CloudTrail

What is CloudTrail?

Aws cloud trail is a web service that records Aws API calls for your account and deliver the log files to you.

Recorded information will have:

1. Identity of API caller.

2. Time of API caller.

3. The source of IP address of API call

4. The request parameters

5. The response elements return by Aws services.

CloudTrail is enabled on your AWS account when you create it. When activity occurs in your AWS account, that activity is recorded in a CloudTrail event. You can easily view events in the CloudTrail console by going to **Event history**.

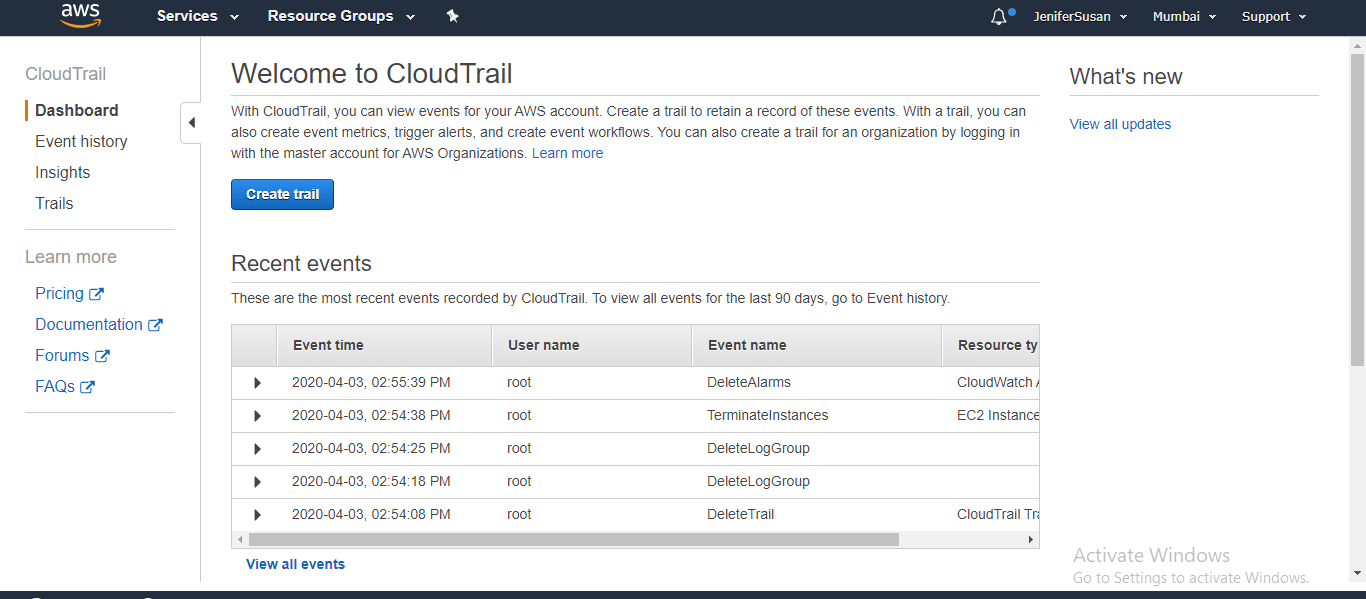
Event history allows you to view, search, and download the past 90 days of activity in your AWS account. In addition, you can create a CloudTrail trail to archive, analyze, and respond to changes in your AWS resources. A trail is a configuration that enables delivery of events to an Amazon S3 bucket that you specify. You can also deliver and analyze events in a trail with Amazon CloudWatch Logs and Amazon CloudWatch Events. You can create a trail with the CloudTrail console, the AWS CLI, or the CloudTrail API.

**Uses &benefits:**

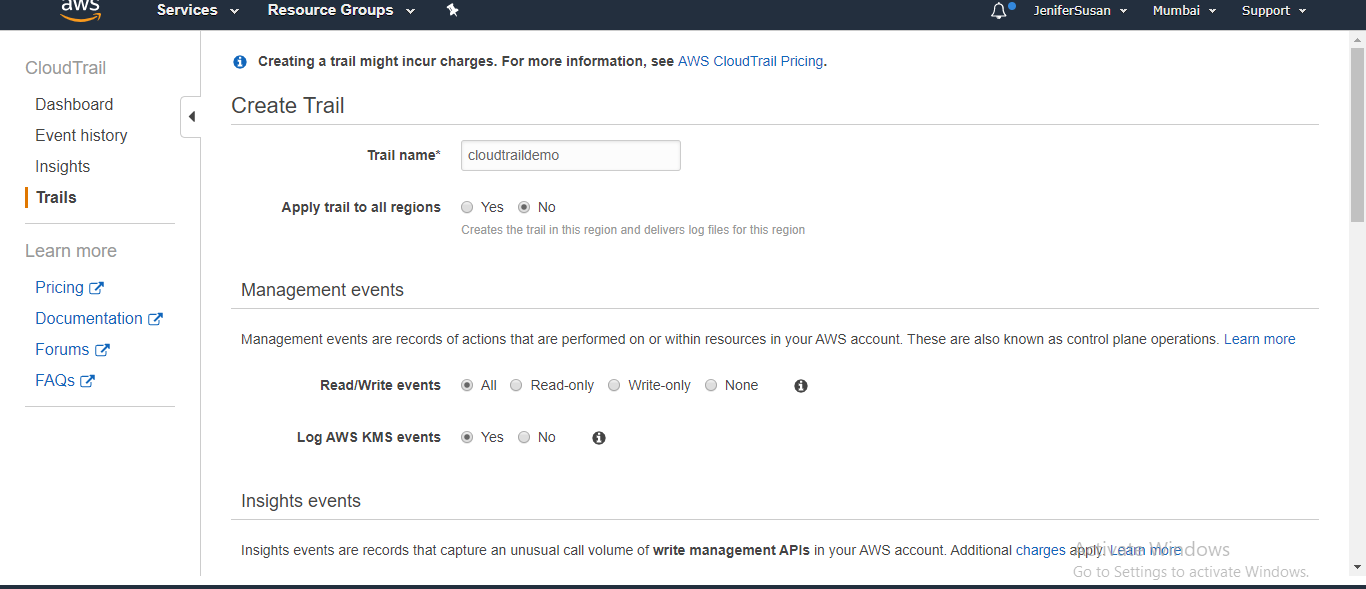
* Increases your visibility what happened in your Aws environment
* Who did what and when from where
* Receive notification of log file delivery using amazon simple notification service (SNS)

