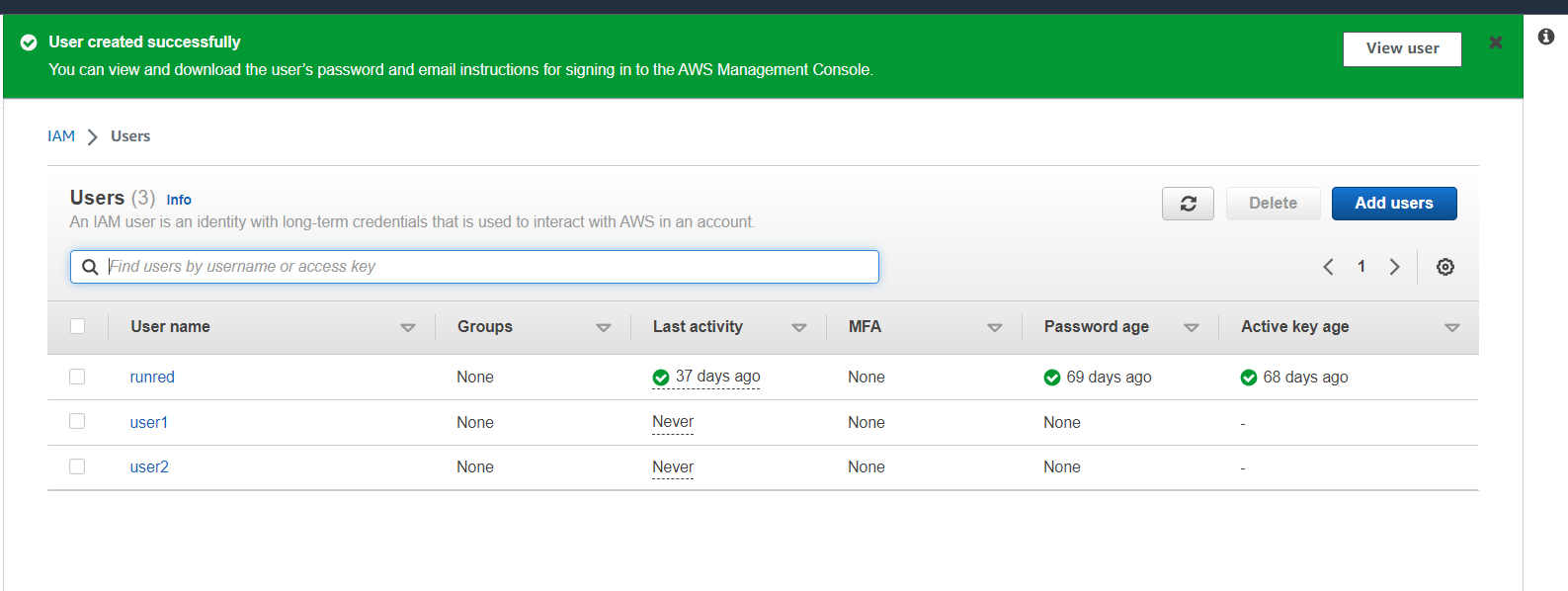
**TASK – 1**

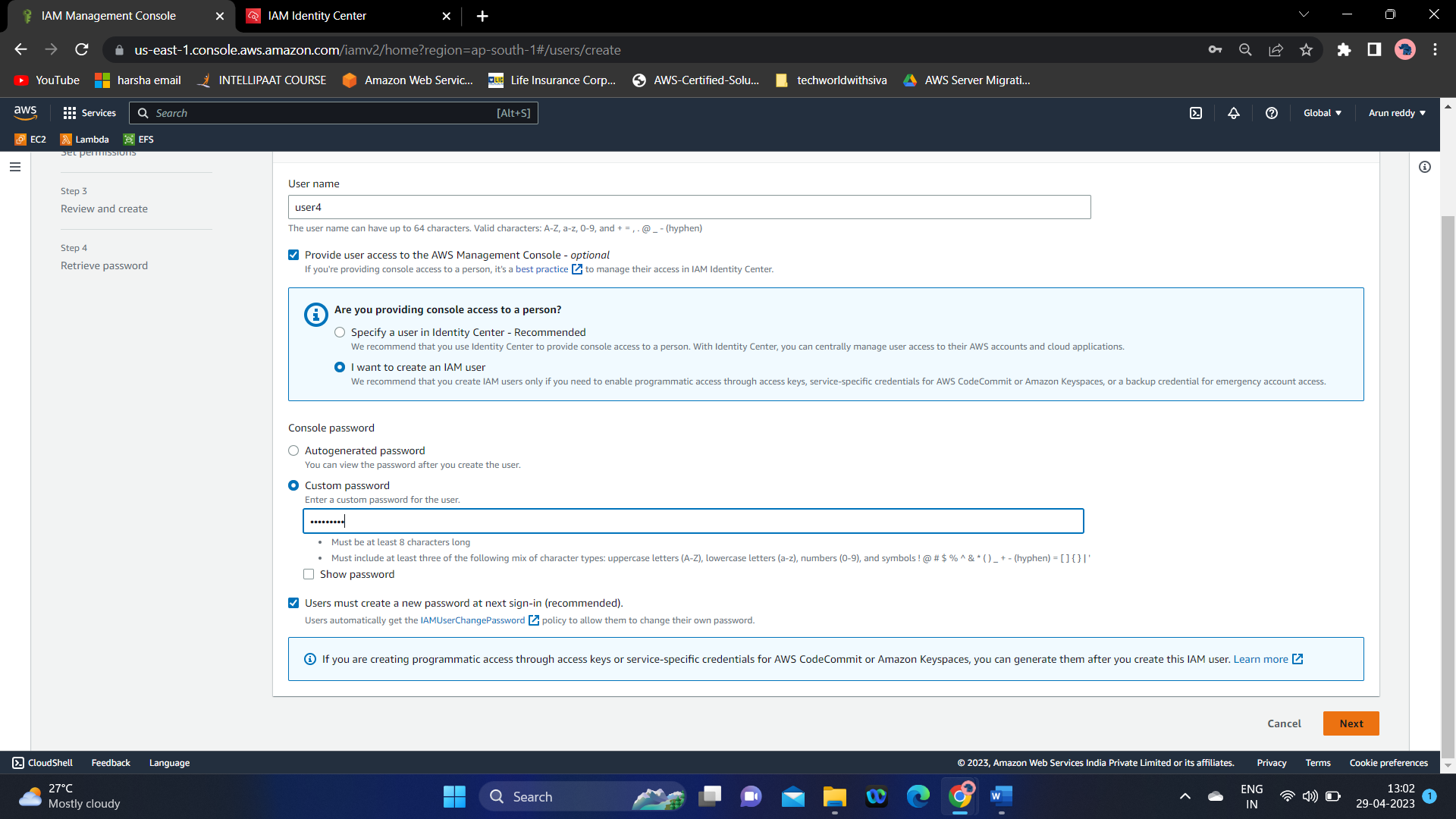
**1. Create a 4 IAM users name “user1”, “user2”, “user3”, and “user4”**

