Andhra Pradesh State Skill Development Corporation

Skill AP
APSSDC

Skill AP
Learn Anytime Anywhere
Andhra Pradesh State Skill Development Corporation

AWS CLOUD COMPUTING

CONFIGURATION OF IDENTITY ACCESS MANAGEMENT (IAM) SERVICE

Configuration of Identity Access Management (IAM) Service

Configuration of IAM Users, Groups and Policies

Allow a **User** to **Manage IAM Users**. The following **policy** allows a **user** to perform all the tasks associated with **managing IAM users** but not to perform actions on other entities, such as creating **groups** or **policies**.

AWS IAM Overview

- AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources for your users.
- IAM is used to control
  - **Identity** – who can use your AWS resources (authentication)
  - **Access** – what resources they can use and in what ways (authorization)
- IAM can also keep your account credentials private.
- With IAM, multiple IAM users can be created under the umbrella of the AWS account or temporary access can be enabled through identity federation with corporate directory. Or third-party providers
- I AM also enabling access to resources across AWS accounts.

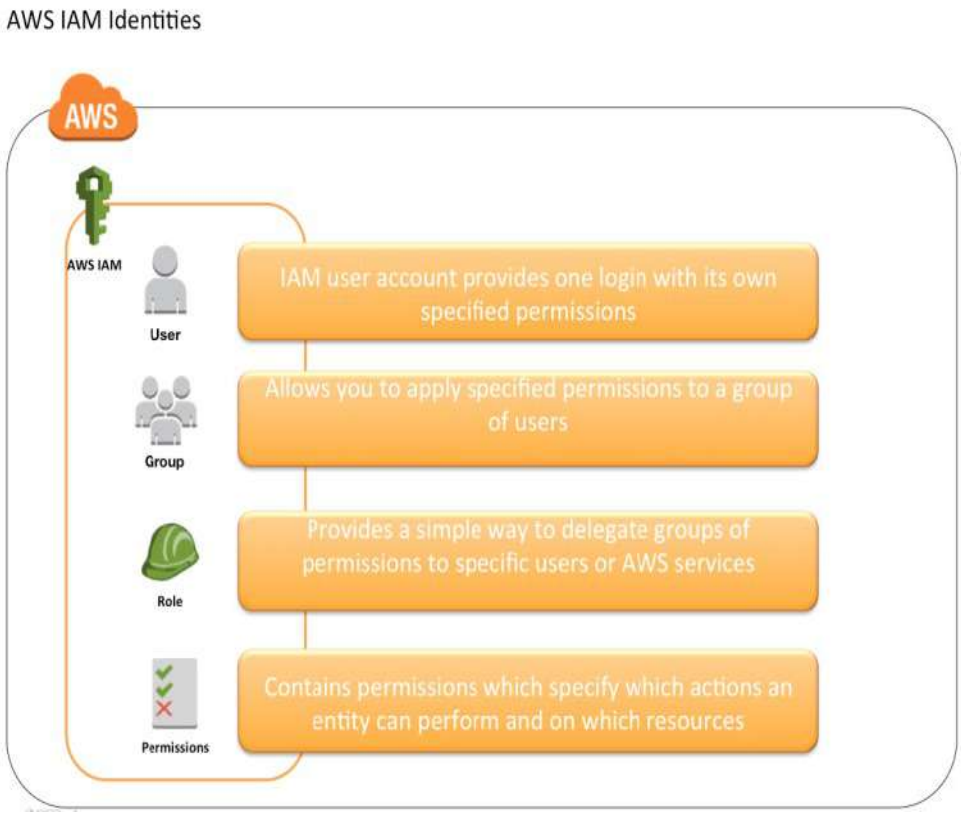
IAM Features

- Shared access to your AWS account
  - Grant other people permission to administer and use resources in your AWS account without having to share your password or access key.
- Granular permissions
  - Each user can be granted with different set granular permissions as required to perform their job
- Secure access to AWS resources for applications that run on EC2\
  - IAM can help provide applications running on EC2 instance temporary credentials that they need in order to access other AWS resources
- Identity federation
  - IAM allows users to access AWS resources, without requiring the user to have accounts with AWS, by providing temporary credentials for e.g. through corporate network or Google or Amazon authentication
- Identity information for assurance
  - CloudTrail can be used to receive log records that include information about those who made requests for resources in the account.
- PCI DSS Compliance
  - IAM supports the processing, storage, and transmission of credit card data by a merchant or service provider, and has been validated as being Payment Card Industry Data Security Standard (PCI DSS) compliant
- Integrated with many AWS services

- IAM integrates with almost all the AWS services
- Eventually Consistent
  - IAM, like many other AWS services, is eventually consistent and achieves high availability by replicating data across multiple servers within Amazon's data centers around the world.
  - Changes made to IAM would be eventually consistent and hence would take some time to reflect
- Free to use
  - IAM is offered at no additional charge and charges are applied only for use of other AWS products by your IAM users.
- AWS Security Token Service
  - IAM provides STS which is an included feature of the AWS account offered at no additional charge.
  - AWS charges only for the use of other AWS services accessed by the AWS STS temporary security credentials.

Identities

IAM identities determine who can access and help to provide authentication for people and processes in your AWS account

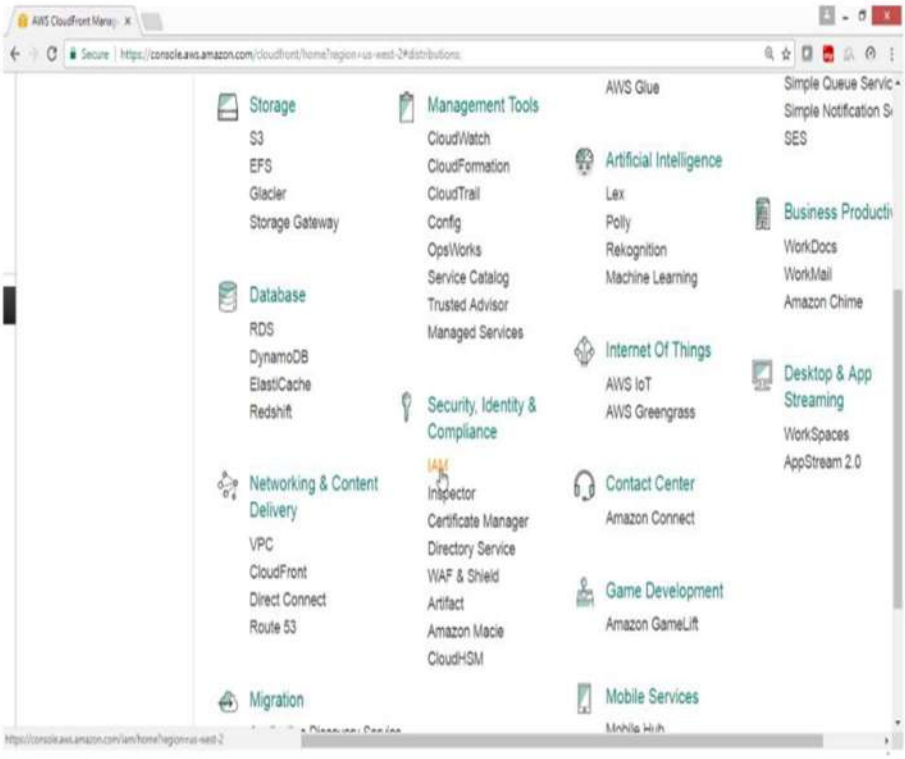


To configure IAM with the following task.

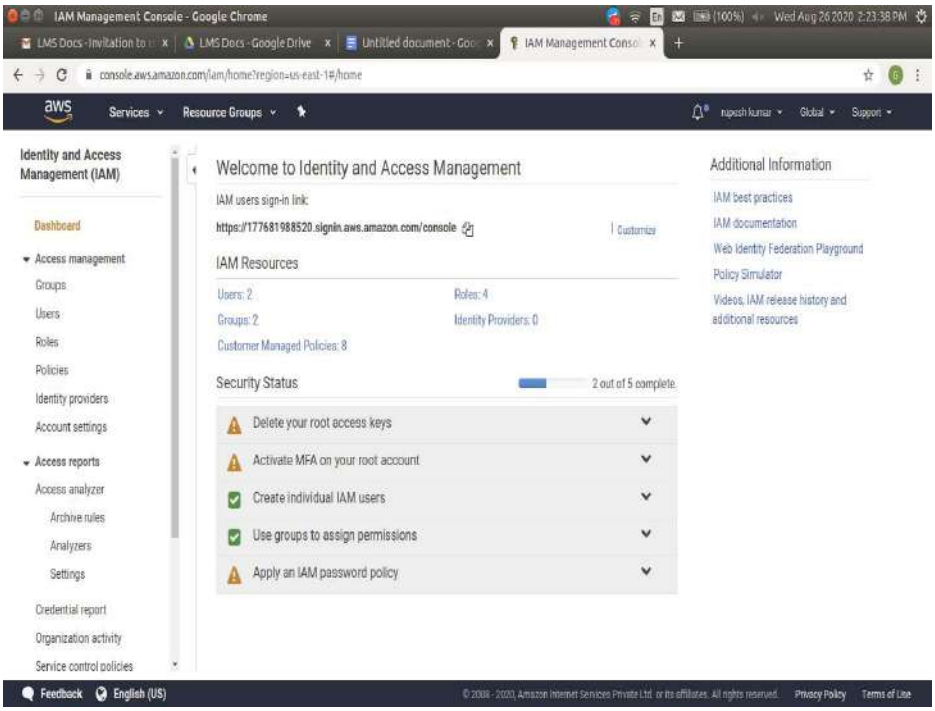
Create IAM users, assign password and change password policy
Create IAM group
Add users to a group
Add policies to Groups and Users
Create your own policies.
Users Login to sign-in page.
Deleting users and groups.

Creating an IAM role to login other users.

