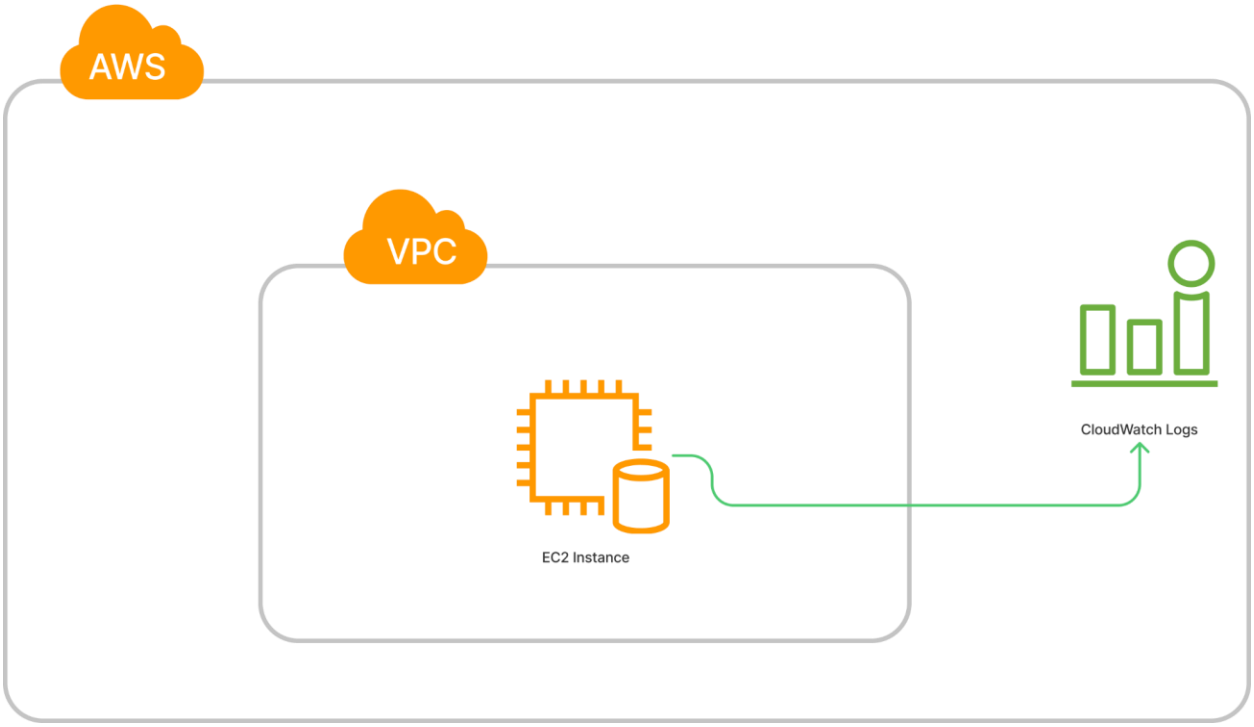
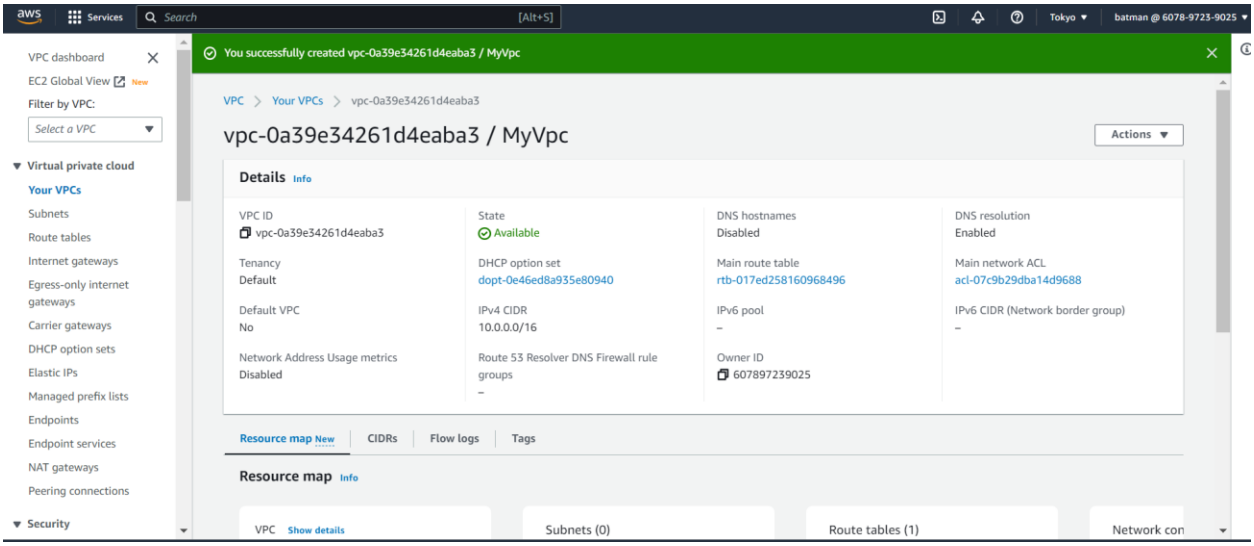
Ques 1: Follow Up the below AWS Architecture Diagram and Create the same in AWS, after created store the store the cloudwatch logs in the **logs.txt** file.

