Day32

DIY

Problem Statement: How to Monitor Malicious Activity or Unauthorized Behavior via GuardDuty?

Use Case:When we deploy any resources in AWS —whether it's public-facing or private —the hackers always attempt to break into the resources and steal the confidential data to exploit them to their advantage. This resource can be an EC2 instance, an S3 Bucket, an RDS instance, or anything else. While the hackers always look for loopholes to break into the systems, the onus is on the company to protect themselves before hackers can exploit the vulnerabilities to compromise your systems.

To address this challenge, AWS provides Amazon GuardDuty: A managed service that continuously monitors your resources for any malicious activity or unauthorized behavior, thus helping you protect your AWS accounts and workloads. Once Amazon GuardDuty is enabled, it automatically monitors for

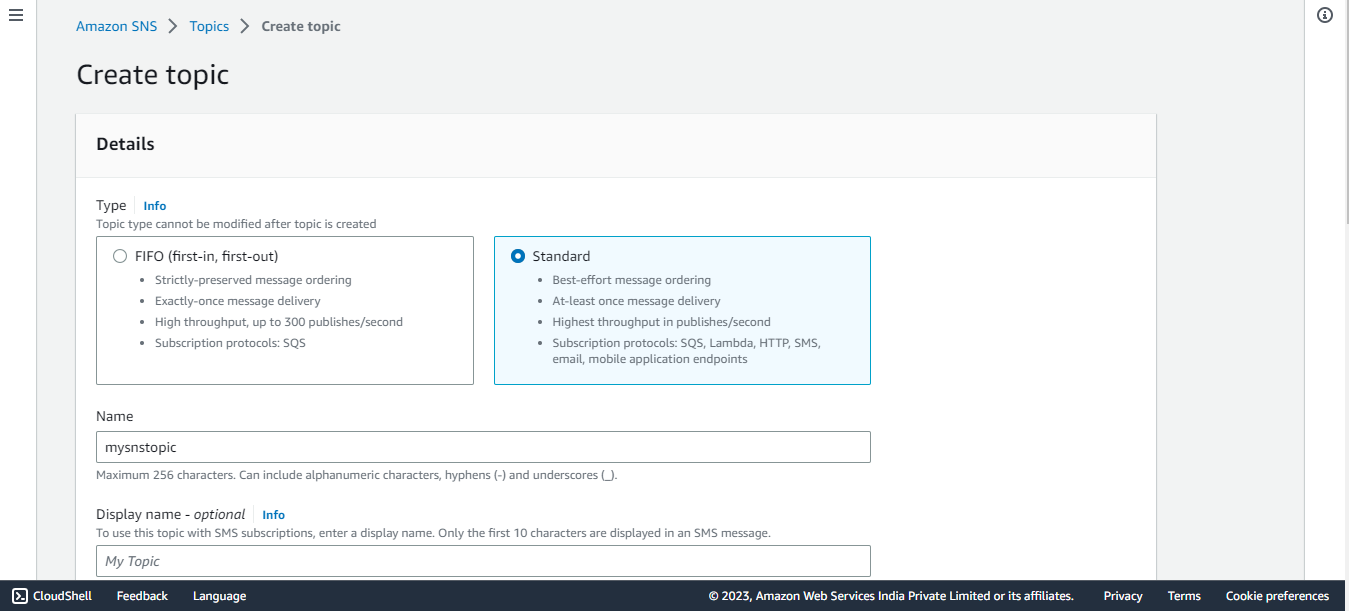
•Anomalous API activity

•Potentially unauthorized deployments and compromised instances

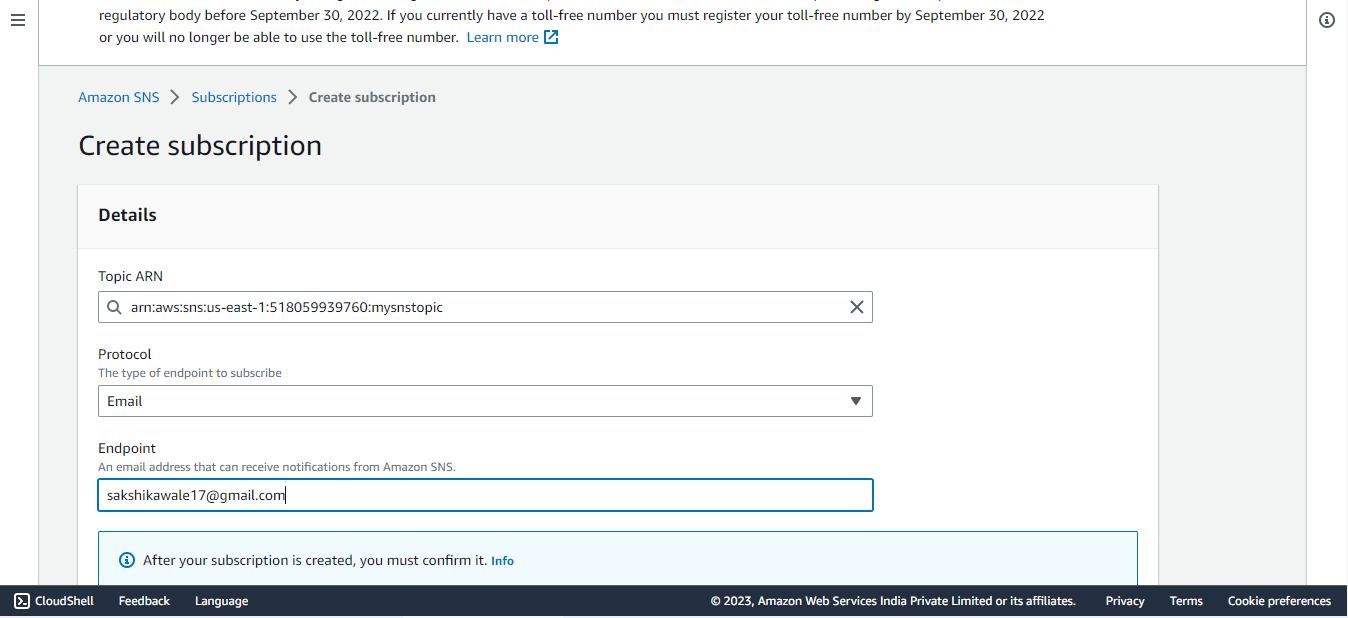
•Reconnaissance by attackers

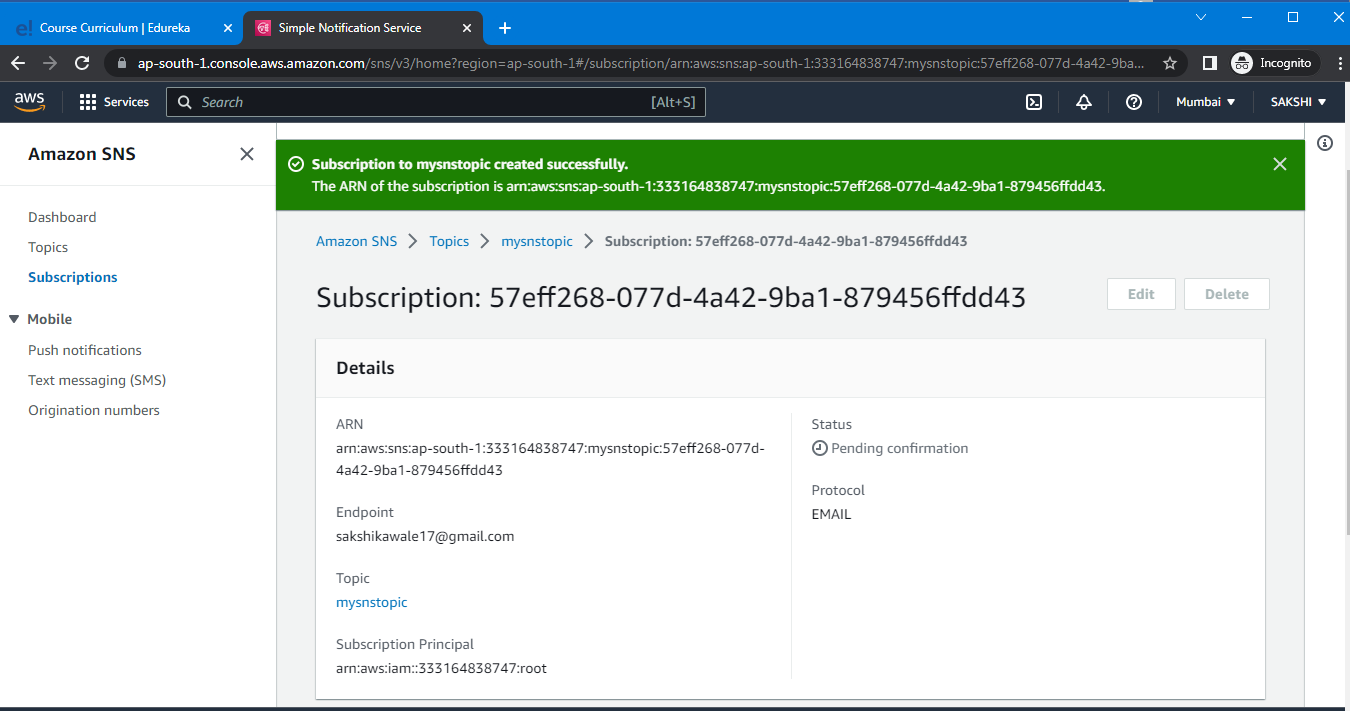
Ans:

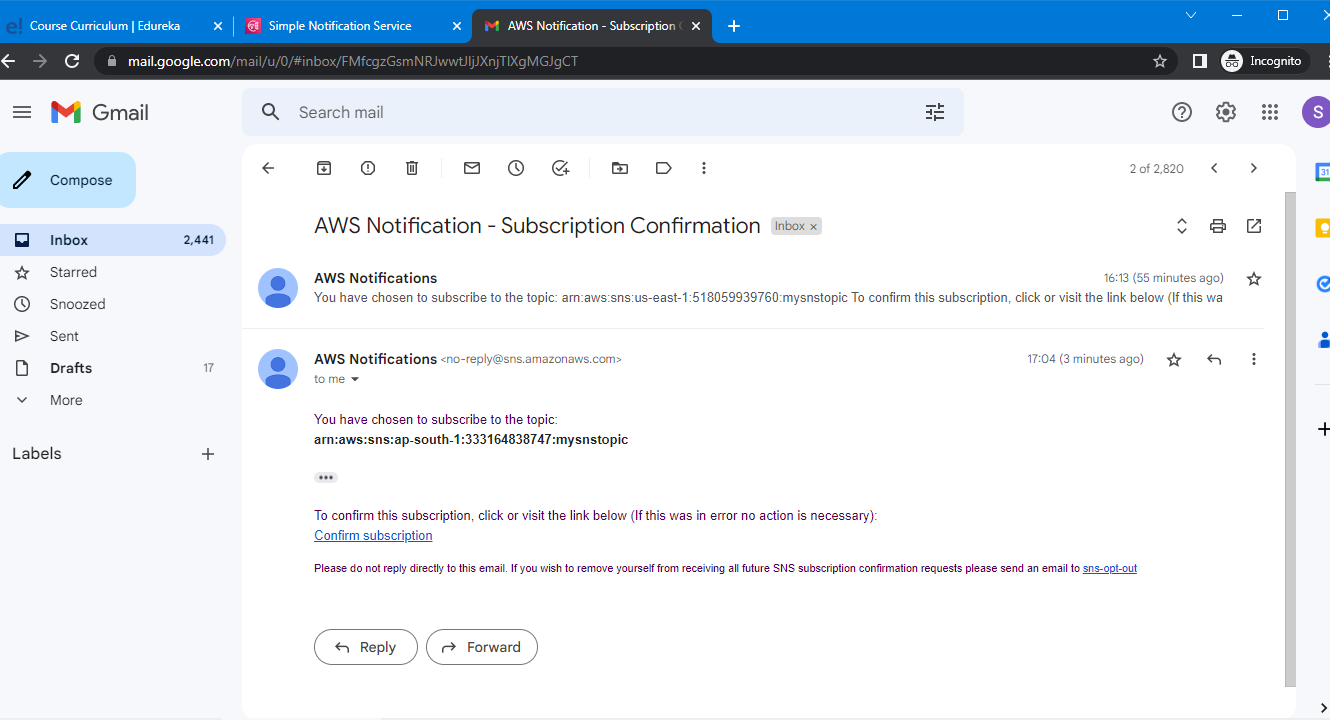
1. Create sns notification

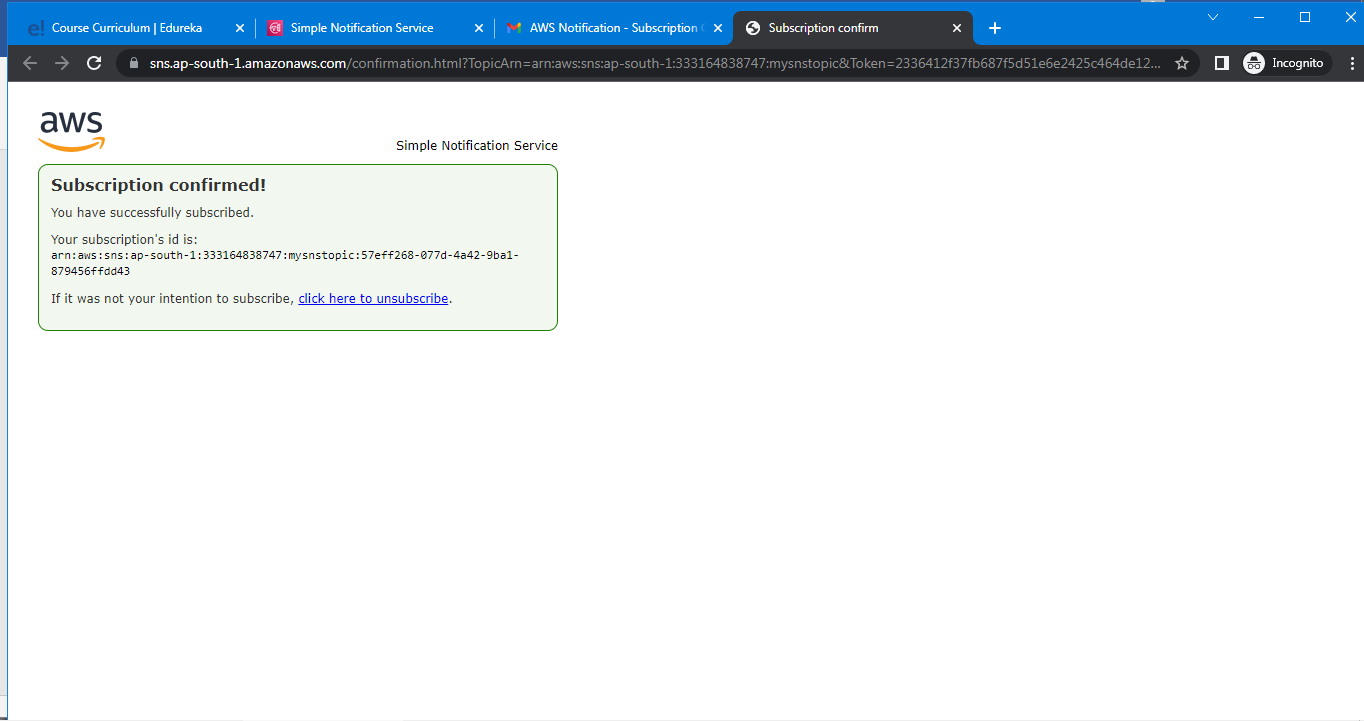


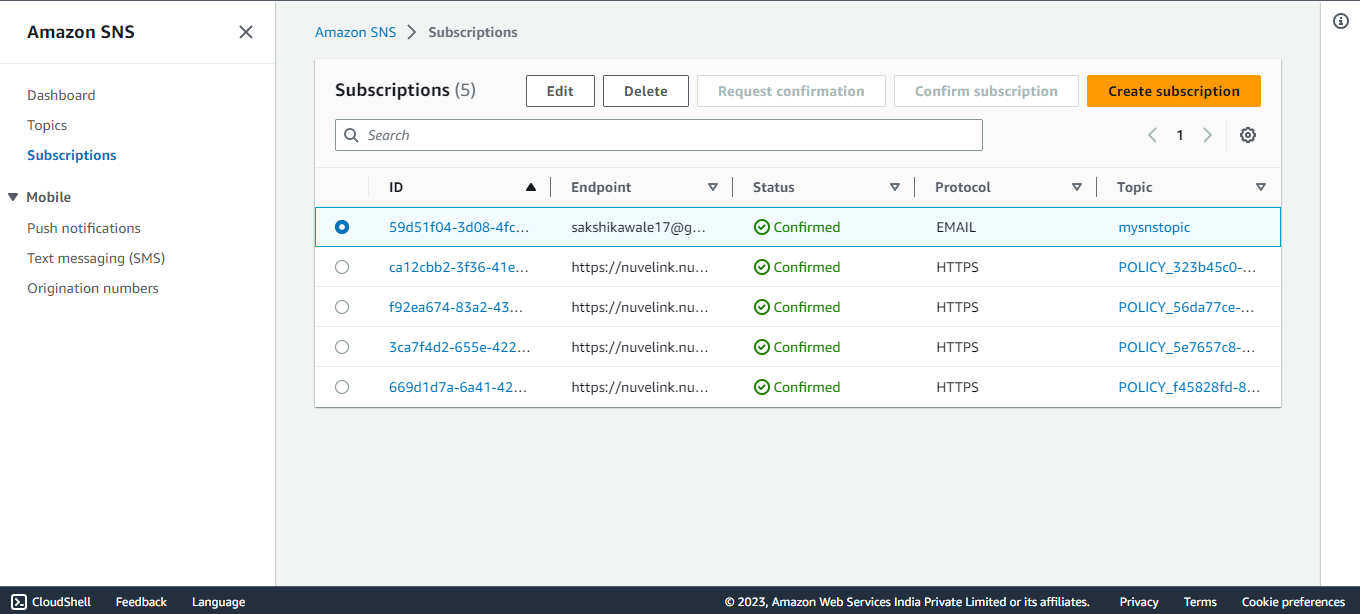
Now create subscription