Create 4 users named user1, user2, user3, user

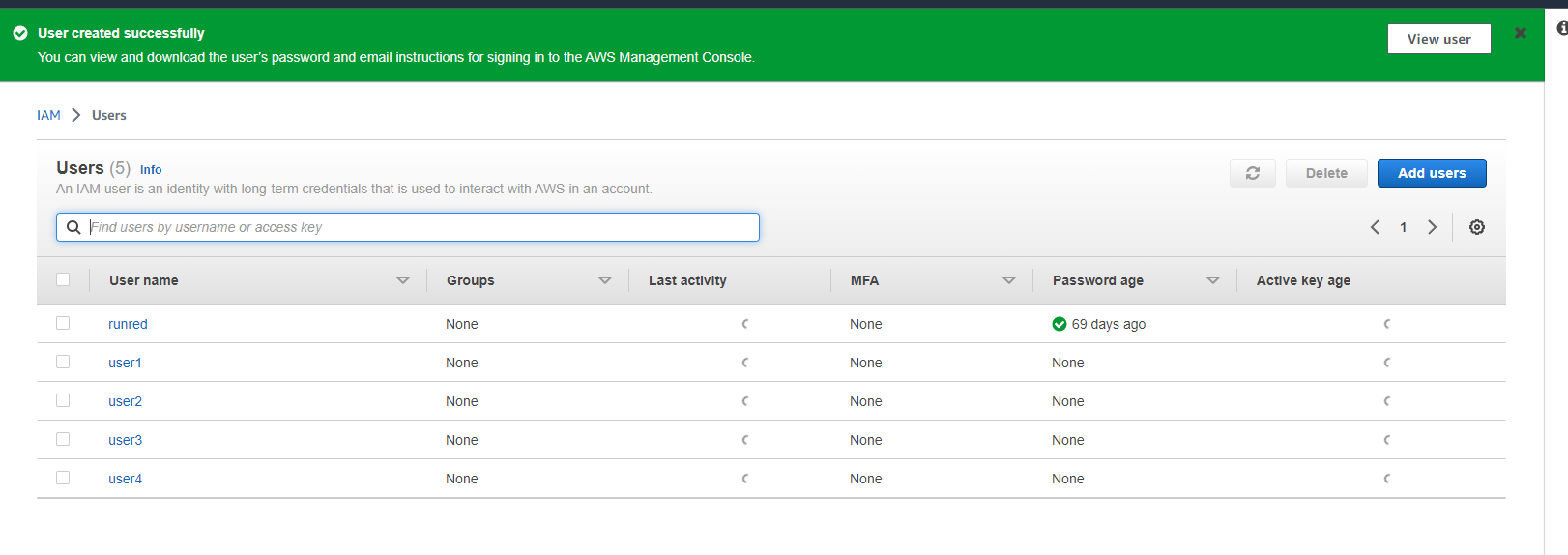




By clicking on the add users you can give the details and create users

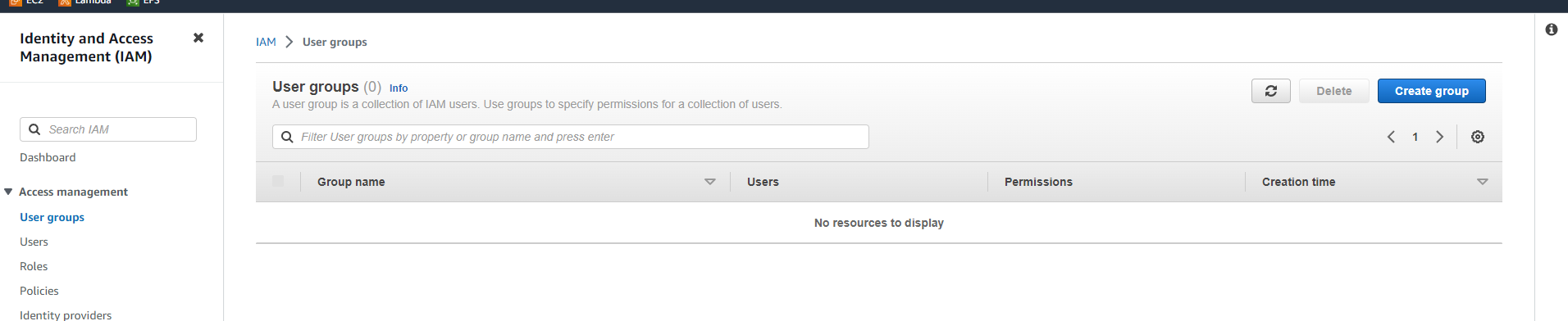


Users created



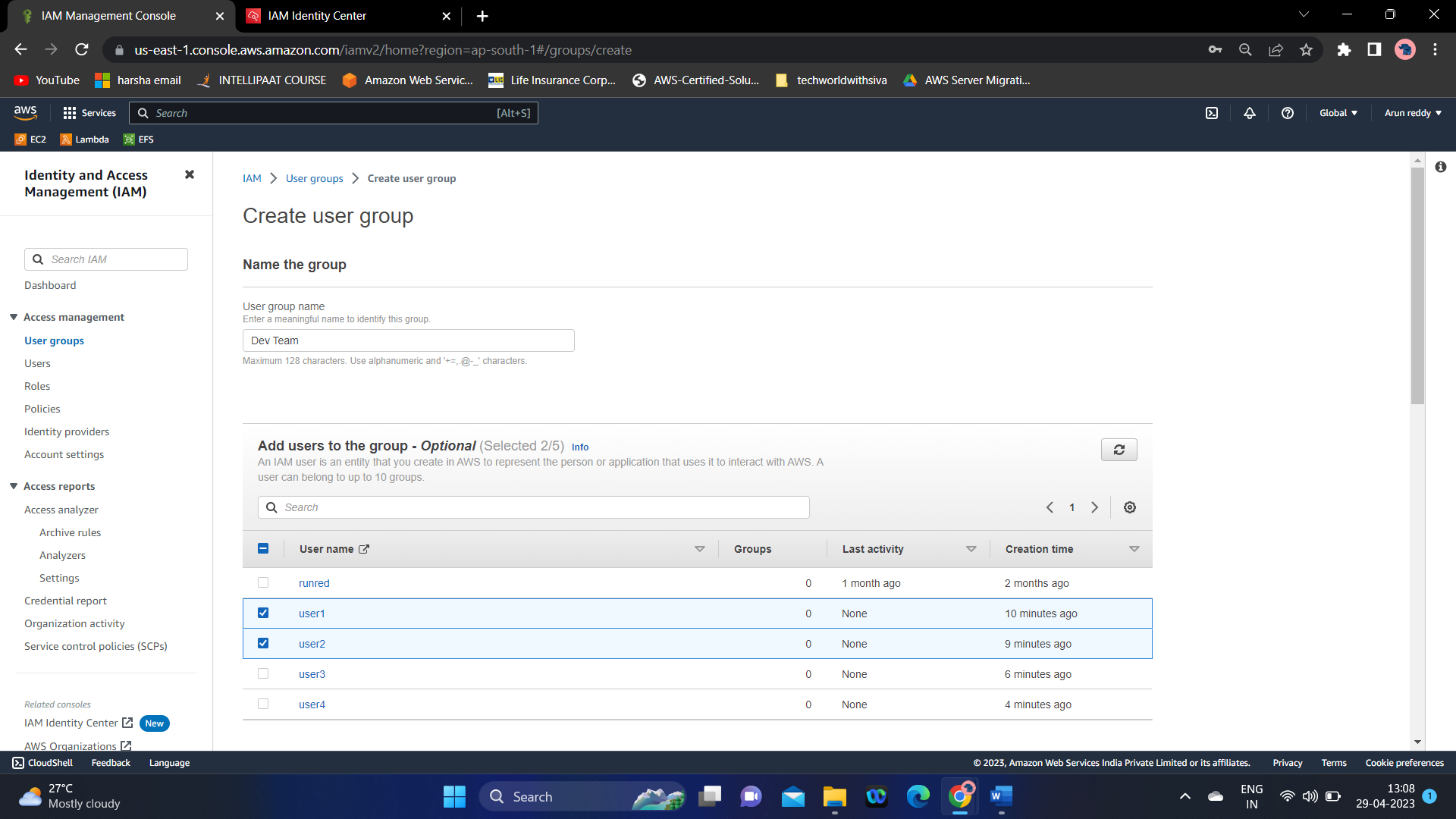
**2. Create 2 Groups named “Dev Team” and “Ops Team”**