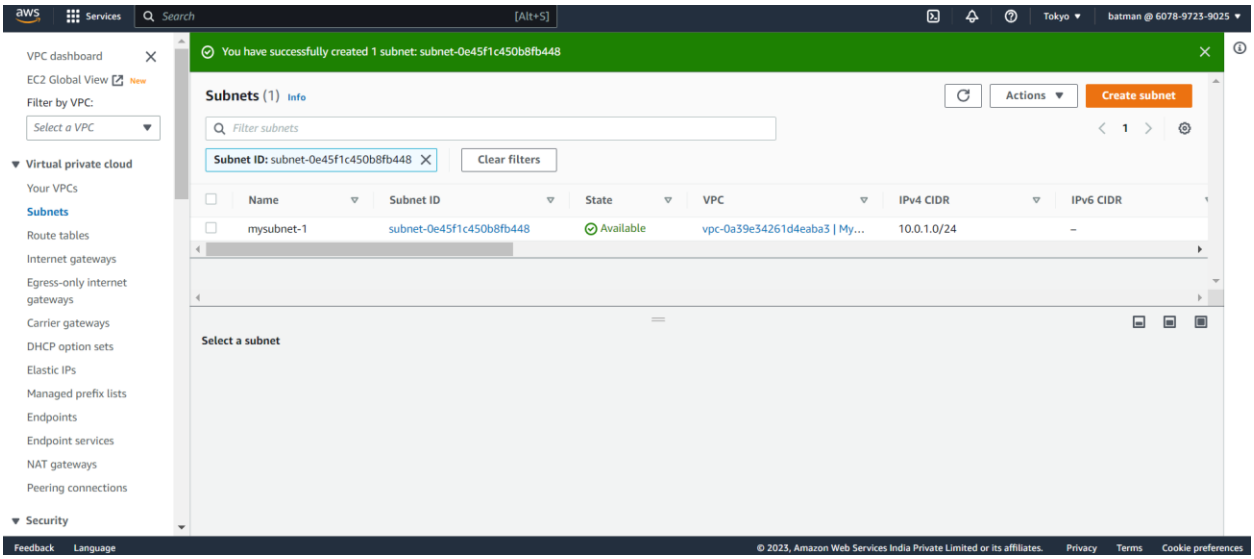


Solution:

