VPC EndPoints

Endpoints allows to connect aws services using private network instead of public network

Not required NAT Gateways, Internet Gateways to connect the services

Types:

Interface : Provisioning an ENI(private address) as an entry point (must attach security group)

Gateway : Provisions a target and must be used in route table(ex: s3 and dynamodb)

Create VPC (10.0.0.0/16)

Create two subnets(private(10.0.1.0/28) and public(10.0.2.0/28))

Create internet gateway and attach to VPC

Create route table(public-rt) , attach public subnet and internet gateway.

Create two instances(one is in public and another is in private)

The server which is created under public subnet, it can have the internet access

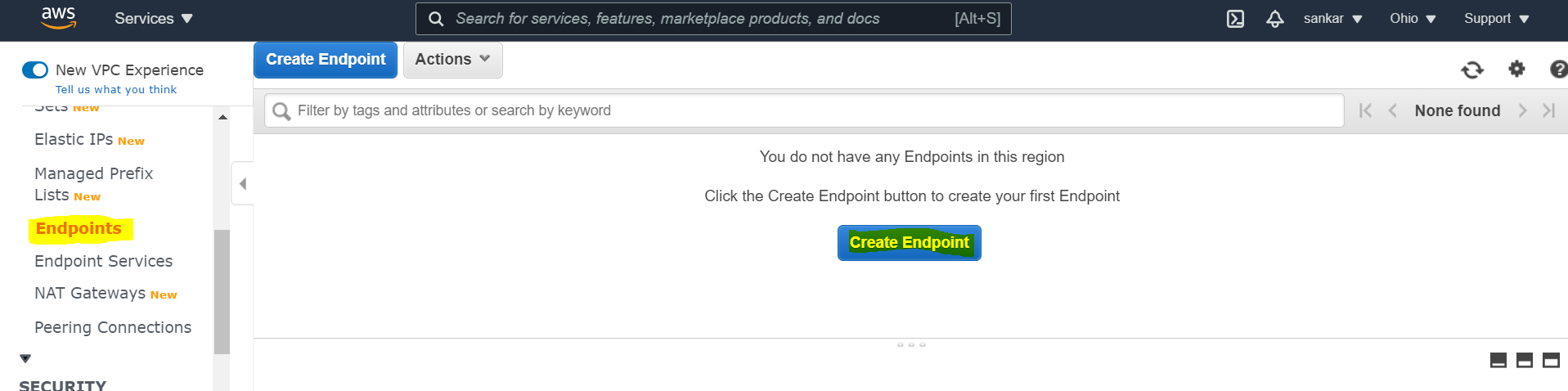
The server which is created under private, it is not having internet access

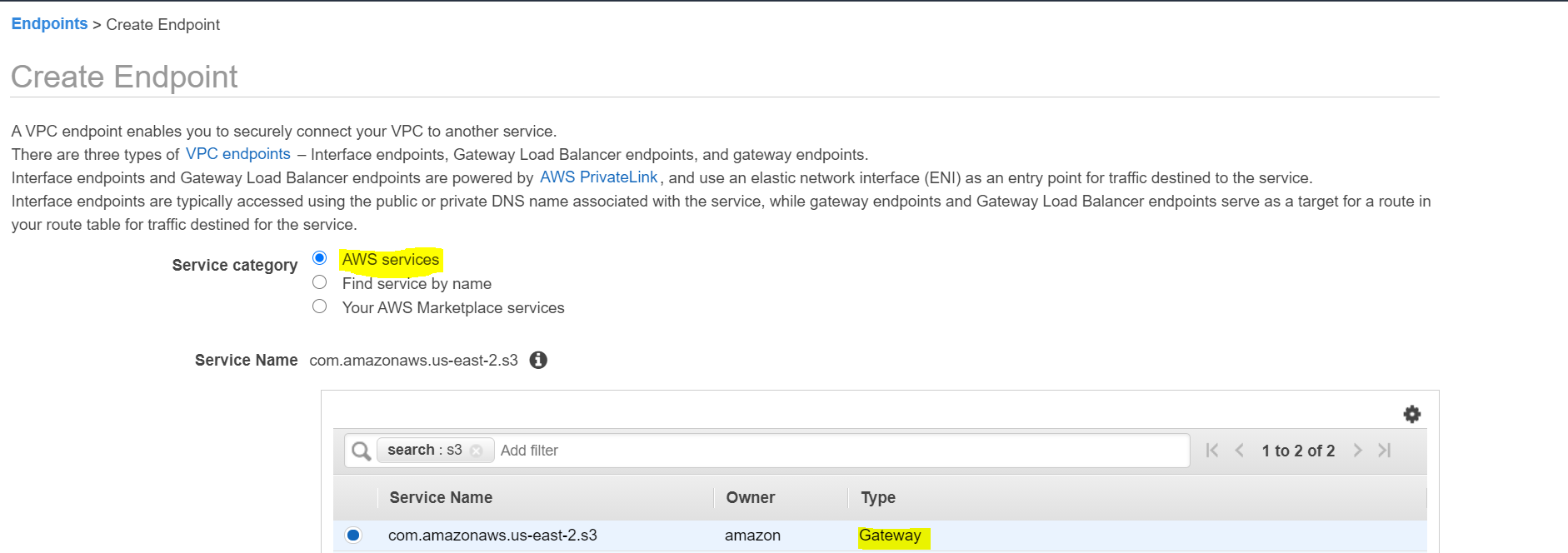
Create Role(s3fullaccess) and attach the role to private server