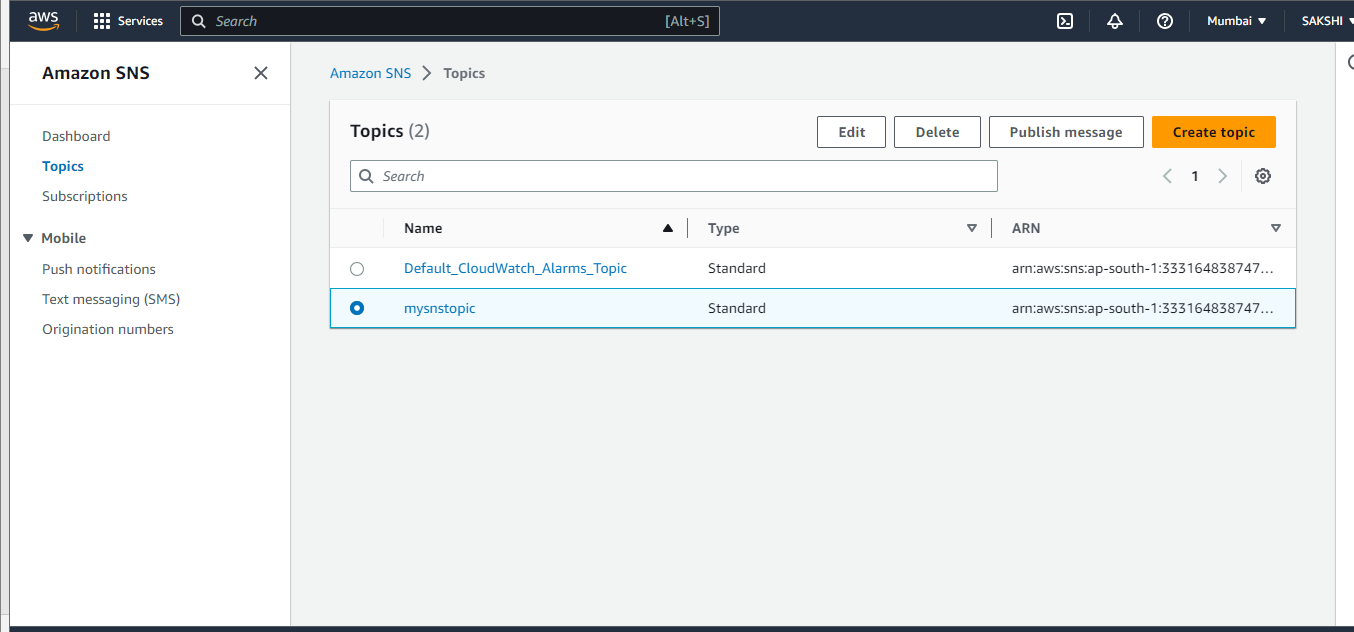


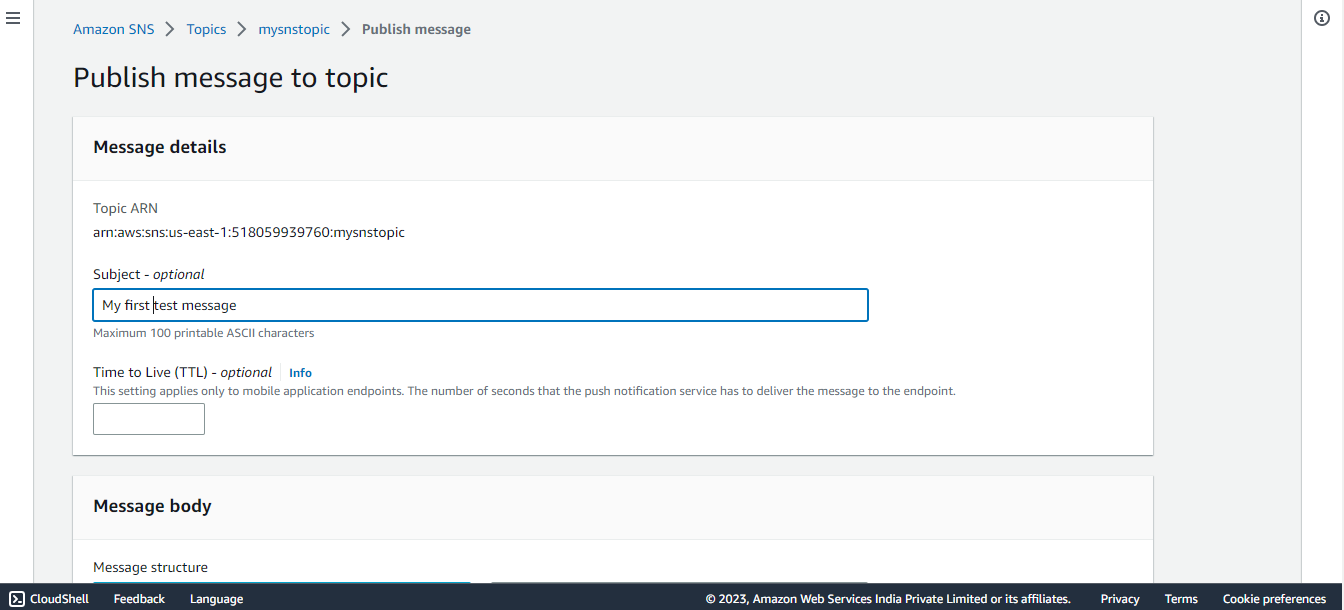


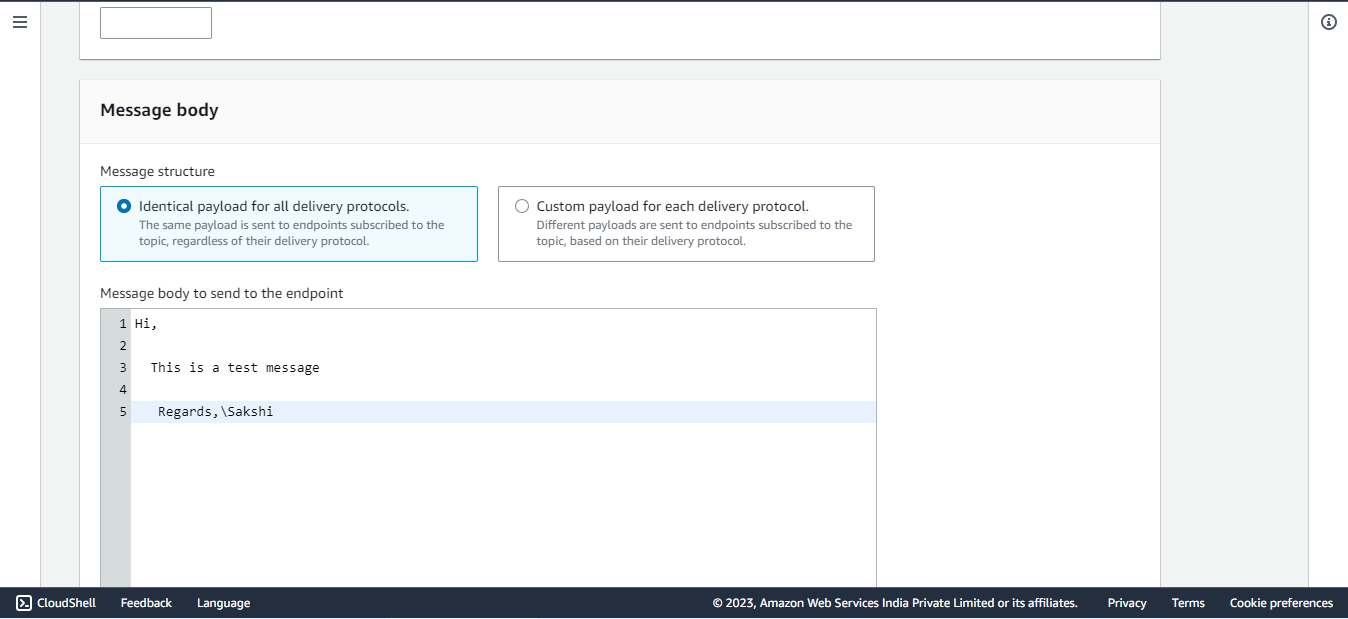


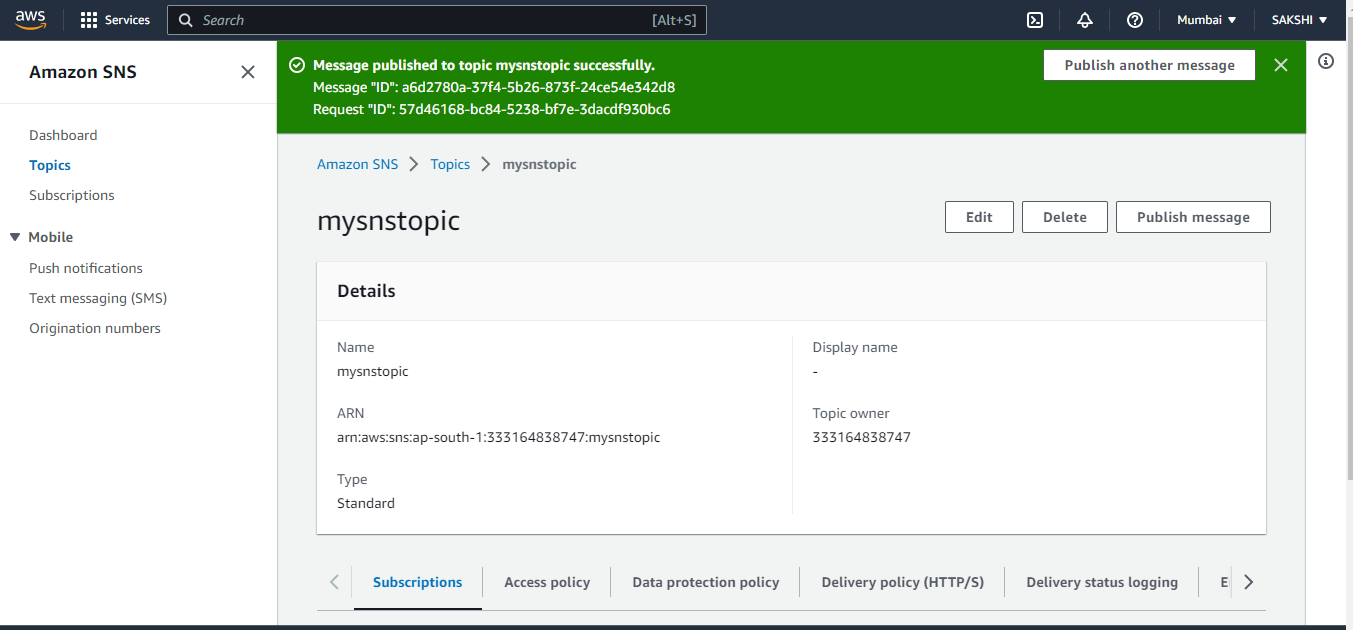


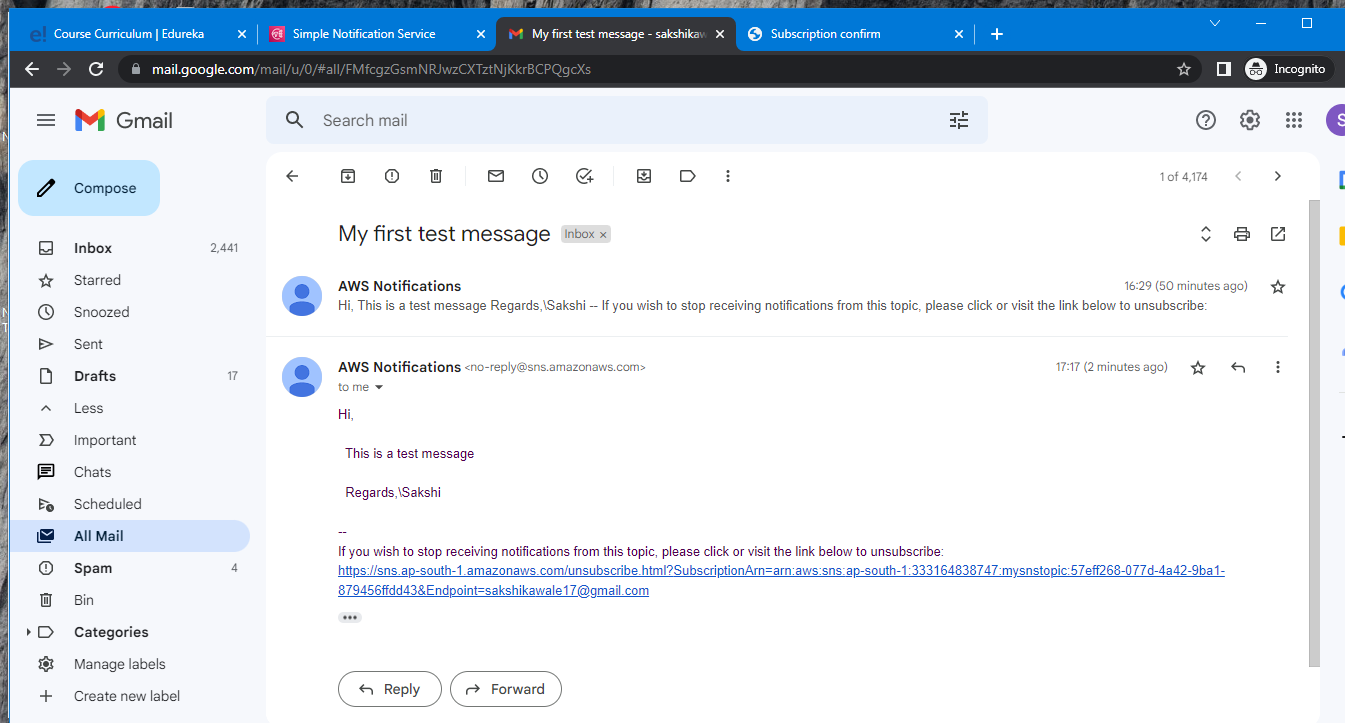