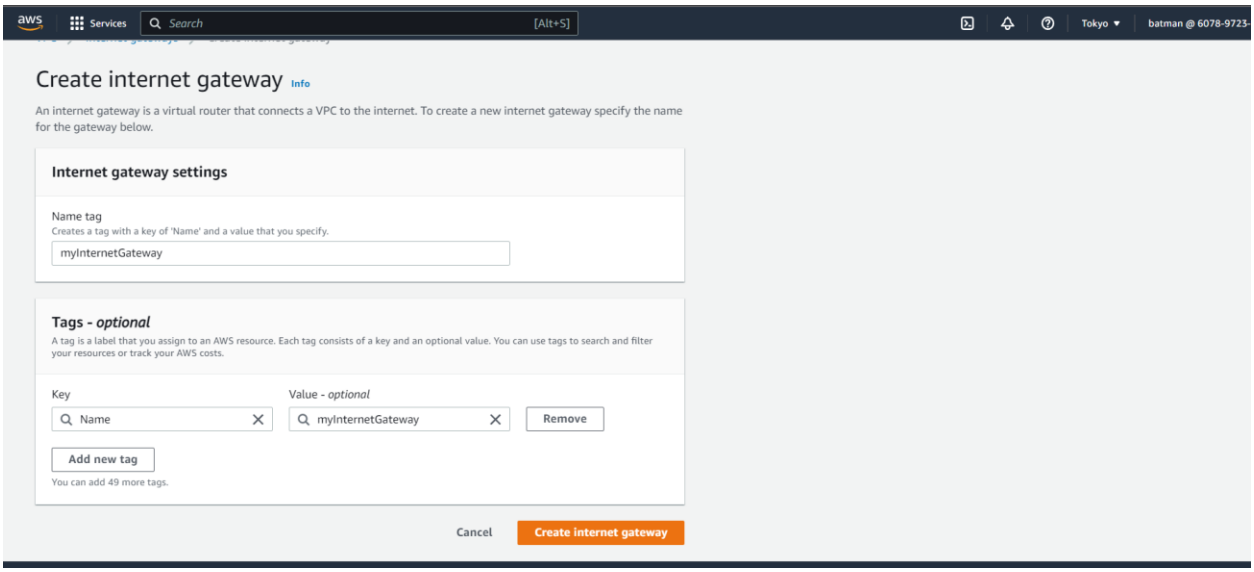
- **Creating VPC for EC2:**

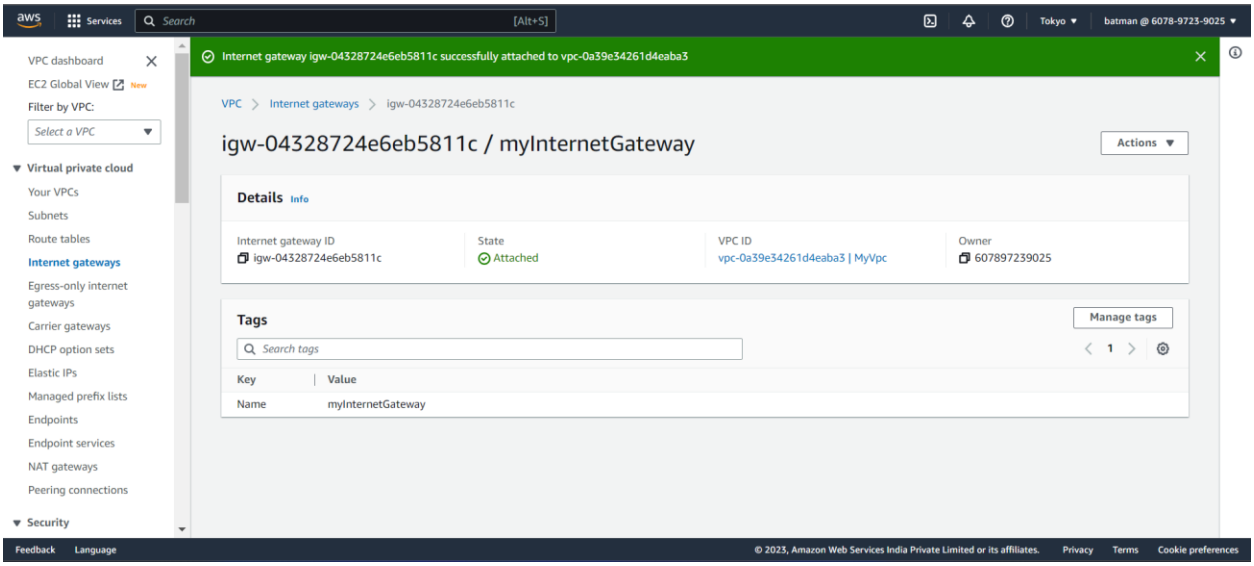


