

11 - CRIANDO UM FLOW LOG

Qual tipo de trafego esta passando pela ACL

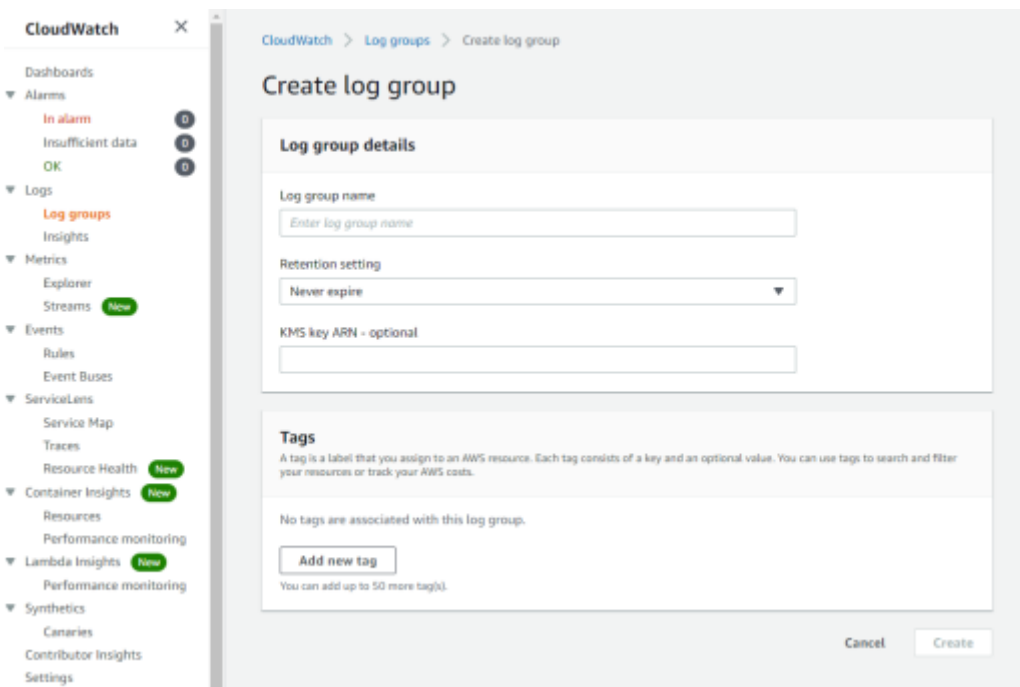
FLOW LOG -> Queremos que todas as informações que passem dentro da ACL sejam monitorados, gerando um log de eventos.

- Para habilitar

services> vpc> abre a vpc> action> create flow log

- Na parte de escolher o tipo de trafego, em um ambiente de produção, é aconselhavel fazer a distinção (dois logs) para o trafego rejeitado e para o trafego aceito.

- Como vamos colocar no cloud watch, temos que criar um log group



- Entenda que para que o log seja criado o sistema de log tem que ter permissões na ACL, permissões dentro da VPC.

- Como não temos nenhum IAM roles com logs, vamos precisar criar essa regra para logs, que permite o acesso ao serviço.
setup permissions

VPC Flow Logs is requesting permission to use resources in your account

Click Allow to give Flow Logs write access to CloudWatch groups in your account. This allows Flow Logs to publish metrics to your cloudwatch group.

▼ Hide Details

Role Summary ⓘ

Role Description Provides creation and write access to AWS Cloudwatch groups.

IAM Role Create a new IAM Role

Role Name flowlogsRole

► [View Policy Document](#)

CloudWatch > Log groups > ACL-Log-VPC

ACL-Log-VPC

Actions ▼

[View in Logs Insights](#)

[Search log group](#)

▼ Log group details

Retention	Creation time	Stored bytes	ARN
Never expire	4 minutes ago	-	arn:aws:logs:us-west-2:060436466943:log-group:ACL-Log-VPC*
KMS key ID	Metric filters	Subscription filters	Contributor Insights rules
-	0	0	-

[Log streams](#)

[Metric filters](#)

[Subscription filters](#)

[Contributor Insights](#)

[Tags](#)

Log streams (1)



Delete

[Create log stream](#)

[Search all](#)

< 1 > ⓘ

<input type="checkbox"/>	Log stream	Last event time
<input type="checkbox"/>	eni-01601019c1d267eb8-all	2021-06-03 12:10:24 (UTC-03:00)

CloudWatch > Log groups > ACL-Log-VPC > eni-01601019c1d267eb8-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](#)

Clear

1m

30m

1h

12h

Custom ⓘ



Timestamp	Message
No older events at this moment. Retry	
2021-06-03T12:10:24.000-03:00	2 060436466943 eni-01601019c1d267eb8 10.1.2.213 10.1.1.186 54353 123 17 1 76 1622733024 1622733037...
2021-06-03T12:10:24.000-03:00	2 060436466943 eni-01601019c1d267eb8 162.142.125.154 10.1.1.186 56940 2086 6 1 44 1622733024 16227...
2021-06-03T12:10:30.000-03:00	2 060436466943 eni-01601019c1d267eb8 10.1.2.213 10.1.1.186 35480 123 17 1 76 1622733039 1622733045...
2021-06-03T12:10:39.000-03:00	2 060436466943 eni-01601019c1d267eb8 10.1.2.213 10.1.1.186 59056 123 17 1 76 1622733039 1622733045...
2021-06-03T12:10:30.000-03:00	2 060436466943 eni-01601019c1d267eb8 162.142.125.146 10.1.1.186 45341 8118 6 1 44 1622733039 16227...
2021-06-03T12:10:48.000-03:00	2 060436466943 eni-01601019c1d267eb8 10.1.2.213 10.1.1.186 48845 123 17 1 76 1622733048 1622733048...
2021-06-03T12:11:00.000-03:00	2 060436466943 eni-01601019c1d267eb8 162.142.125.148 10.1.1.186 1529 12495 6 1 44 1622733068 16227...
No newer events at this moment. Auto retry paused. Resume	