Day 33

DIY

Problem Statement: Setup AWS Config to evaluate compliance for the resources in your environment

Use Case:

You are the Cloud Engineer in one of the Pharma companies that has multiple workloads running in their AWS account. Your IT manager wants you to ensure proper security checks are put in place for compliance and take appropriate remediate action in case of non-compliance. You are instructed to deploy an AWS Config solution that should meet the following requirements.

Requirement 1

a. Check whether you’re running EC2 instances are using approved AMIs.

b. If non-compliance is found, configure Remediation Action to stop the EC2 instance automatically.

c. Identify who created the non-compliant resource using AWS CloudTrail

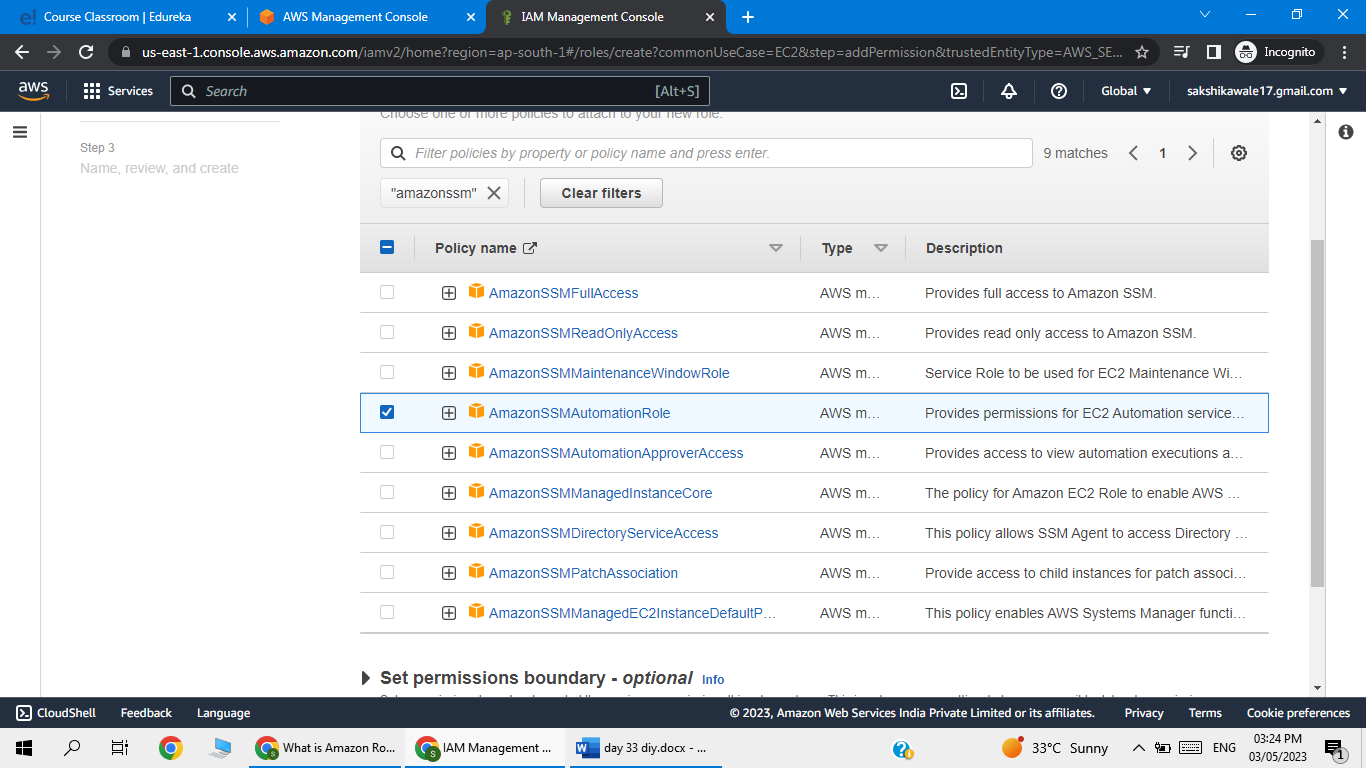
Requirement 2

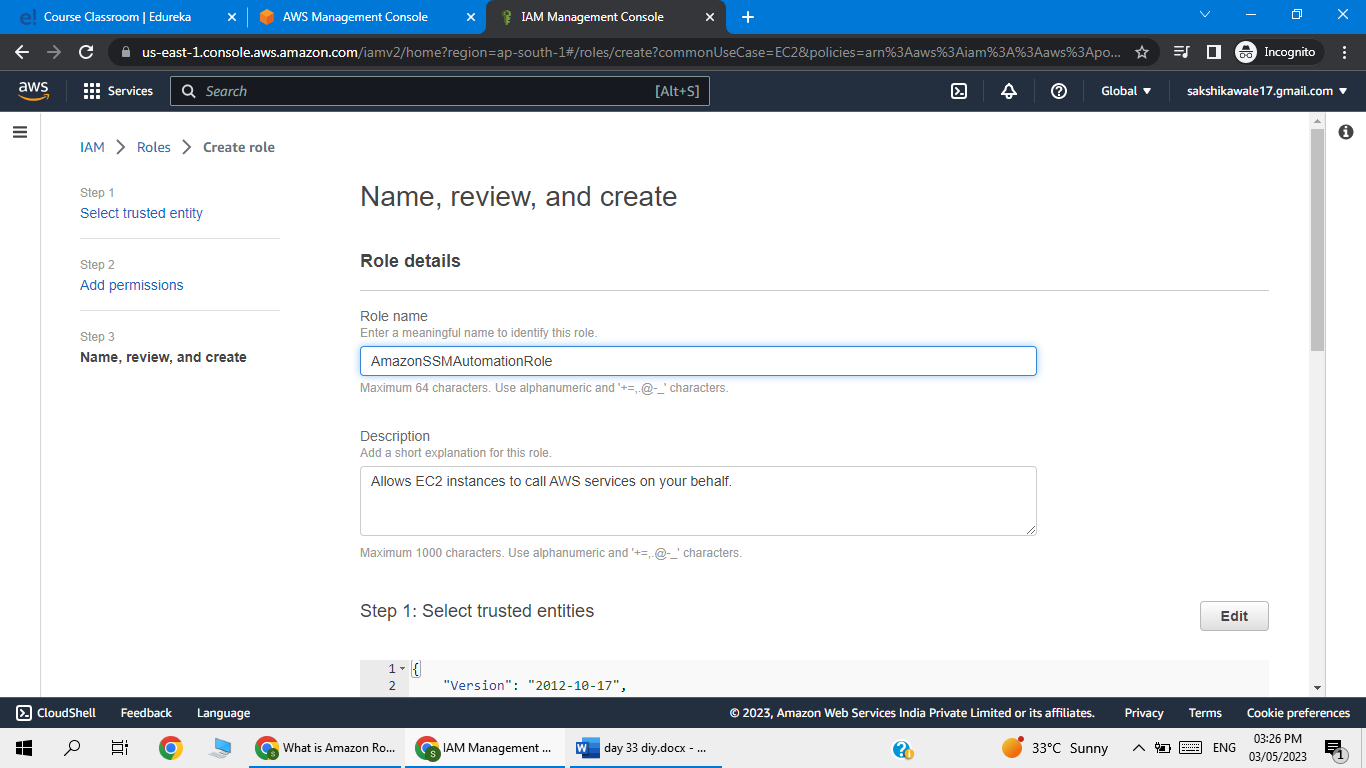
a. Identify if public read access is enabled for any S3 bucket.

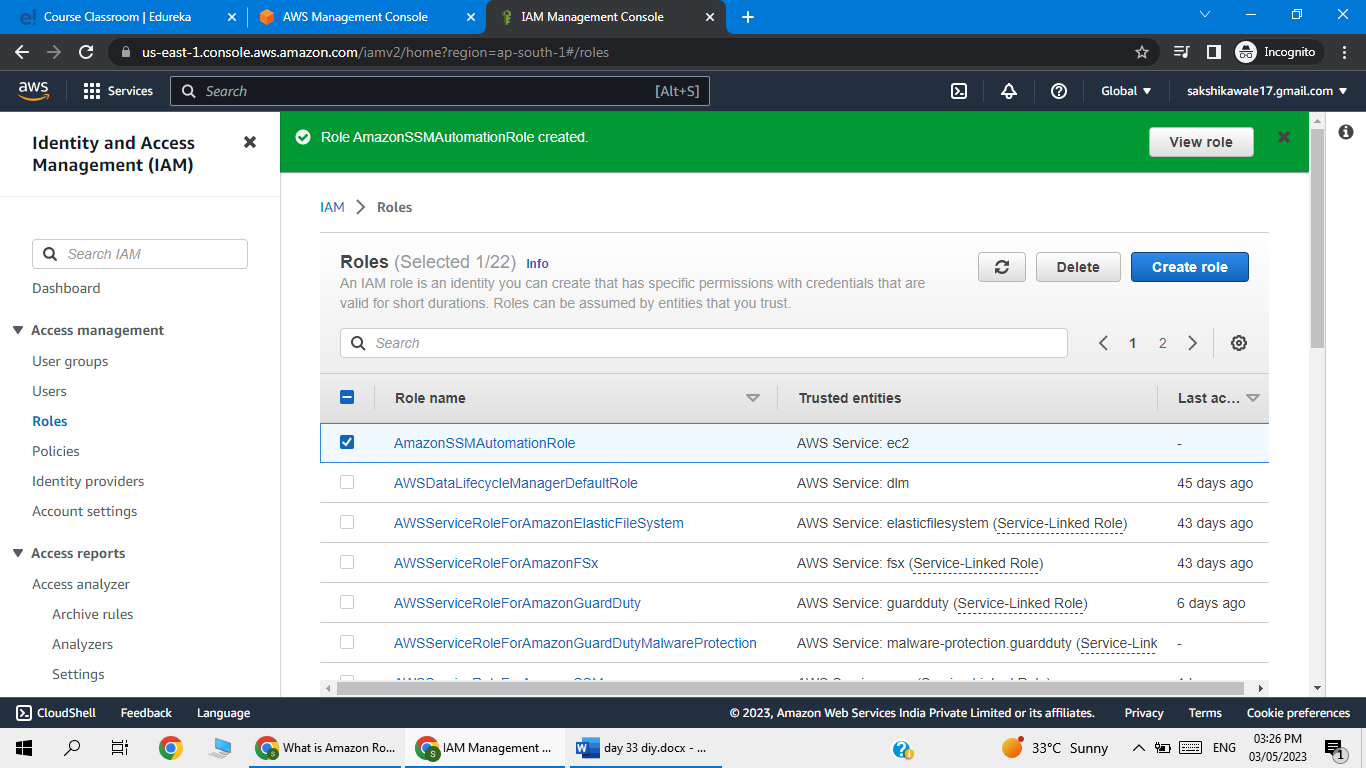
b. If non-compliance, configure Remediation Action to send a notification to the Security Team