- **Creating Subnet For EC2:**

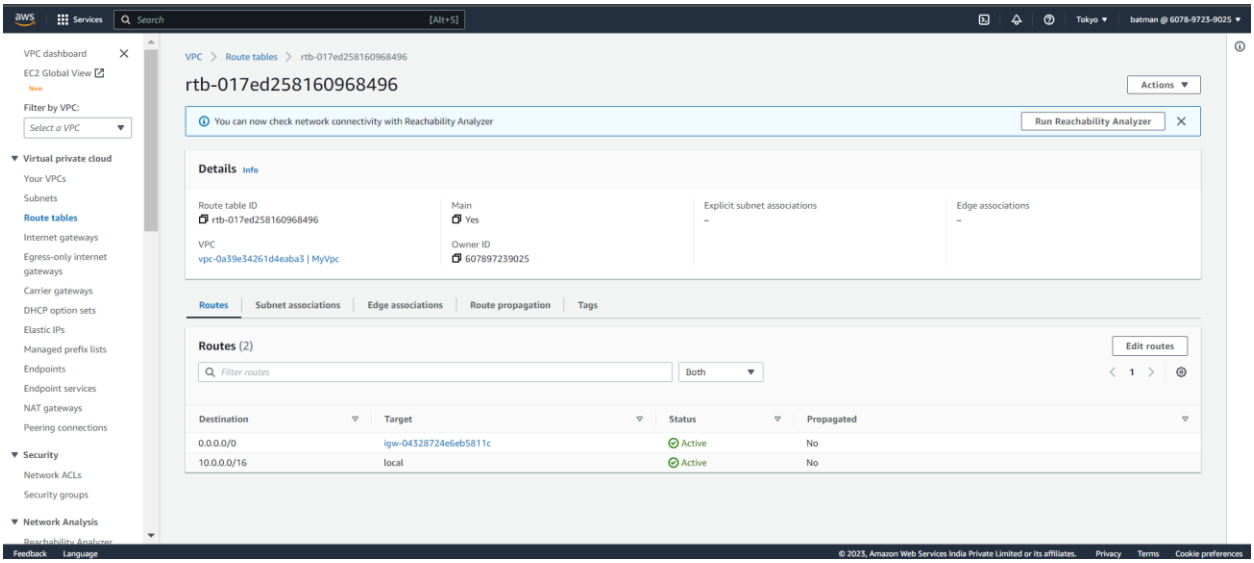


- **Creating Internet Gateway:**

