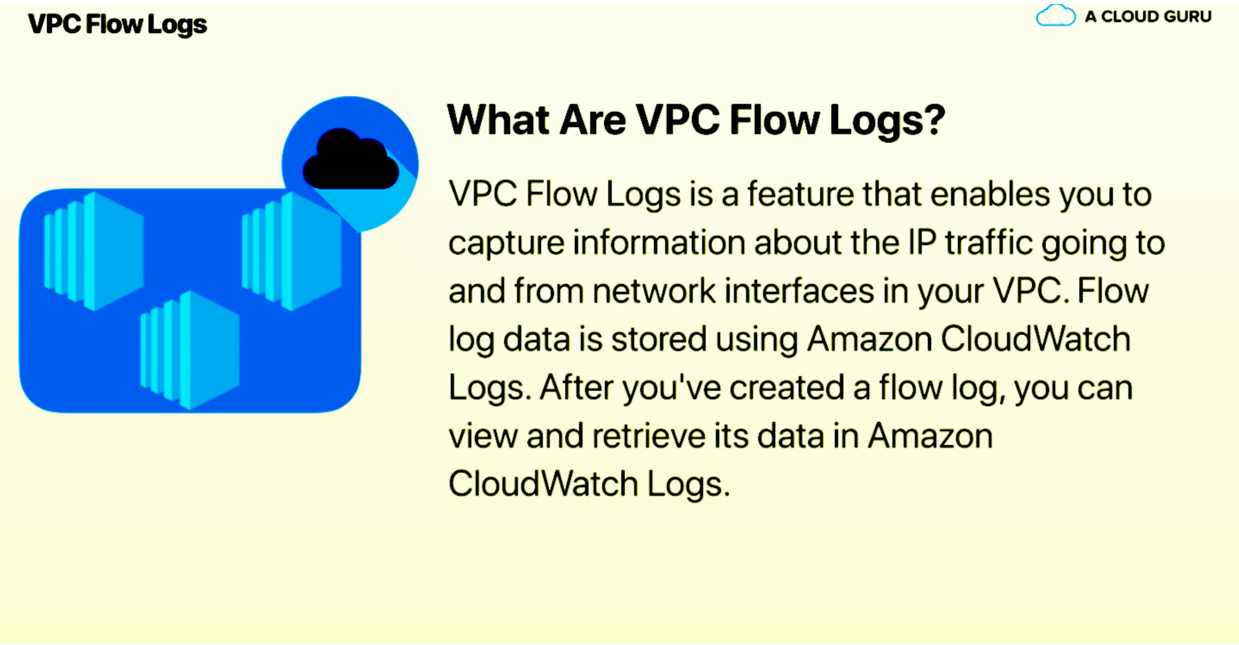


75. VPC Flow Logs

A CLOUD GURU

VPC Flow Logs - LAB

Ryan Kroonenburg
AWS COMMUNITY HERO & ALEXA CHAMPION
FOUNDER OF A CLOUD GURU

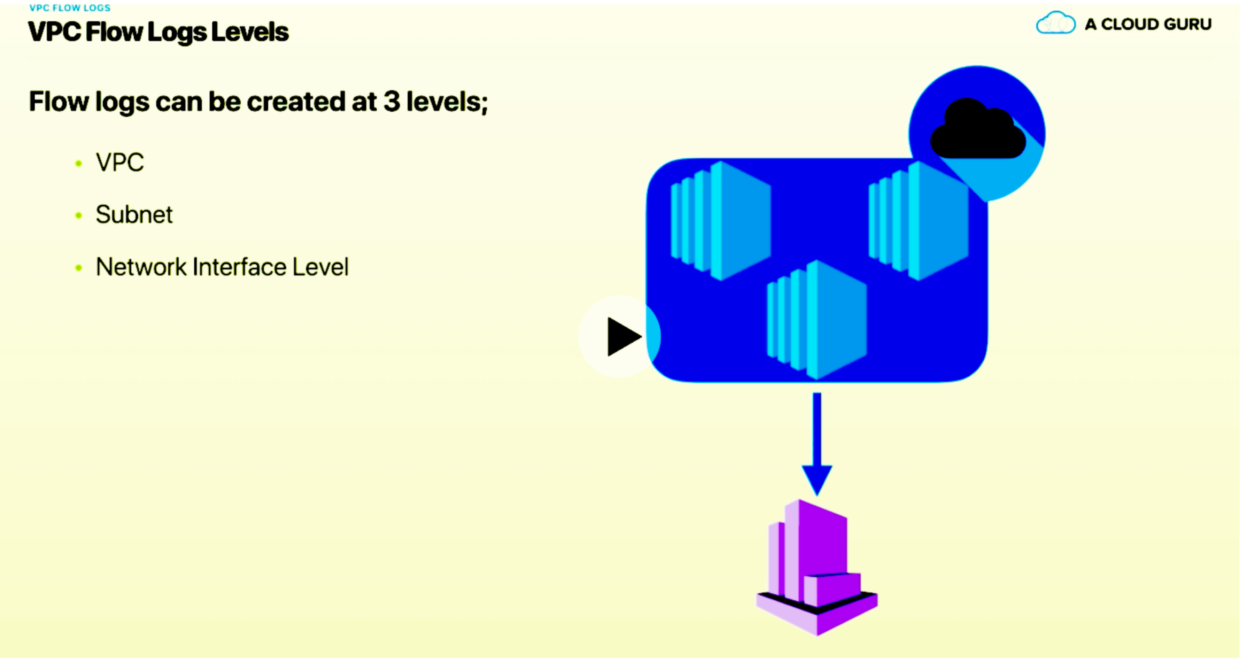


VPC Flow Logs

A CLOUD GURU

What Are VPC 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 is stored using Amazon CloudWatch Logs. After you've created a flow log, you can view and retrieve its data in Amazon CloudWatch Logs.