Open AWS console and select Security, Identity & Compliance
Click on **IAM** service

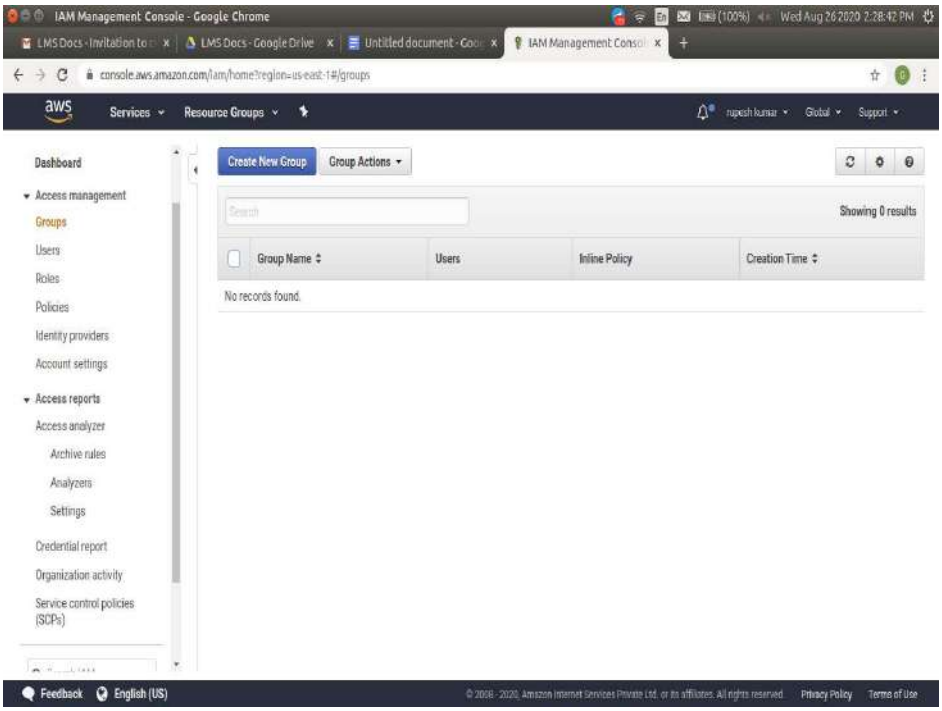


IAM Dashboard panel available

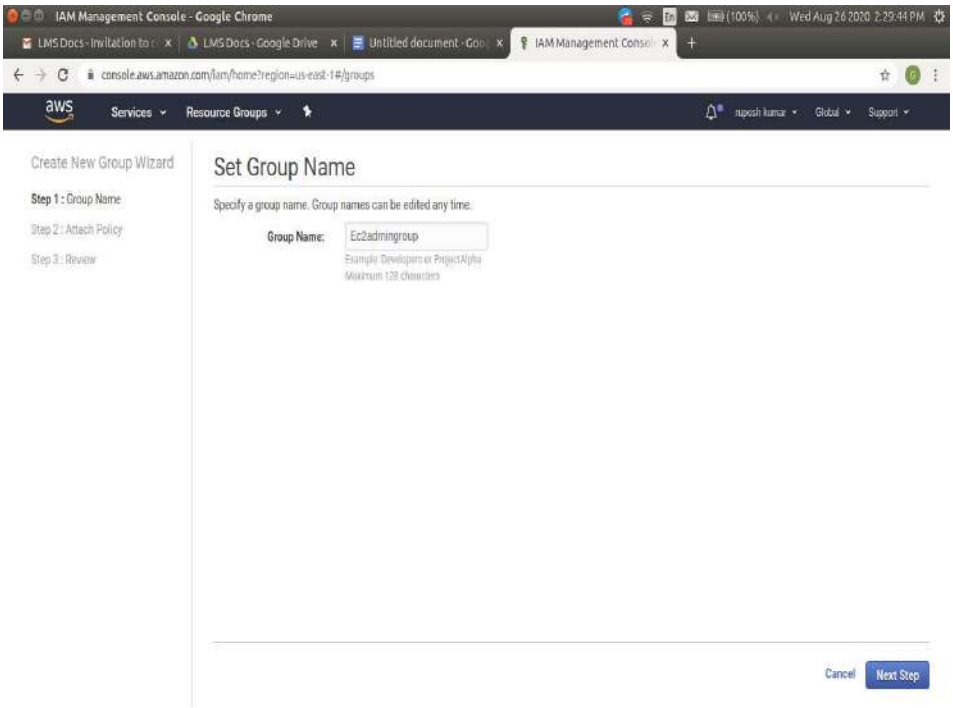


To Manage groups and apply policies

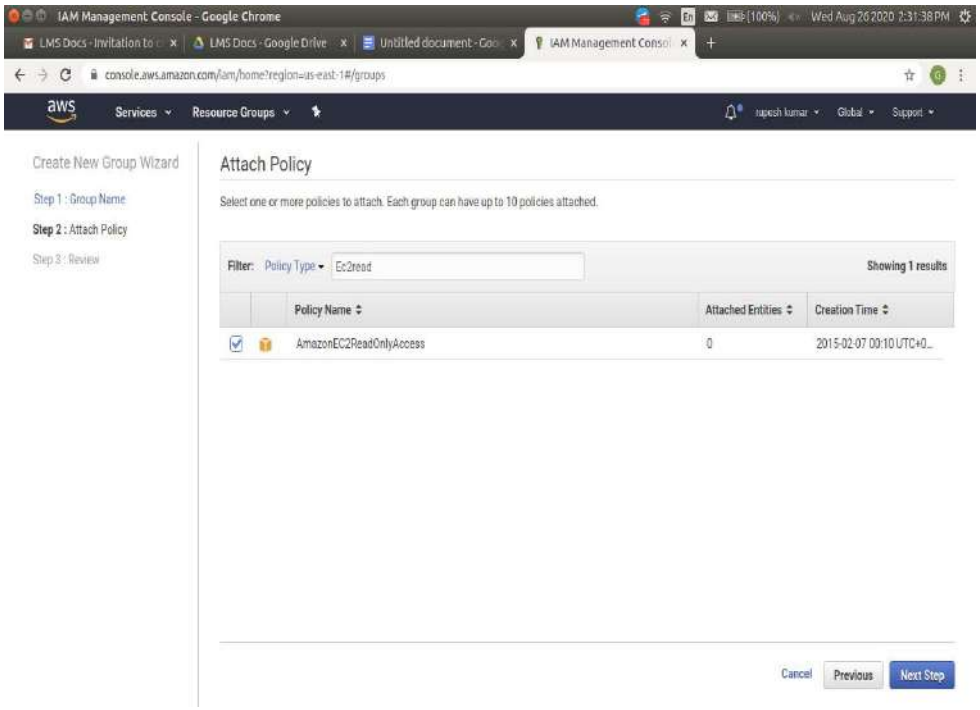
From IAM dashboard, select Groups. Click on Create New Group button



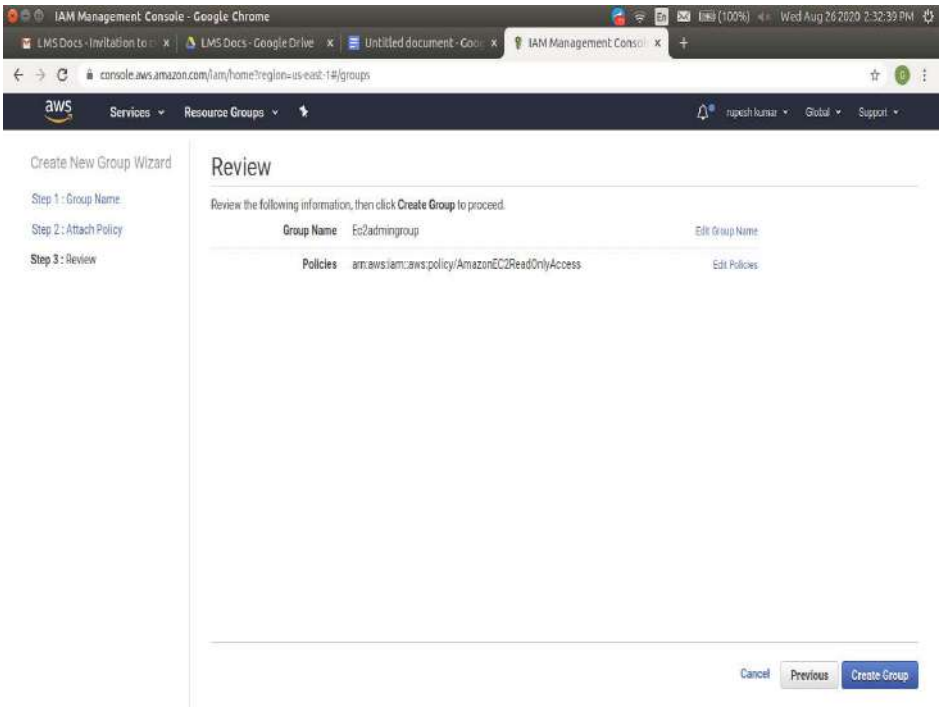
Give Group Name → EC2admingroup
Click on Next Step button



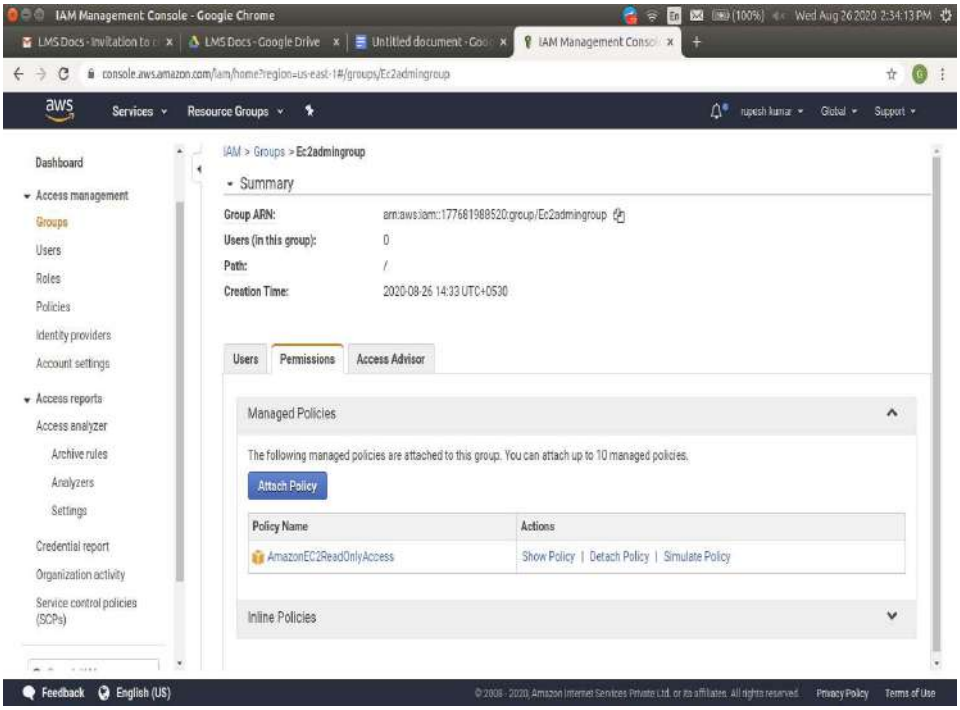
In Filter type → EC2 Read Only access
Select check box for Amazon EC2 Read Only access
Click on Next Step button