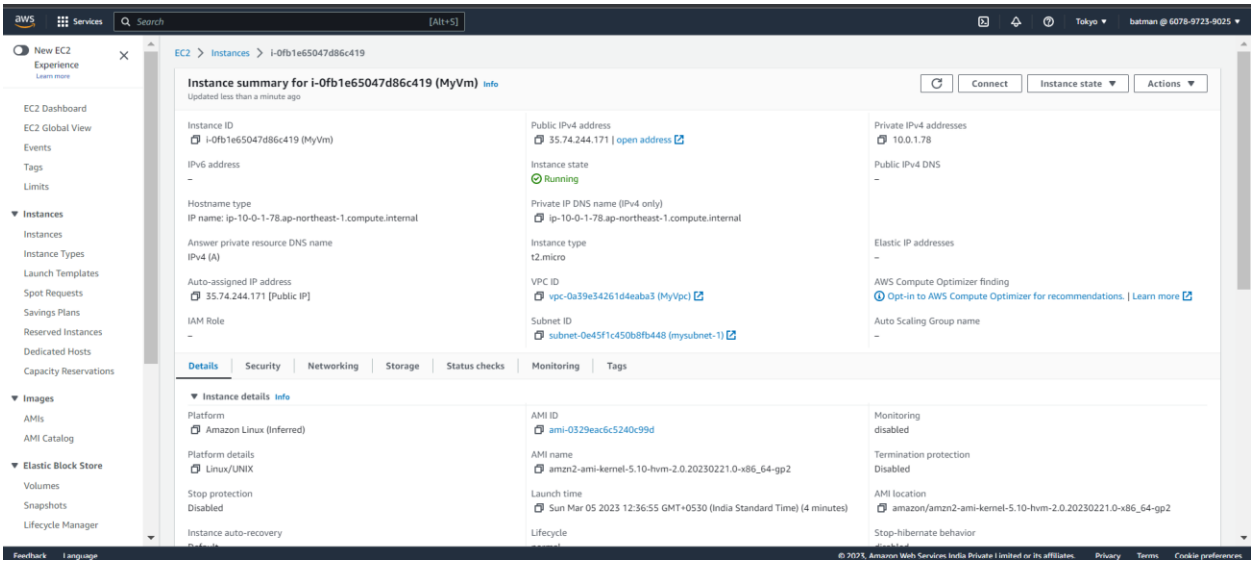




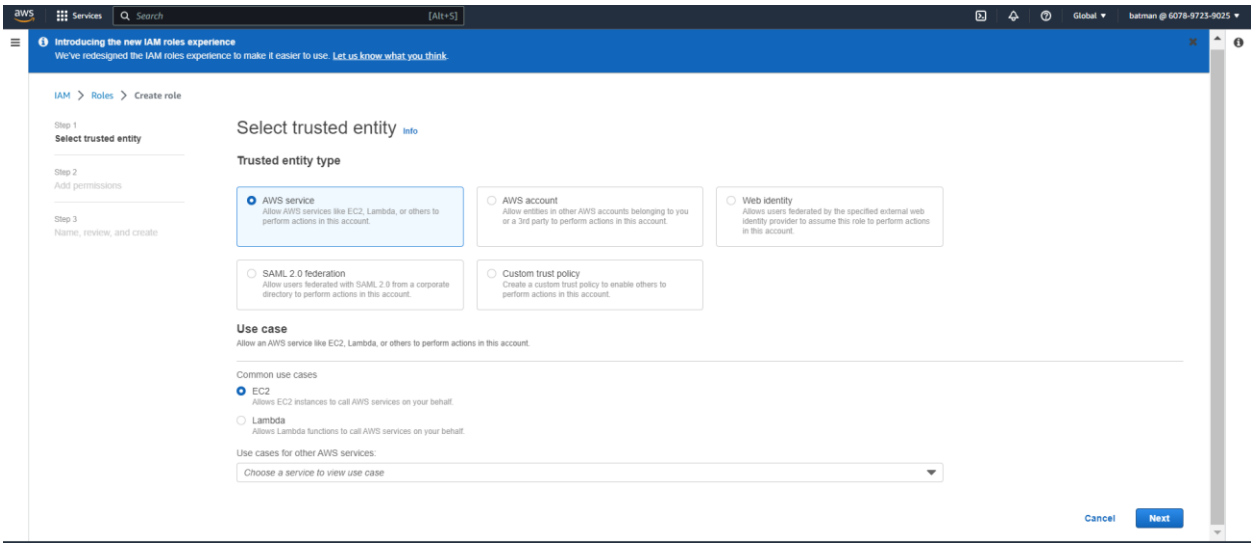
- Creating Route table:



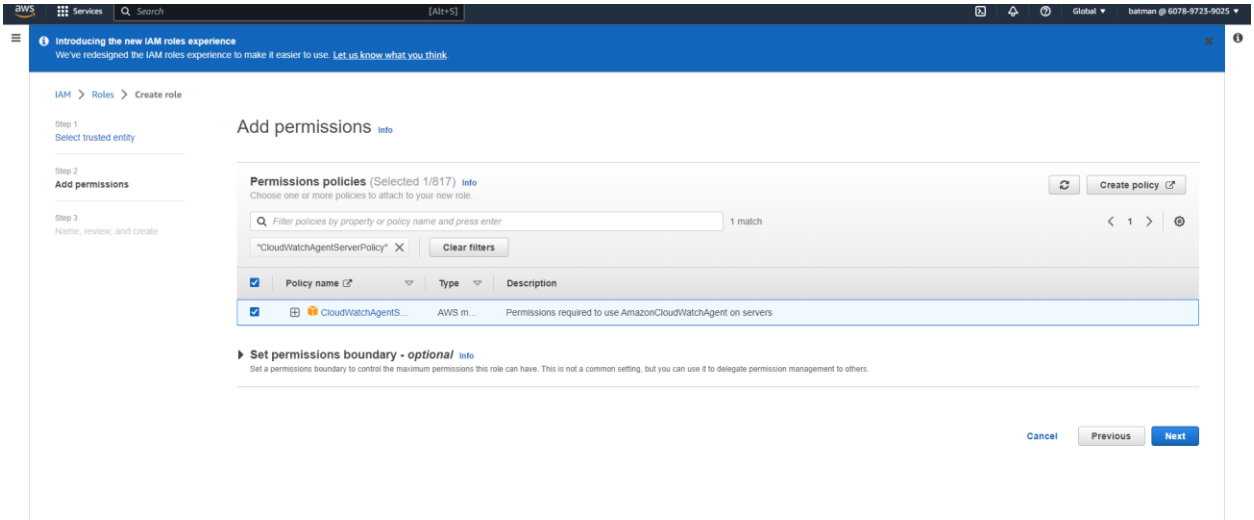
- **Ec2 created:**



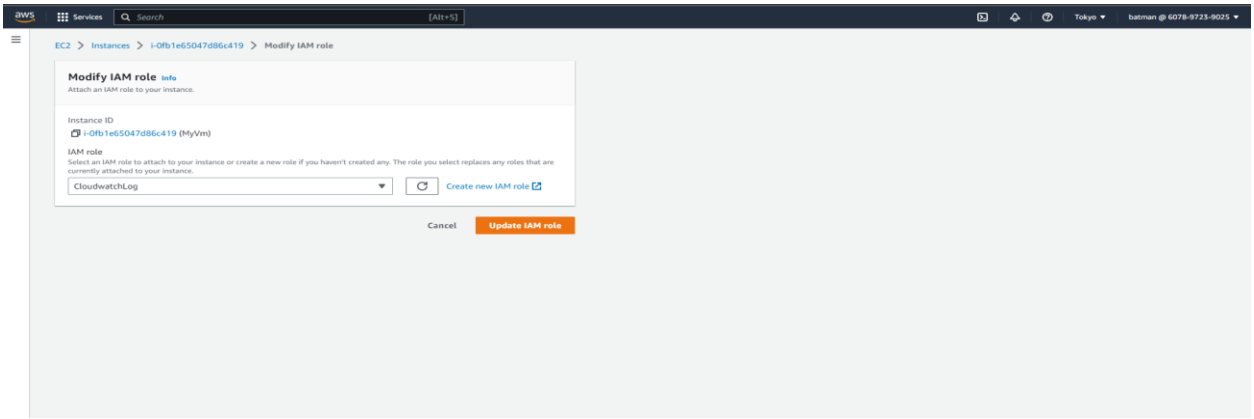
- **Creating IAM role that will allow the EC2 instance to communicate with Cloudwatch:**