To communicate other aws services from the private server

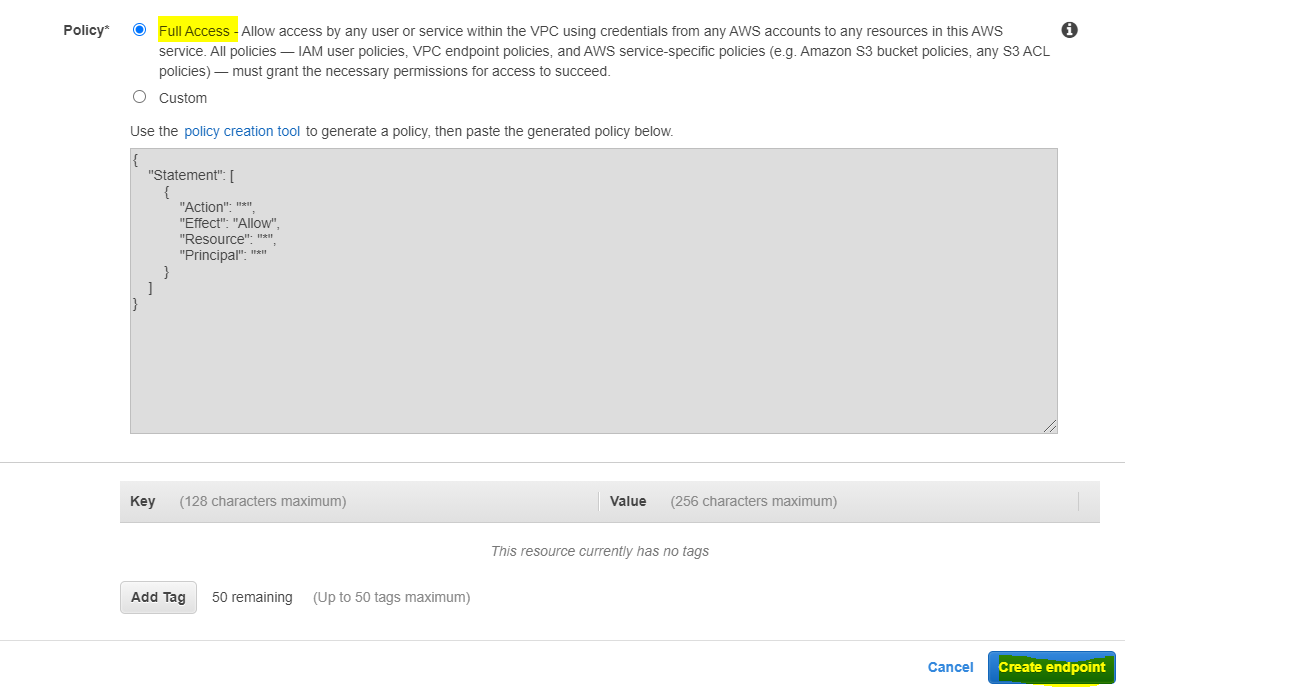
1. With the help of NAT Gateway and Role , private server can communicate with other services.
2. Using VPC Endpoints

Create VPC Endpoint:

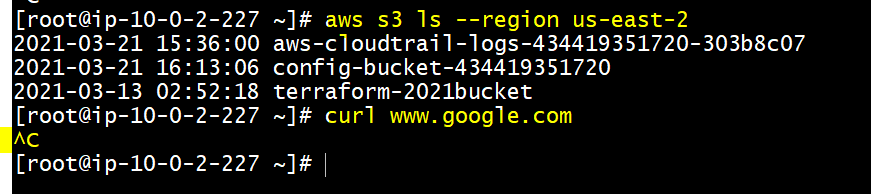








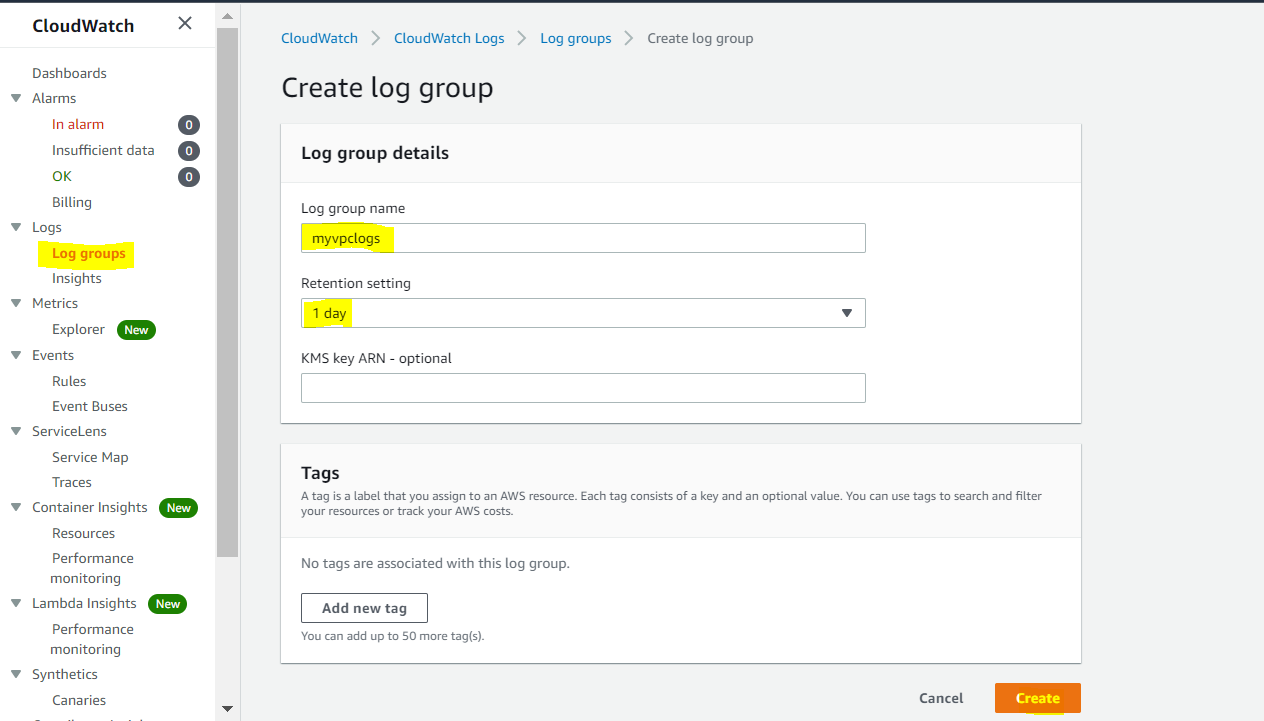
Try to access S3 buckets



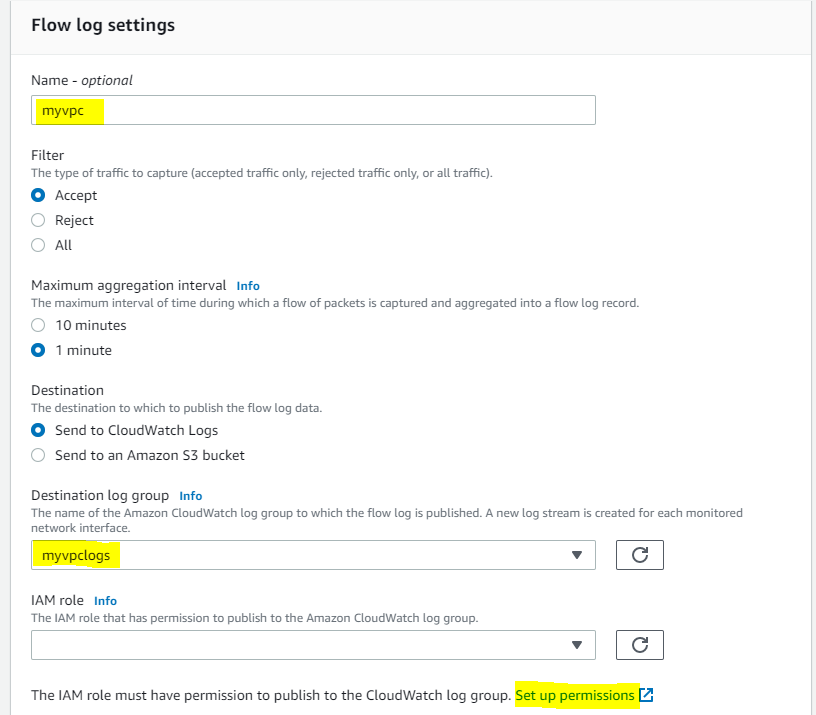
Service is reachable but internet is not reachable