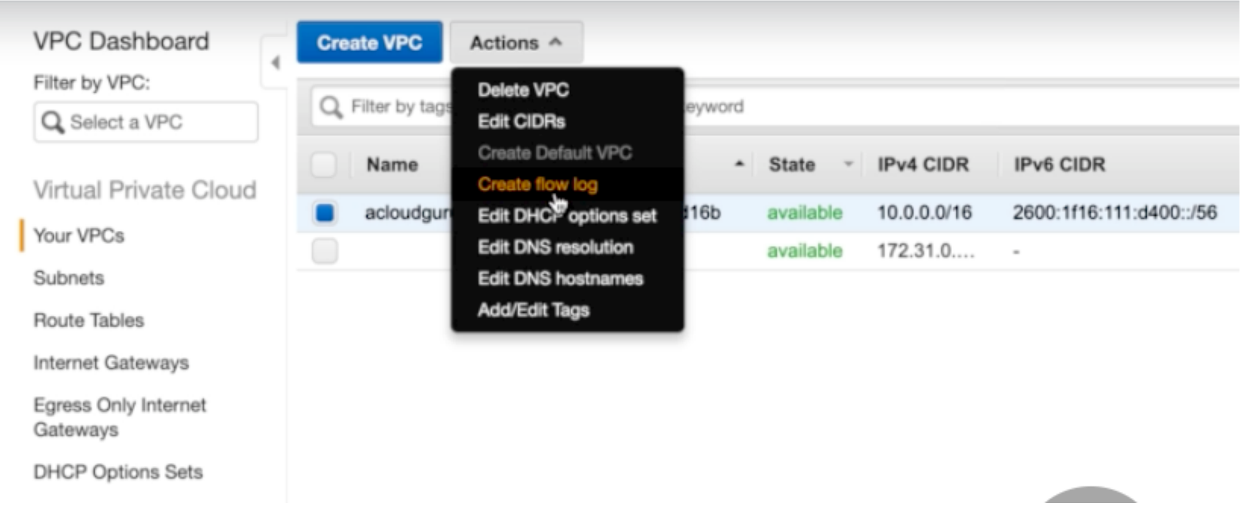


VPC FLOW LOGS

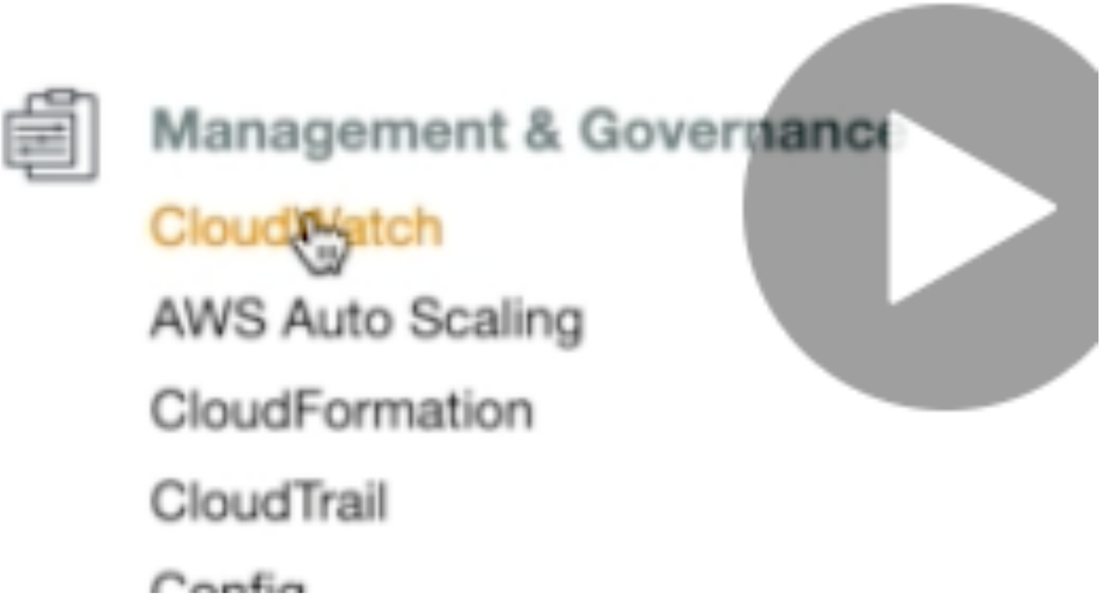
VPC Flow Logs Levels

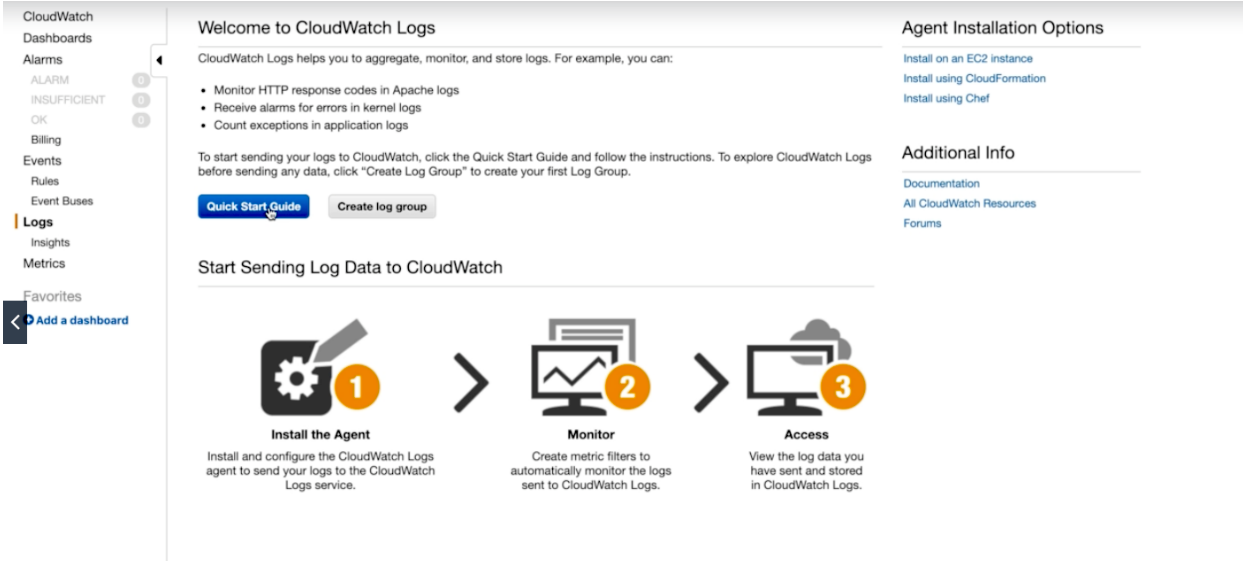
Flow logs can be created at 3 levels;

- VPC
- Subnet
- Network Interface Level



Name		State	IPv4 CIDR	IPv6 CIDR
acloudgur	16b	available	10.0.0.0/16	2600:1f16:111:d400::/56
		available	172.31.0....	-





Welcome to CloudWatch Logs

CloudWatch Logs helps you to aggregate, monitor, and store logs. For example, you can:

- Monitor HTTP response codes in Apache logs
- Receive alarms for errors in kernel logs