In user groups section click on Create Group

****

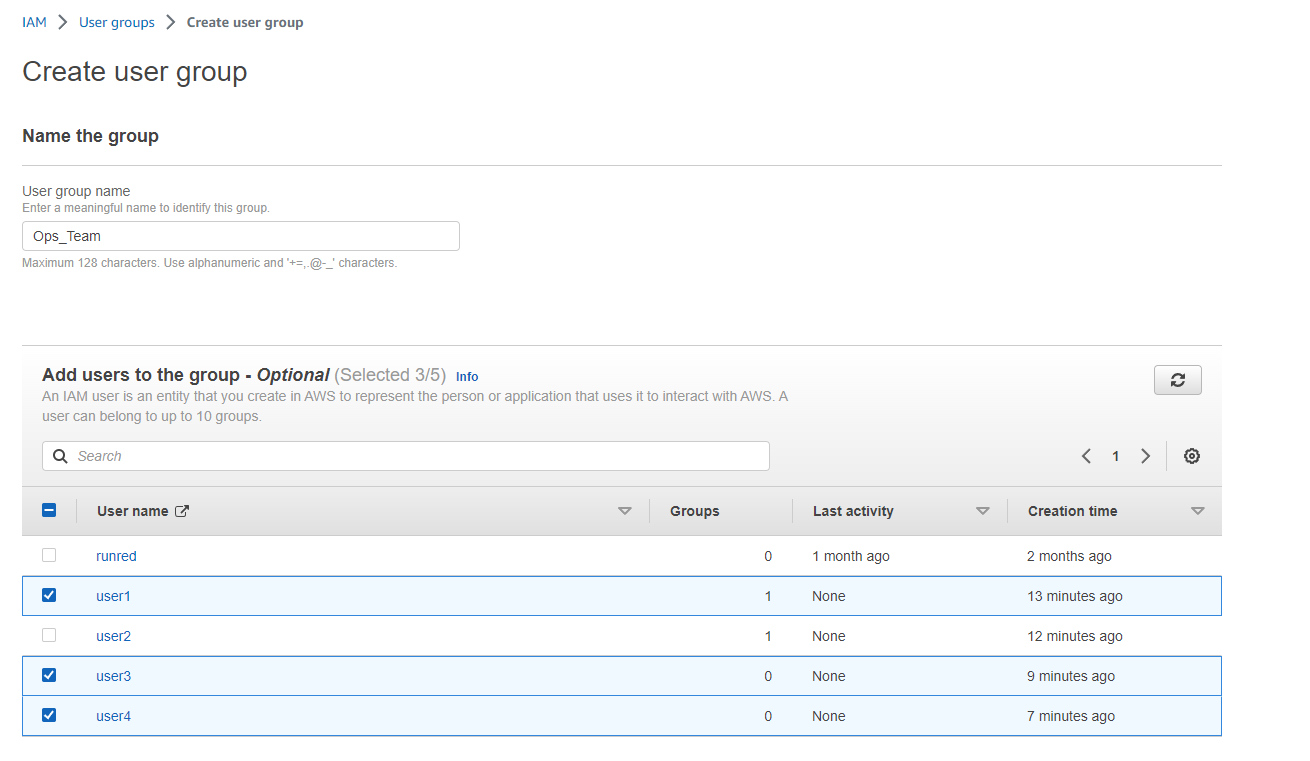
**3. Add user1 and user2 to the Dev Team**

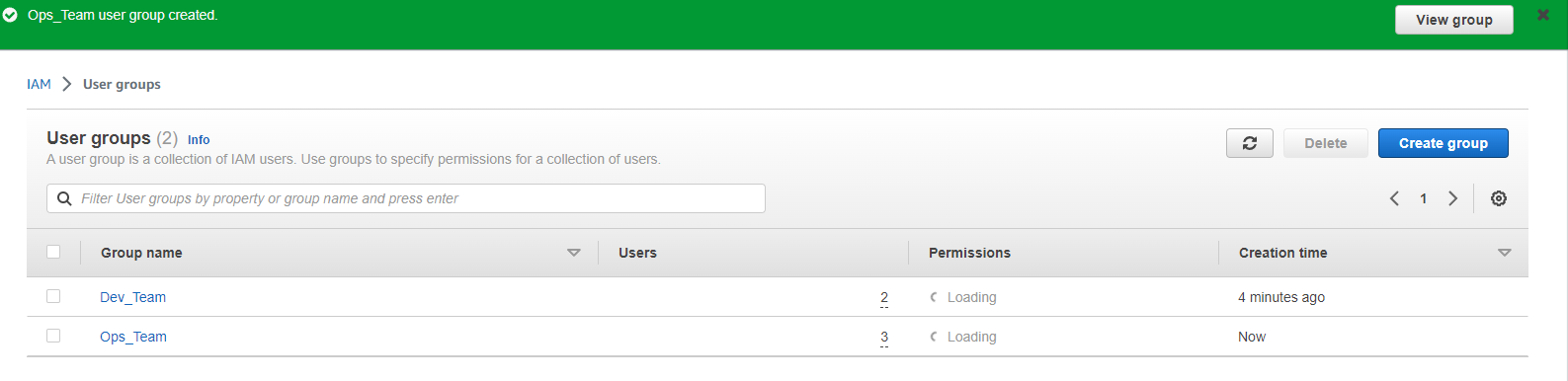
Select user1 and user2 to add to this group

****

**4. Add user1, user3 and user4 to the Ops team**

Select User1, user3, user4 to add in this group

****

****

**TASK – 1 COMPLETED.**

**TASK – 2**

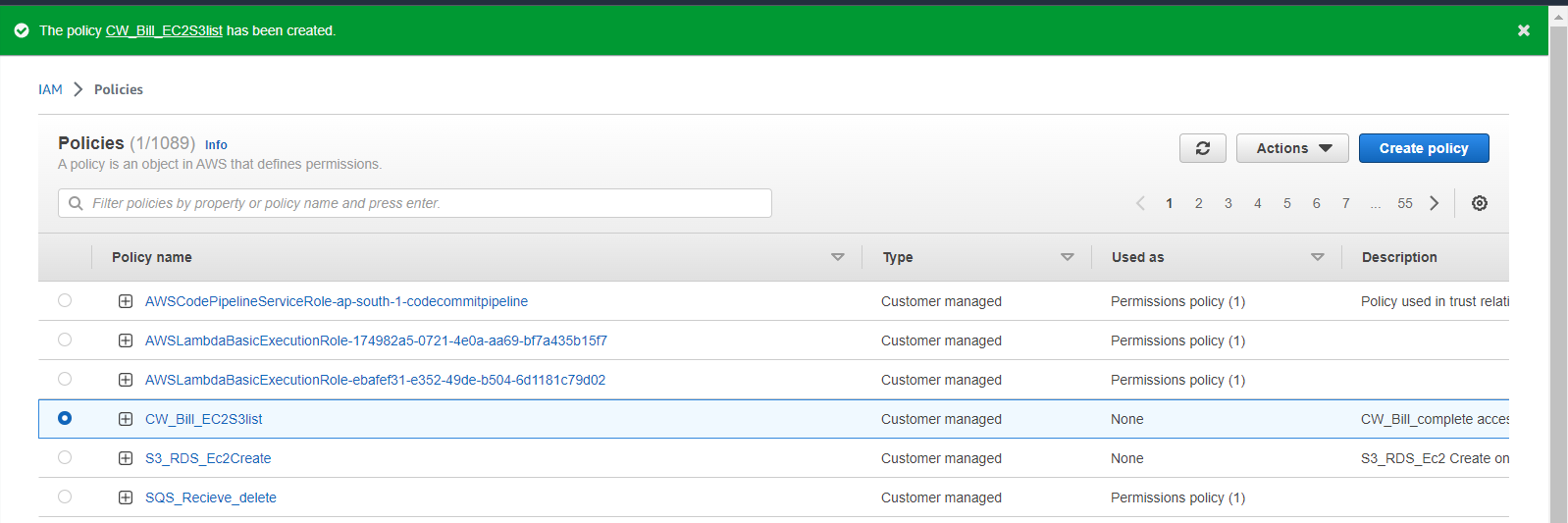
1. Create a policy number 1 which lets the users to:

* Access S3 completely
* Only create EC2 instances
* And full access to RDS
* {
* "Version": "2012-10-17",
* "Statement": [
* {
* "Sid": "AllowS3Access",
* "Effect": "Allow",
* "Action": "s3:\*",
* "Resource": "\*"
* },
* {
* "Sid": "AllowEC2Access",
* "Effect": "Allow",
* "Action": [
* "ec2:RunInstances",
* "ec2:DescribeInstances",
* "ec2:DescribeImages",
* "ec2:DescribeKeyPairs",
* "ec2:DescribeSecurityGroups",
* "ec2:CreateSecurityGroup",
* "ec2:AuthorizeSecurityGroupIngress",
* "ec2:CreateTags"
* ],
* "Resource": "\*"
* },
* {
* "Sid": "AllowRDSAccess",
* "Effect": "Allow",
* "Action": [
* "rds:\*"
* ],
* "Resource": "\*"
* }
* ]
* }

2. Create a policy number 2 which allows the users to:

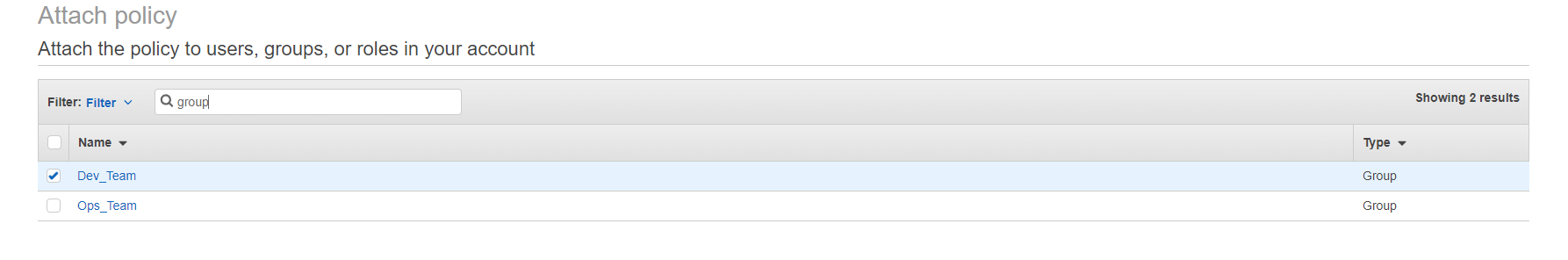
* Access CloudWatch and Billing completely
* And can only list EC2 and S3 resources
* {
* "Version": "2012-10-17",
* "Statement": [
* {
* "Sid": "AllowCloudWatchAndBillingAccess",
* "Effect": "Allow",
* "Action": [
* "cloudwatch:\*",
* "aws-portal:\*"
* ],
* "Resource": "\*"
* },
* {
* "Sid": "AllowListEC2AndS3",
* "Effect": "Allow",
* "Action": [
* "ec2:Describe\*",
* "s3:List\*"
* ],
* "Resource": "\*"
* }
* ]
* }

Created both the policies



3. Attach policy number 1 to Dev Team from task 1

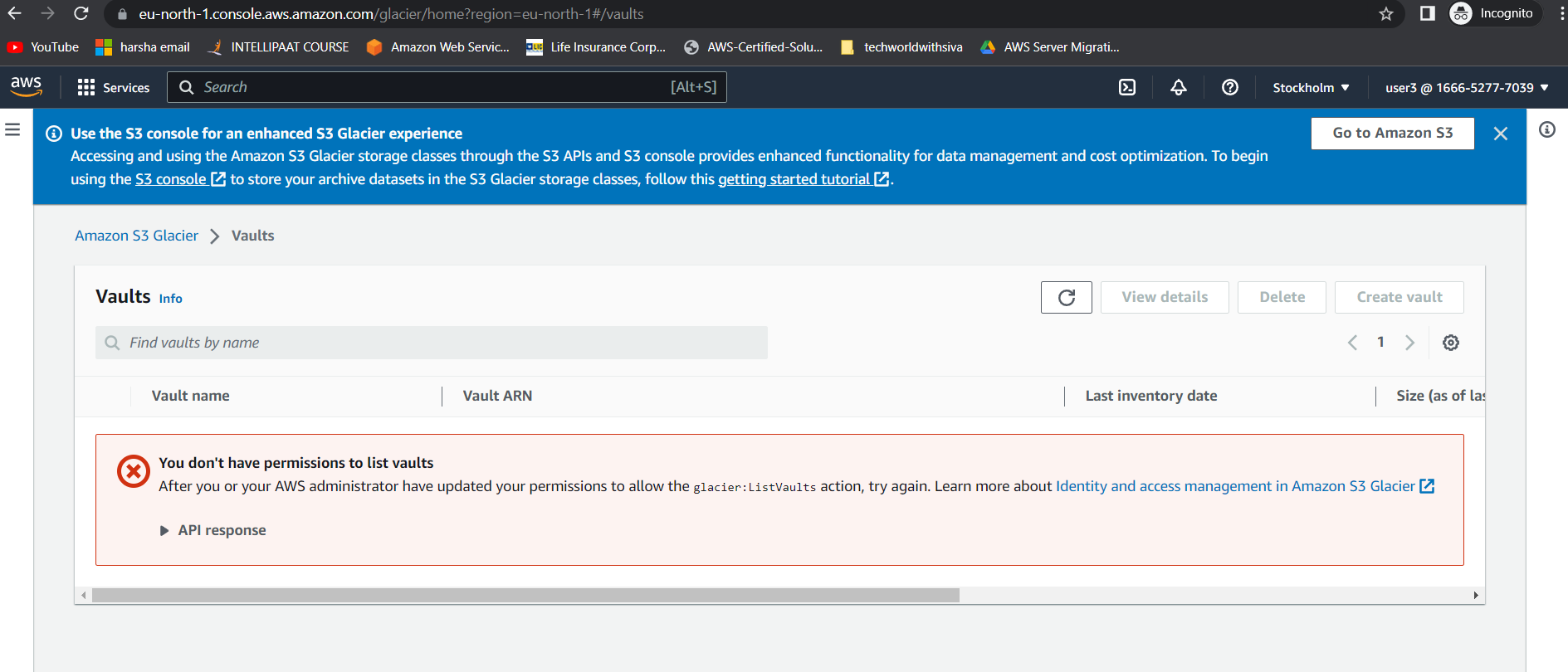
In Action from policies select Attah policy option