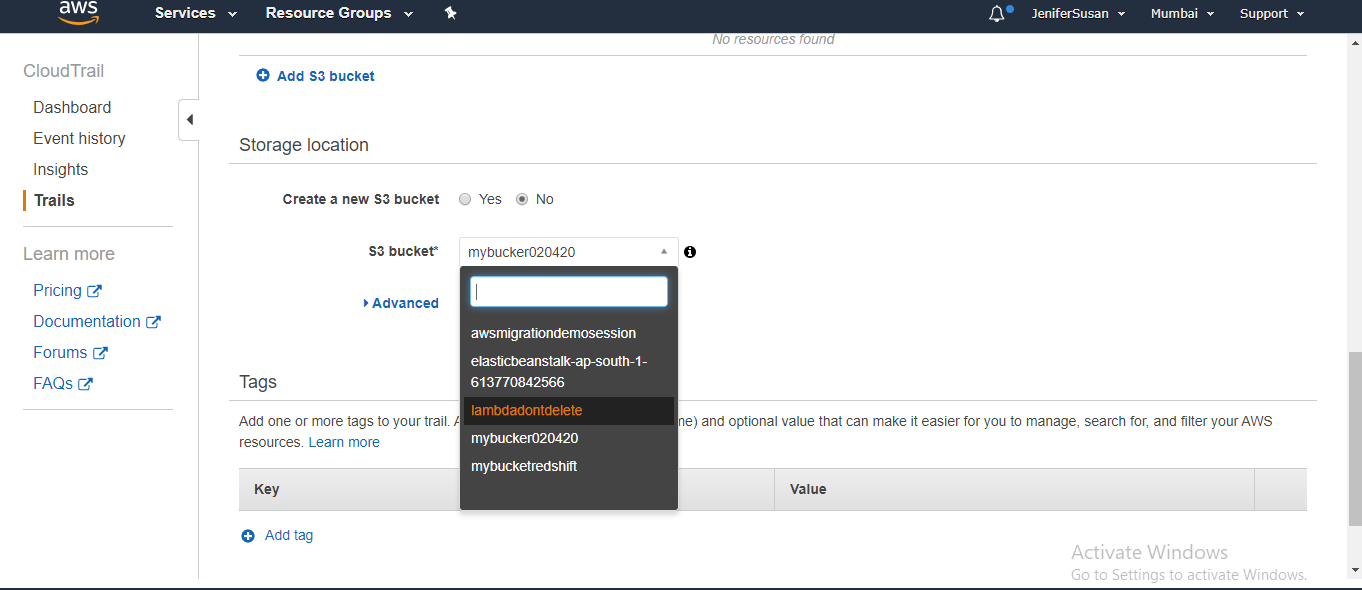
**Steps to create:**

1. Create a cloudtrail name cloudtraildemo.
2. Select a existing bucket or create new bucket where log file has to be sent.
3. Check the specified bucket in S3 console page whether log file folder has been created.
4. Click the cloudtraildemo and configure the cloudwatch where log need to push from cloudtrail to cloudwatch.
5. Configure SNS topic to receive notification.
6. Create a new metric filter for the event and set an alarm by sending notification to SNS.
7. Login to Aws console select the service CloudTrail

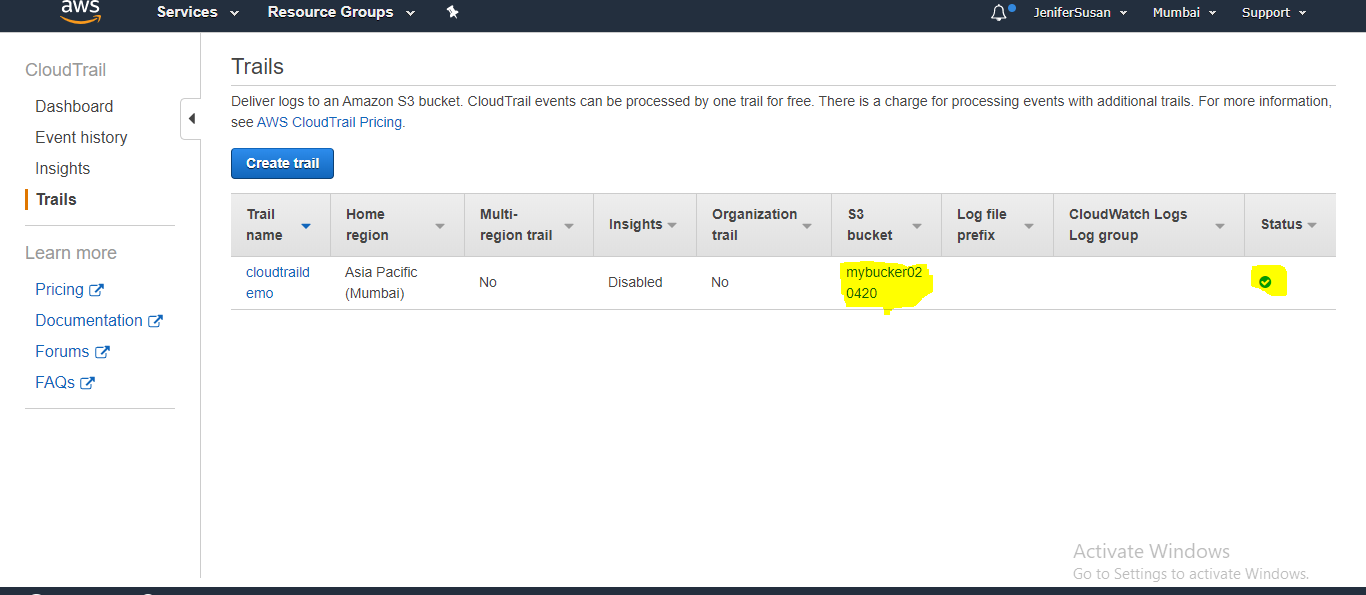


2. Select the option creates cloudTrail and enter the trail name and also select the existing bucket of s3 where log has sent