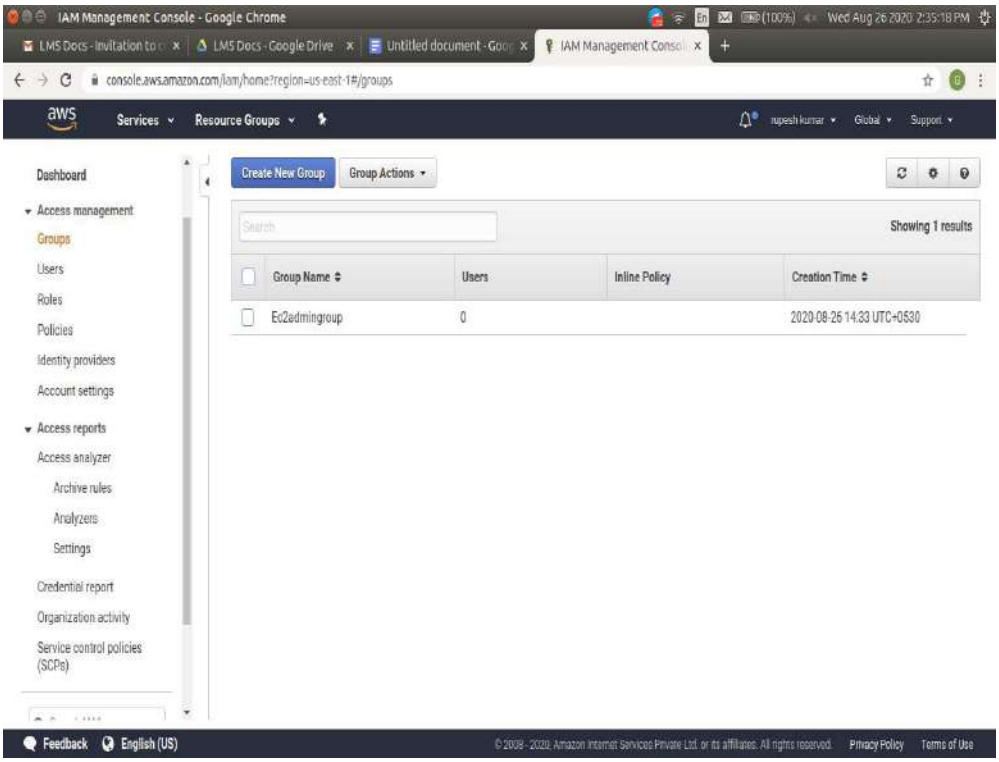
Click on Create Group



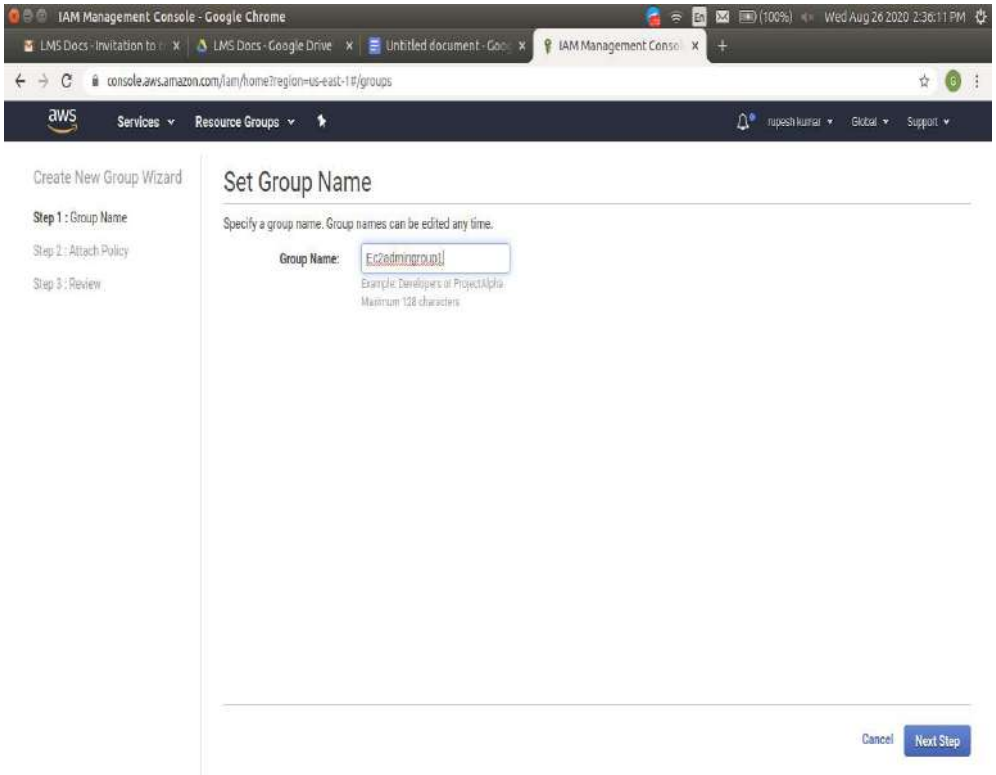
Verify Group EC2admingroup got created with Amazon EC2ReadOnlyAccess



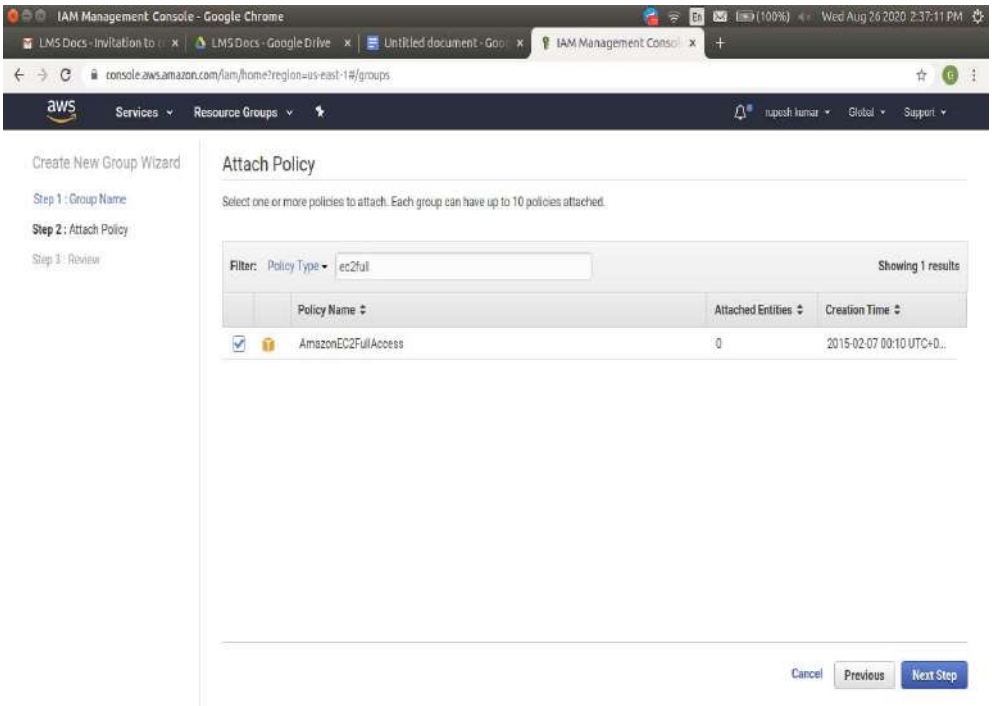
Now again create Another Group
Click on Create Group



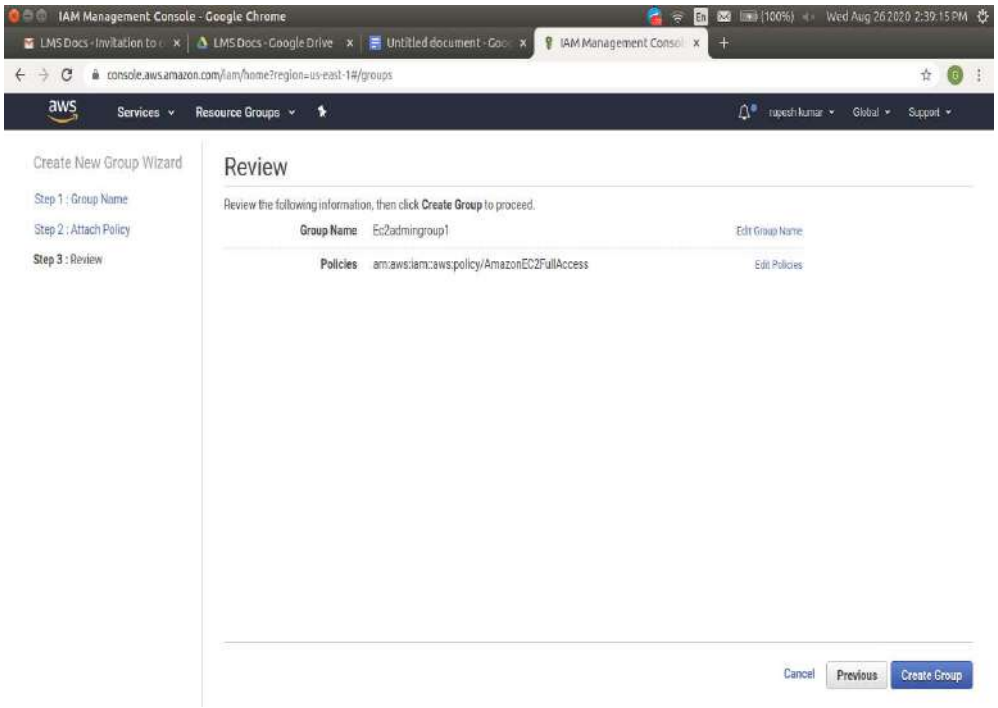
Give Group Name → EC2admingroup1
Click on Next Step button