Click on publish message





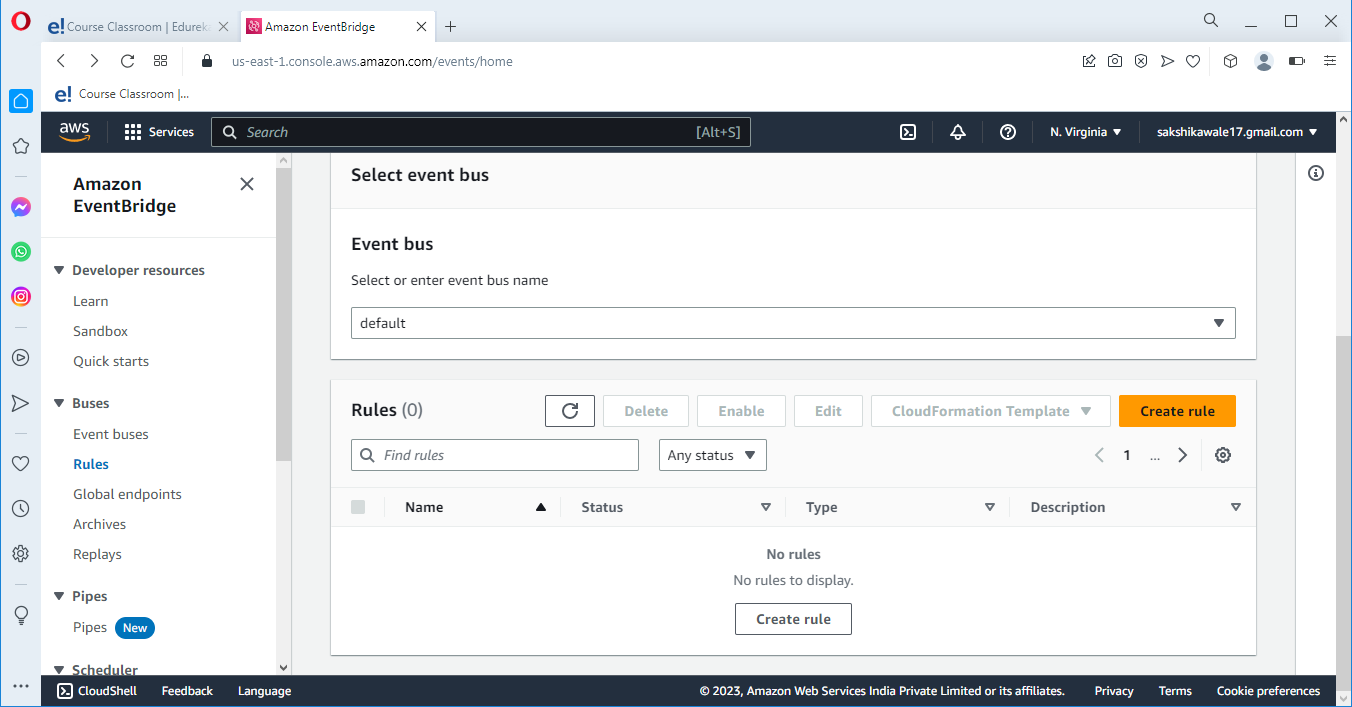


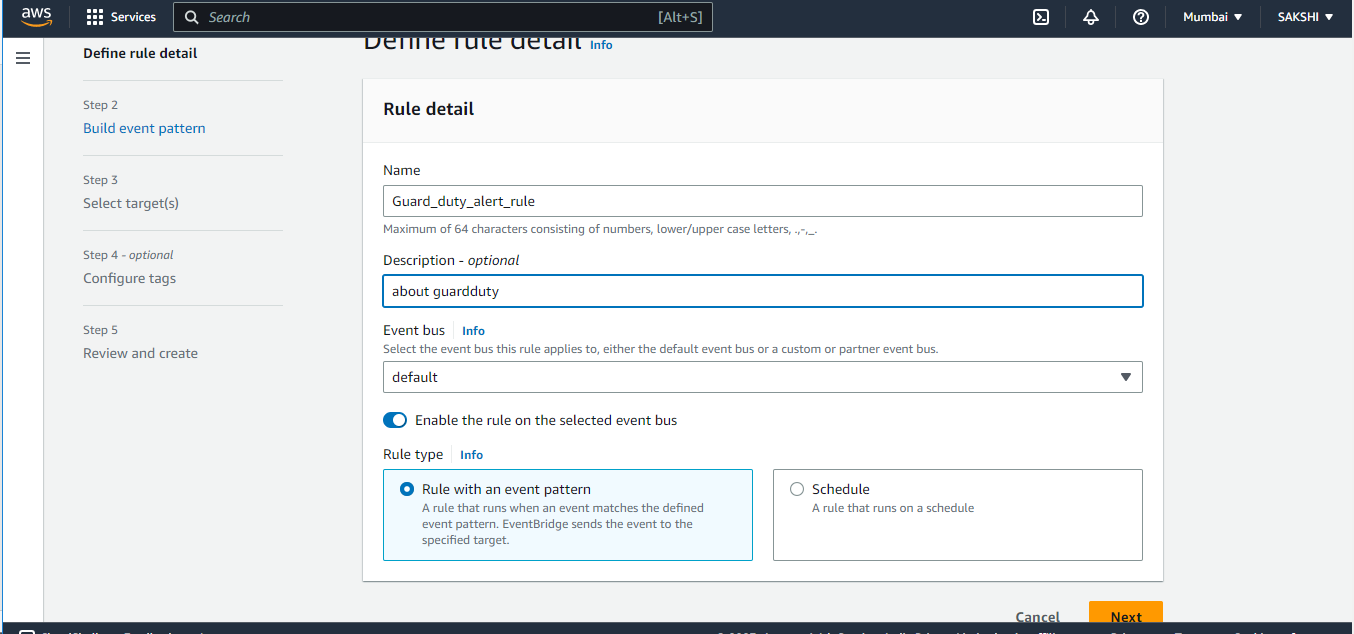


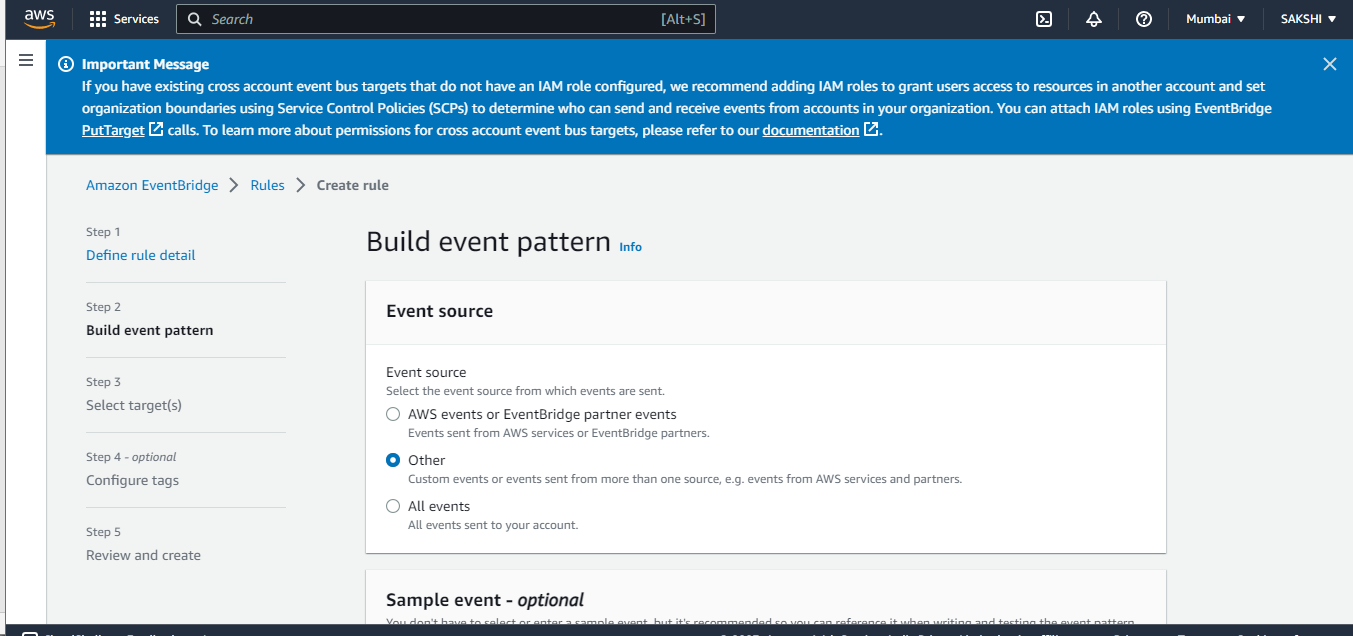


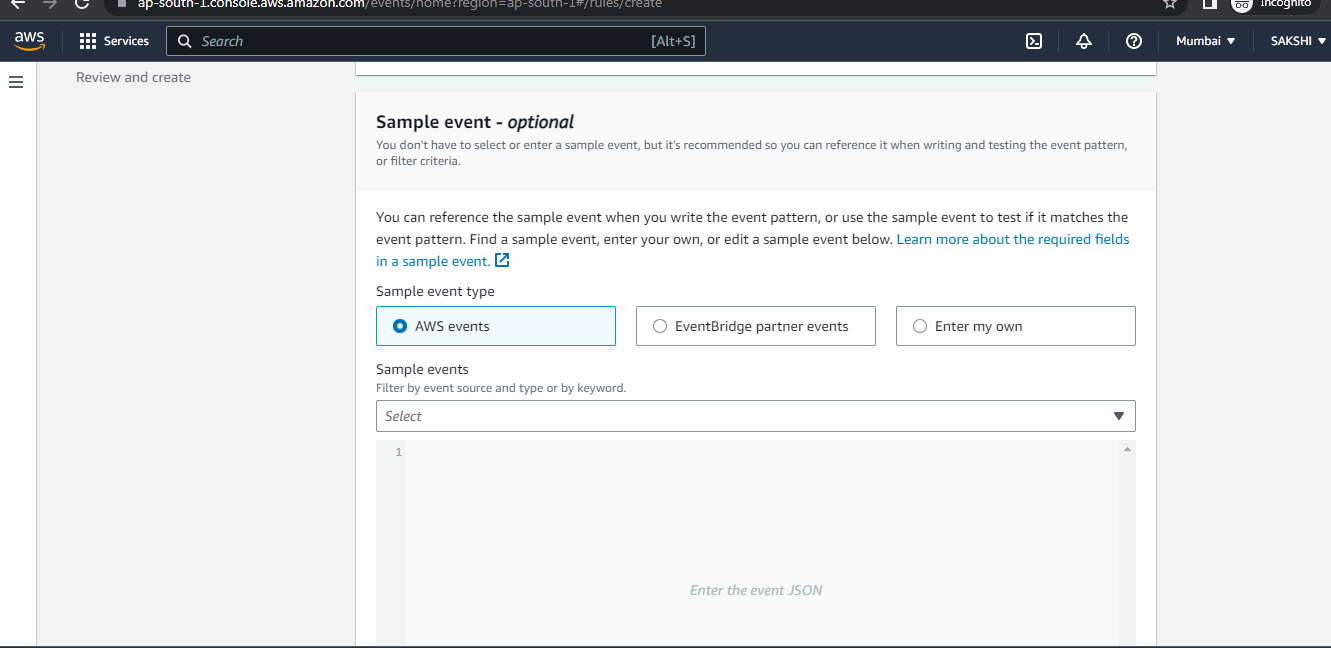