- Count exceptions in application logs

To start sending your logs to CloudWatch, click the Quick Start Guide and follow the instructions. To explore CloudWatch Logs before sending any data, click "Create Log Group" to create your first Log Group.

Start Sending Log Data to CloudWatch

1 Install the Agent

Install and configure the CloudWatch Logs agent to send your logs to the CloudWatch Logs service.

2 Monitor

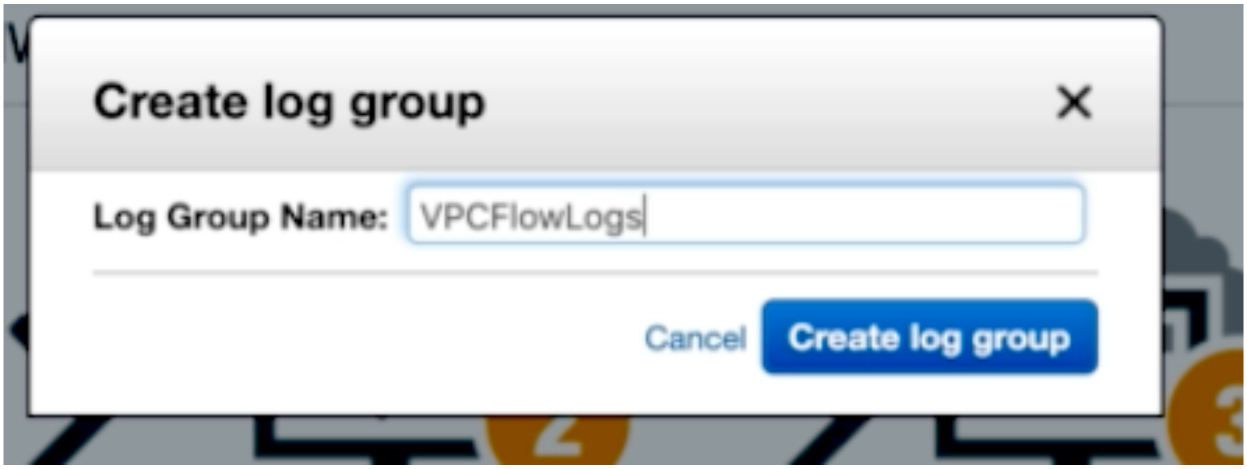
Create metric filters to automatically monitor the logs sent to CloudWatch Logs.