VPC Flow Logs:

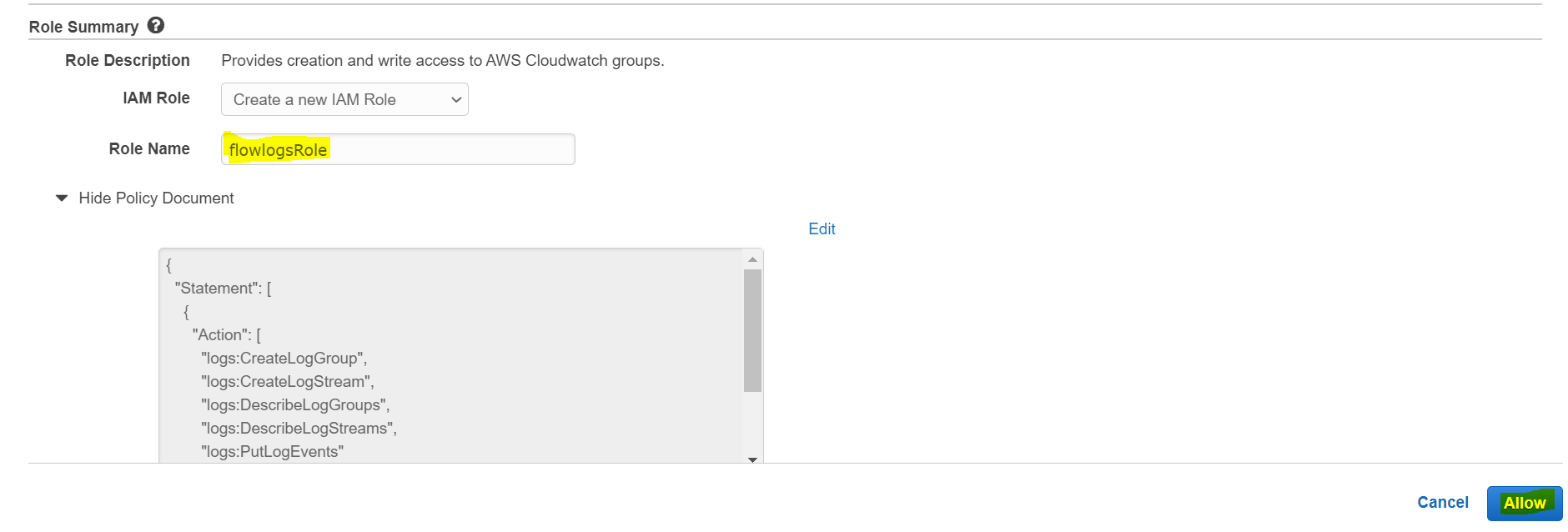
Create log group in cloudwatch



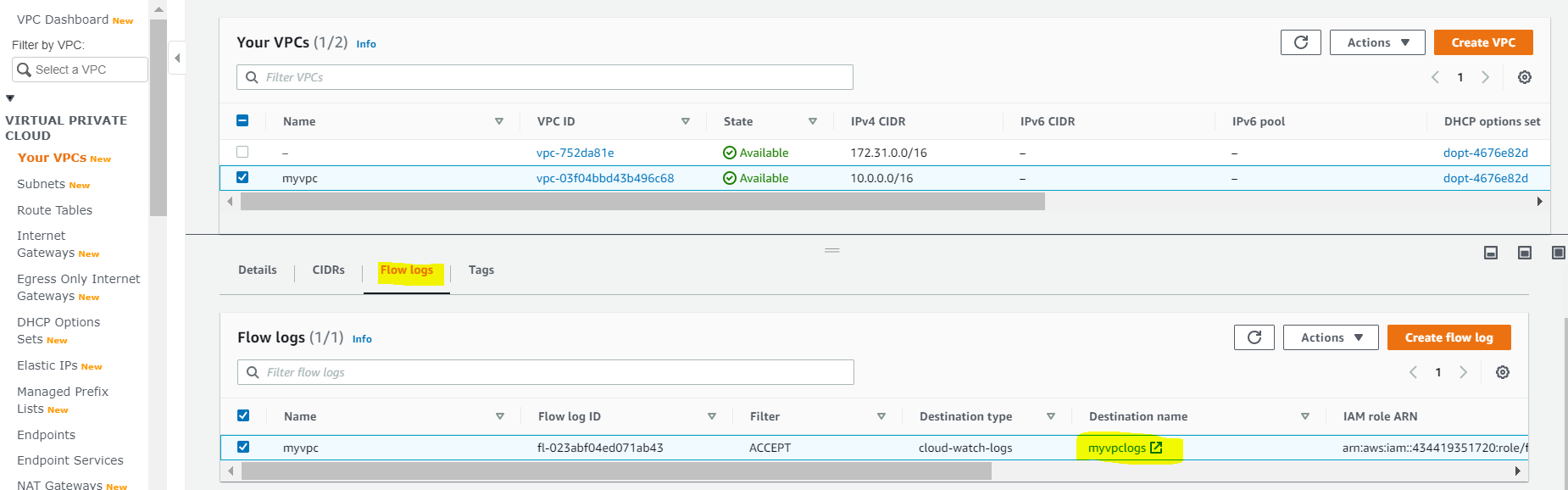
Create VPC Flow Log