1. Now go to cloudwatch

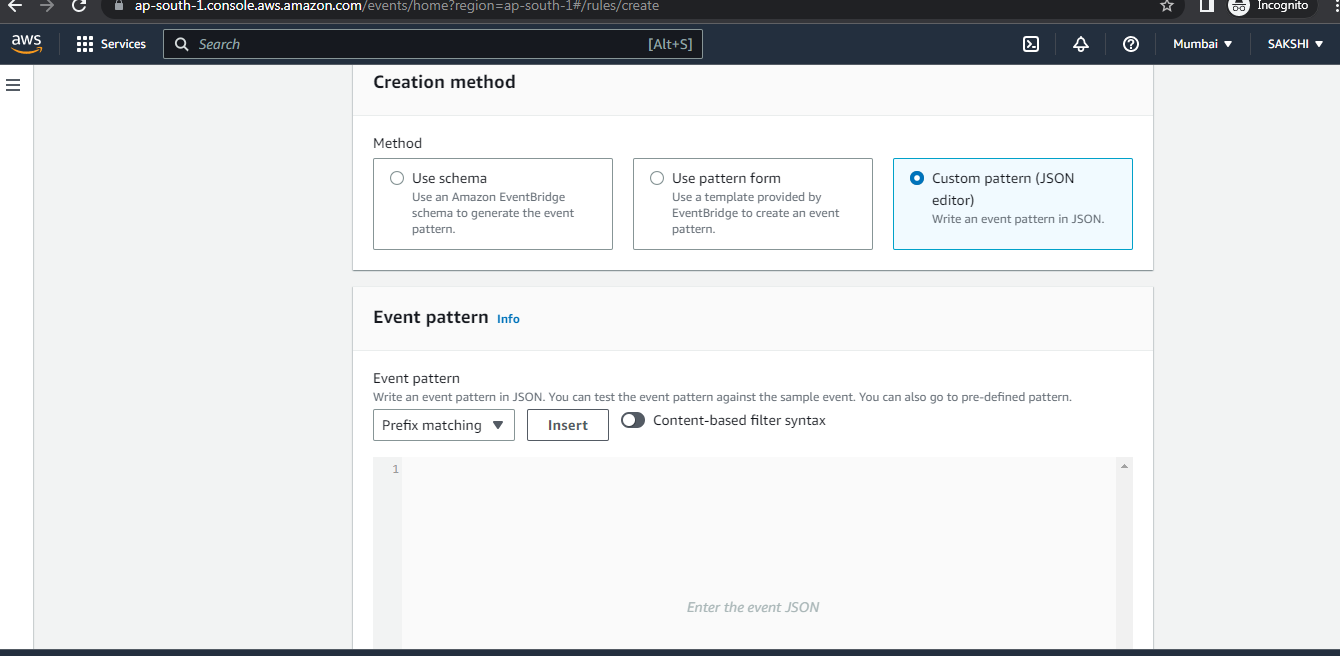
Create rule

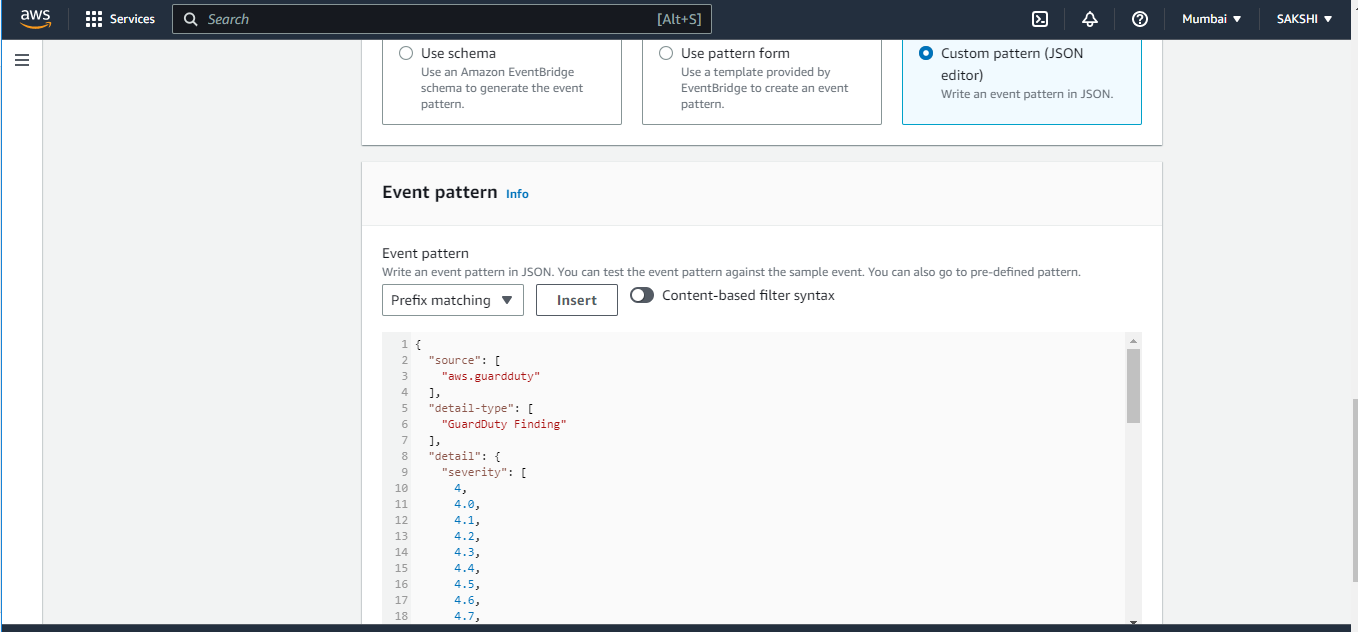




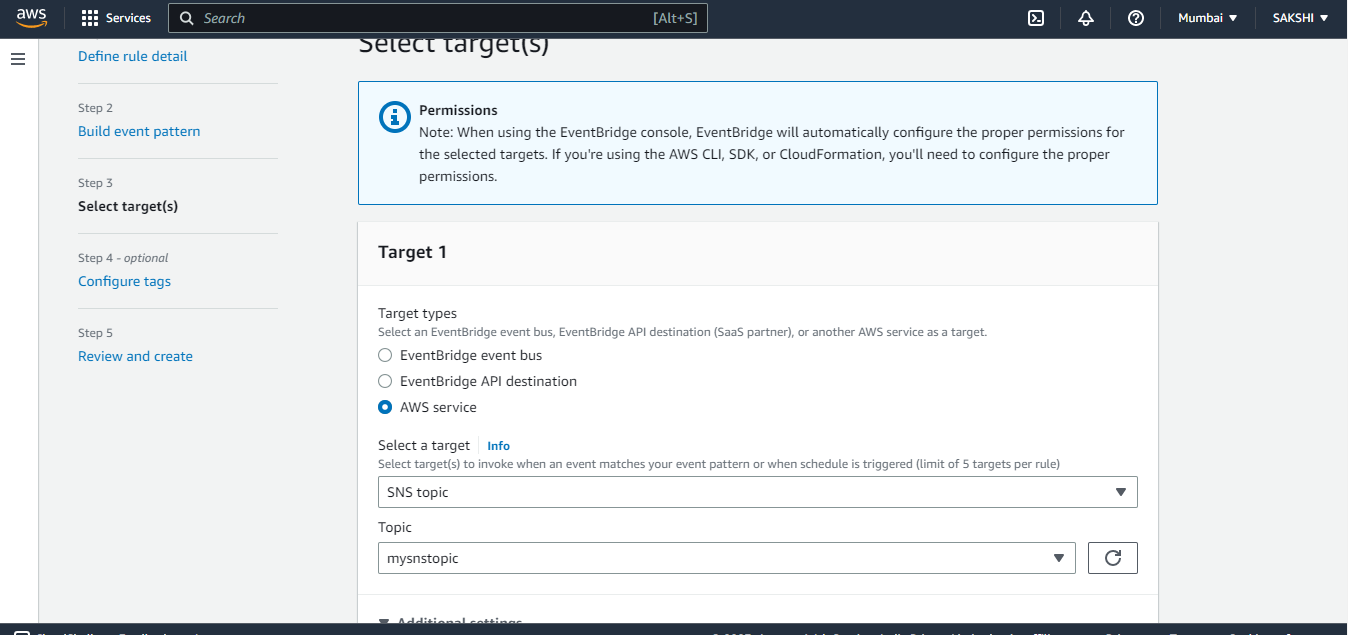


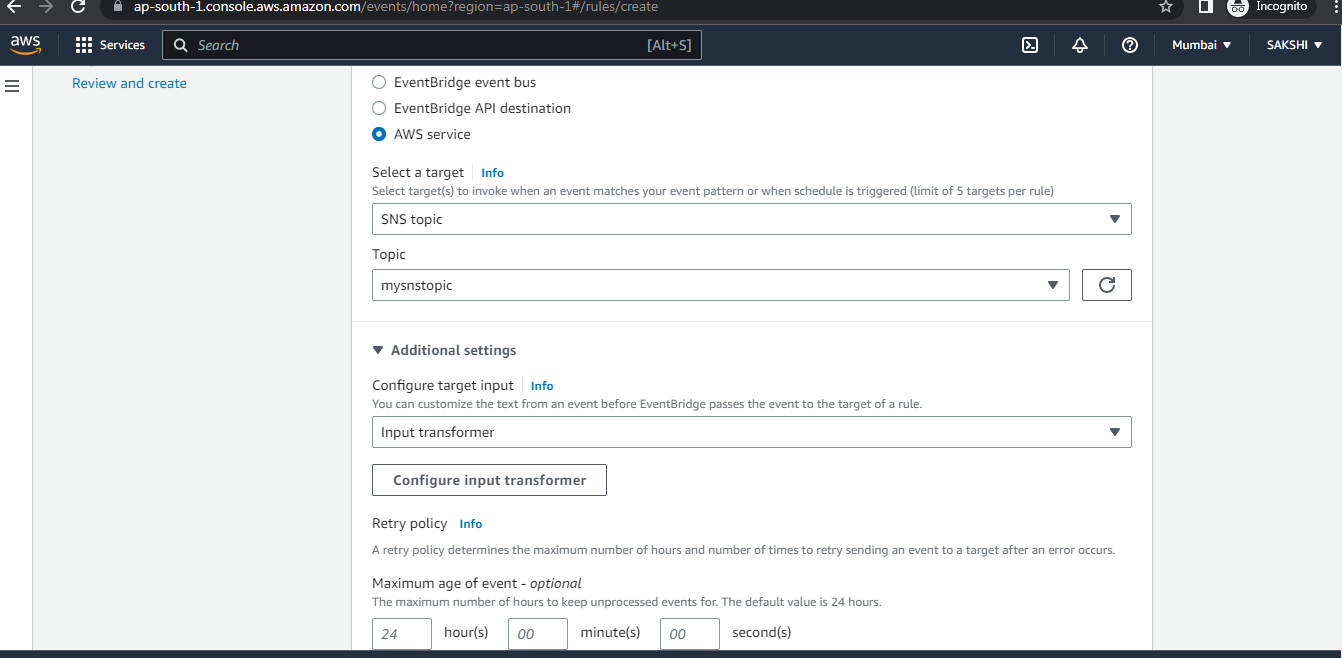