4. Attach policy number 2 to Ops Team form task 1

Follow the same steps from above to attch the policy2 to Ops\_team group

Login to user3 and check the S3glacier access, which we don’t have access





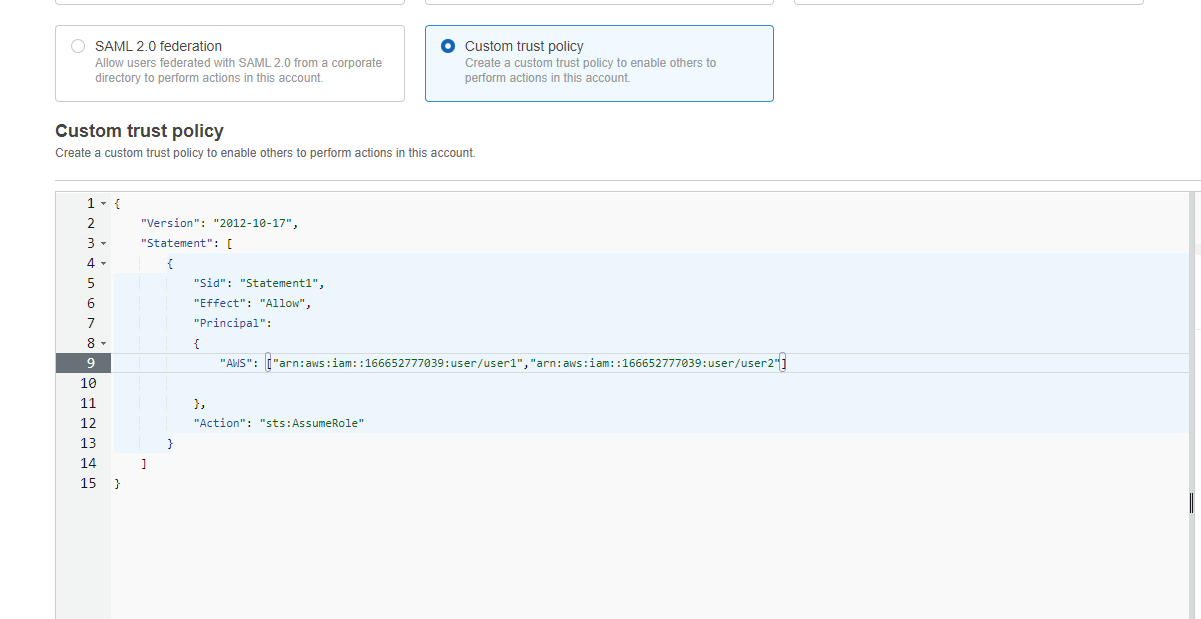
**Task-2 is completed.**

**TASK – 3**

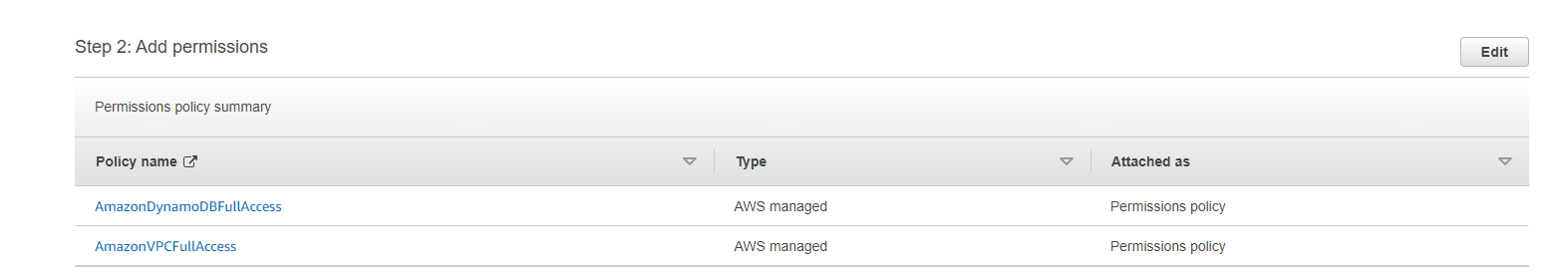
**1. Create a Role which only lets user1 and user2 from task 1 to have complete access to VPCs and DynamoDB**

**2. Login into user1 and shift to the role to test out the feature**

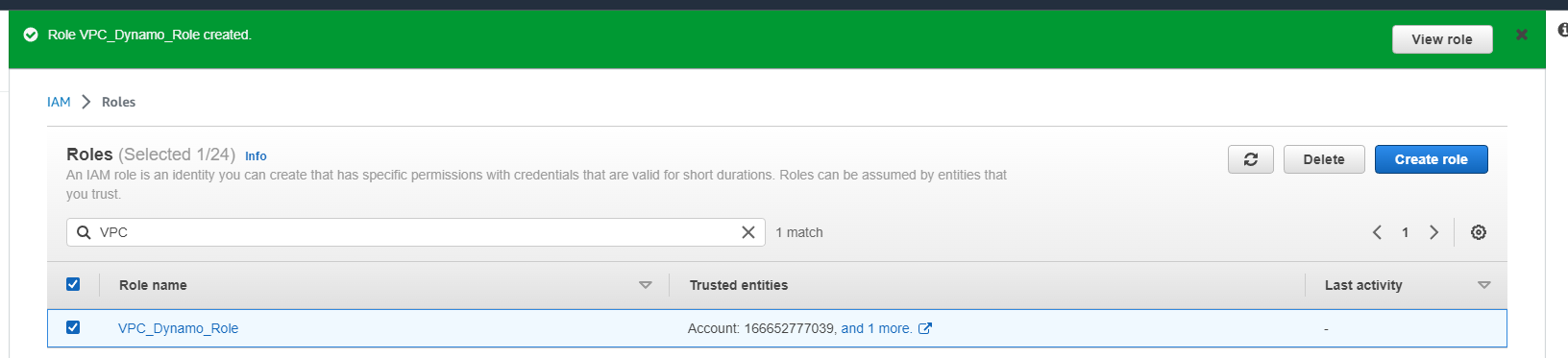
Create a custom trust policy in create role



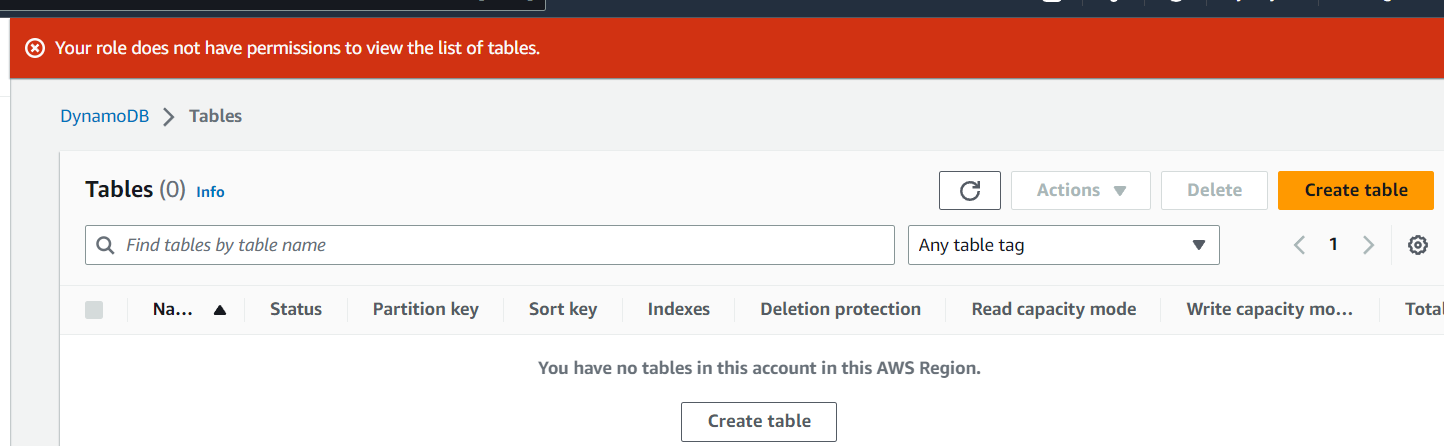
Add VPC and DynamoDb Full access to the role