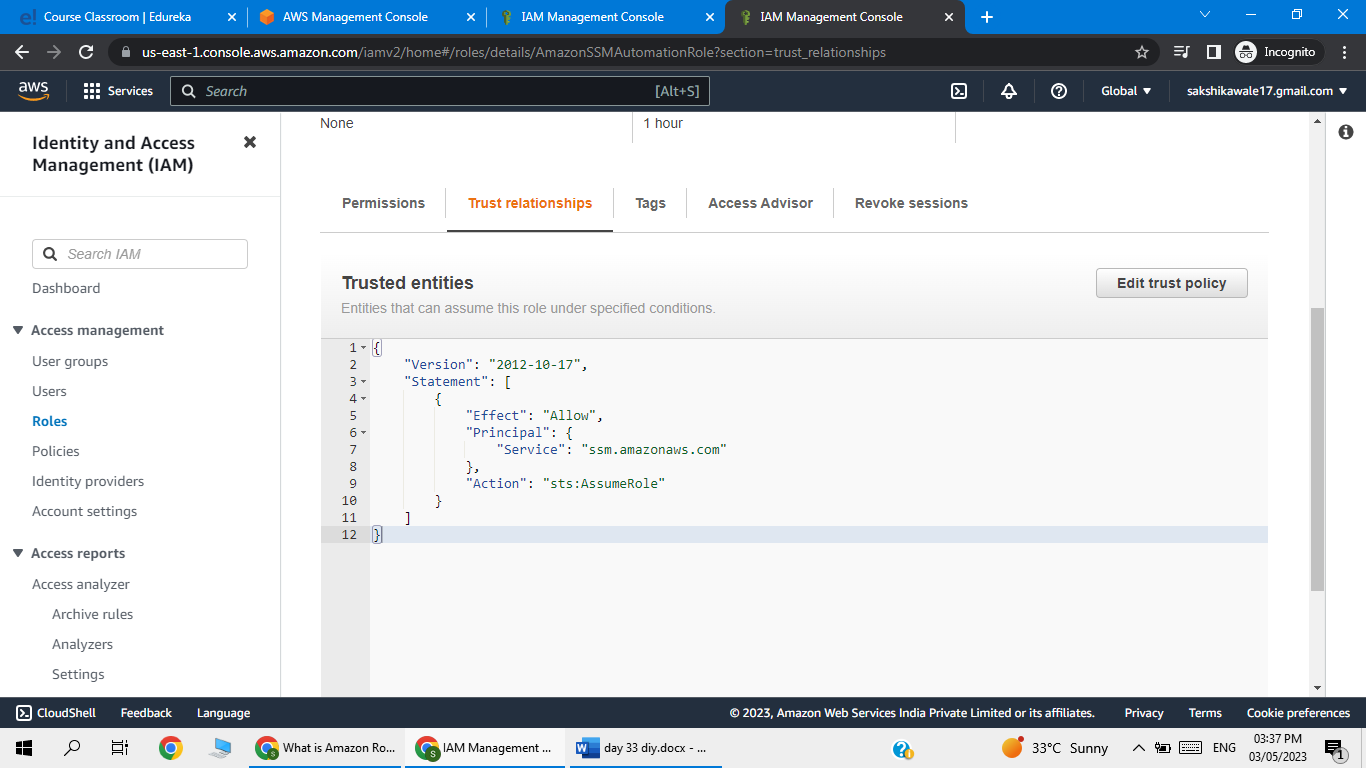
c. Identity who created the non-compliant resource using AWS CloudTrail

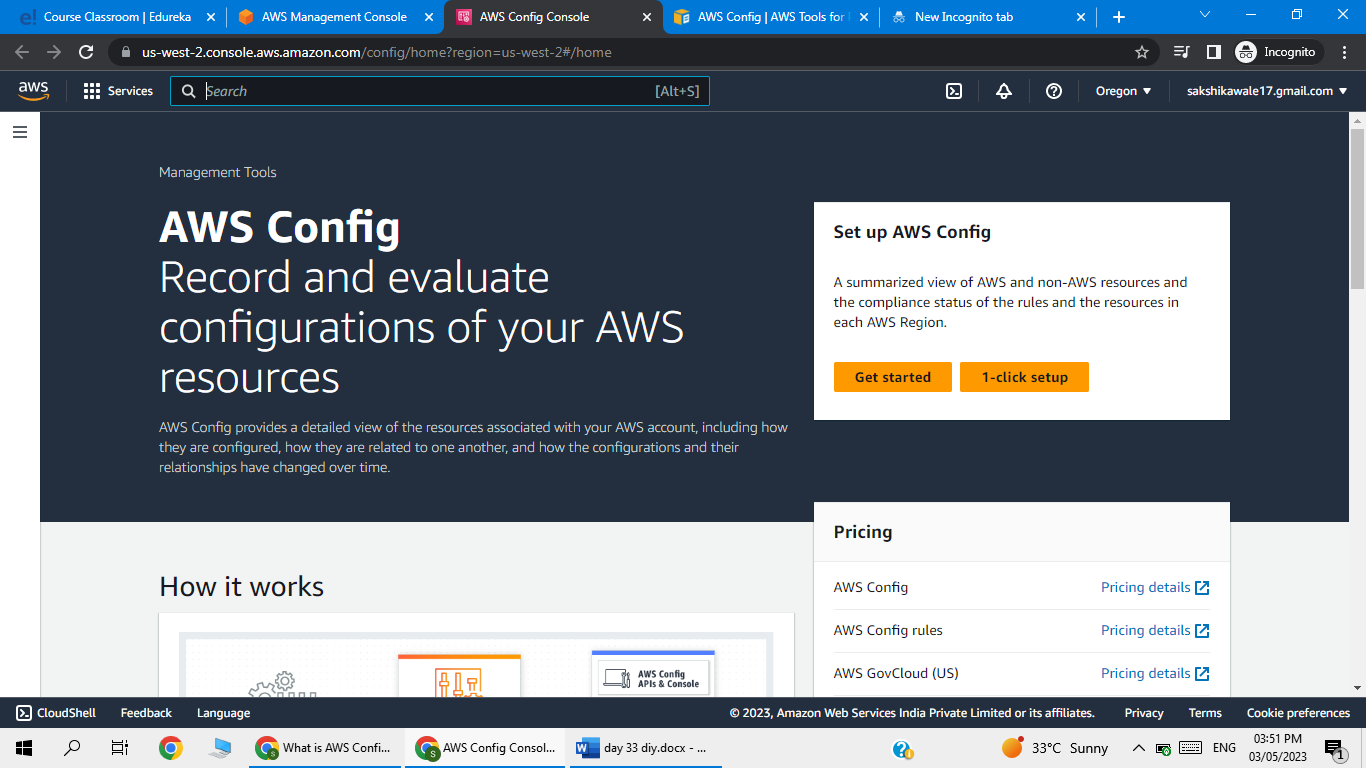
Objective: You will learn how to setup AWS Config to evaluate compliance for the resources in your environment.