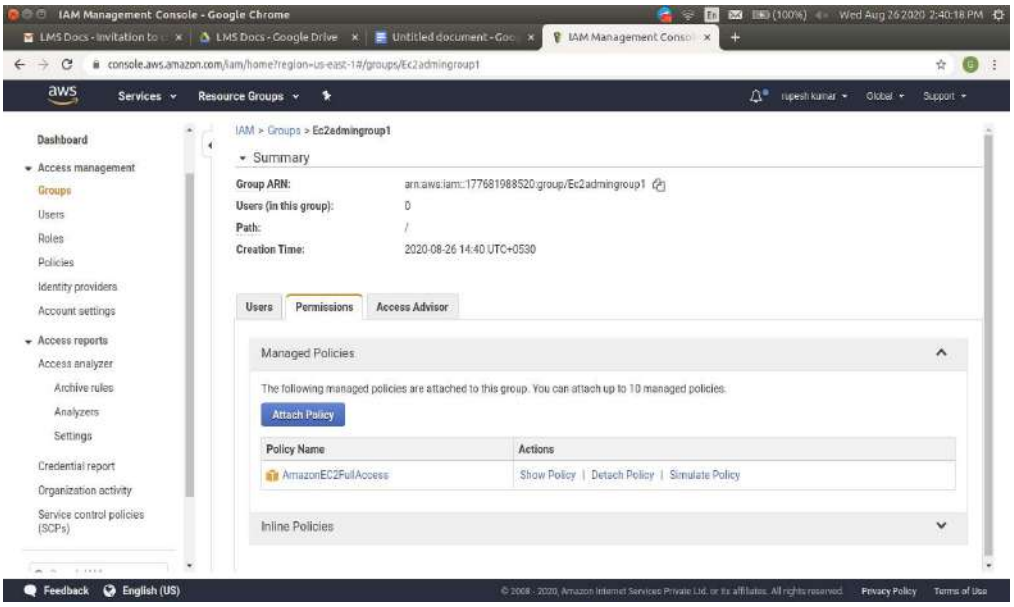
In Filter type → EC2FullAccess
Select check box for AmazonEC2FullAccess
Click on Next Step button



Click on Create Group



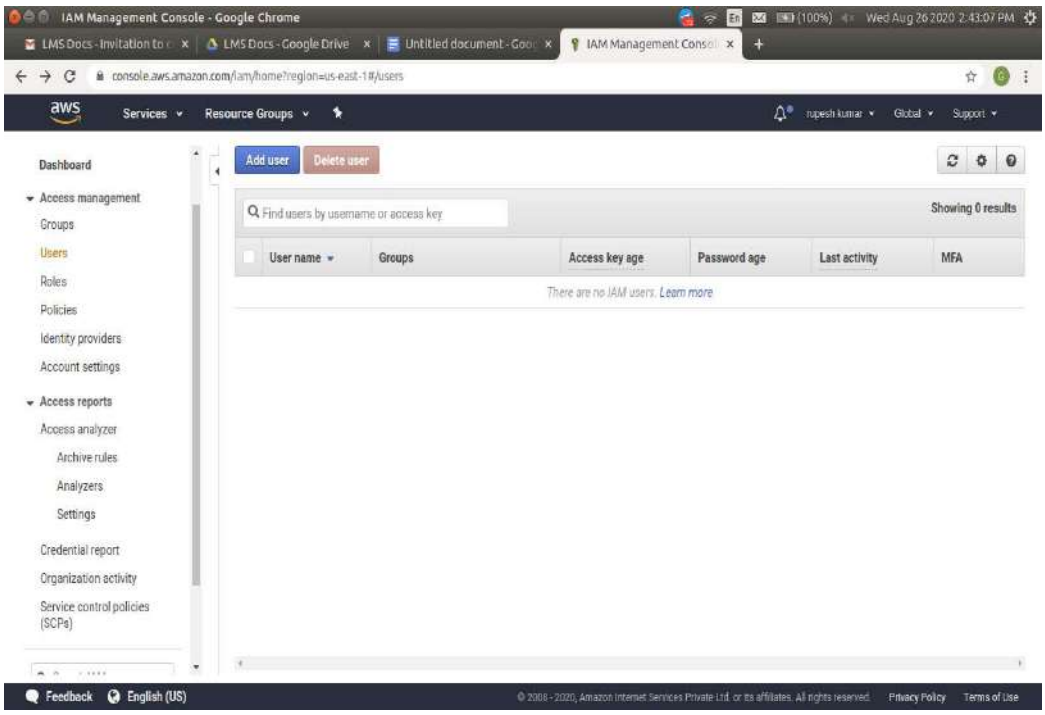
Verify Group EC2admingroup1 got created with AmazonEC2FullAccess



Create user **ram** join to EC2admingroup
Create user **sdc** join to EC2admingroup1

Create user **ram** and add **EC2ReadOnlyAccess Policy** and Create user **sdc** and add **EC2fullAccess Policy**

From IAM dashboard
Select Users Click on ADD Users button



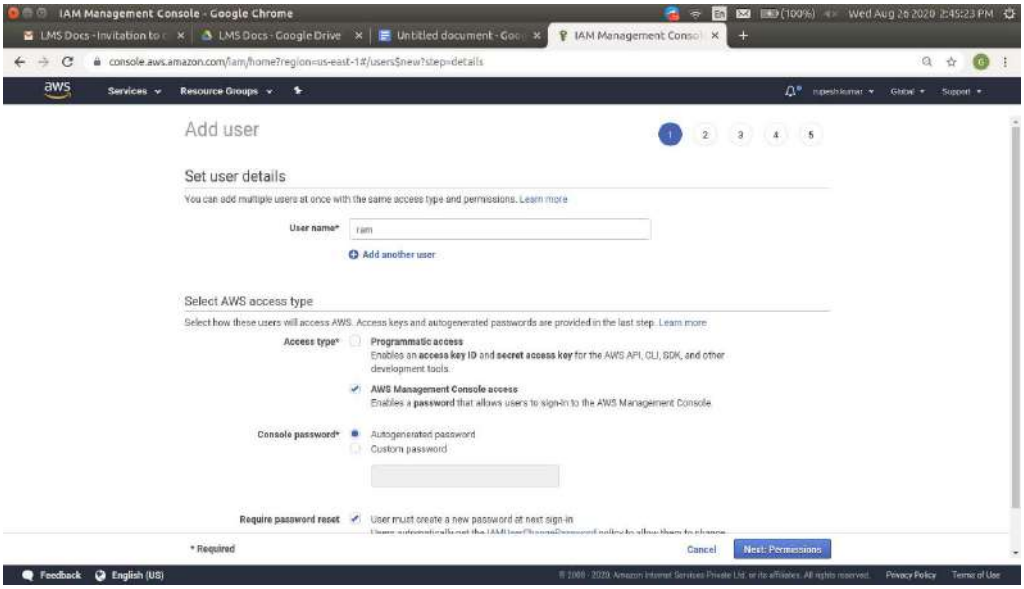
1. **Scenario**

   Create user **ram** to **EC2admingroup**

   For username → ram

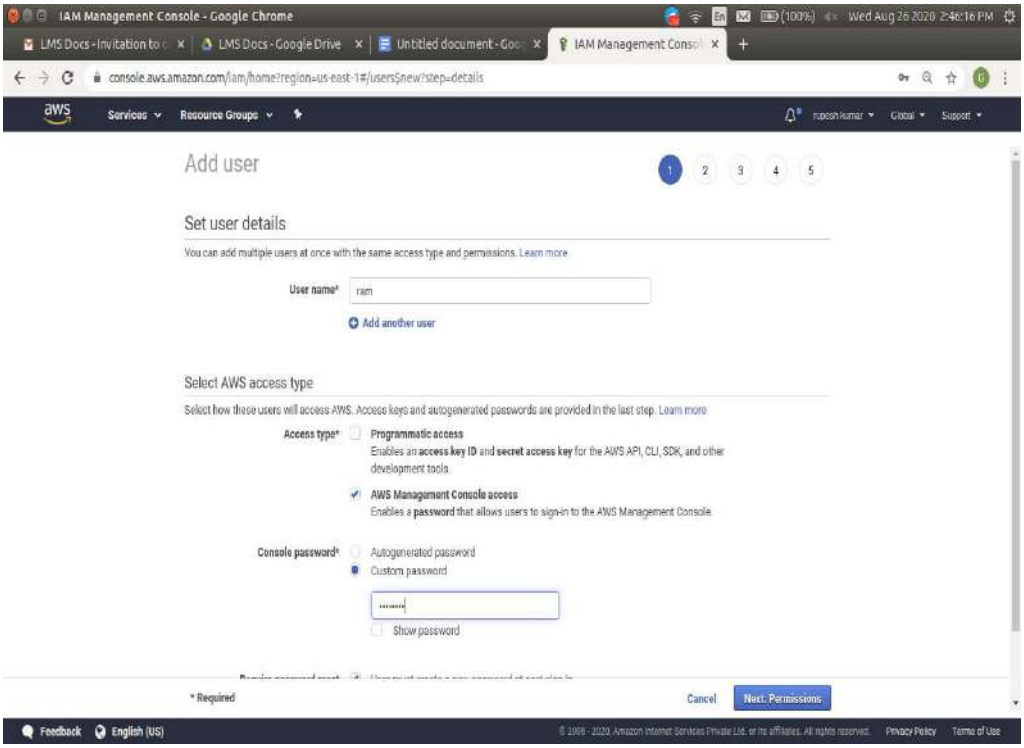
   For Access type → AWS Management Console access