3 Access

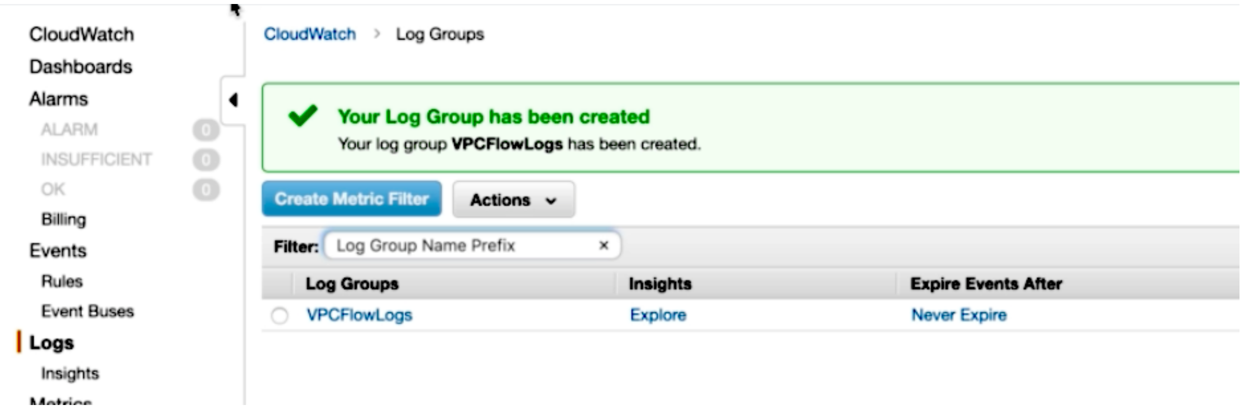
View the log data you have sent and stored in CloudWatch Logs.