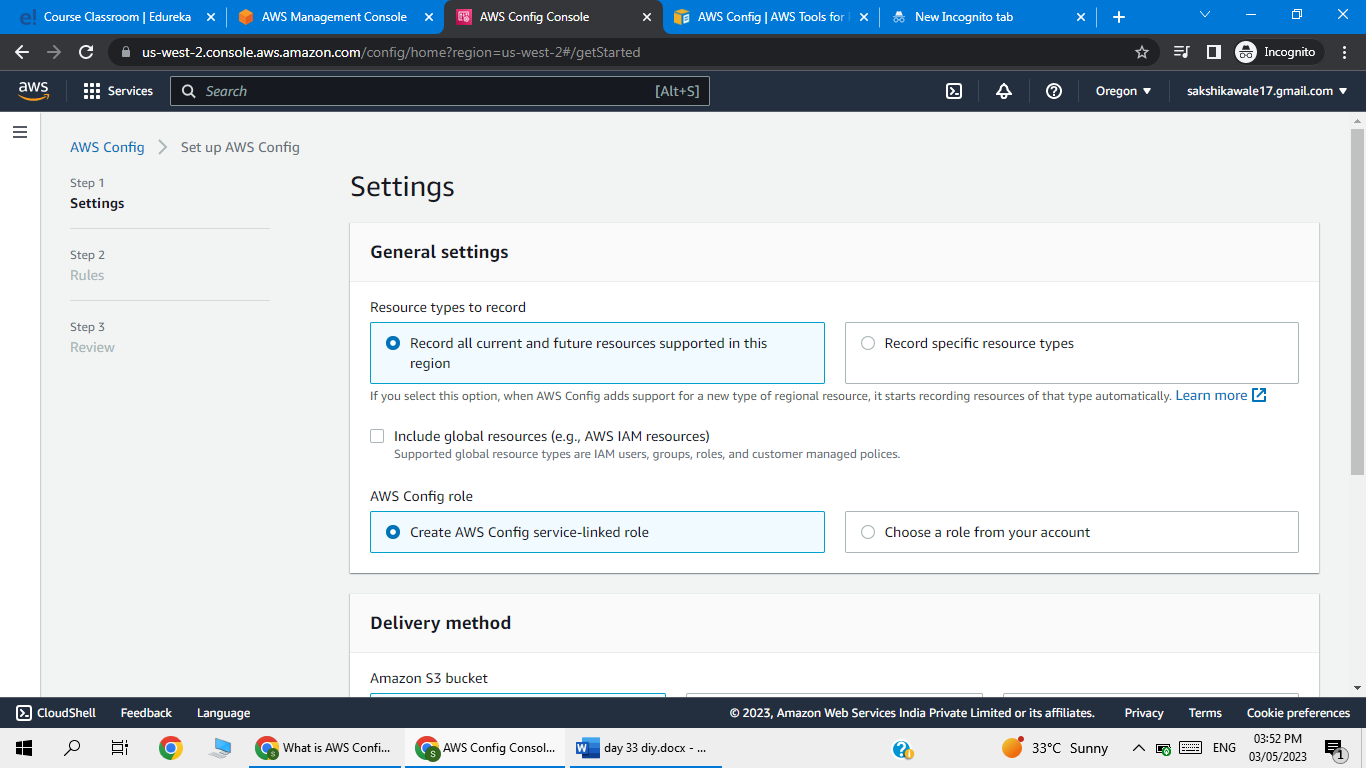


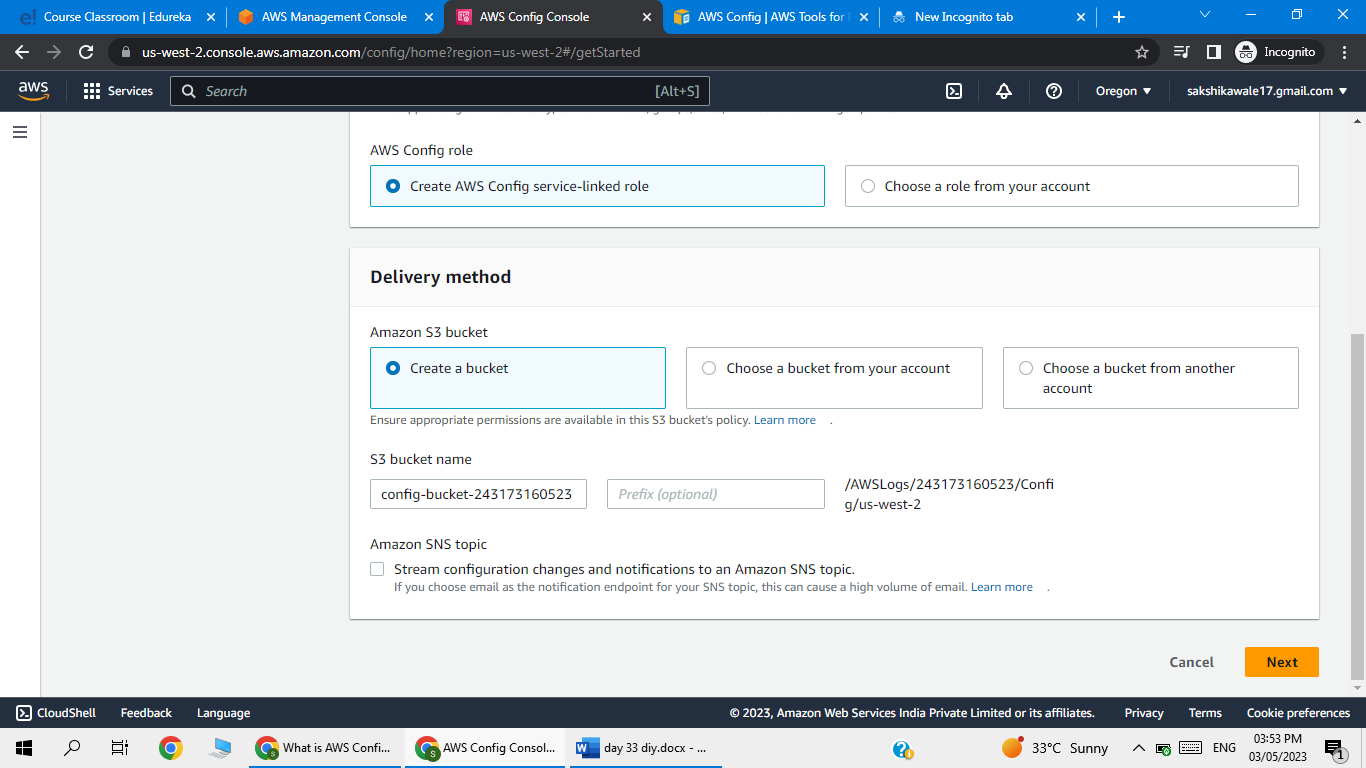


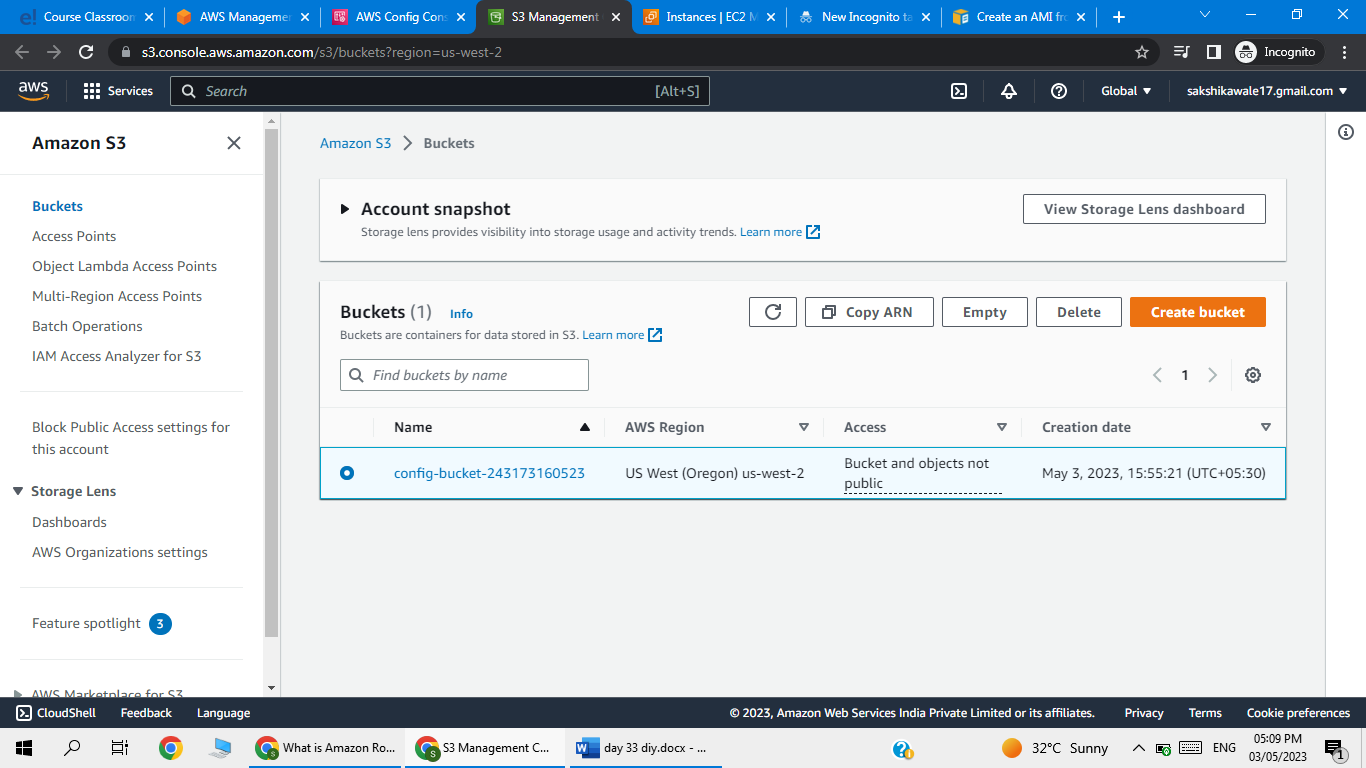