Drag down

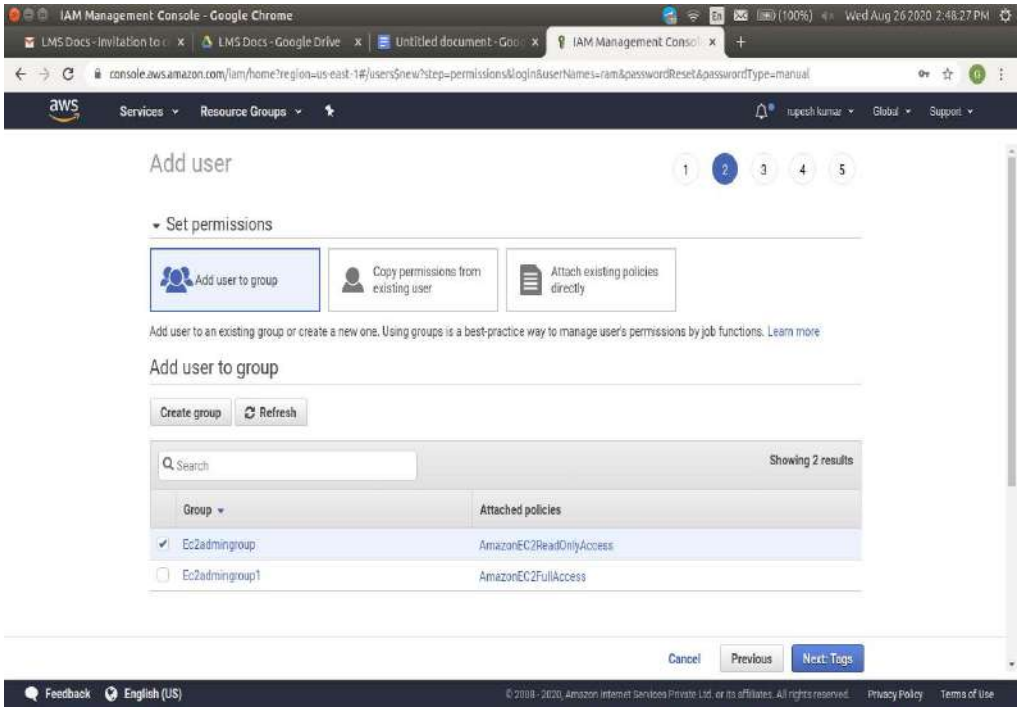


For Console password → ********

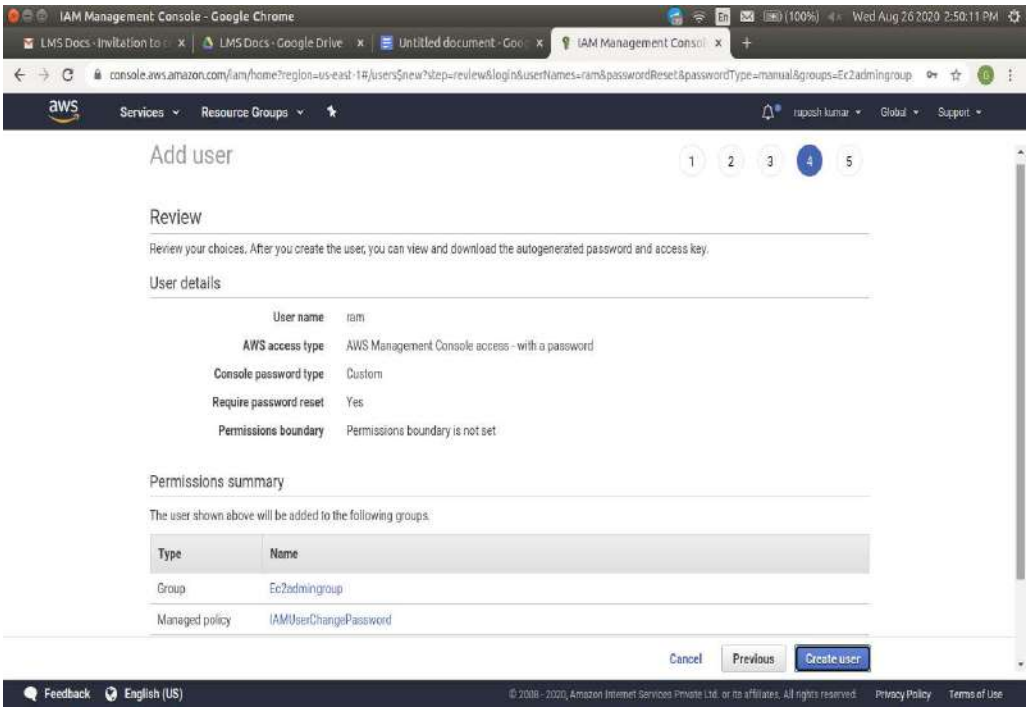
Click on Next Permission button



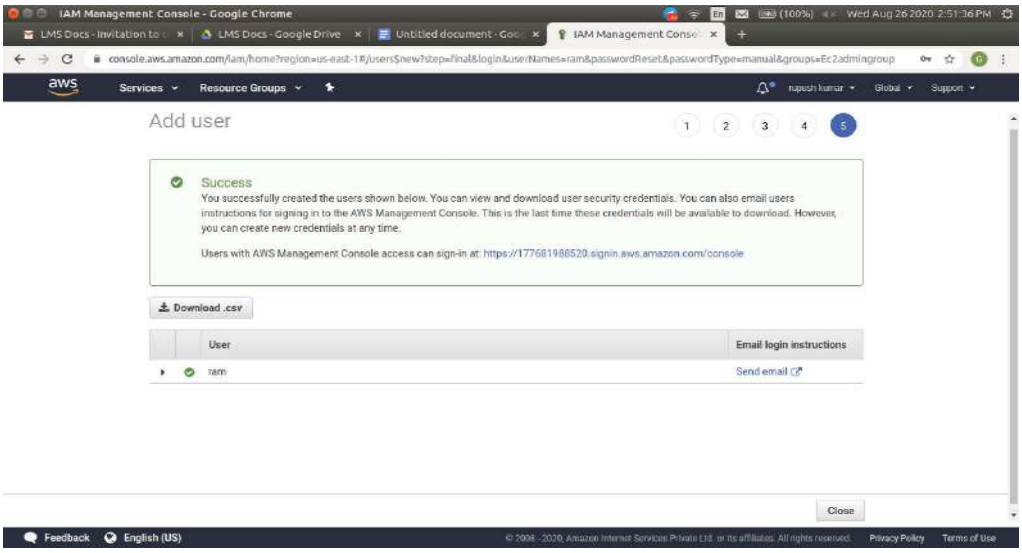
Under Group column, Select EC2admingroup
Click on Next Review