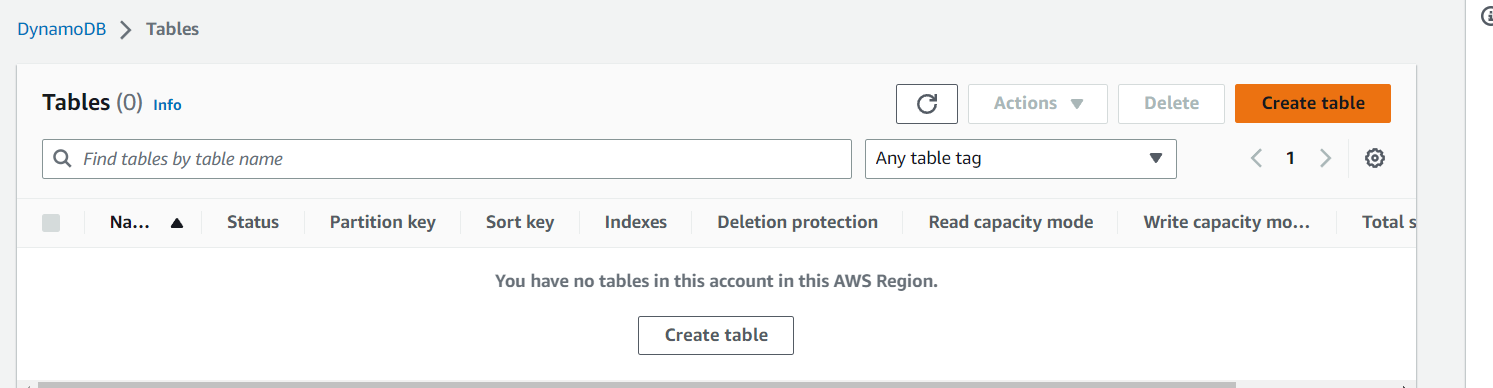
Role Created successfully.



Unable to access DynamoDb tables with User1 as we still did not switched to role , to acces the policies in role, we need to switch to user role