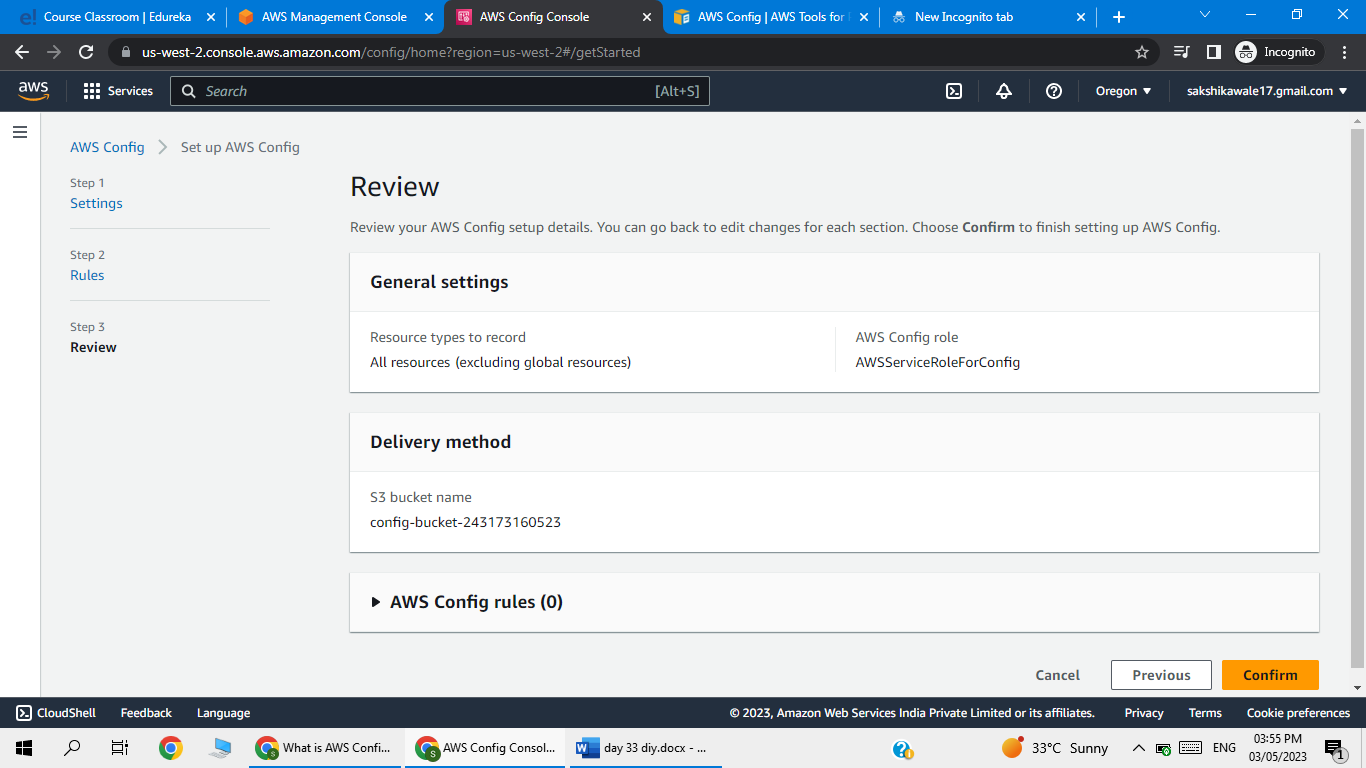


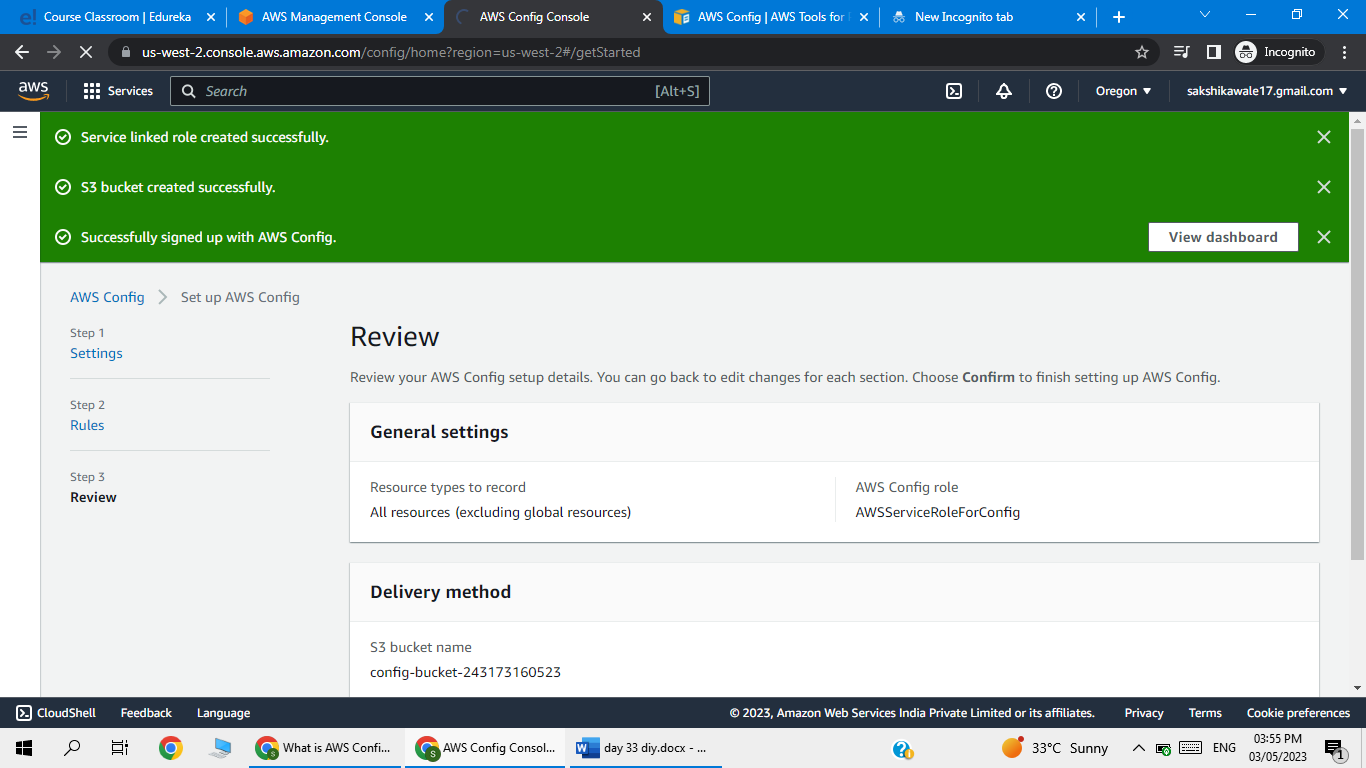






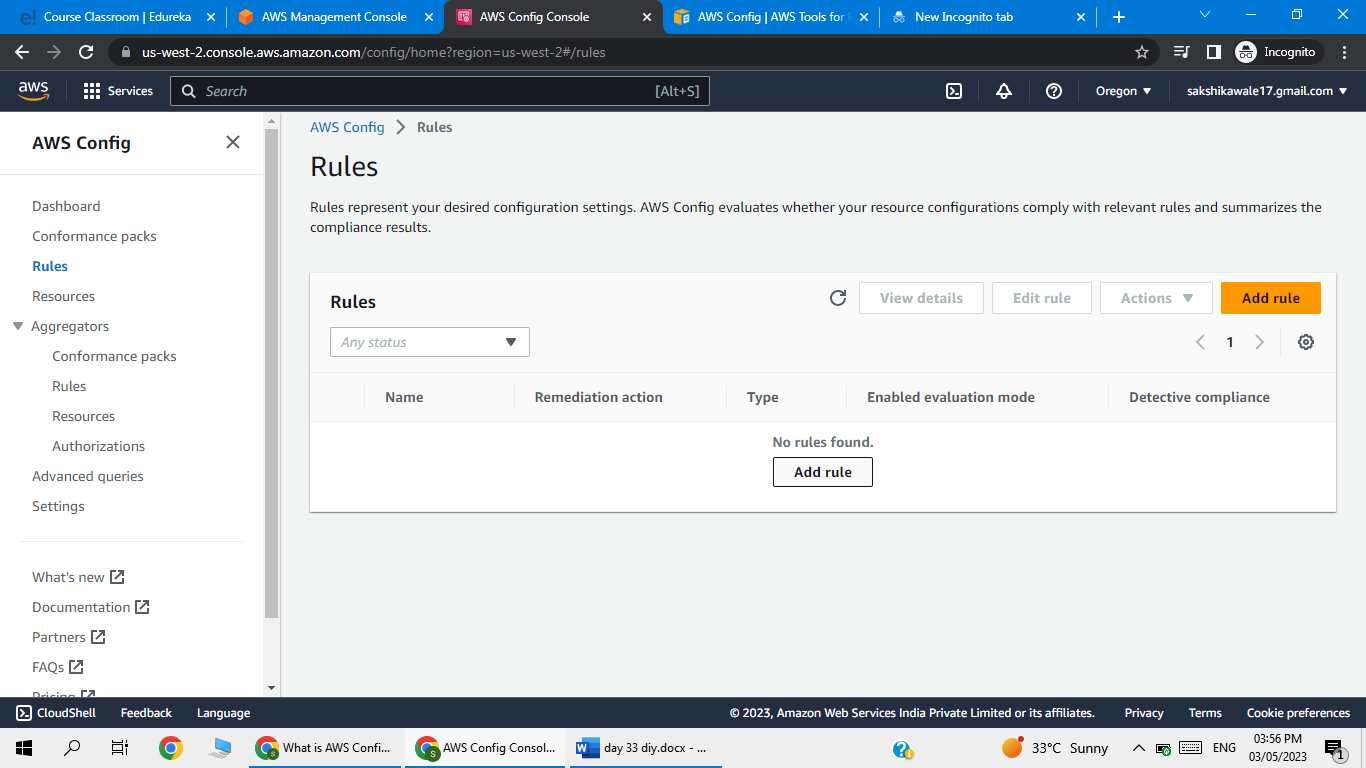