Verify users details
Click on Create user button



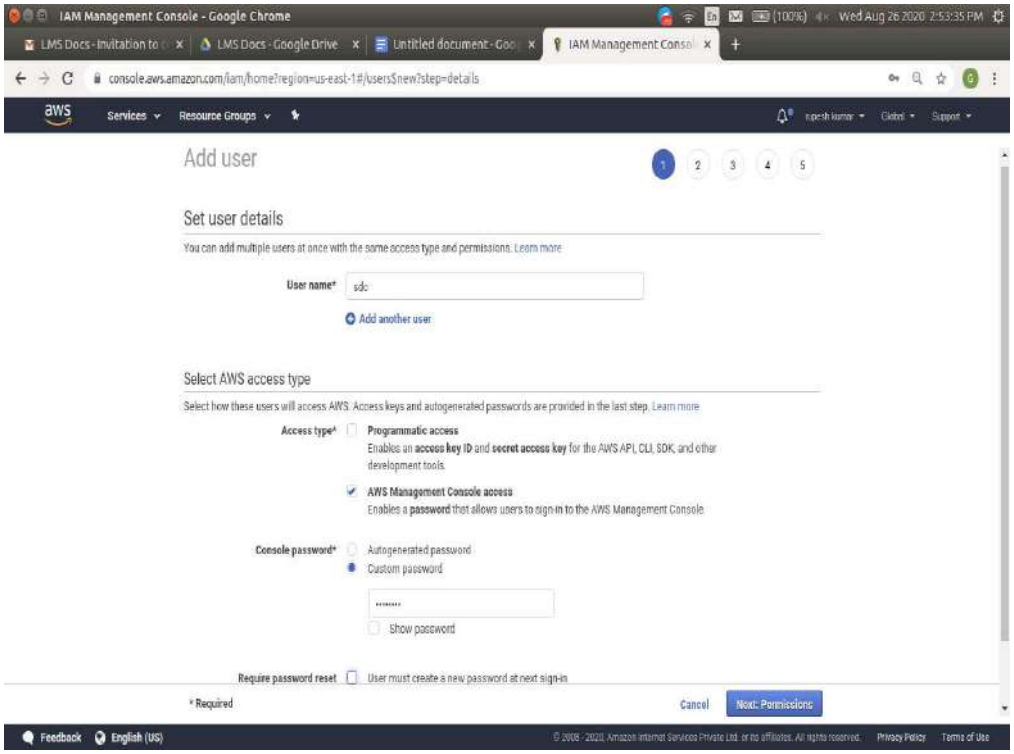
Click on close button



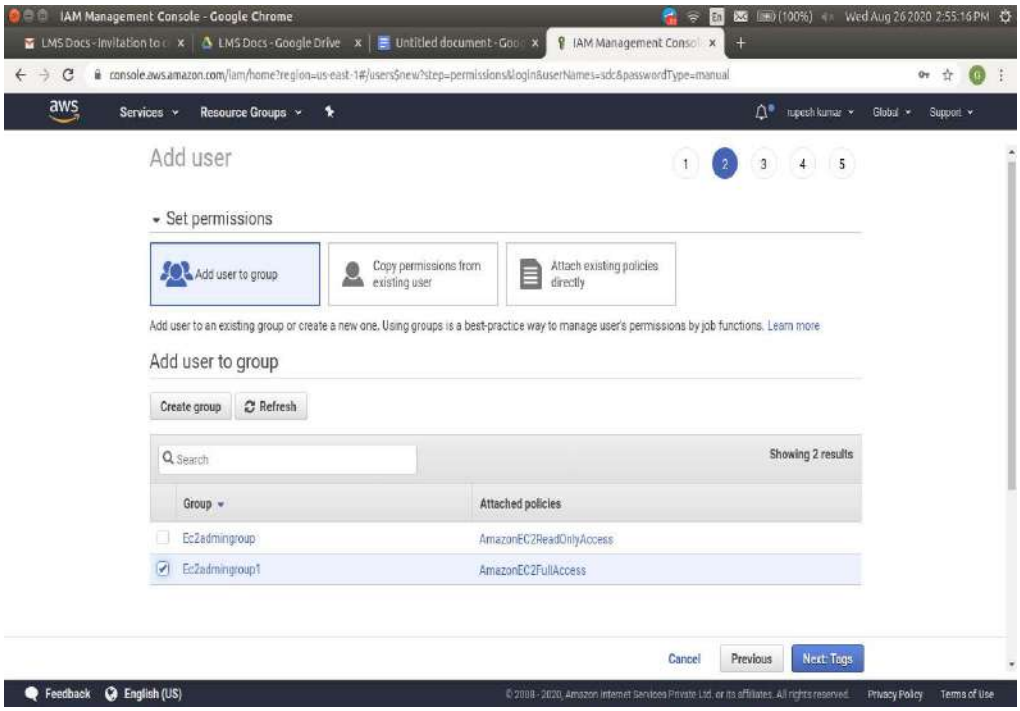
2. Scenario

Create user **sdc** to **EC2admingroup1**
Select user
Click on Add user button
For Console password → ********

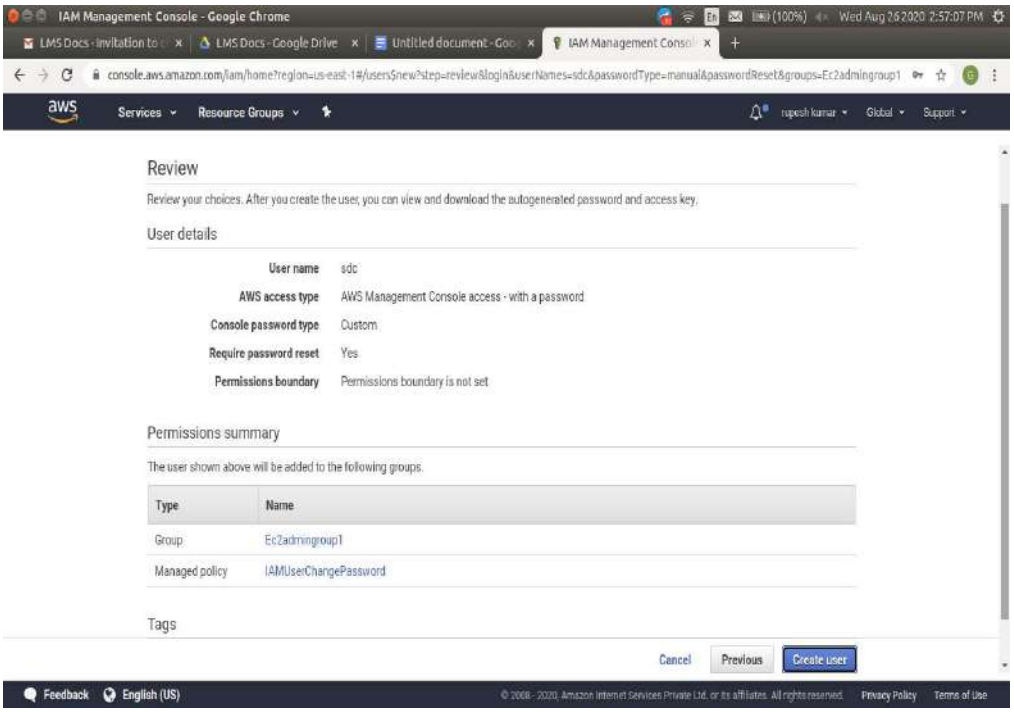
Click on Next Permission button



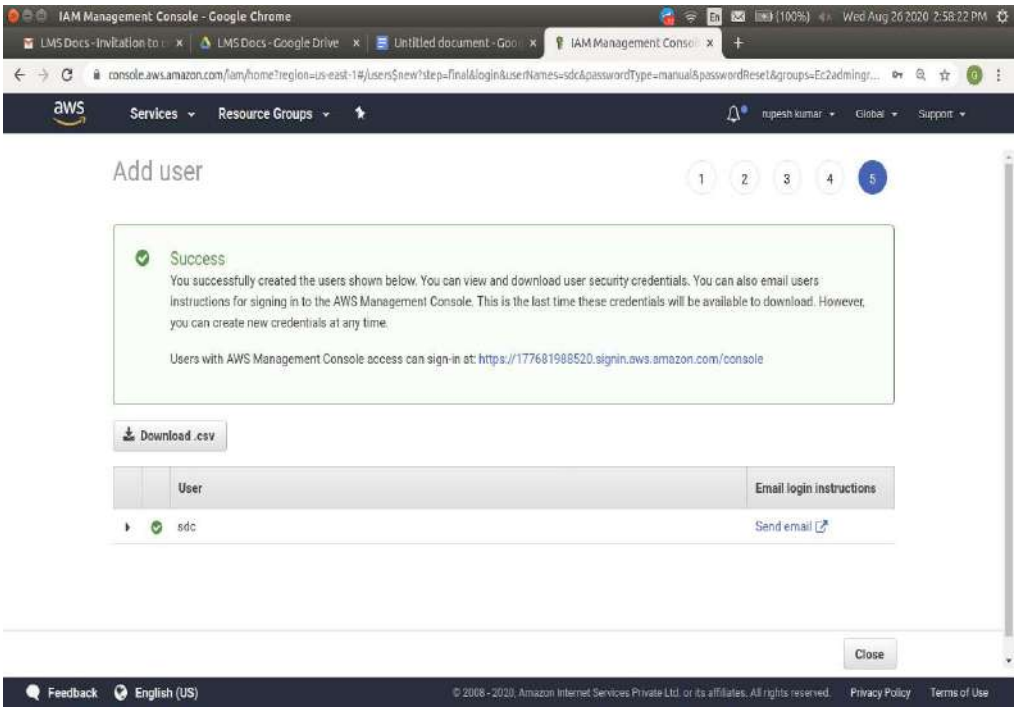
Under Group column, Select EC2admingroup1
Click on Next Review



Verify users details
Click on Create user button

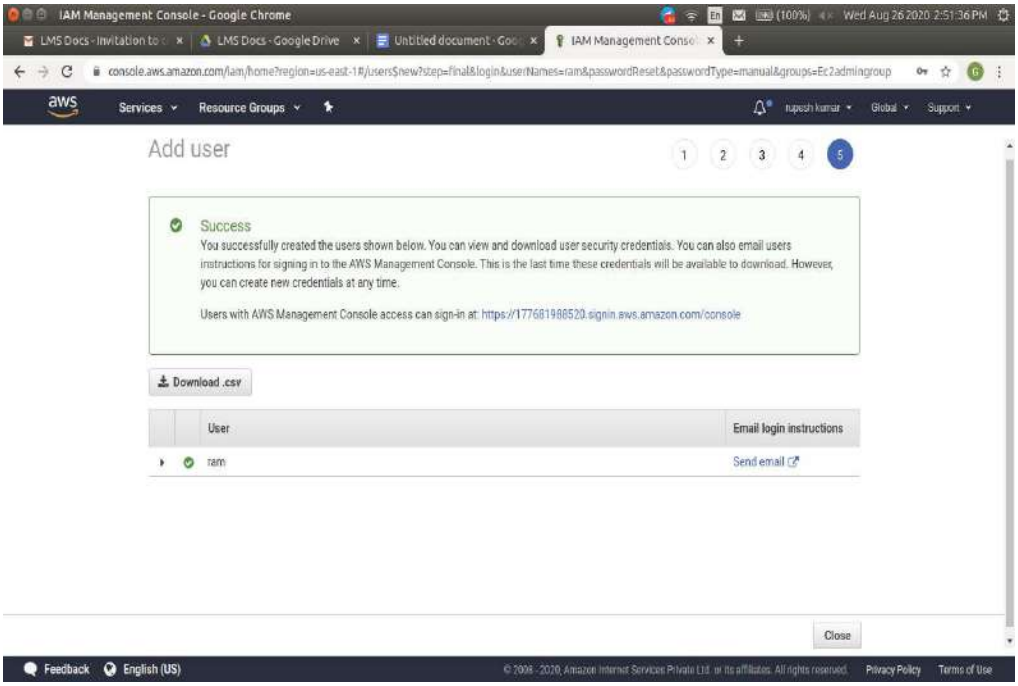


Click on close button



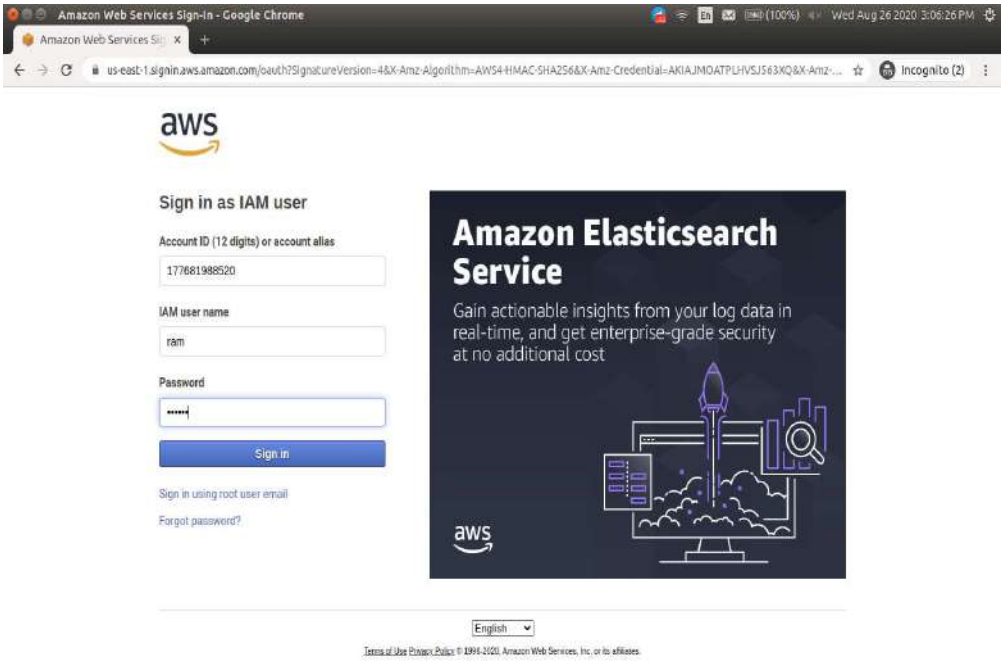
Creating an IAM role to Access EC2 read only, Ec2 Full access only