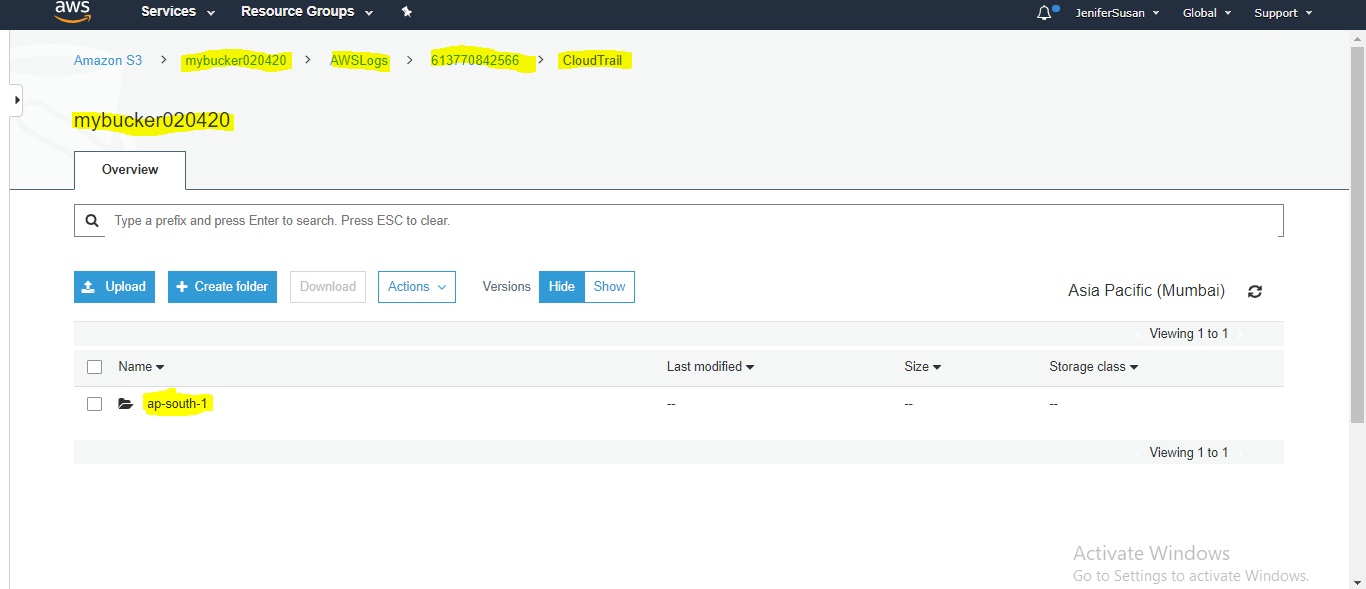




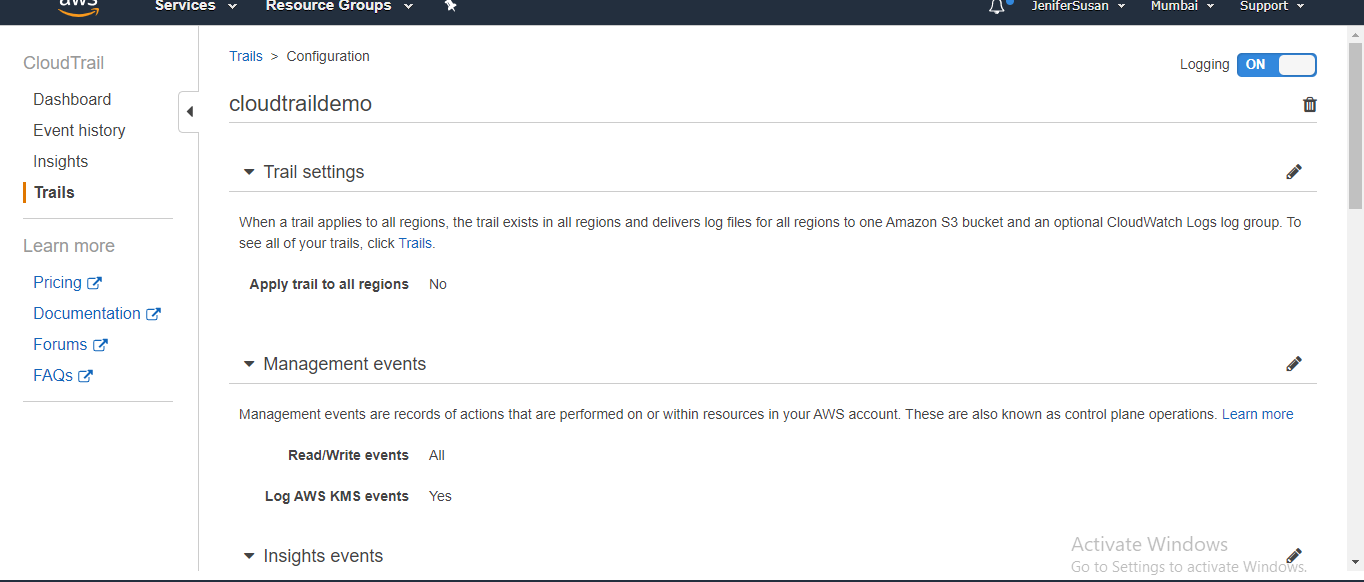
CloudTrail is successfully created

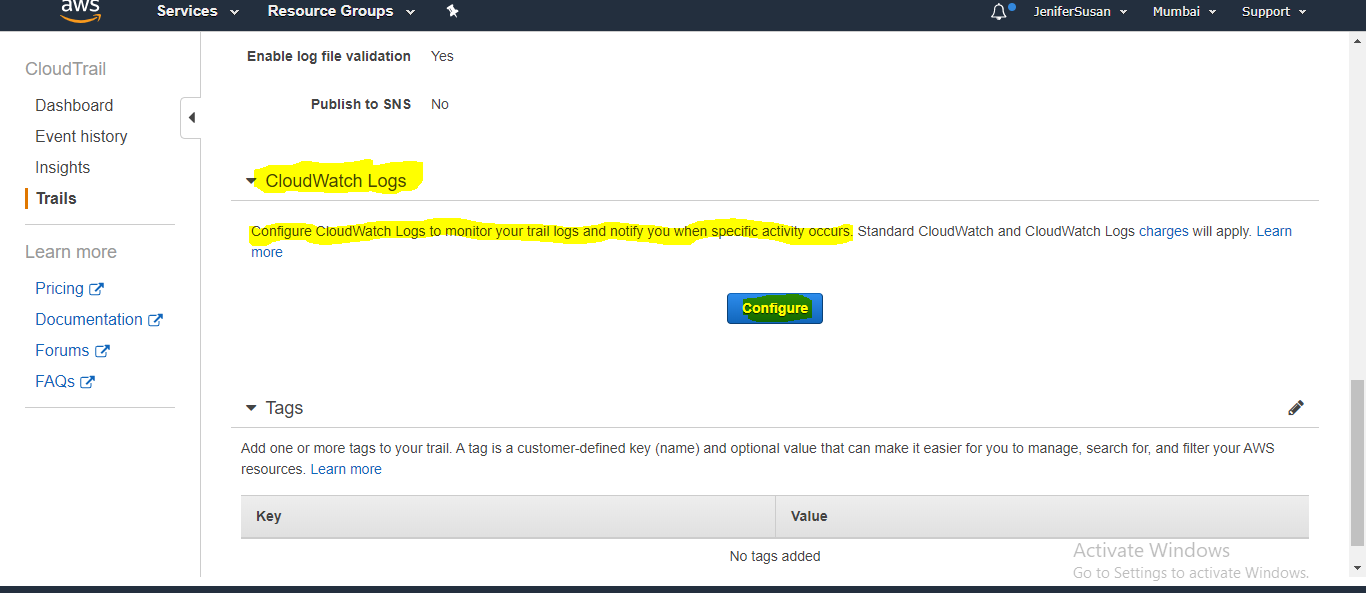


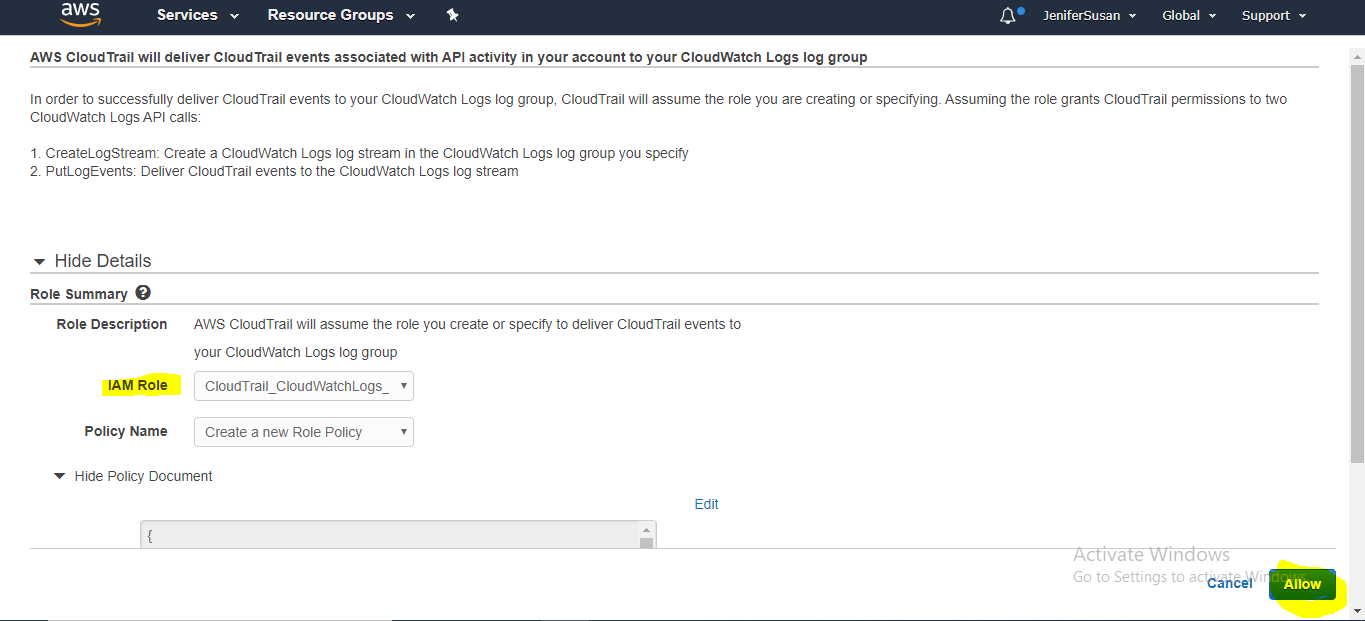