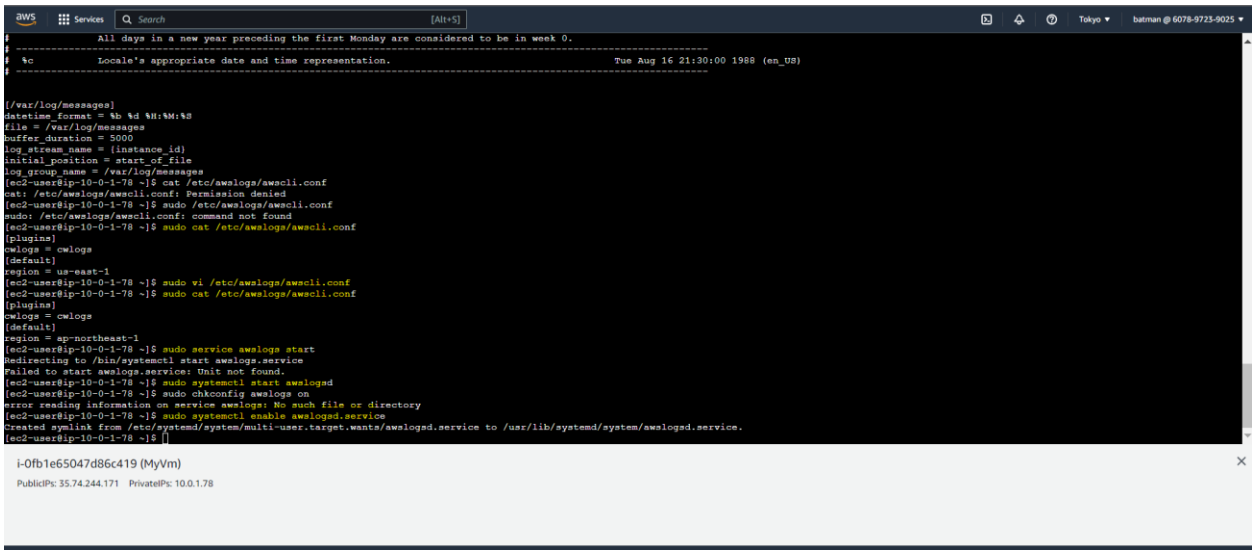
- **Selecting the** CloudWatchAgentServerPolicy **policy**



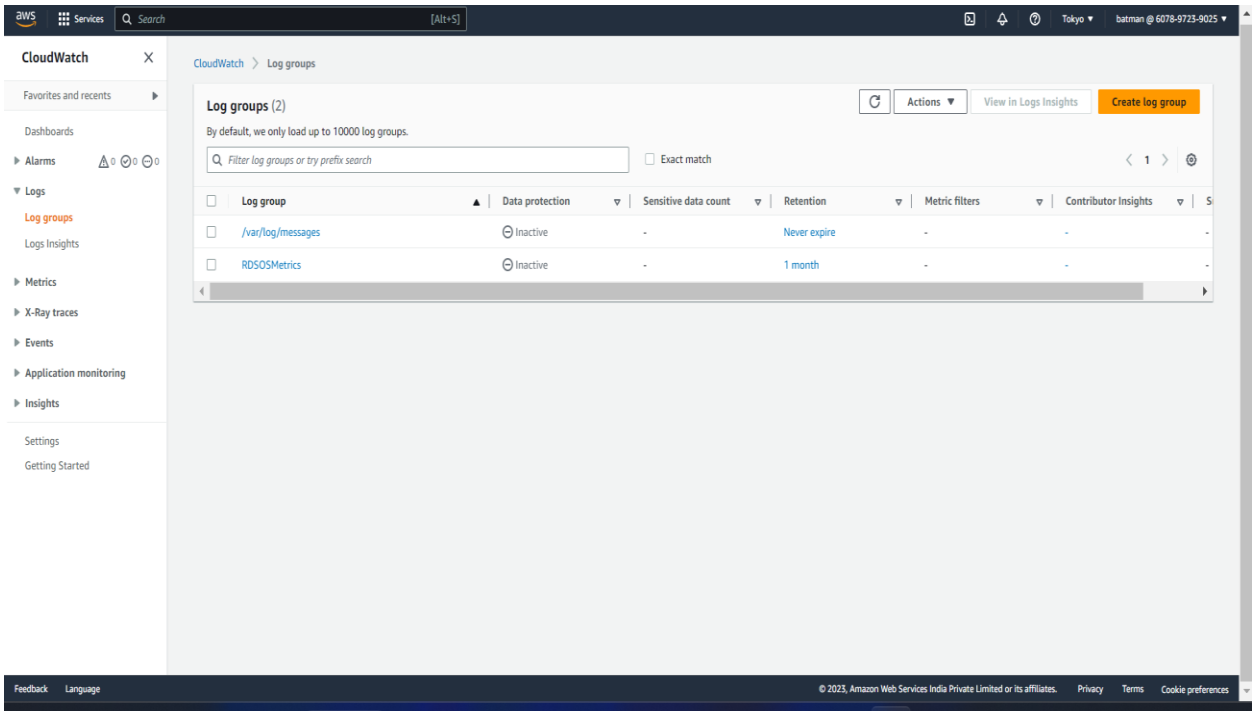
- **Attach the IAM Role to the EC2 instance**