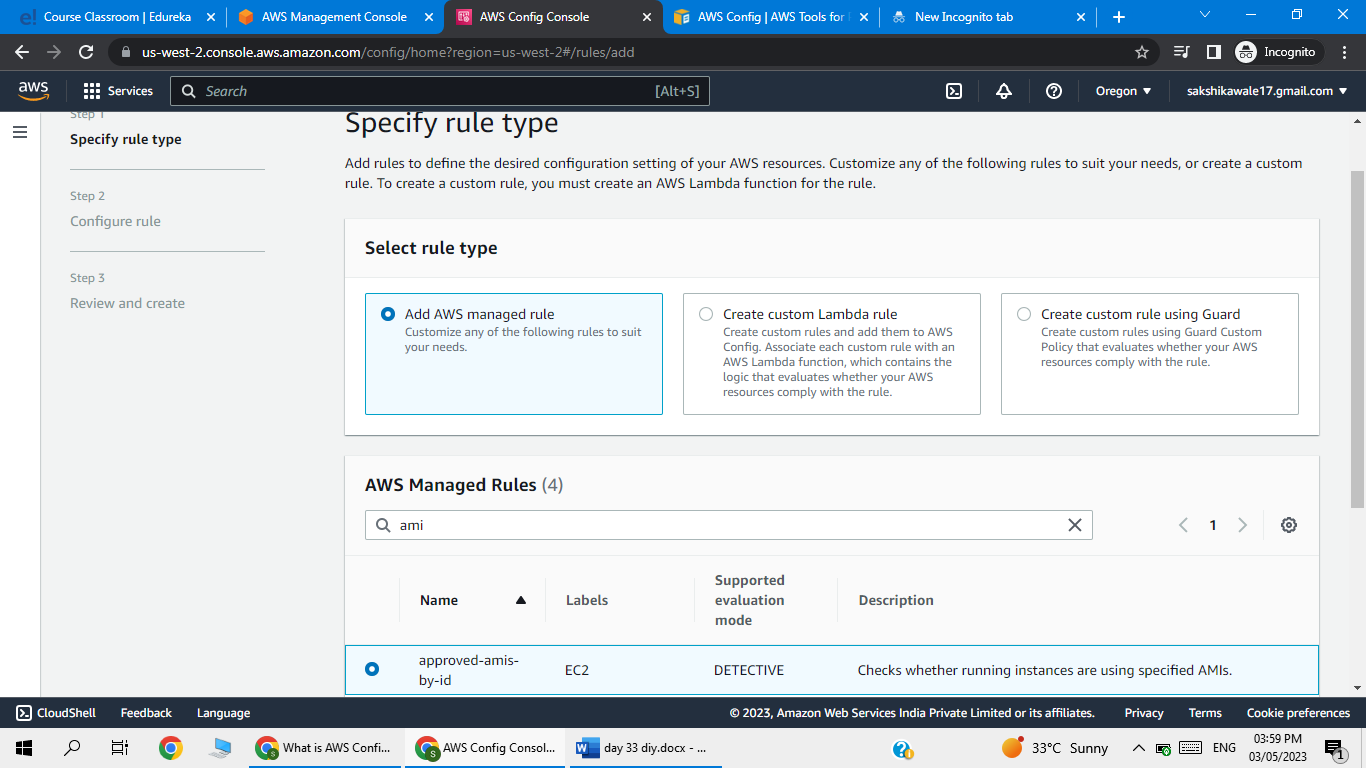


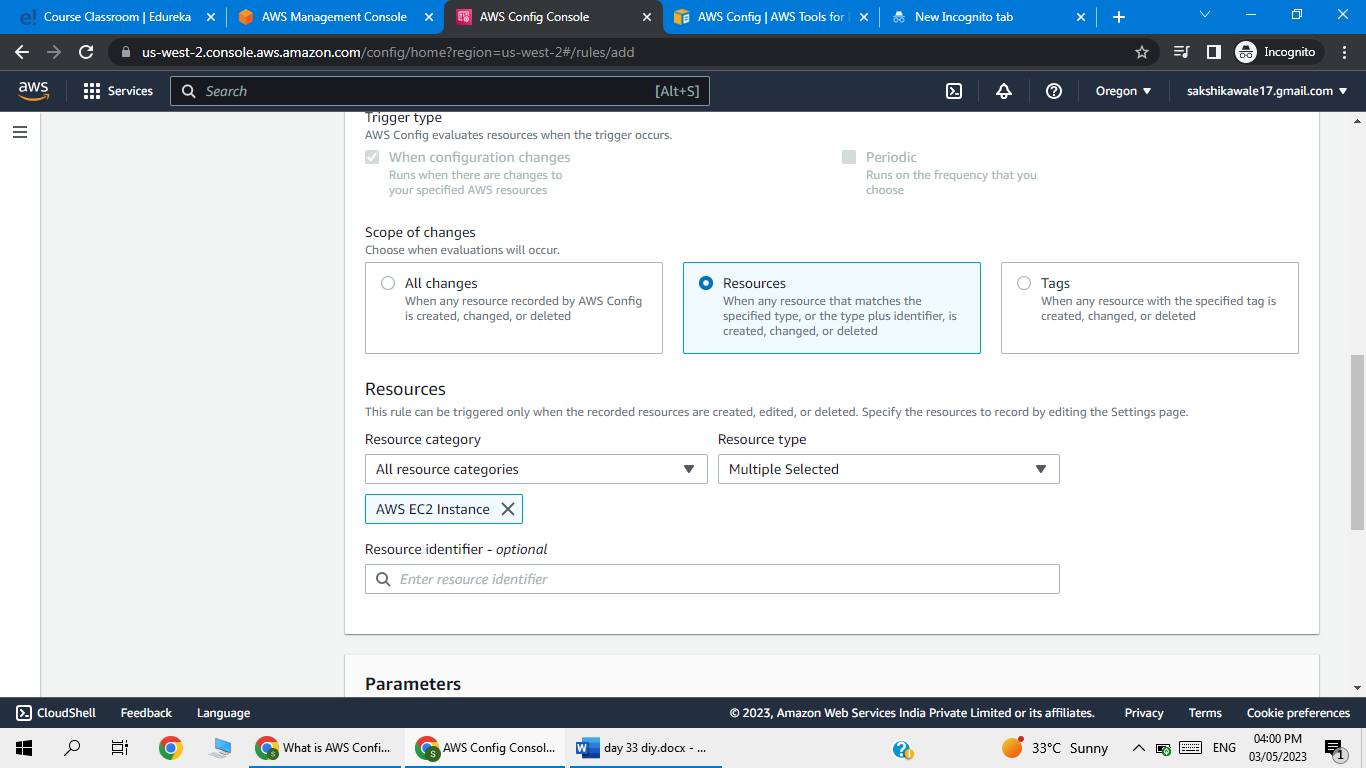


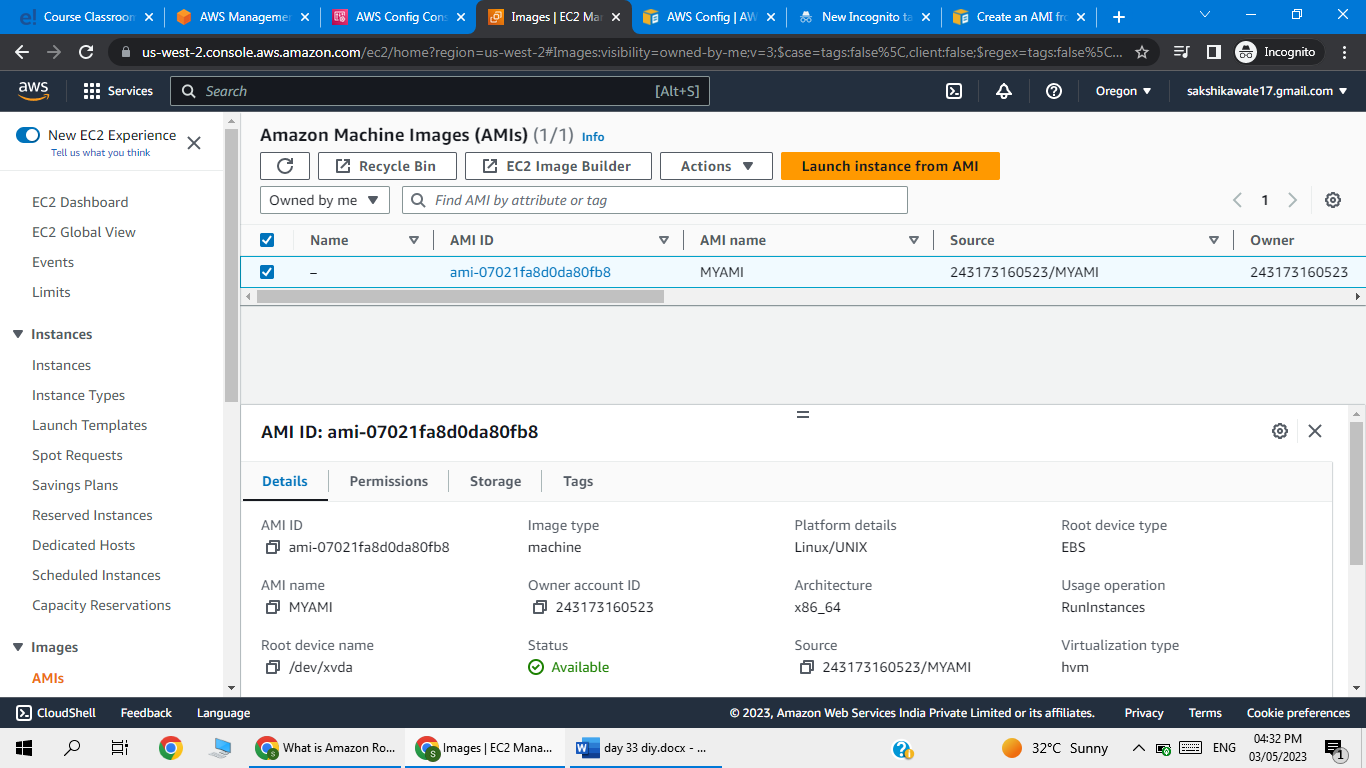
Go to rule