3. Check in s3 bucket which you have created whether log file has been sent or not



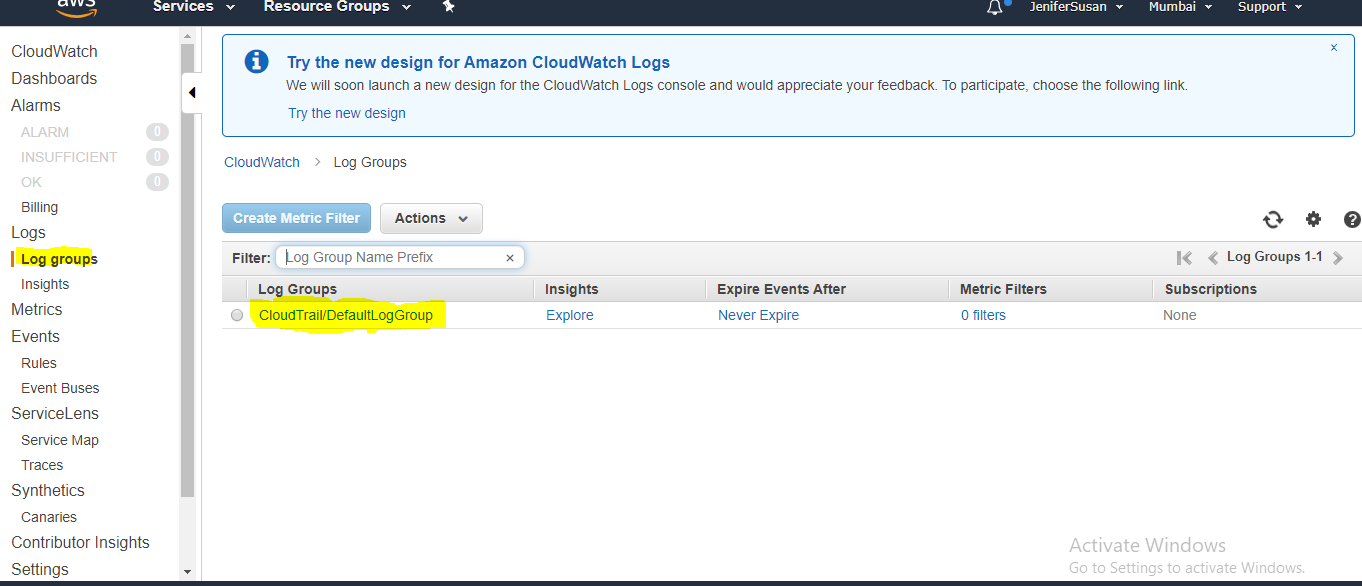
4. Click the cloudtraildemo and configure the cloudwatch where log need to push from cloudtrail to cloudwatch