Able to create Tables in DynamoDb with the use of switch role

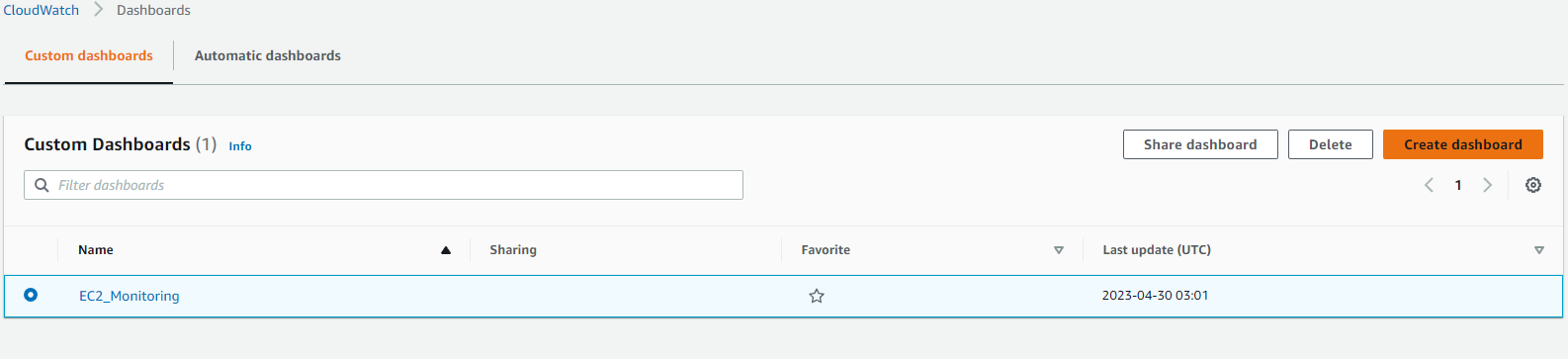


**Task – 3 Completed.**

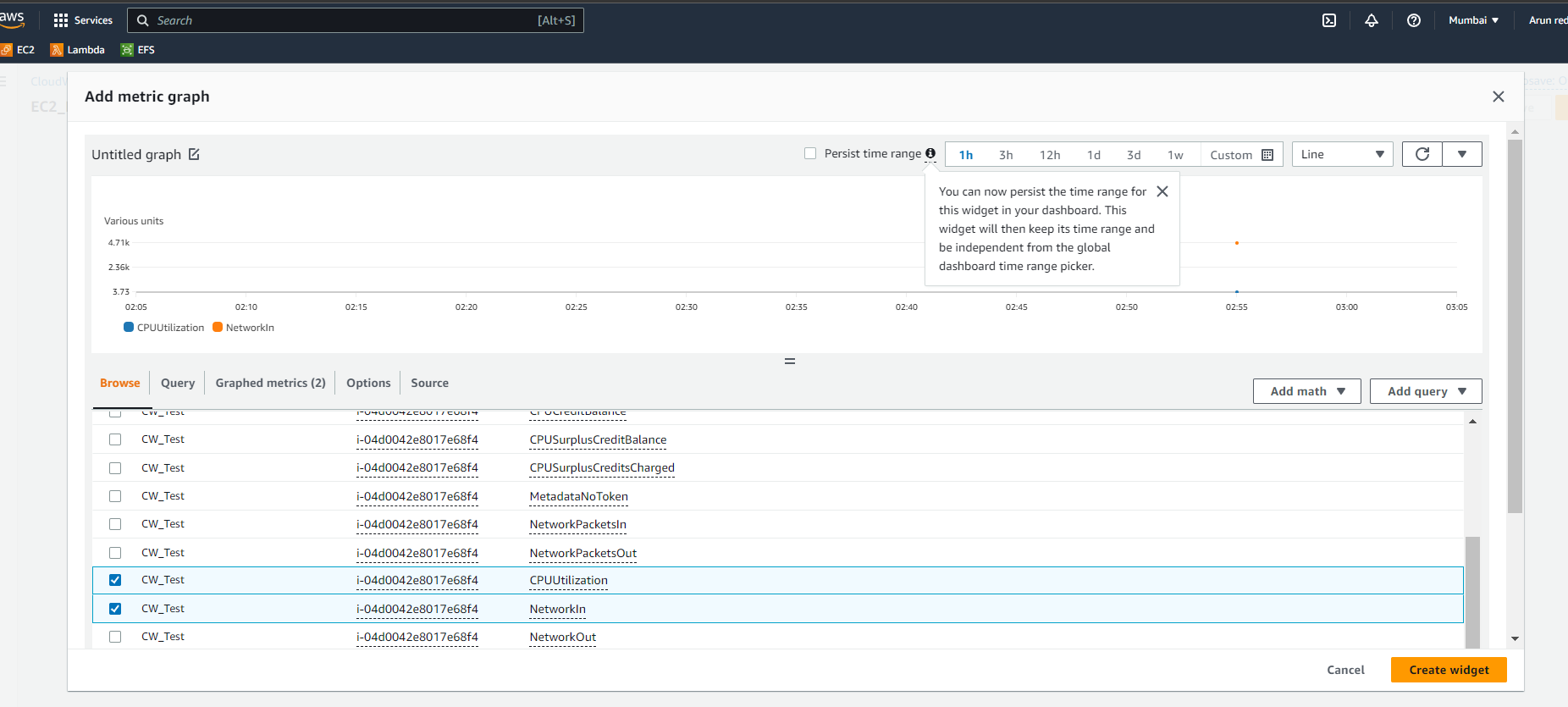
**Task-4**

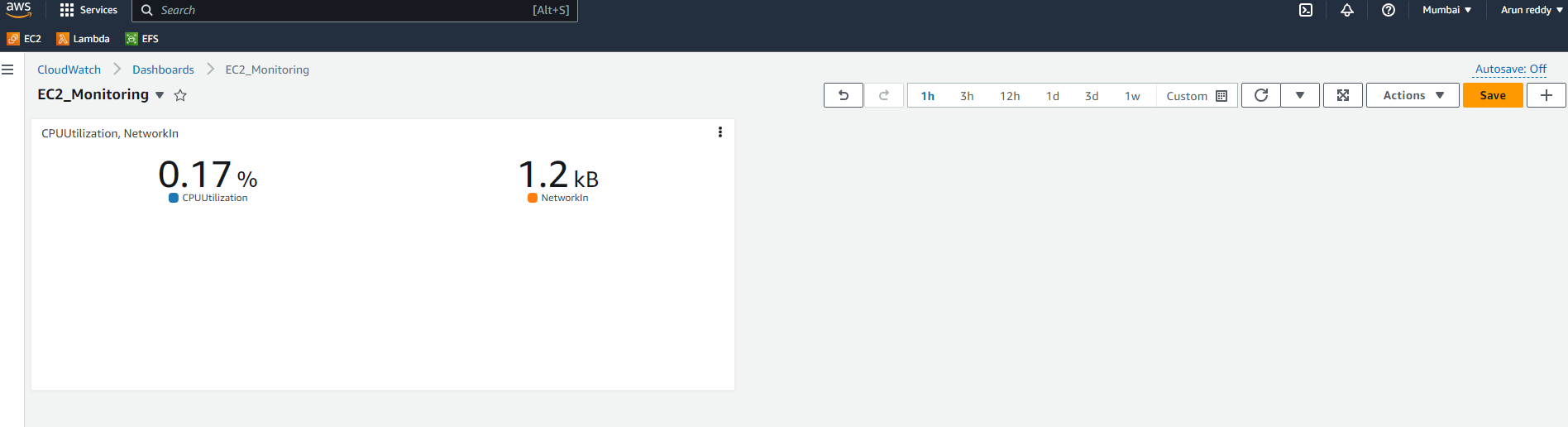
**1. Create a dashboard which lets to check the CPU Utilization and NetworkIn for a particular EC2 instance**

* Create an EC2 instance
* Copy the instance id**(**[i-04d0042e8017e68f4](https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#InstanceDetails:instanceId=i-04d0042e8017e68f4))
* Create Dashborad for Ec2 instance monitoring



* Add metrics for dashboard, Select CPU Utilization and NetworkIn and Create Widget.



****

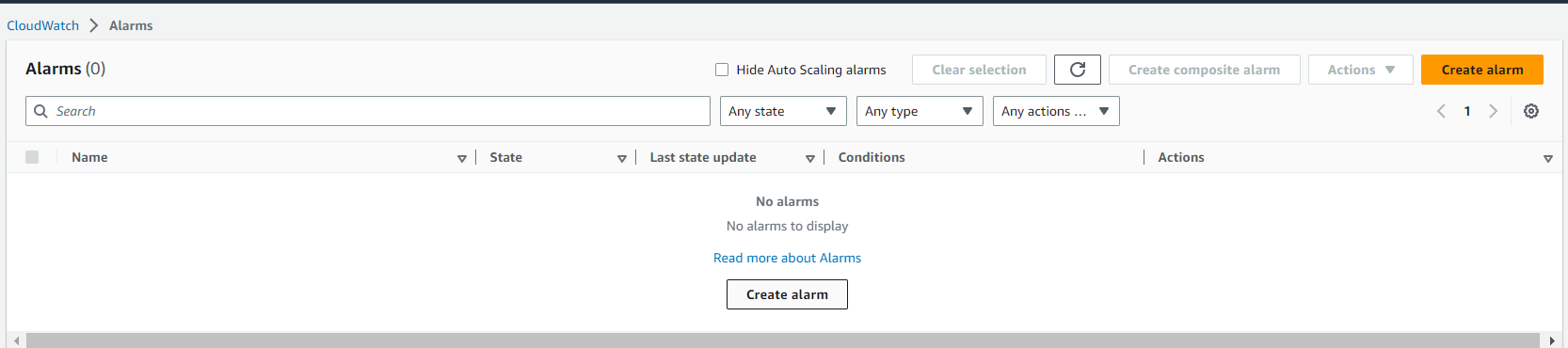
**Dashboard is created Successfully.**

**TASK – 5**

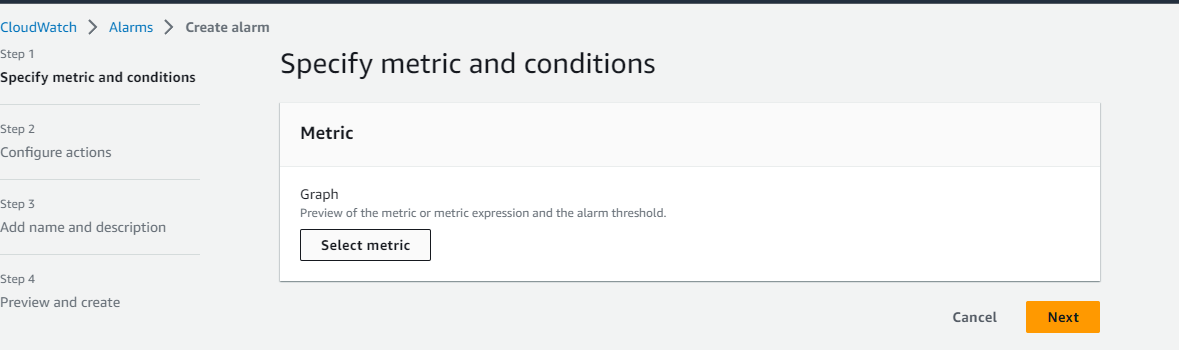
**1. Create a CloudWatch Billing Alarm which goes off when the Estimated Charges goes above 500$**

**Note: For Billing Alarm we cannot create in Any other region except N.Virginia as it is the major data centre of AWS**

* Create an alarm in Cloud watch Alarms

****

* Select metric

****

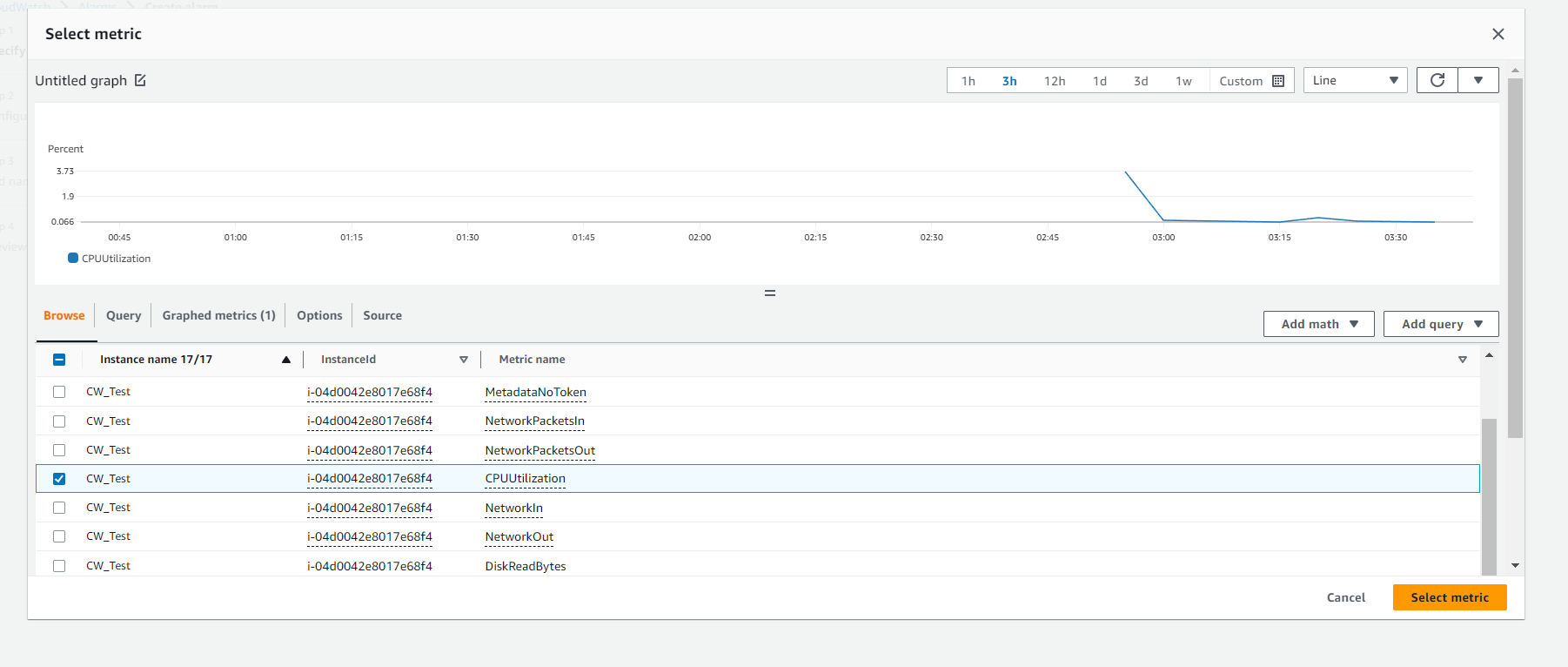
**Now give the threshold value as > 500 usd for billing.**