Agent Installation Options

Additional Info

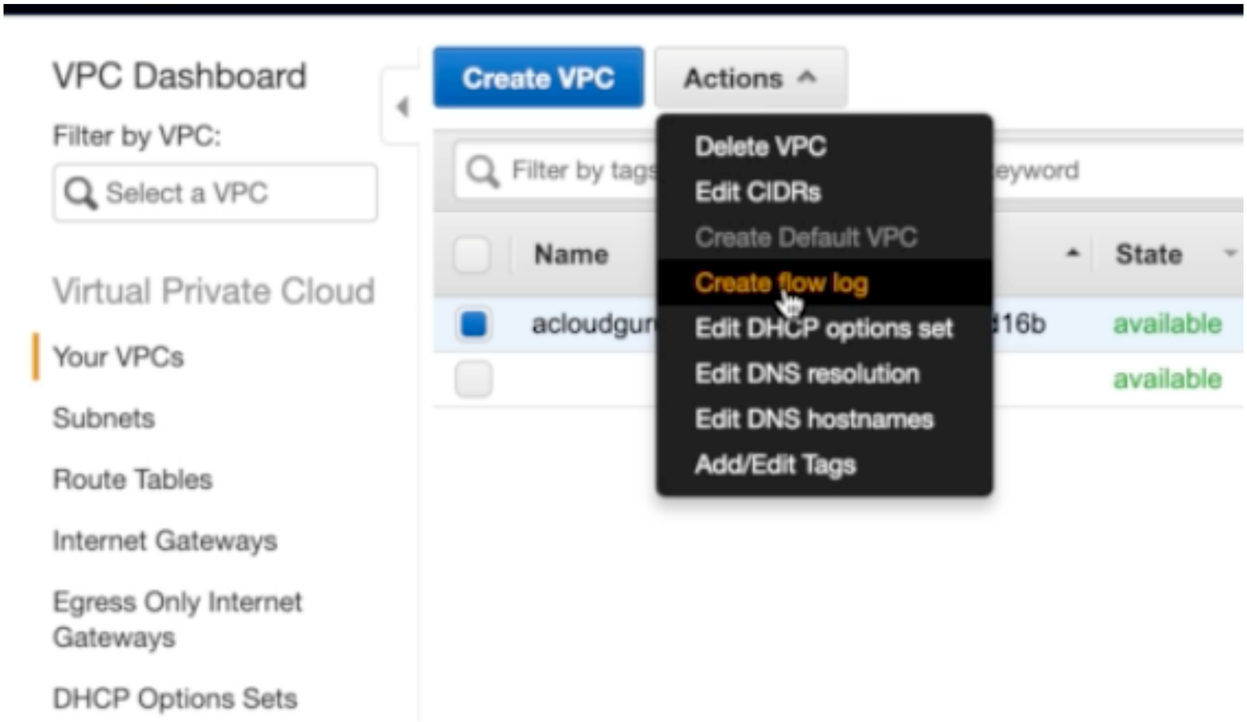


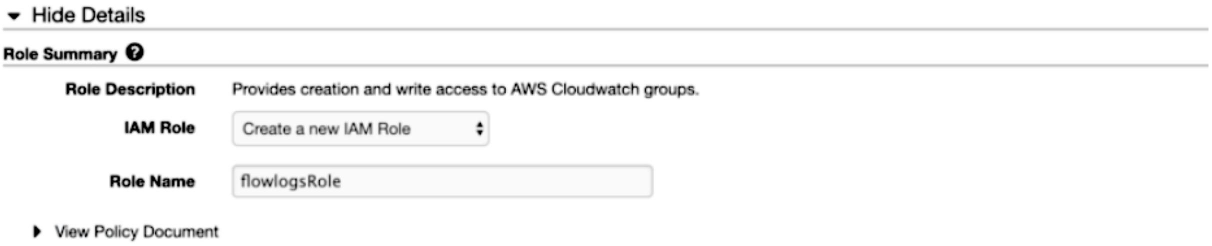
Log Group Name: VPCFlowLogs



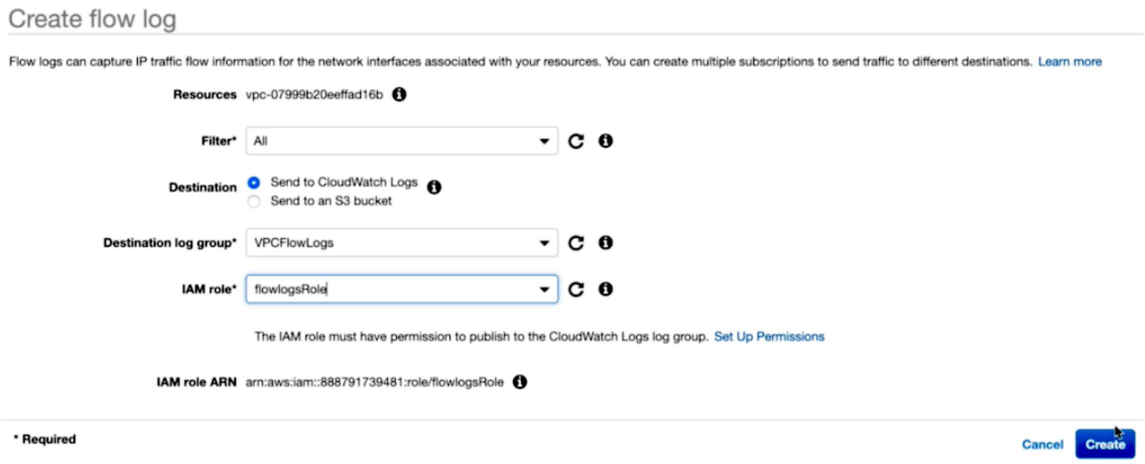
Your Log Group has been created
Your log group **VPCFlowLogs** has been created.

	Log Groups	Insights	Expire Events After
○	VPCFlowLogs	Explore	Never Expire





Role Description	Provides creation and write access to AWS Cloudwatch groups.
IAM Role	Create a new IAM Role
Role Name	flowlogsRole



Create flow log

Flow logs can capture IP traffic flow information for the network interfaces associated with your resources. You can create multiple subscriptions to send traffic to different destinations. Learn more

Resources vpc-07999b20eeffad16b

Filter* All

Destination ● Send to CloudWatch Logs
○ Send to an S3 bucket

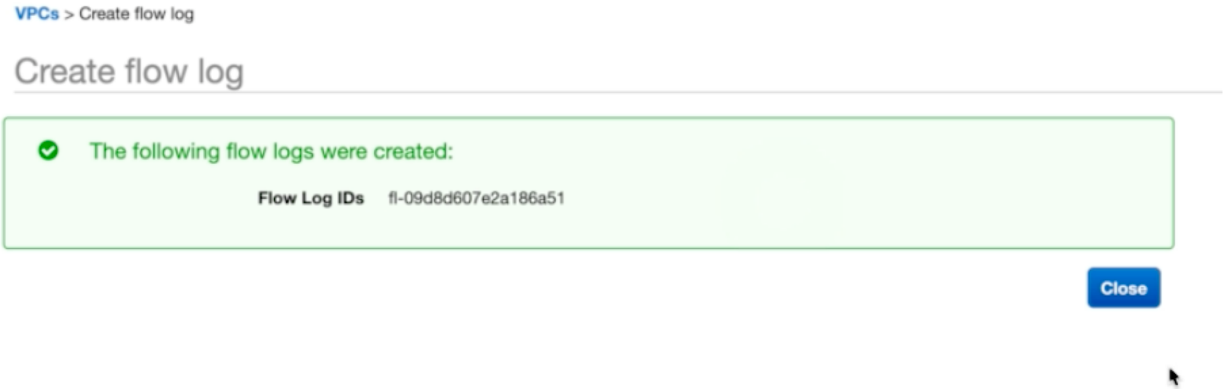
Destination log group* VPCFlowLogs

IAM role* flowlogsRole

The IAM role must have permission to publish to the CloudWatch Logs log group. Set Up Permissions