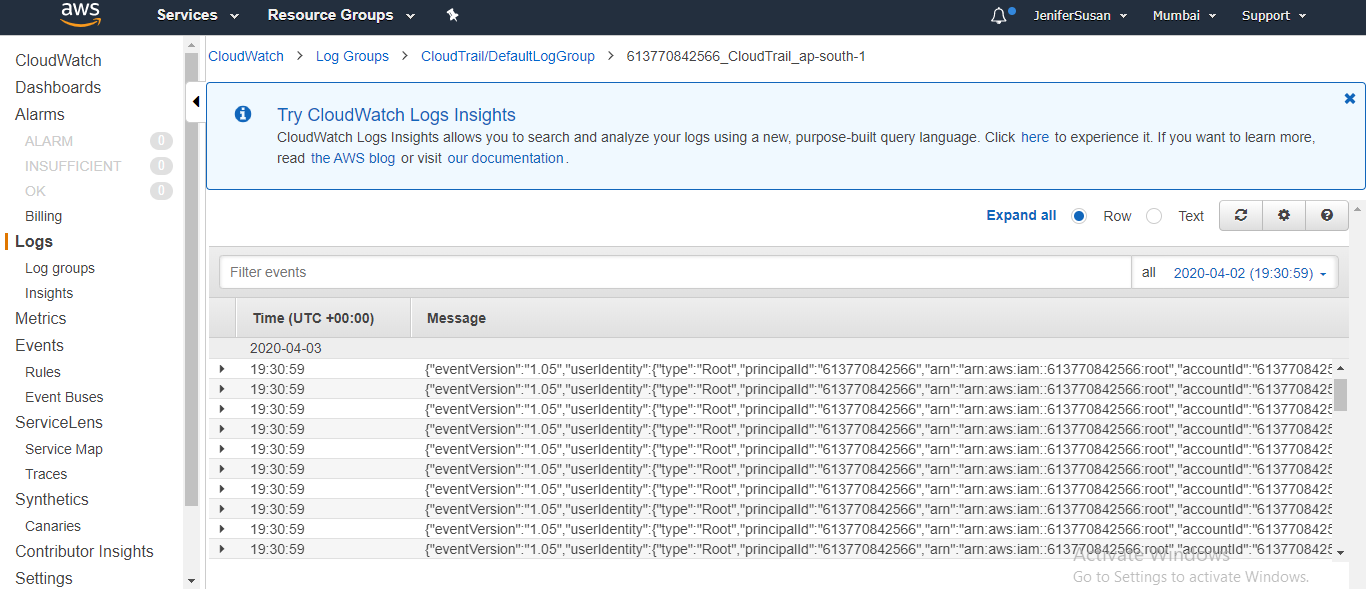




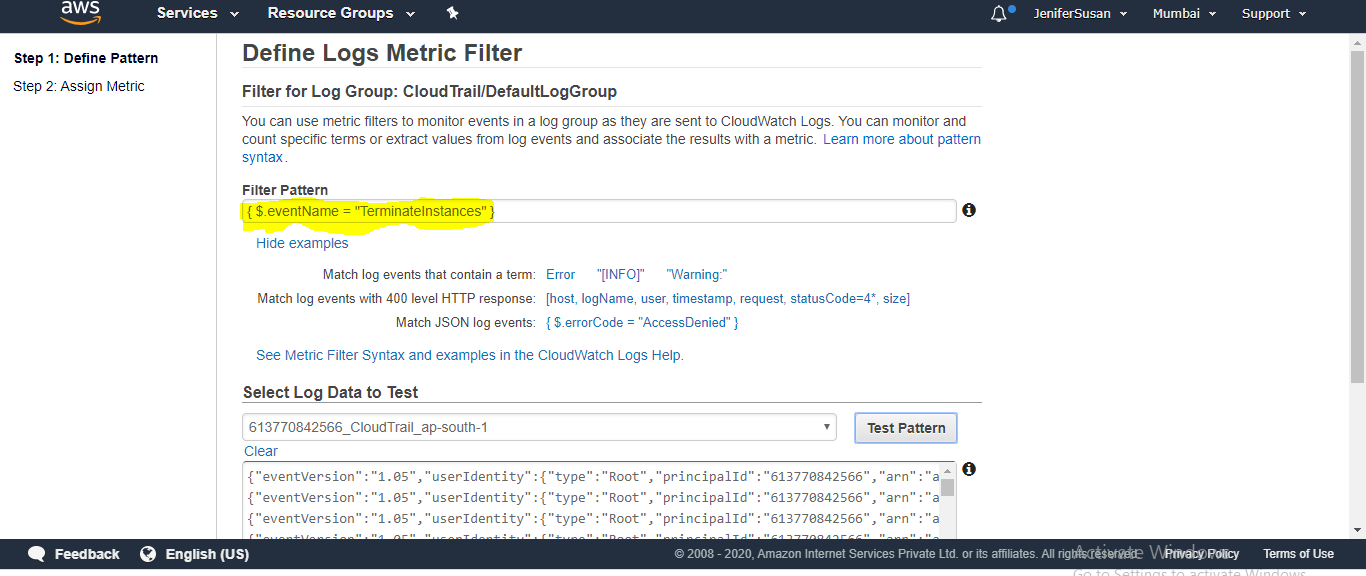


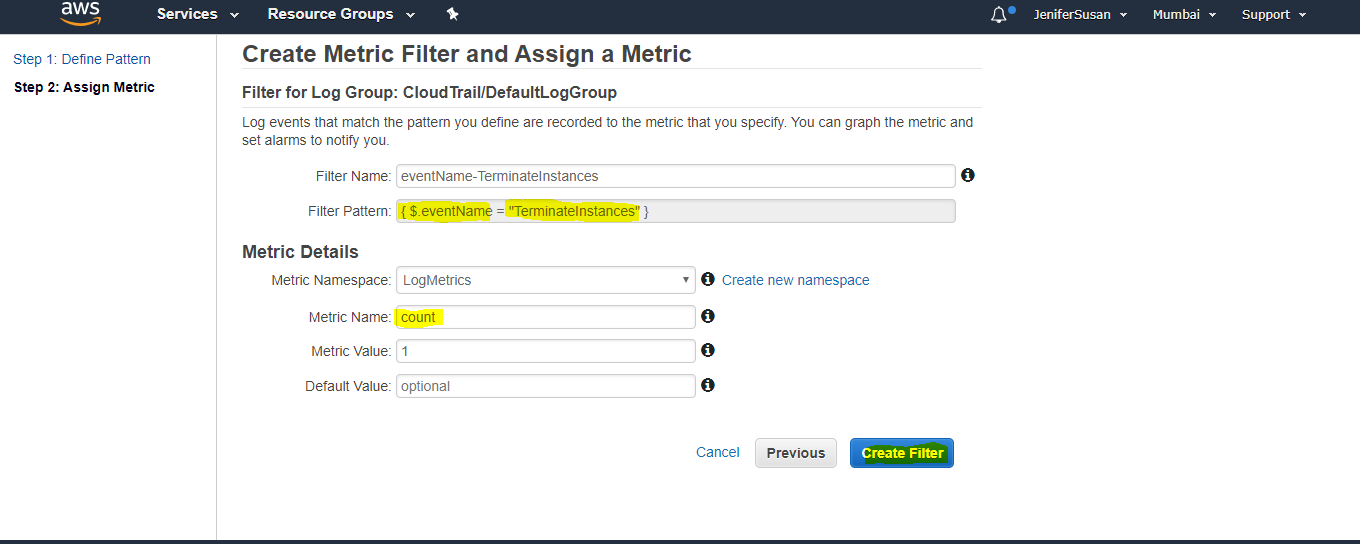
Goto cloudwatch check in log groups