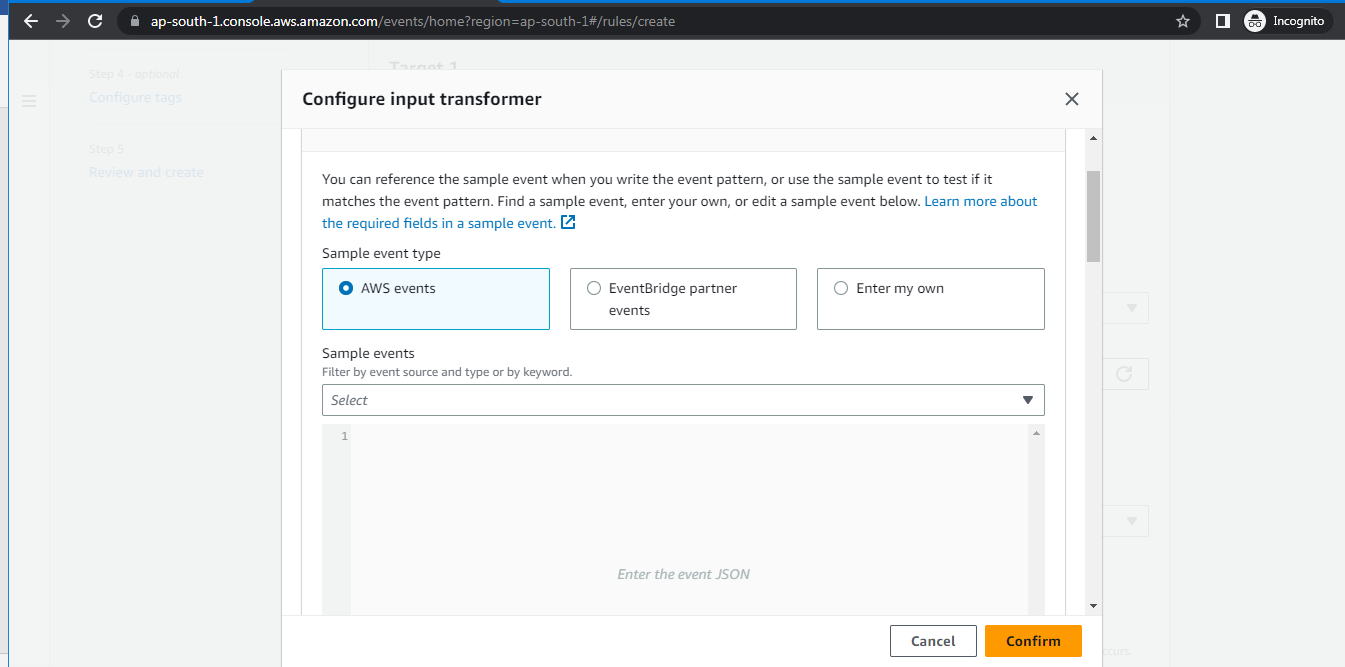


Click on next

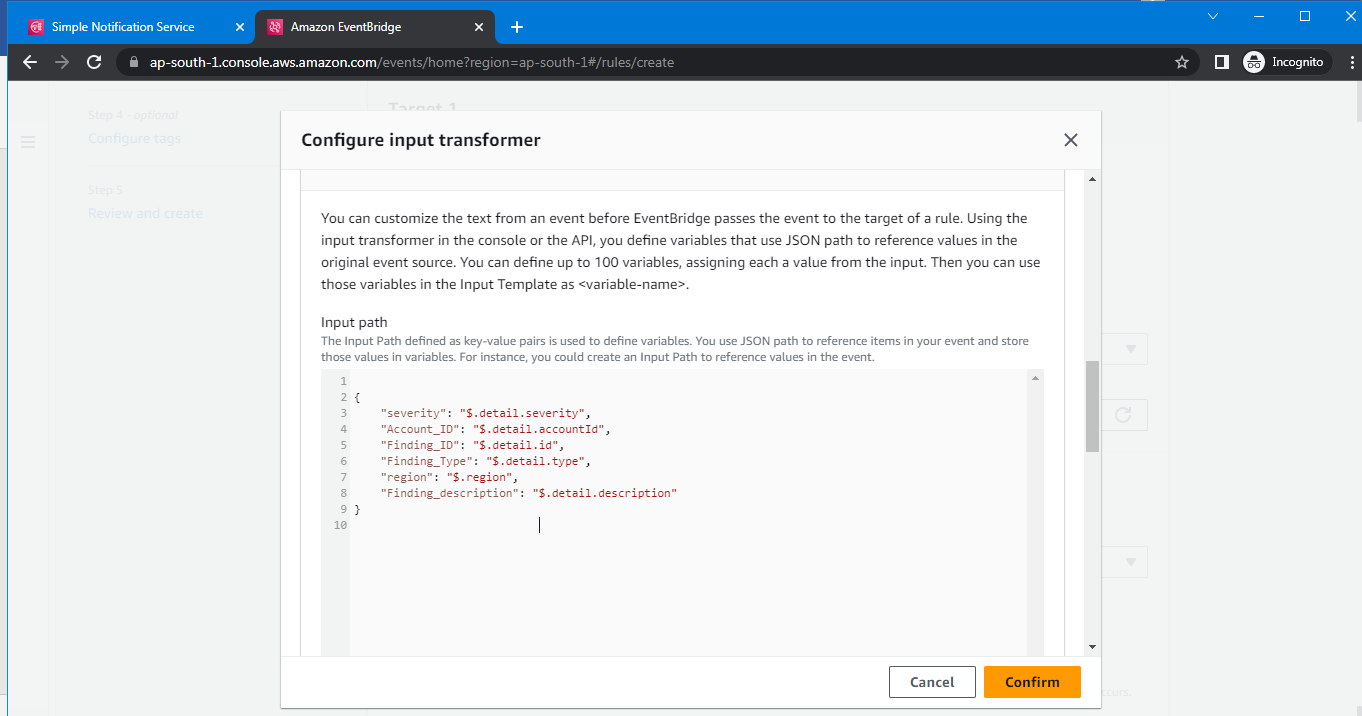




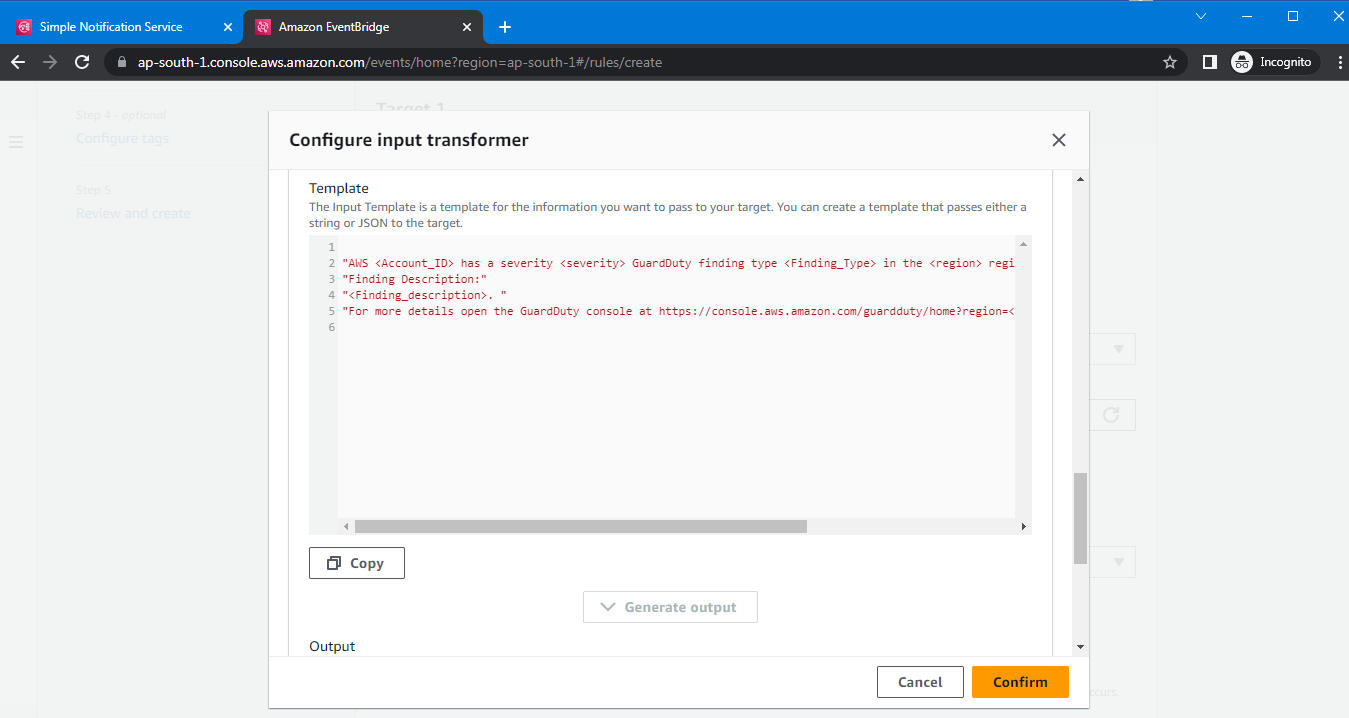
Now click on configure input transformer



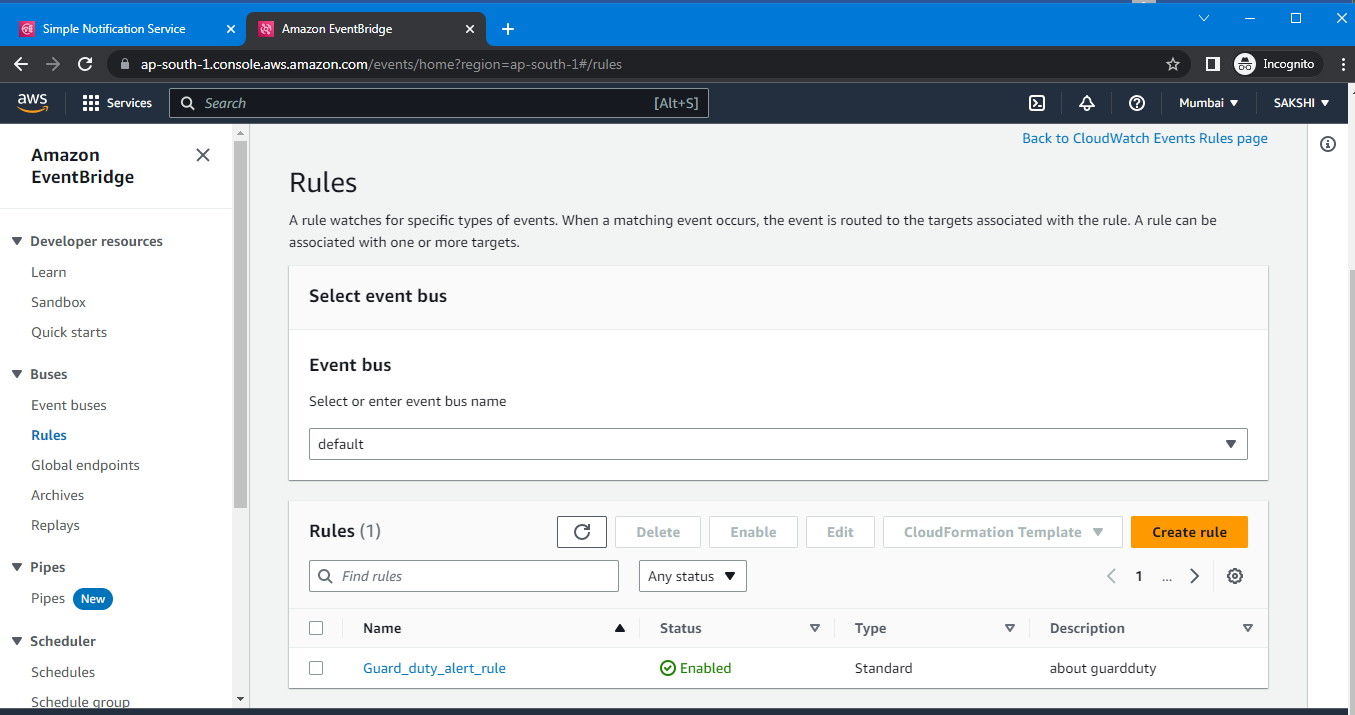
Enter the code for input path

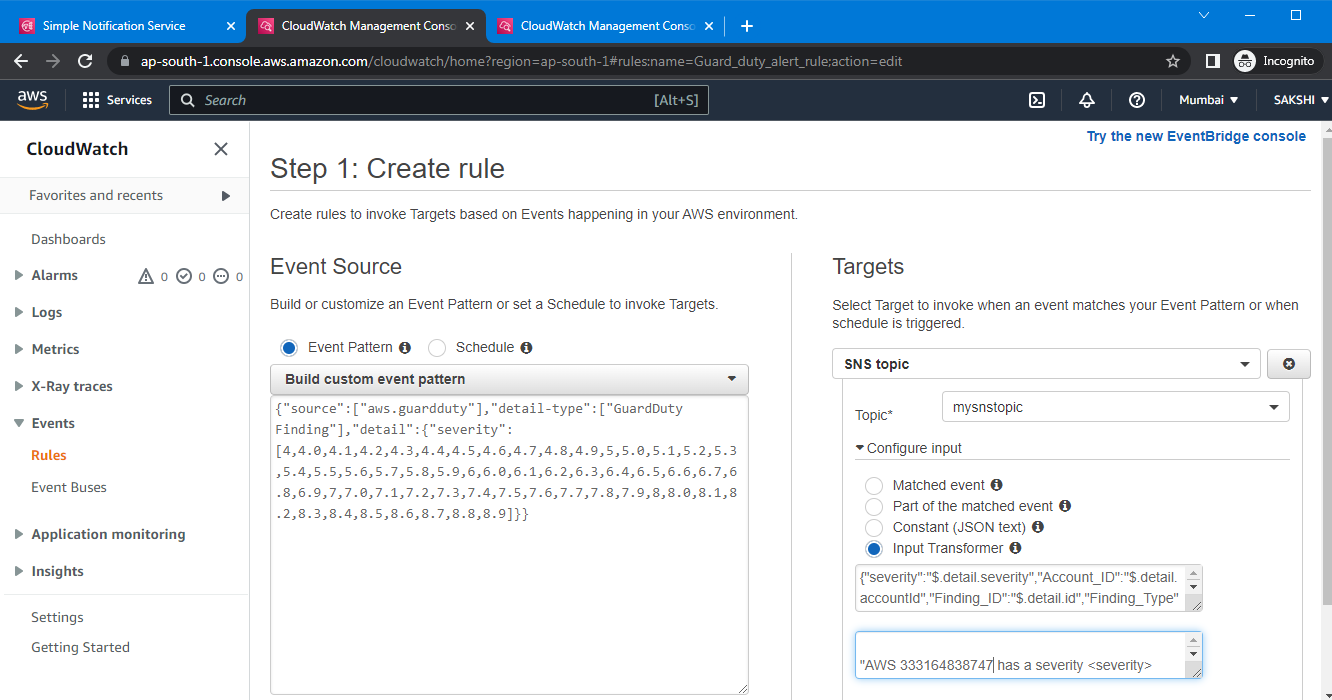


Enter the code for populate input template

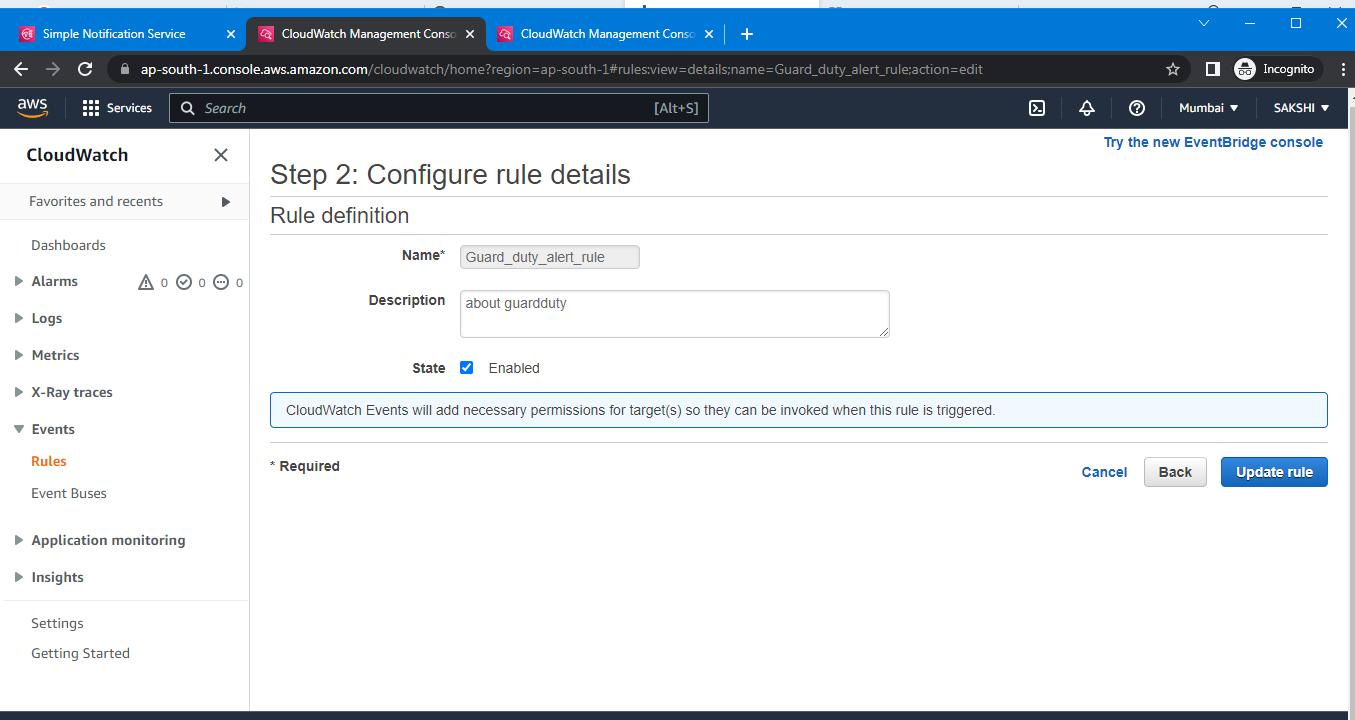


Click on confirm



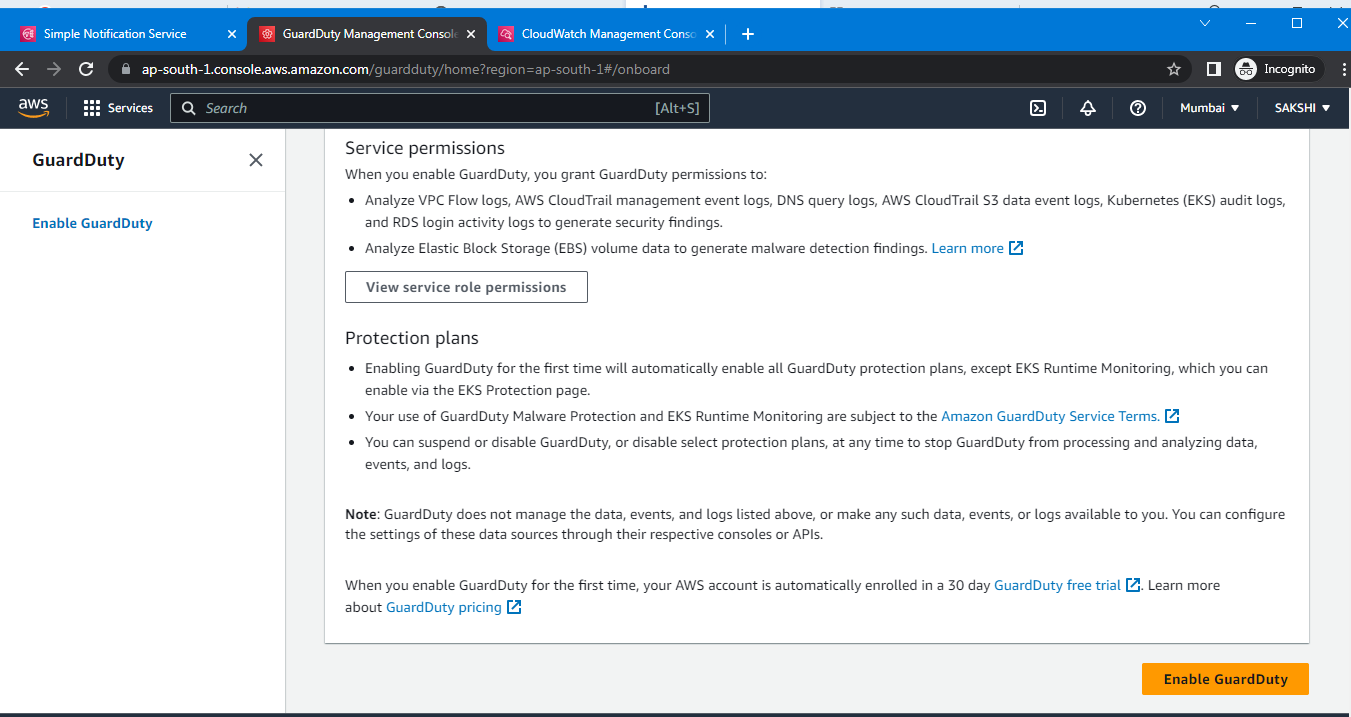