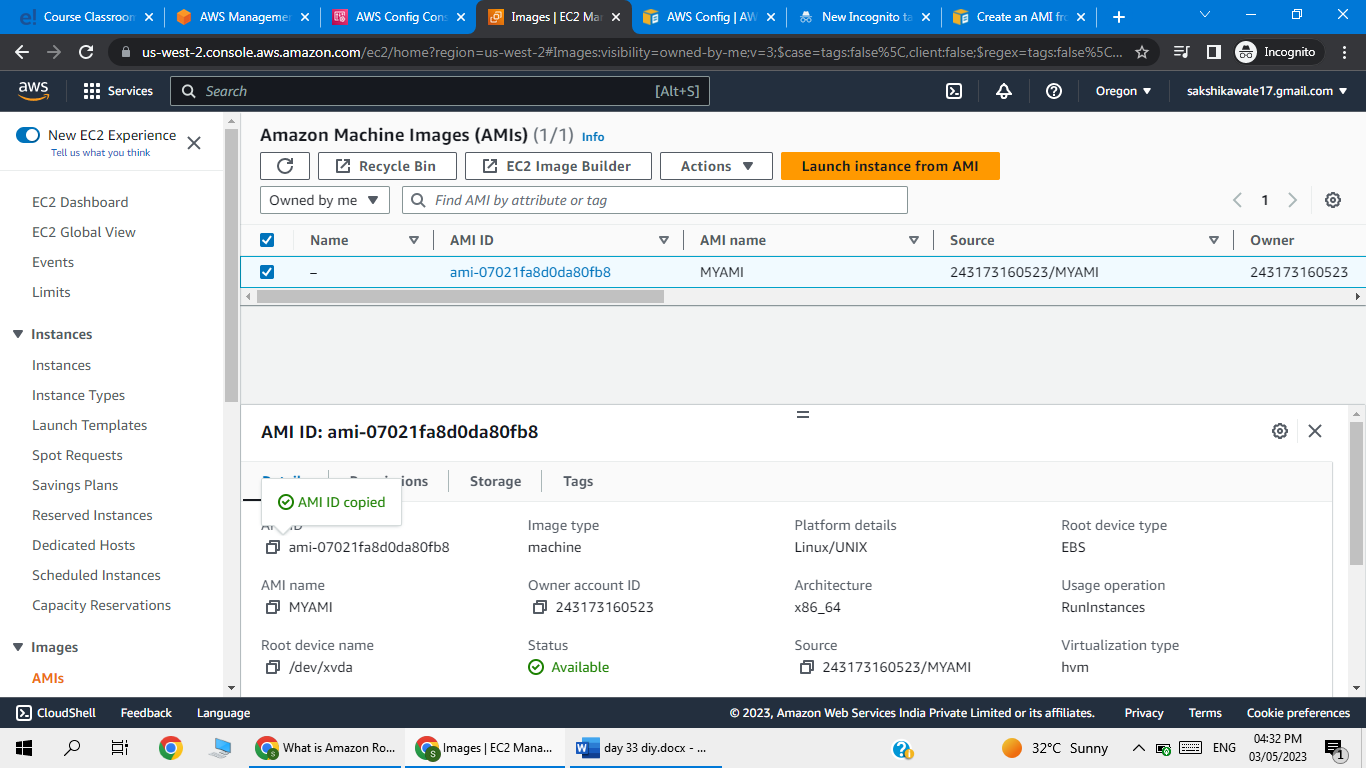
Click on add rule

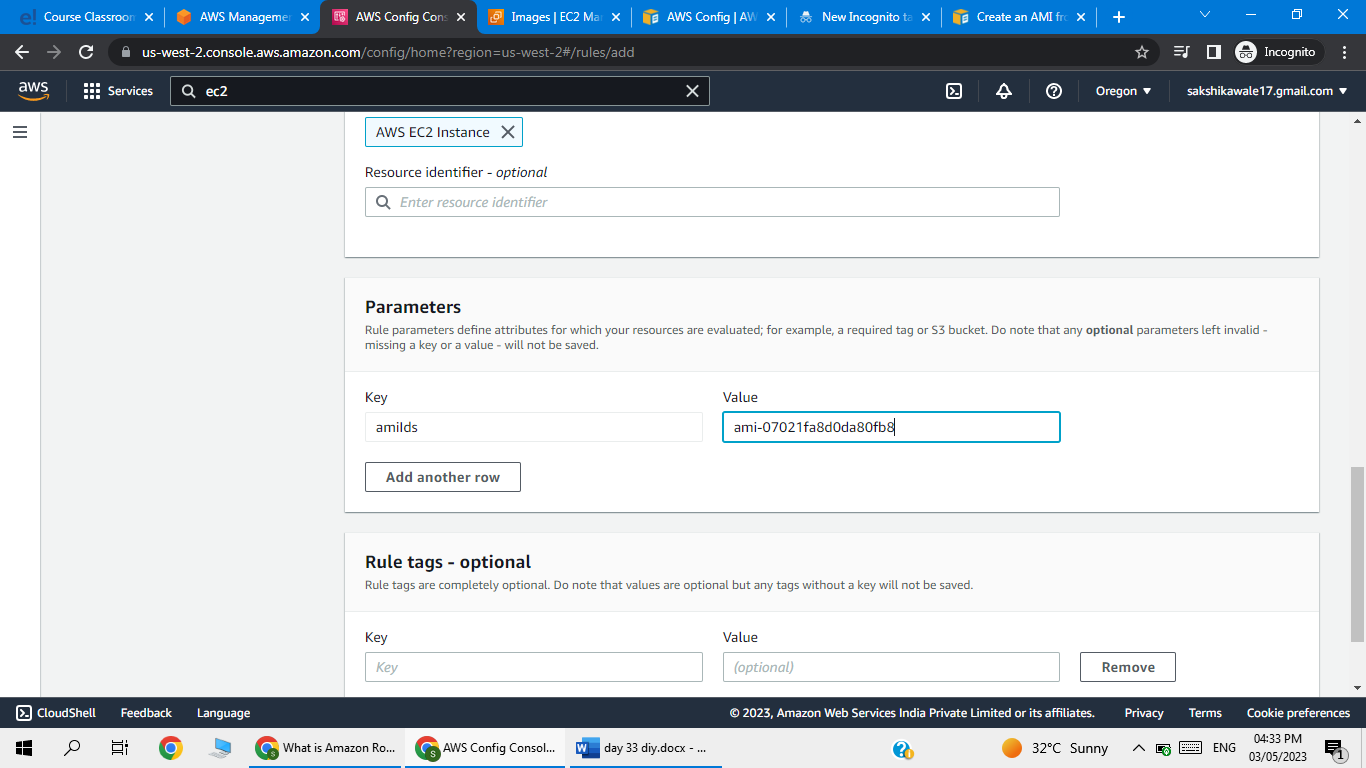


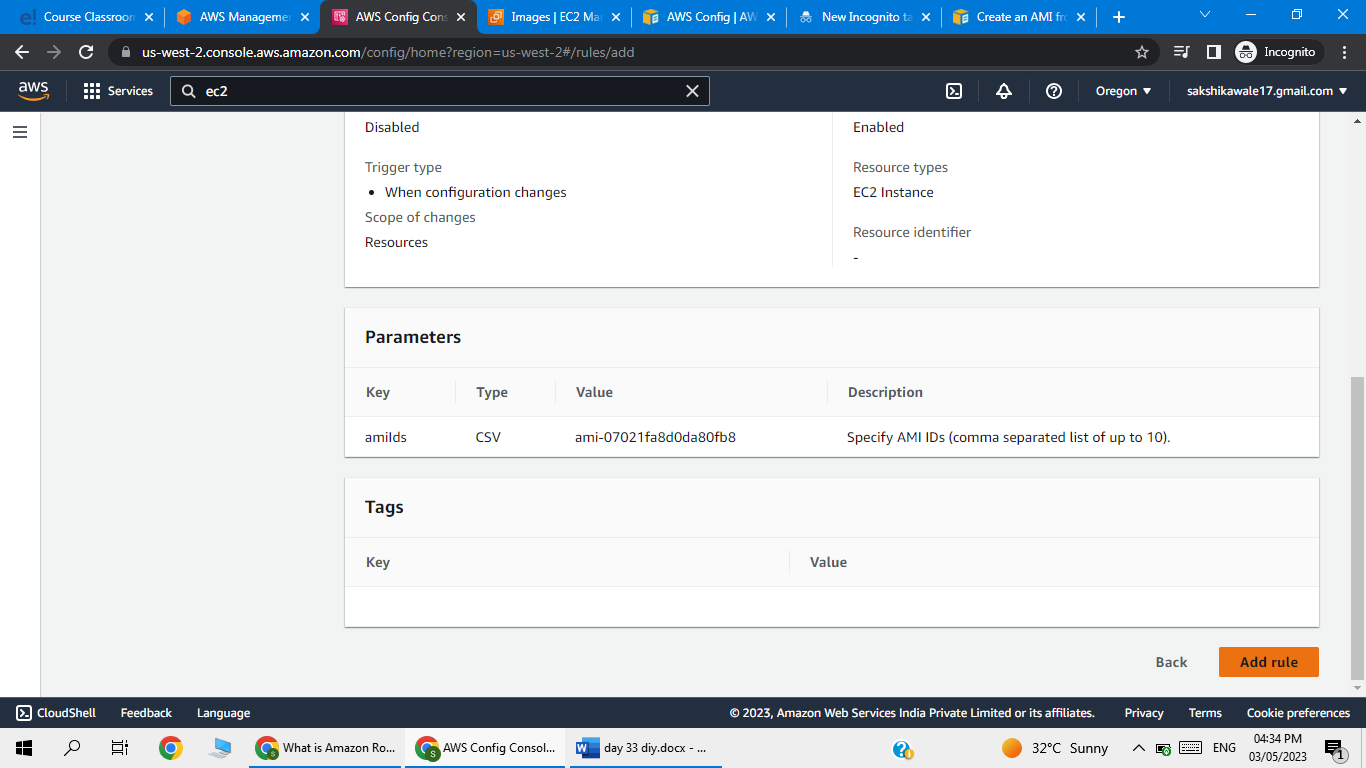