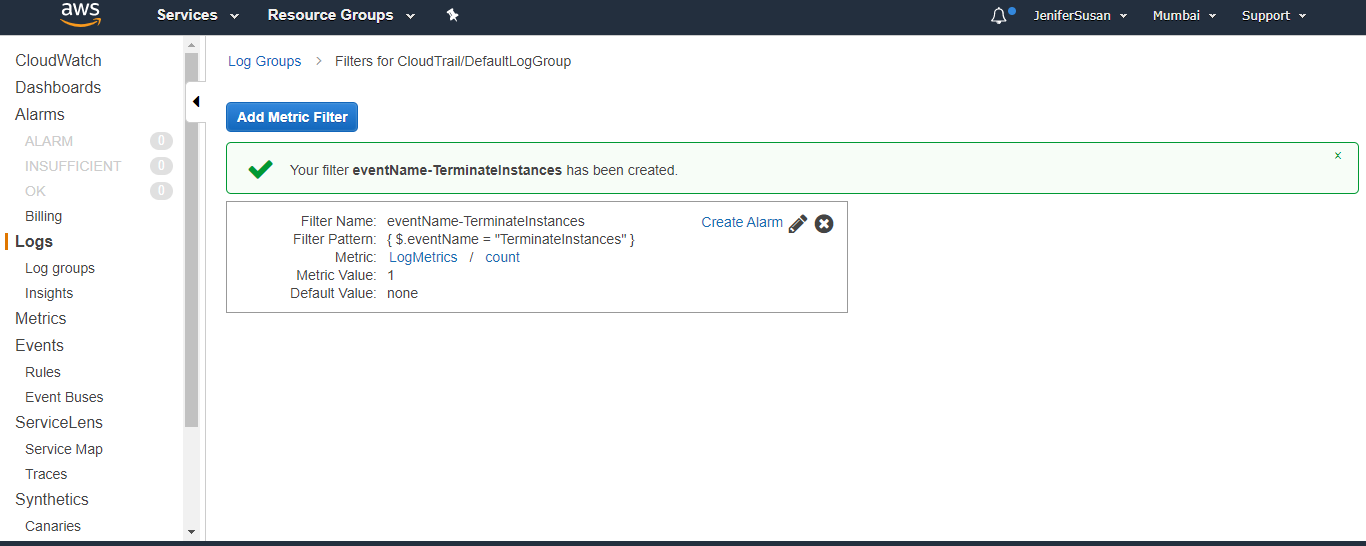




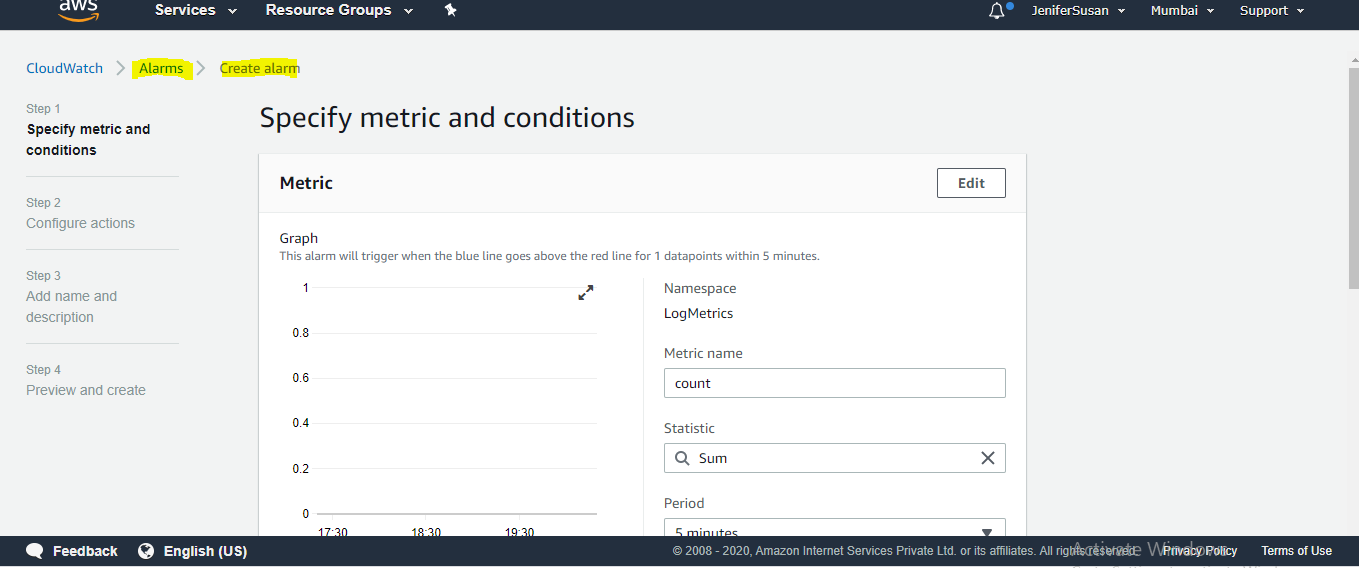
5. Create a new metric filter for the event activity to display the number of count for TerminateInstances