Add account id in template, we can also add it while creating rule

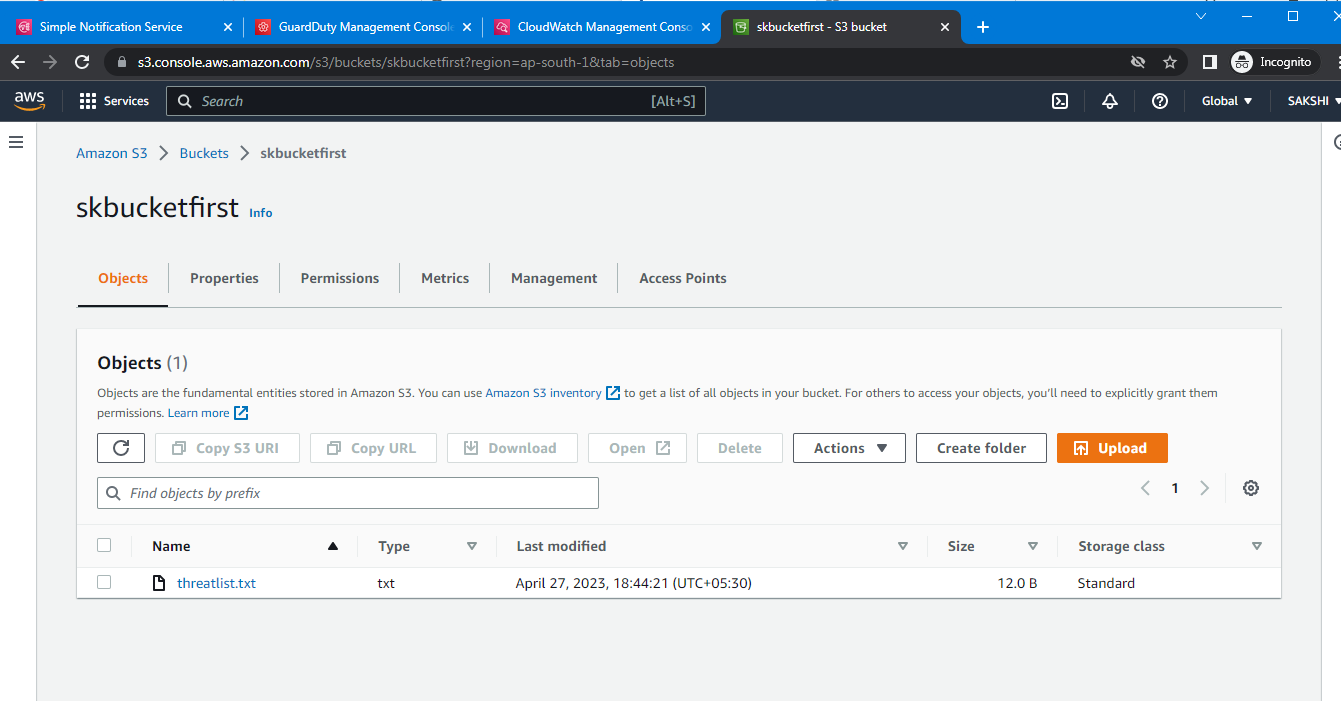


Click on update rule

1. Now go to gurad duty and enable it



1. Go to s3 , create bucket and insert file which has ip address of pc



1. Again go to guardduty

Go to list

- **Add a threat IP list**