IAM role ARN arn:aws:iam::888791739481:role/flowlogsRole

*** Required**

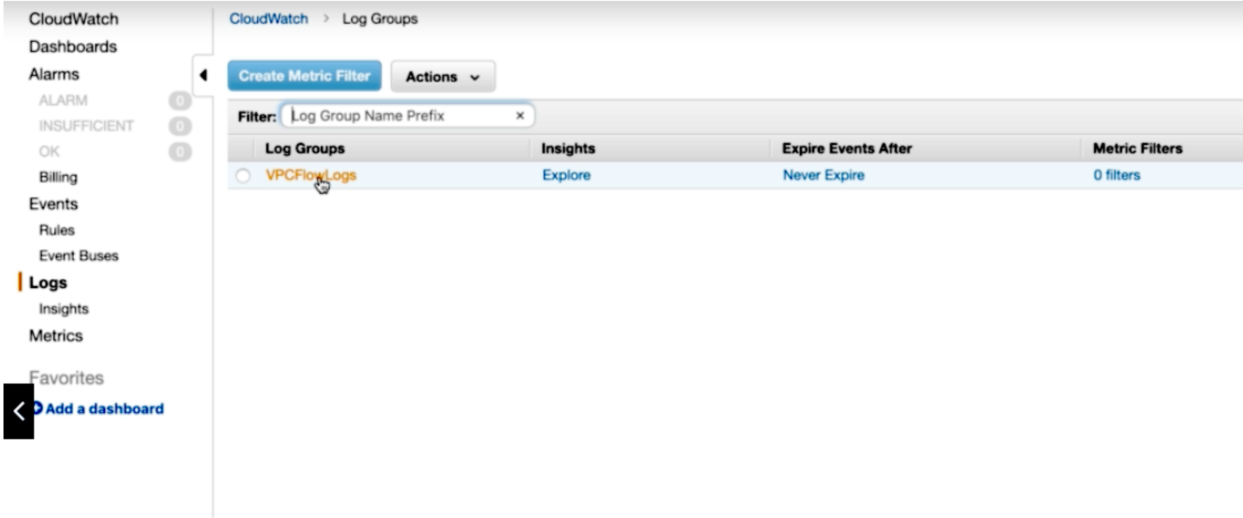


VPCs > Create flow log

Create flow log

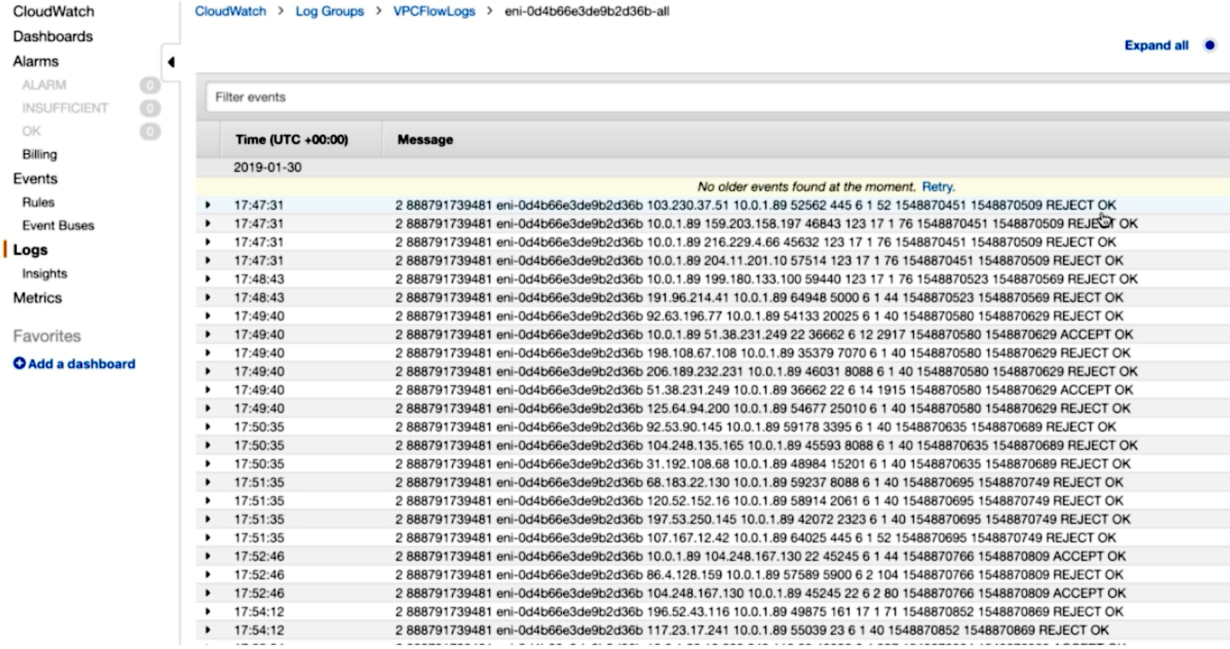
The following flow logs were created:

Flow Log IDs fl-09d8d607e2a186a51

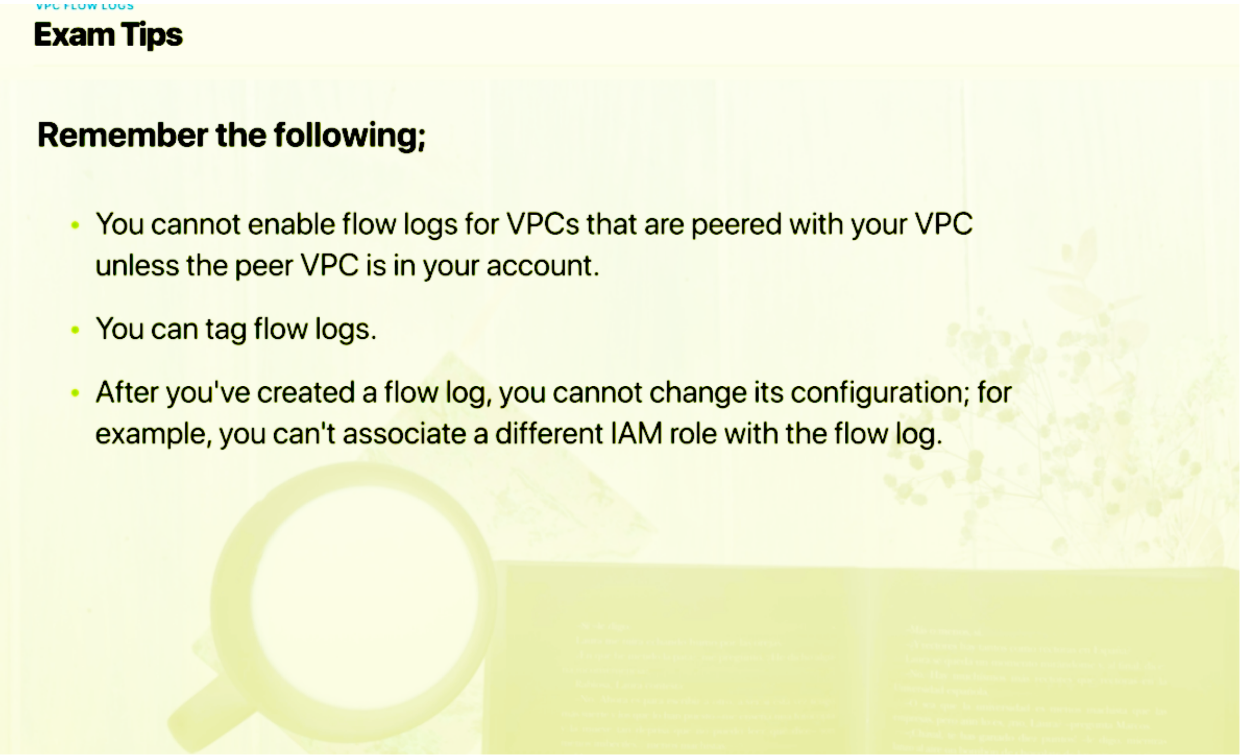


Filter: Log Group Name Prefix

	Log Groups	Insights	Expire Events After	Metric Filters
○	VPCFlowLogs	Explore	Never Expire	0 filters



```
Time (UTC +00:00)   Message
2019-01-30
                    No older events found at the moment. Retry.
17:47:31   2 888791739481 eni-0d4b66e3de9b2d36b 103.230.37.51 10.0.1.89 52562 445 6 1 52 1548870451 1548870509 REJECT OK
17:47:31   2 888791739481 eni-0d4b66e3de9b2d36b 10.0.1.89 159.203.158.197 46843 123 17 1 76 1548870451 1548870509 REJECT OK
17:47:31   2 888791739481 eni-0d4b66e3de9b2d36b 10.0.1.89 216.229.4.66 45632 123 17 1 76 1548870451 1548870509 REJECT OK
17:47:31   2 888791739481 eni-0d4b66e3de9b2d36b 10.0.1.89 204.11.201.10 57514 123 17 1 76 1548870451 1548870509 REJECT OK
17:48:43   2 888791739481 eni-0d4b66e3de9b2d36b 10.0.1.89 199.180.133.100 59440 123 17 1 76 1548870523 1548870569 REJECT OK
17:48:43   2 888791739481 eni-0d4b66e3de9b2d36b 191.96.214.41 10.0.1.89 64948 5000 6 1 44 1548870523 1548870569 REJECT OK
17:49:40   2 888791739481 eni-0d4b66e3de9b2d36b 92.63.196.77 10.0.1.89 54133 20025 6 1 40 1548870580 1548870629 REJECT OK
17:49:40   2 888791739481 eni-0d4b66e3de9b2d36b 10.0.1.89 51.38.231.249 22 36662 6 12 2917 1548870580 1548870629 ACCEPT OK
17:49:40   2 888791739481 eni-0d4b66e3de9b2d36b 198.108.67.108 10.0.1.89 35379 7070 6 1 40 1548870580 1548870629 REJECT OK
17:49:40   2 888791739481 eni-0d4b66e3de9b2d36b 206.189.232.231 10.0.1.89 46031 8088 6 1 40 1548870580 1548870629 REJECT OK
17:49:40   2 888791739481 eni-0d4b66e3de9b2d36b 51.38.231.249 10.0.1.89 36662 22 6 14 1915 1548870580 1548870629 ACCEPT OK
17:49:40   2 888791739481 eni-0d4b66e3de9b2d36b 125.64.94.200 10.0.1.89 54677 25010 6 1 40 1548870580 1548870629 REJECT OK
17:50:35   2 888791739481 eni-0d4b66e3de9b2d36b 92.53.90.145 10.0.1.89 59178 3395 6 1 40 1548870635 1548870689 REJECT OK
17:50:35   2 888791739481 eni-0d4b66e3de9b2d36b 104.248.135.165 10.0.1.89 45593 8088 6 1 40 1548870635 1548870689 REJECT OK
17:50:35   2 888791739481 eni-0d4b66e3de9b2d36b 31.192.108.68 10.0.1.89 48984 15201 6 1 40 1548870635 1548870689 REJECT OK
17:51:35   2 888791739481 eni-0d4b66e3de9b2d36b 68.183.22.130 10.0.1.89 59237 8088 6 1 40 1548870695 1548870749 REJECT OK
17:51:35   2 888791739481 eni-0d4b66e3de9b2d36b 120.52.152.16 10.0.1.89 58914 2061 6 1 40 1548870695 1548870749 REJECT OK
17:51:35   2 888791739481 eni-0d4b66e3de9b2d36b 197.53.250.145 10.0.1.89 42072 2323 6 1 40 1548870695 1548870749 REJECT OK
17:51:35   2 888791739481 eni-0d4b66e3de9b2d36b 107.167.12.42 10.0.1.89 64025 445 6 1 52 1548870695 1548870749 REJECT OK
17:52:46   2 888791739481 eni-0d4b66e3de9b2d36b 10.0.1.89 104.248.167.130 22 45245 6 1 44 1548870766 1548870809 ACCEPT OK
17:52:46   2 888791739481 eni-0d4b66e3de9b2d36b 86.4.128.159 10.0.1.89 57589 5900 6 2 104 1548870766 1548870809 REJECT OK
17:52:46   2 888791739481 eni-0d4b66e3de9b2d36b 104.248.167.130 10.0.1.89 45245 22 6 2 80 1548870766 1548870809 ACCEPT OK
17:54:12   2 888791739481 eni-0d4b66e3de9b2d36b 196.52.43.116 10.0.1.89 49875 161 17 1 71 1548870852 1548870869 REJECT OK
17:54:12   2 888791739481 eni-0d4b66e3de9b2d36b 117.23.17.241 10.0.1.89 55039 23 6 1 40 1548870852 1548870869 REJECT OK
```