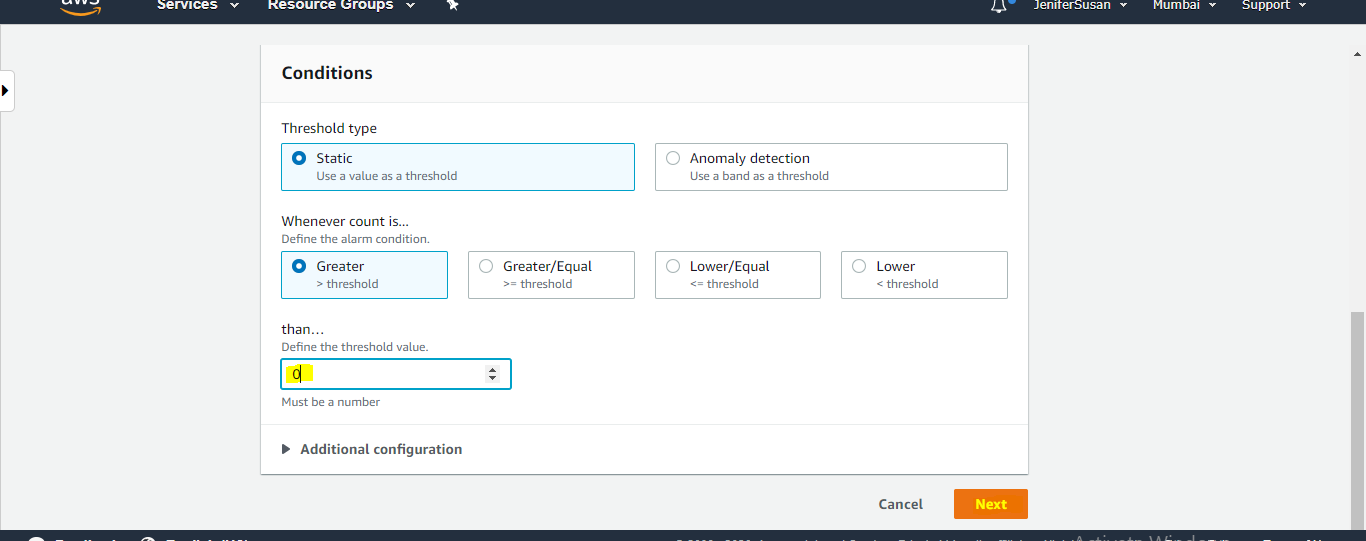




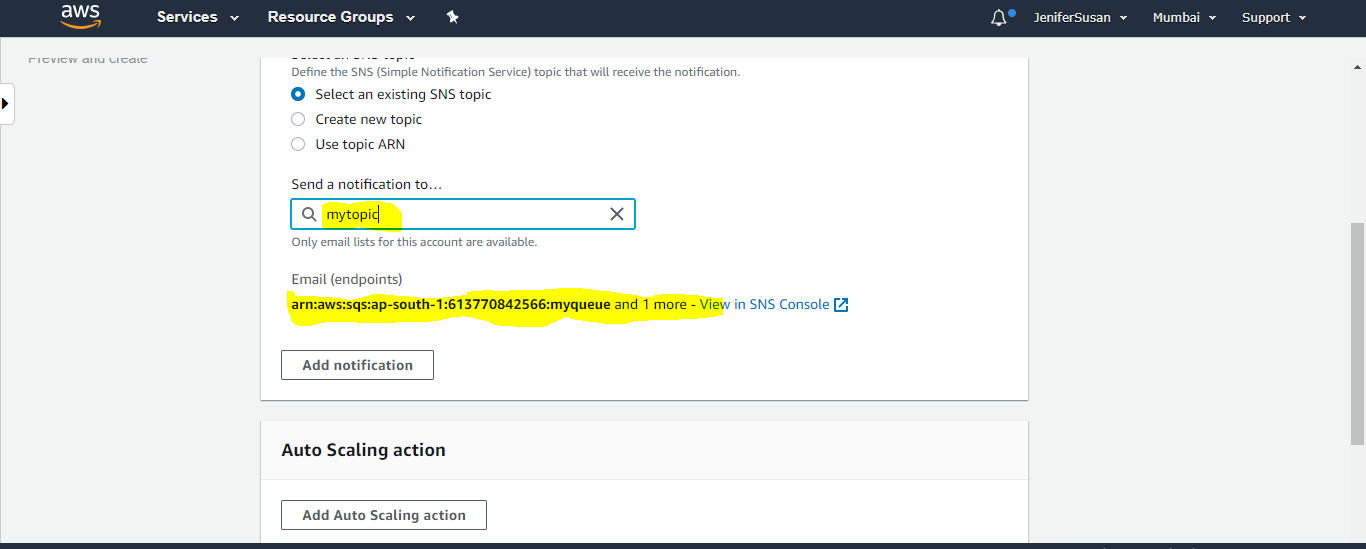


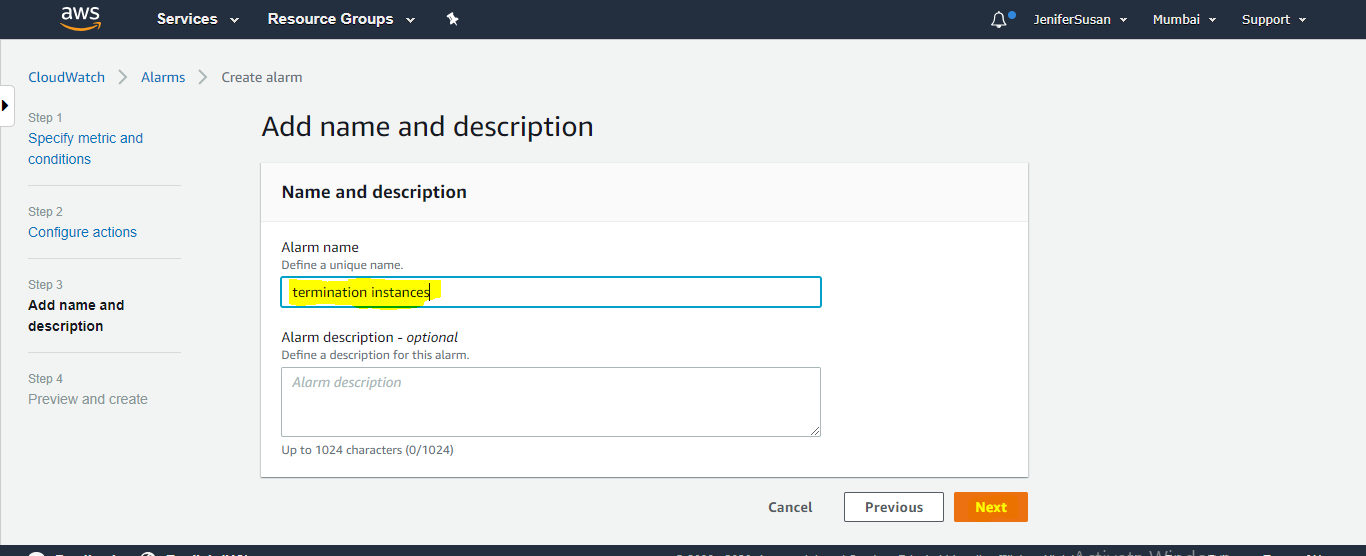
1. Create alarm in cloudwatch with specific metric and condtions and subscribe to SNS