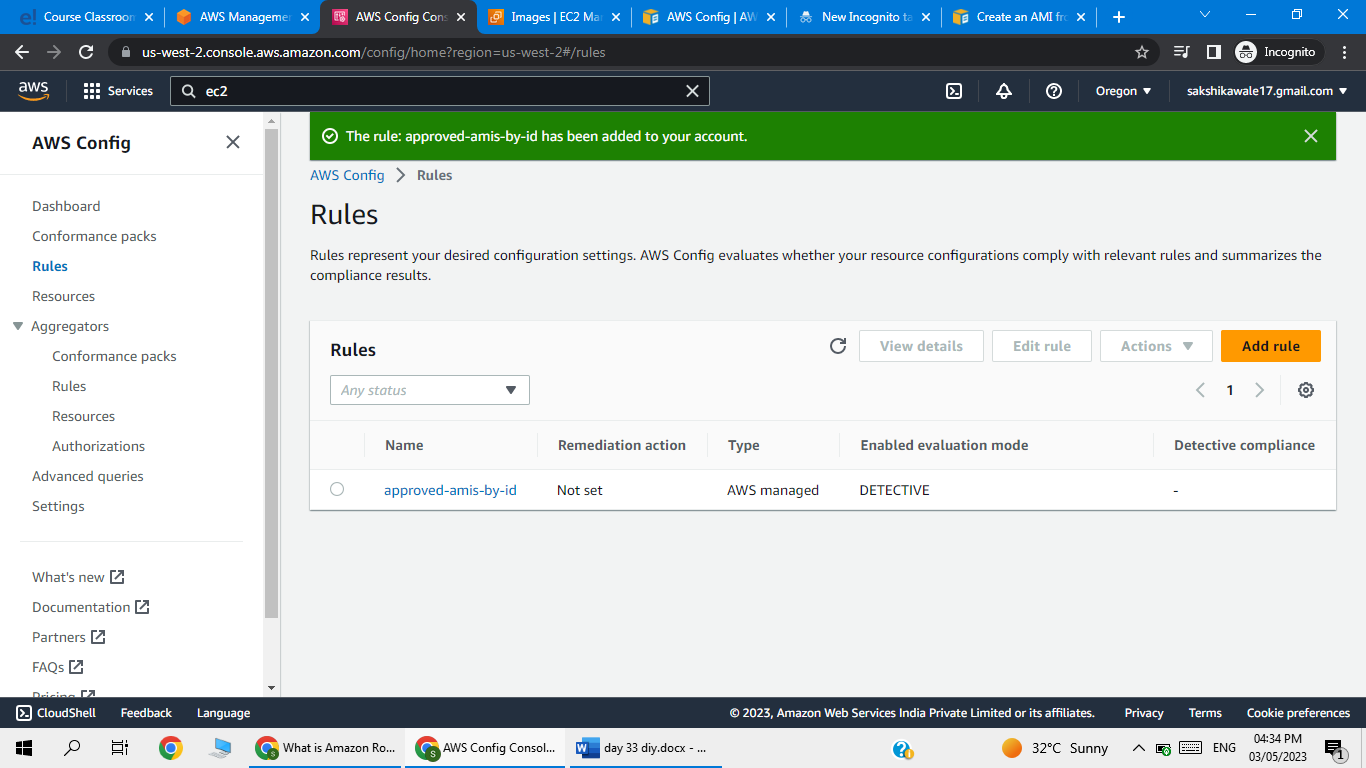




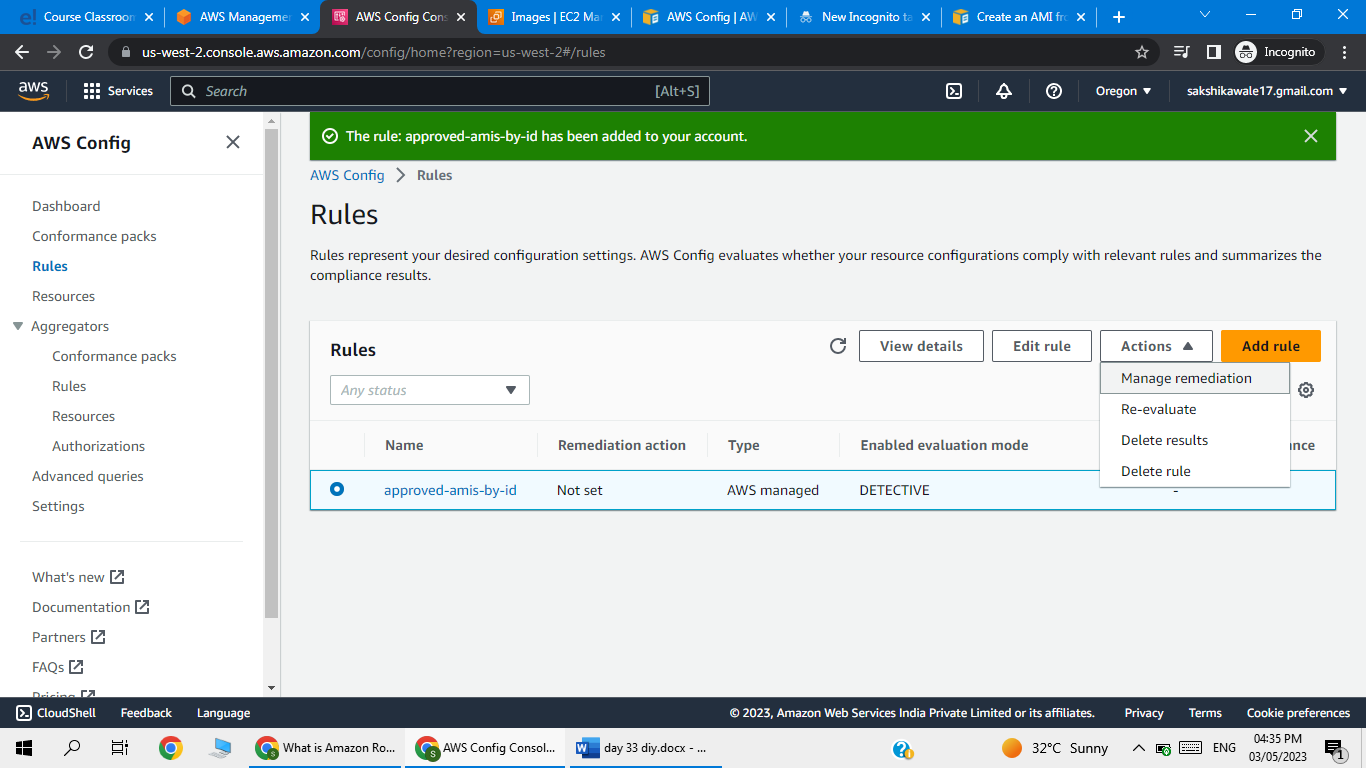


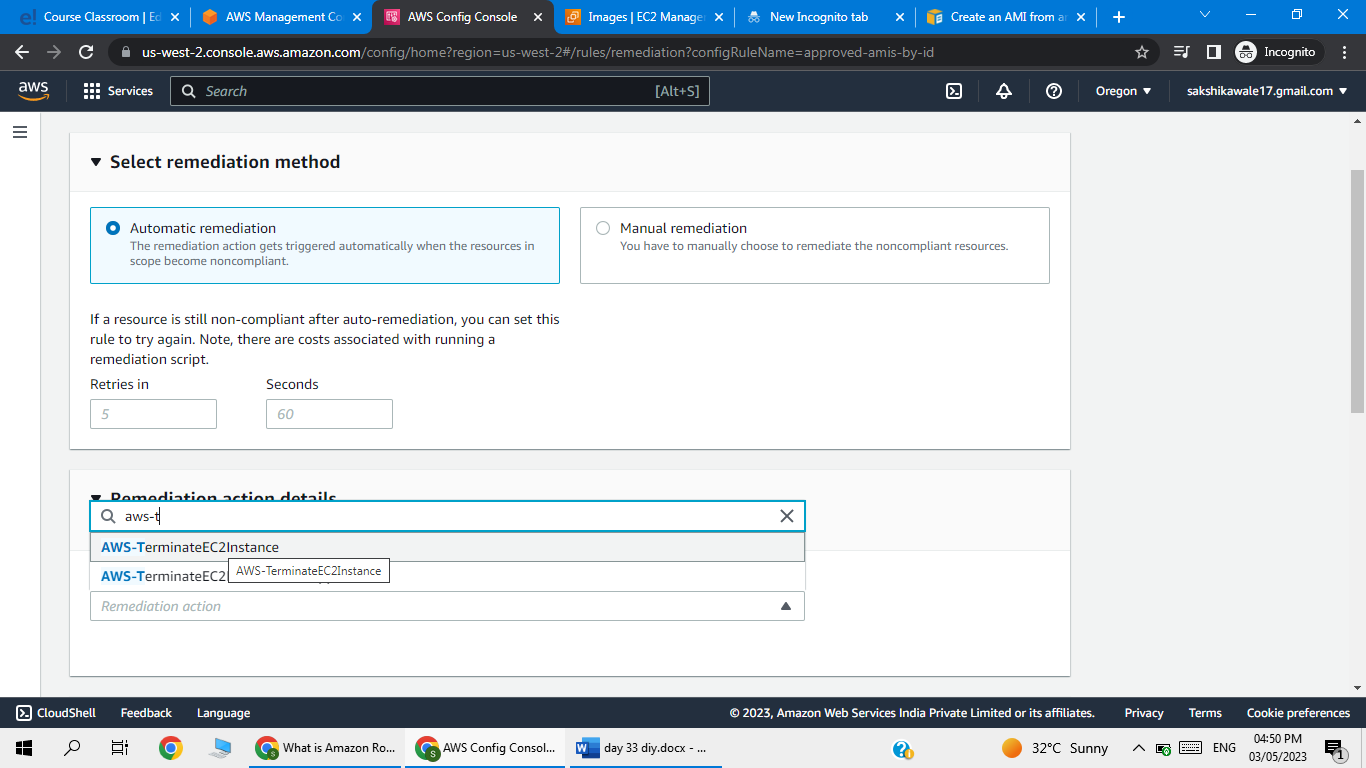