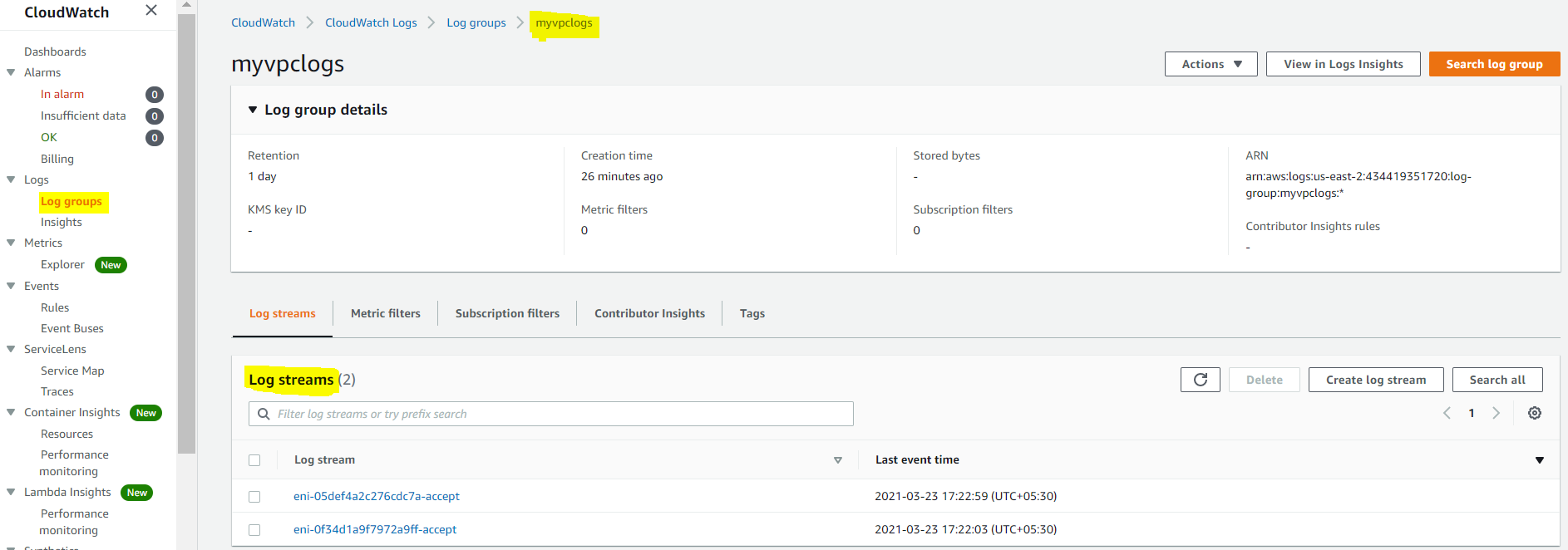
For IAM role , click on set up permissions.



Create flow log



VPC logs will be routed to cloudwatch log group



We can verify the streams