To verify whether users can access particular Service
Login as **ram** user (Use the generated url and sign in into aws management console)

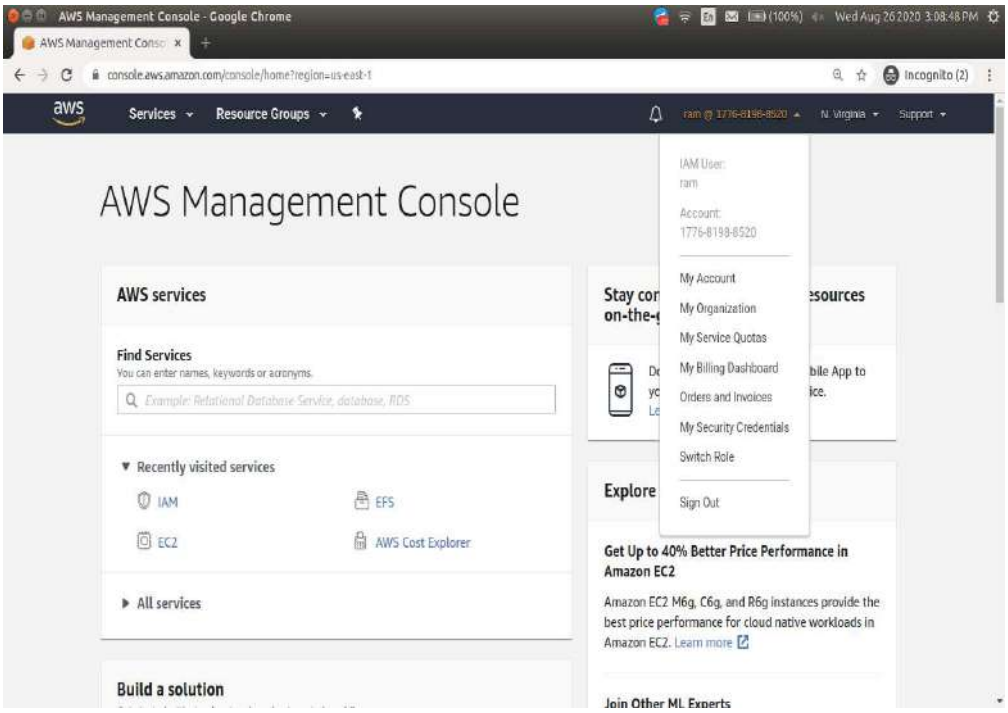


Provide the following url in Browser
https://177681988520.signin.aws.amazon.com/console