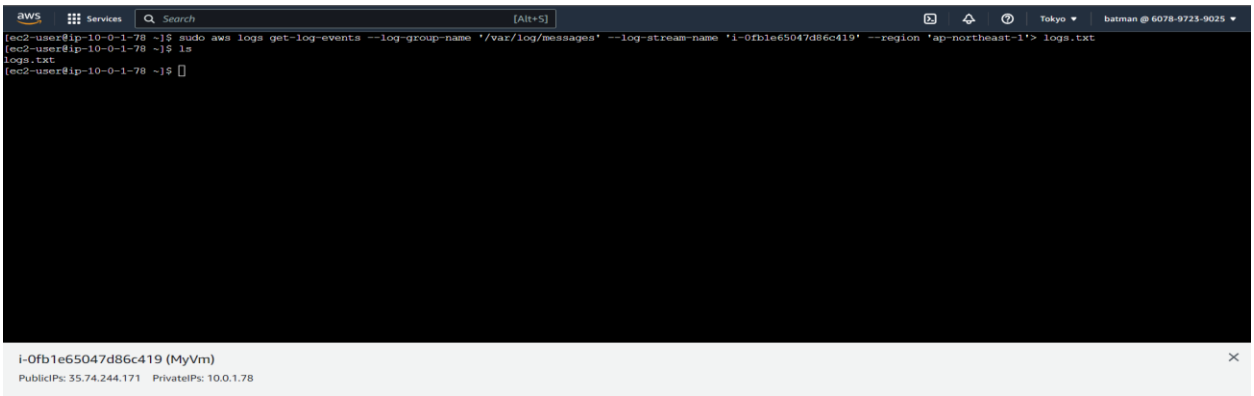
- **Installing Cloudwatch agent on Ec2 using the below command:**
    - **sudo yum update -y**
    - **sudo yum install -y awslogs**
    - **Edit the region on the following path:**
        - `Vi /etc/awslogs/awscli.conf`
    - **sudo systemctl start awslogsd**
    - **sudo systemctl enable awslogsd.service**



- **Now we see newly created log group and log stream in the CloudWatch console after the agent has been running for a few moments**



- **Command to store the logs from cloudwatch into the Logs.txt file**
    - *sudo aws logs get-log-events --log-group-name '/var/log/messages' --log-stream-name 'i-0fb1e65047d86c419' --region 'ap-northeast-1'> logs.txt*



Note:
While getting error of access denied to get the logs from cloudwatch. So modified the IAM role and added "logs:getLogEvents" in the policys so the role can get the details