**Alarm is created successfully.**

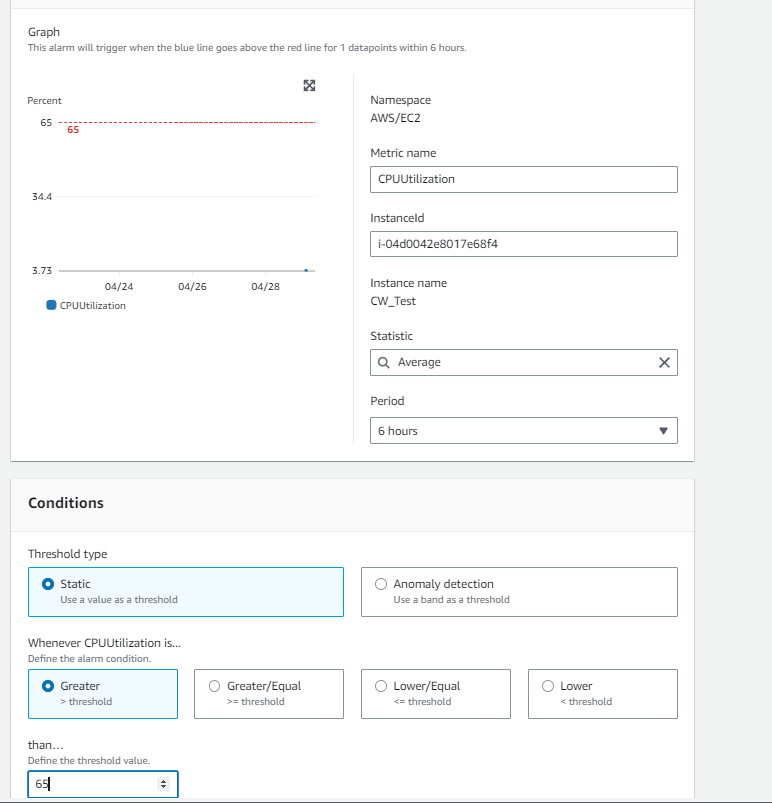
**2. Create a CloudWatch Alarm which goes off to an Alarm state when the CPU utilization of an EC2 instance goes above 65%**

**a. Also add an SNS topic so it notifies the person when the threshold is crossed**

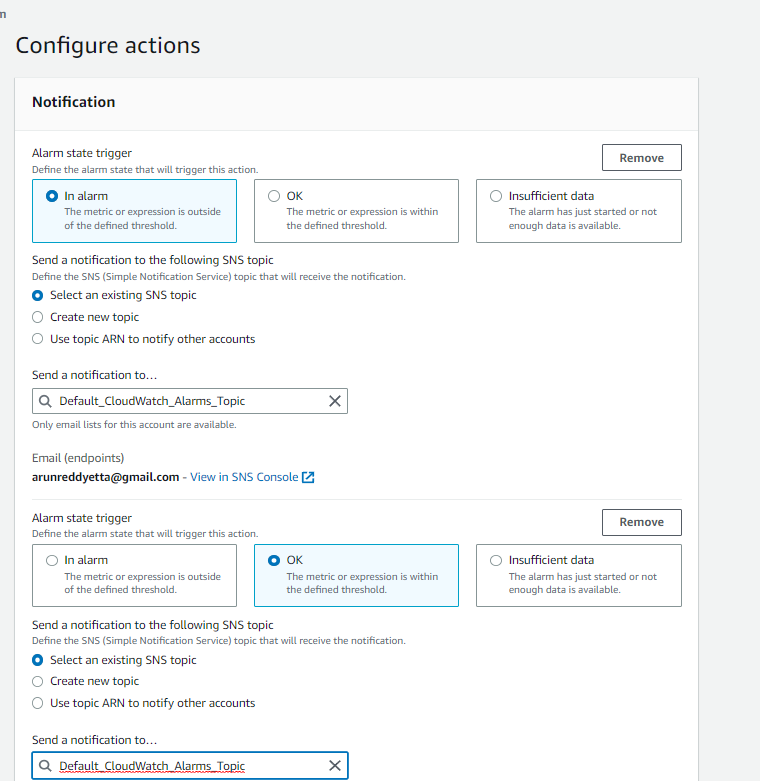
* Create another alarm
* Select metric as Ec2 instance 🡪 Cpu utilization

****

* Give the threshold value as 65% for cpu utilization

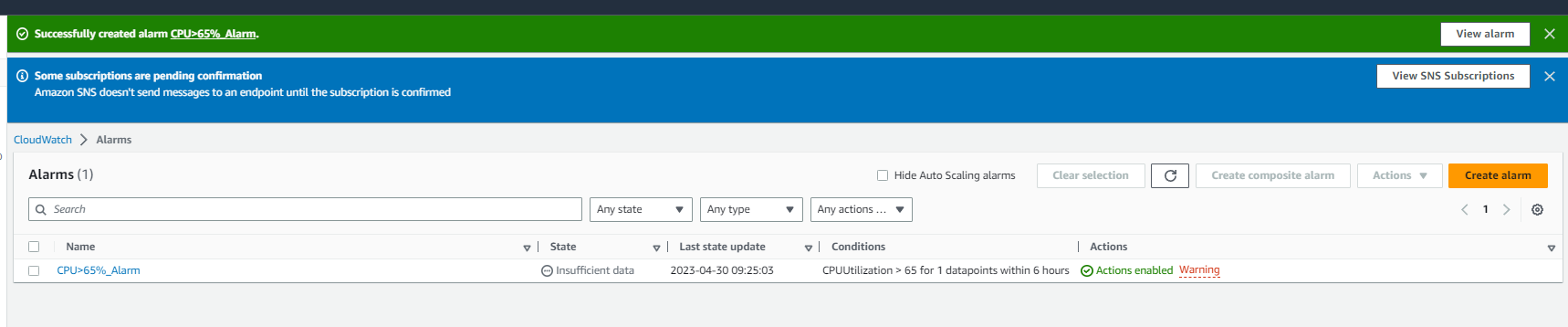
****

* Create a new SNS topic to send notification when the Alarm reaches threshold

****

**Alarm is created successufully , but the subscription is to be confirmed to send notification .**

**Confirm the subscription in the email and it is completed.**

****

**Task - 5 Completed.**