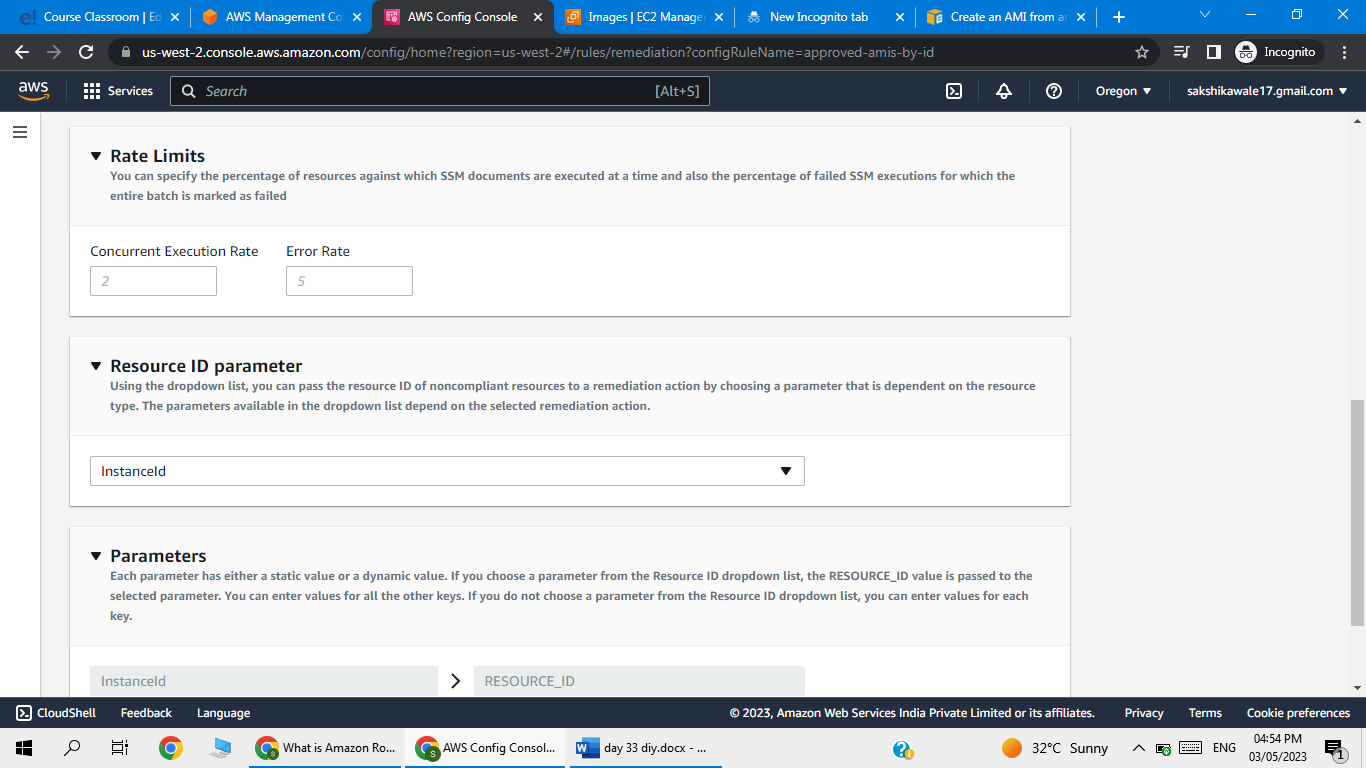




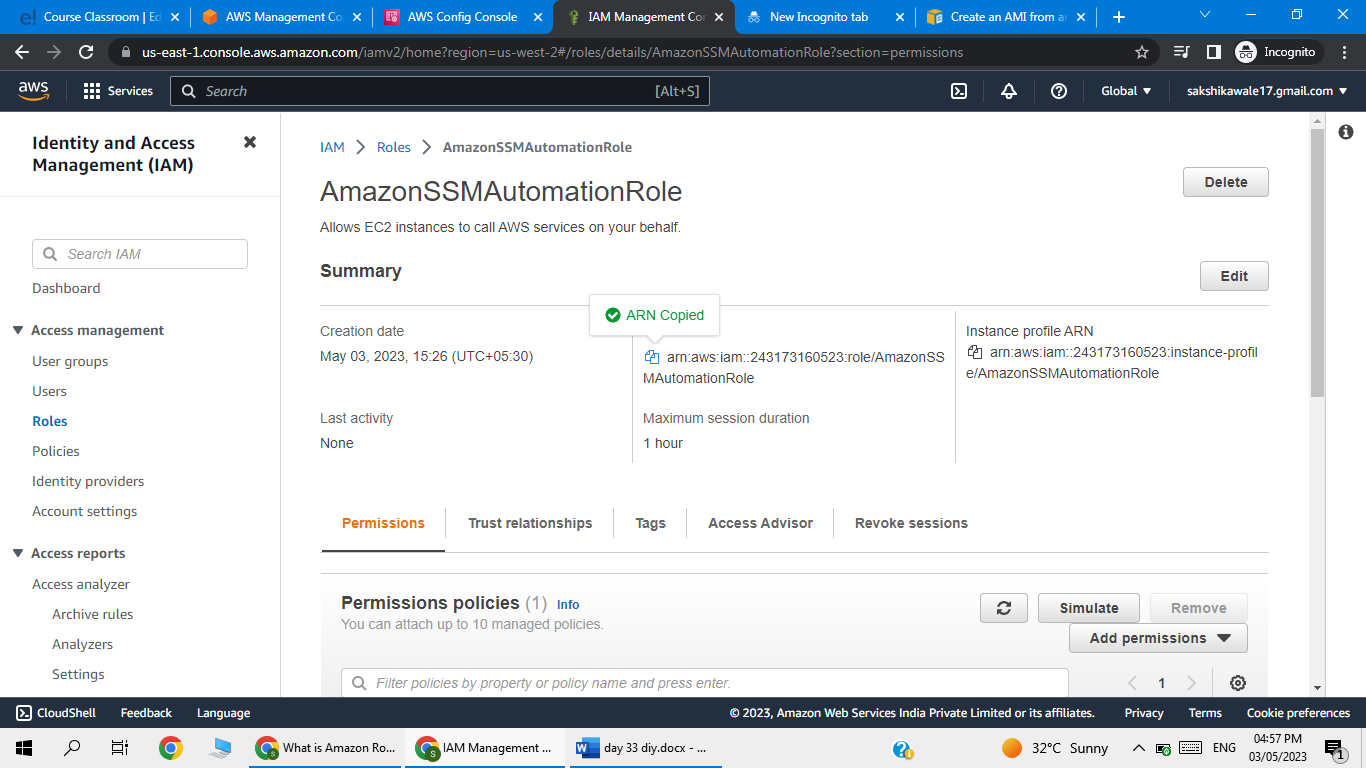
Now perform remediation







Go to IAM-role



Copy ARN and paste