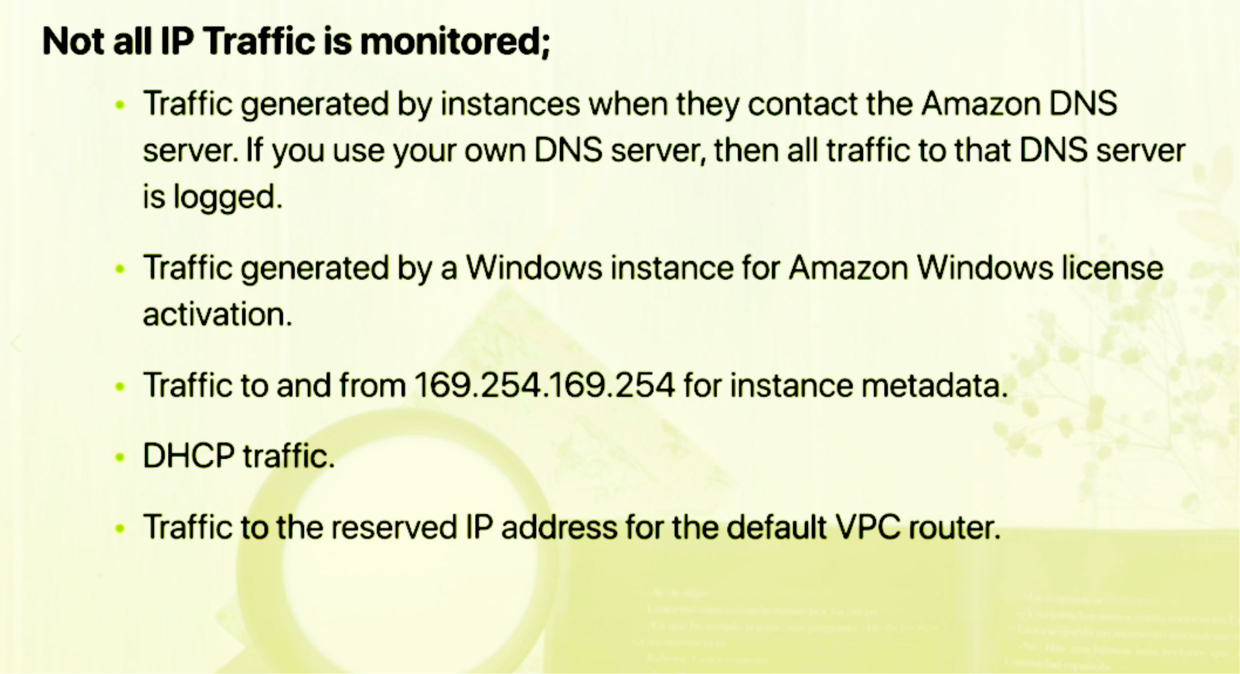


VPC FLOW LOGS

Exam Tips

Remember the following;

- You cannot enable flow logs for VPCs that are peered with your VPC unless the peer VPC is in your account.
- You can tag flow logs.
- After you've created a flow log, you cannot change its configuration; for example, you can't associate a different IAM role with the flow log.



Not all IP Traffic is monitored;

- Traffic generated by instances when they contact the Amazon DNS server. If you use your own DNS server, then all traffic to that DNS server is logged.
- Traffic generated by a Windows instance for Amazon Windows license activation.
- Traffic to and from 169.254.169.254 for instance metadata.
- DHCP traffic.
- Traffic to the reserved IP address for the default VPC router.