Click on Sign in button

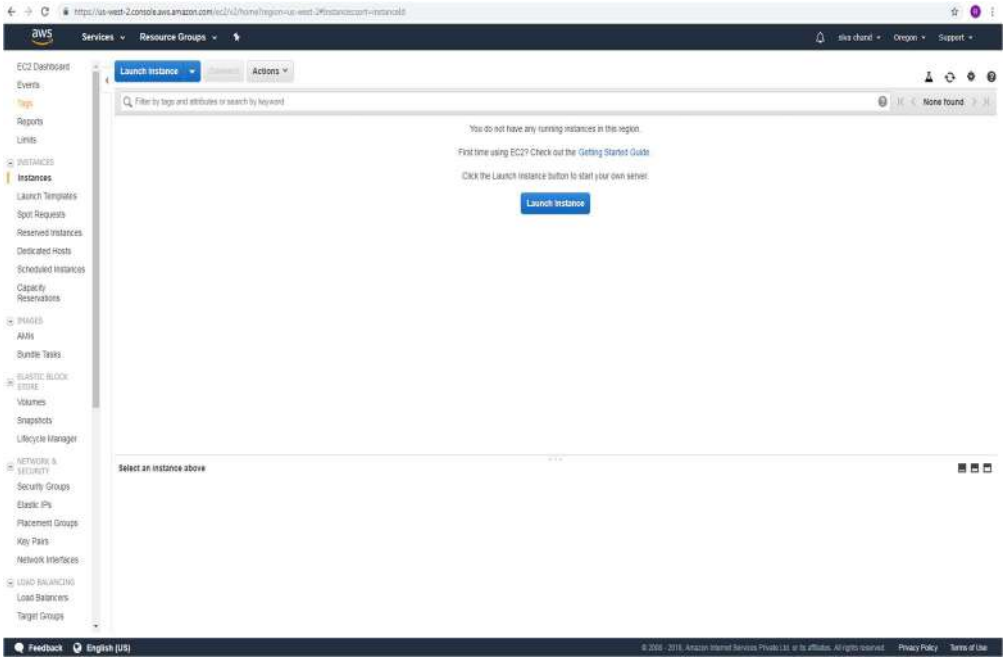


User **ram** is not having **Ec2FullAccess**
Click on EC2 verify the access

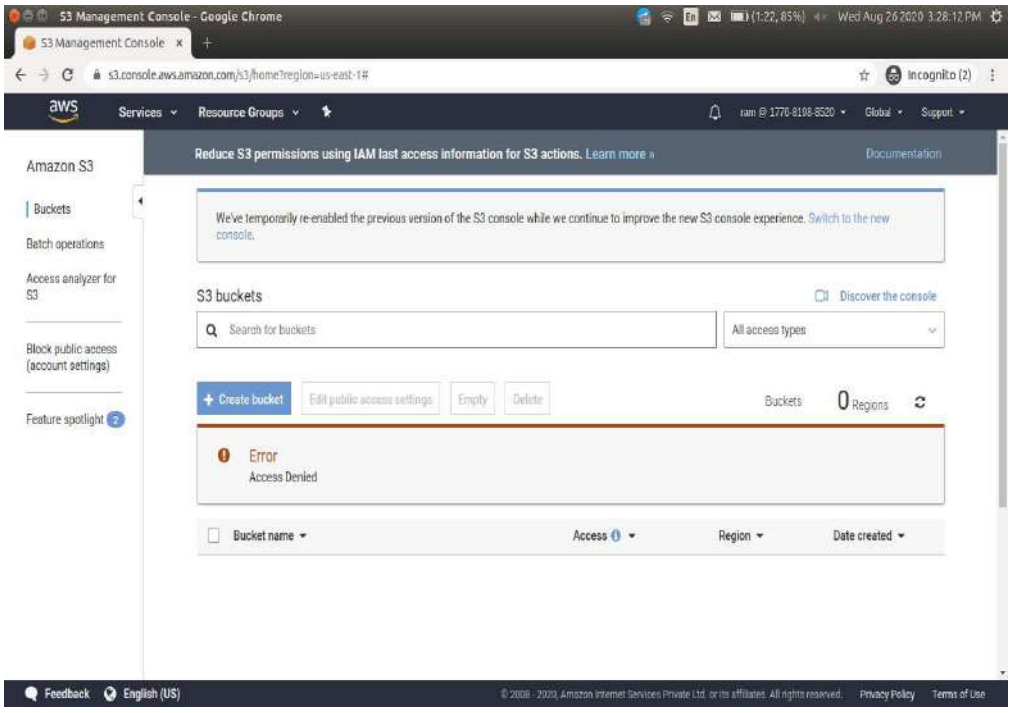


Verification

Click on EC2 verify the access

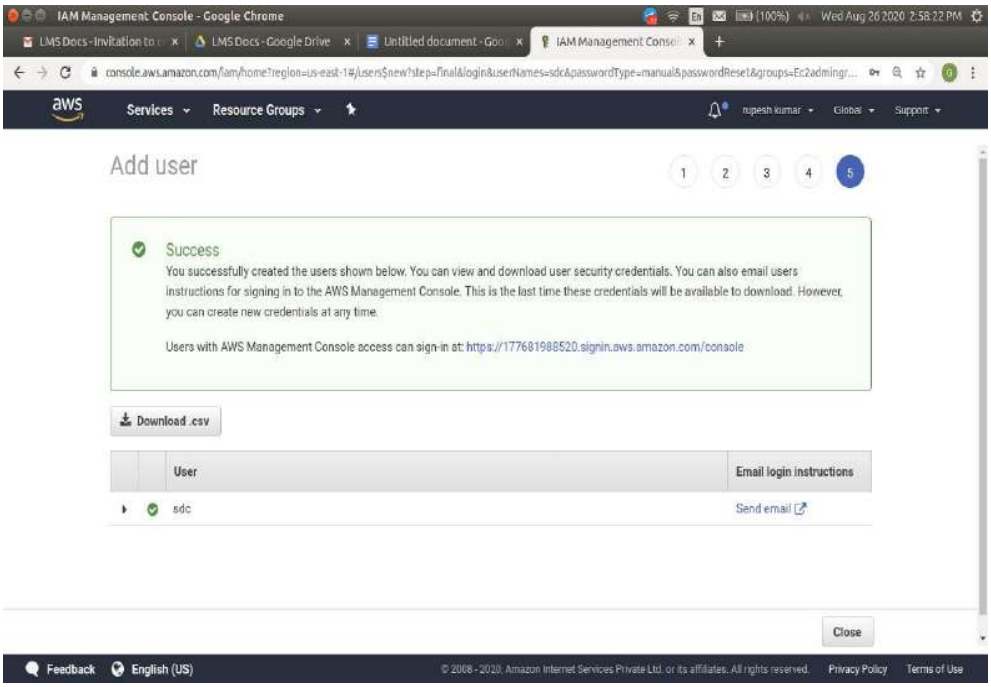


Click on S3 verify the access



To verify whether users can access particular Service

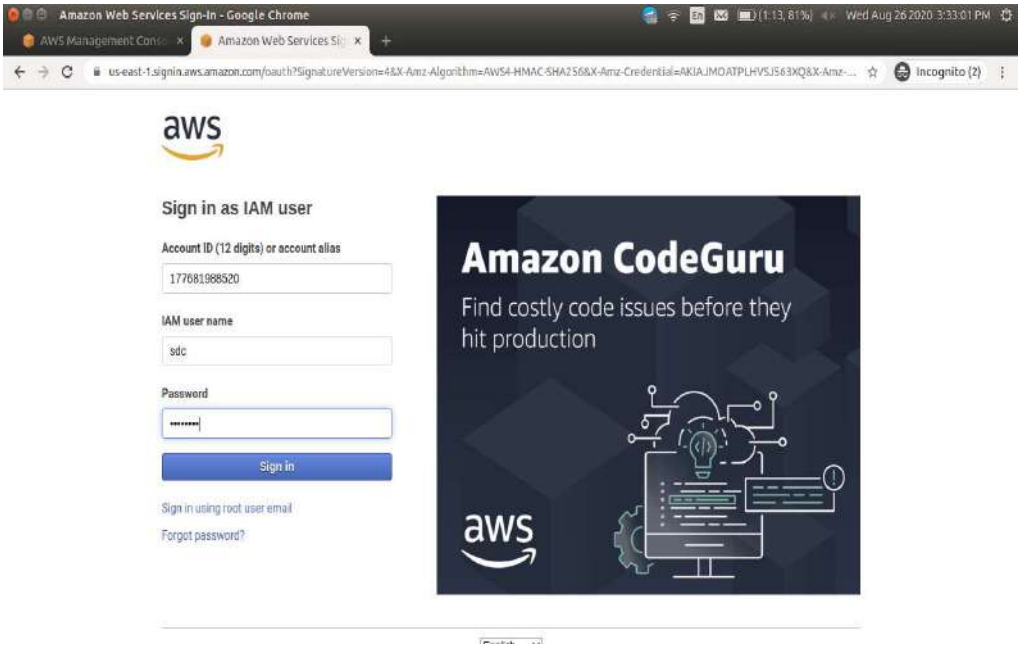
Login as **sdc** user (Use the generated url for the user **sdc** and sign in into the aws management console)



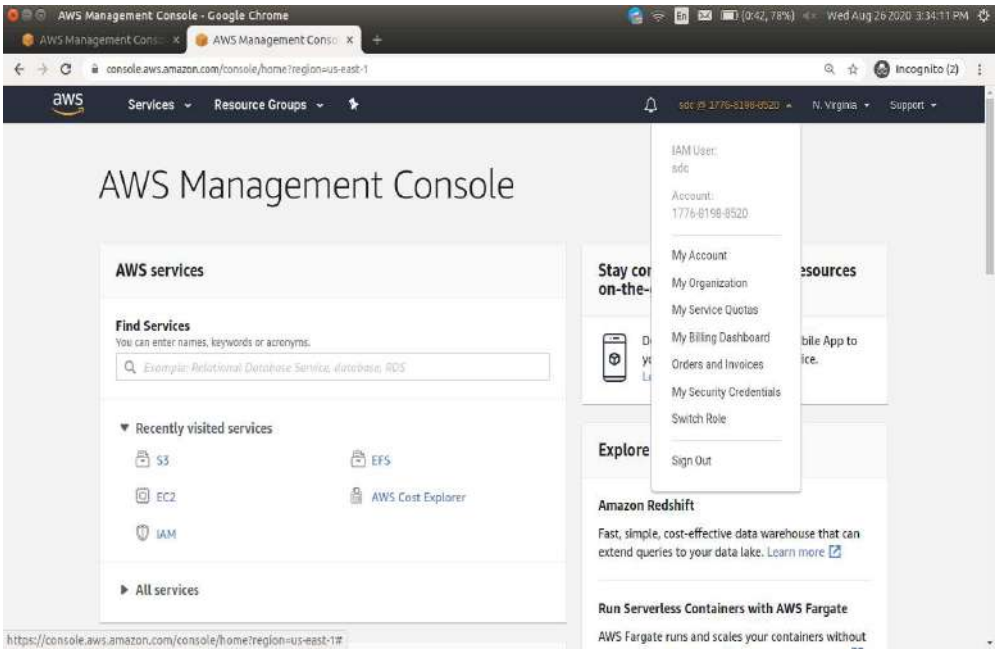
Provide the following url in Browser
https://177681988520.signin.aws.amazon.com/console

Click on Sign in button

Now login as sdc user

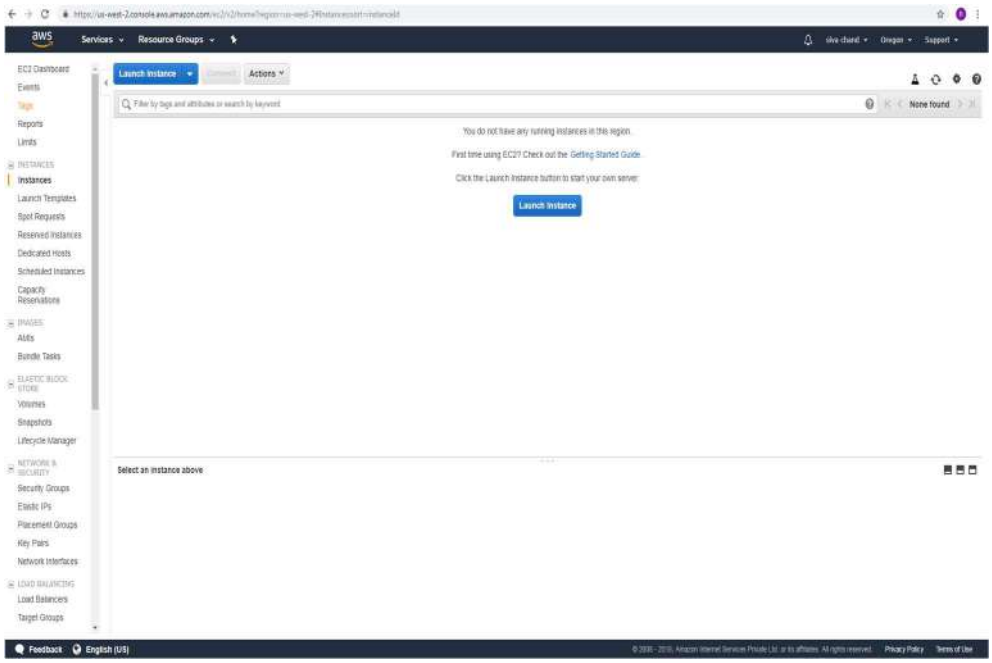


Verify user had successfully logged in

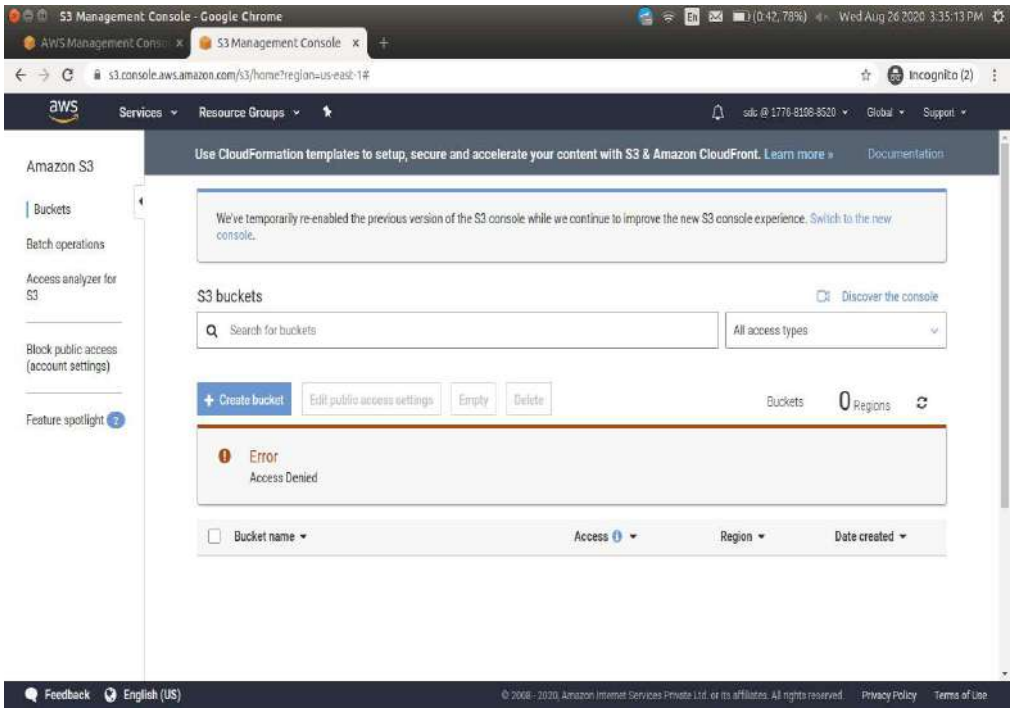


Verification

Click on EC2 verify the access



Click on S3 verify the access


S3 Management Console - Google Chrome
Wed Aug 26 2020 3:35:13 PM
AWS Management Conso
S3 Management Console
s3.console.aws.amazon.com/s3/home?region=us-east-1#
Incognito (2)
aws
Services
Resource Groups
sdc @ 1776-8198-8520
Global
Support
Amazon S3
Buckets
Batch operations
Access analyzer for S3
Block public access (account settings)
Feature spotlight
Use CloudFormation templates to setup, secure and accelerate your content with S3 & Amazon CloudFront. Learn more »
Documentation
We've temporarily re-enabled the previous version of the S3 console while we continue to improve the new S3 console experience. Switch to the new console.
S3 buckets
Discover the console
Search for buckets
All access types
Create bucket
Edit public access settings
Empty
Delete
Buckets
0 Regions
Error
Access Denied
Bucket name
Access
Region
Date created
Feedback
English (US)
© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use