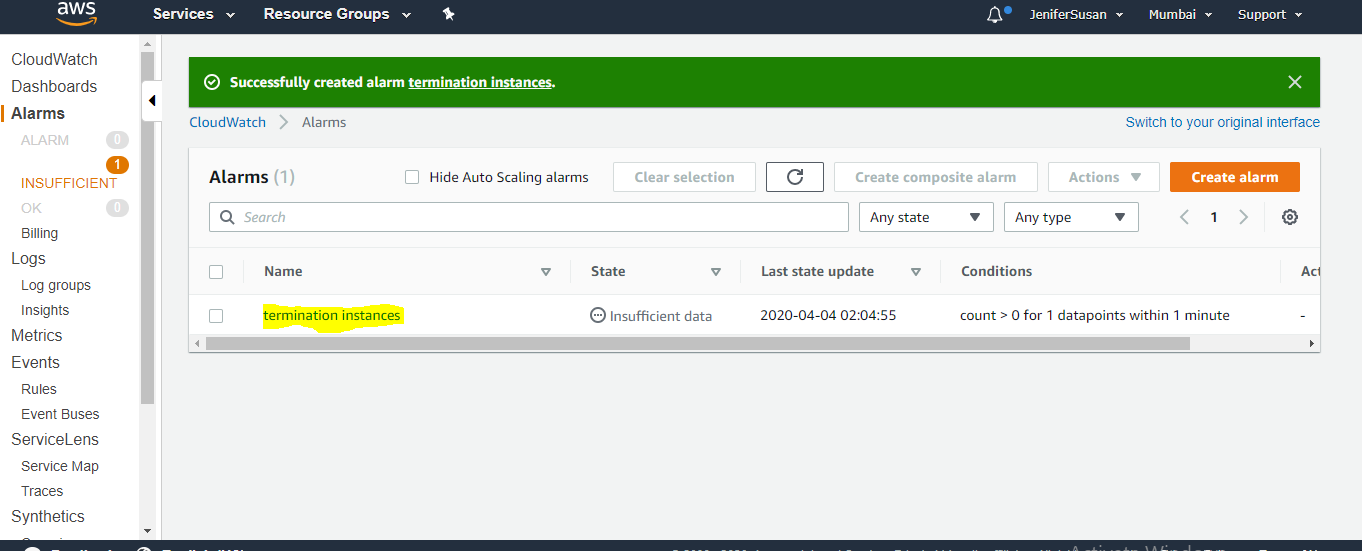


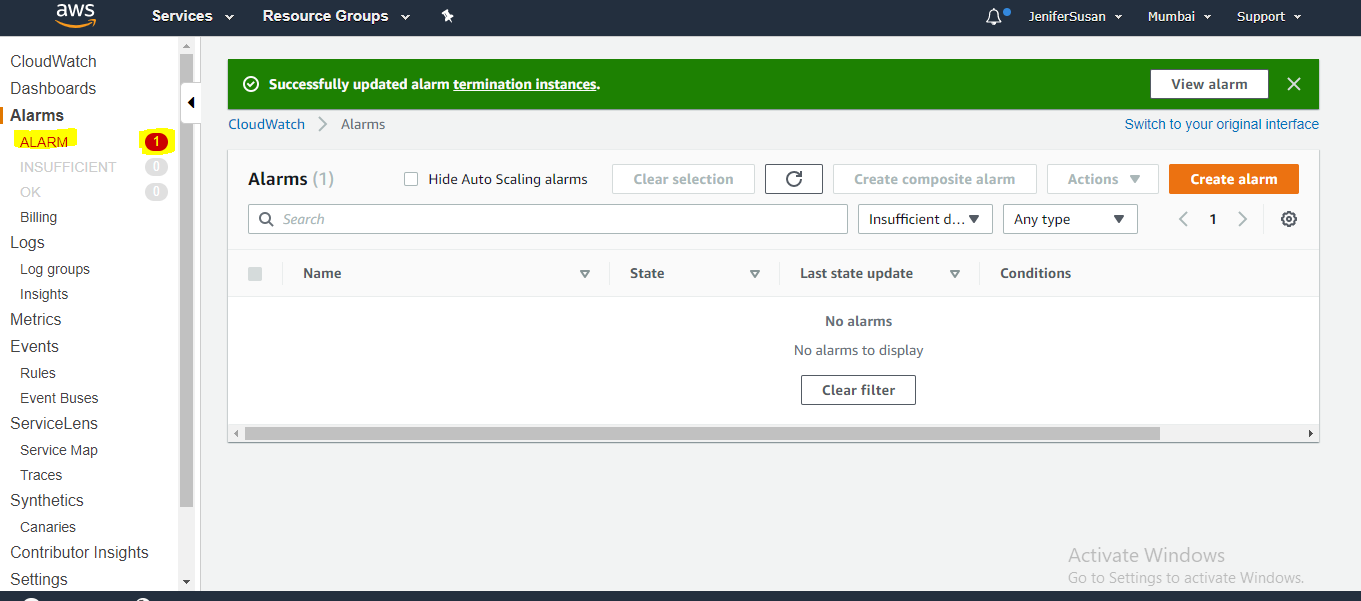


Subscribe to SNS topic









Check the SNS notification in email ID:

