



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
- IAM also enabling access to resources across AWS accounts.

IAM Features

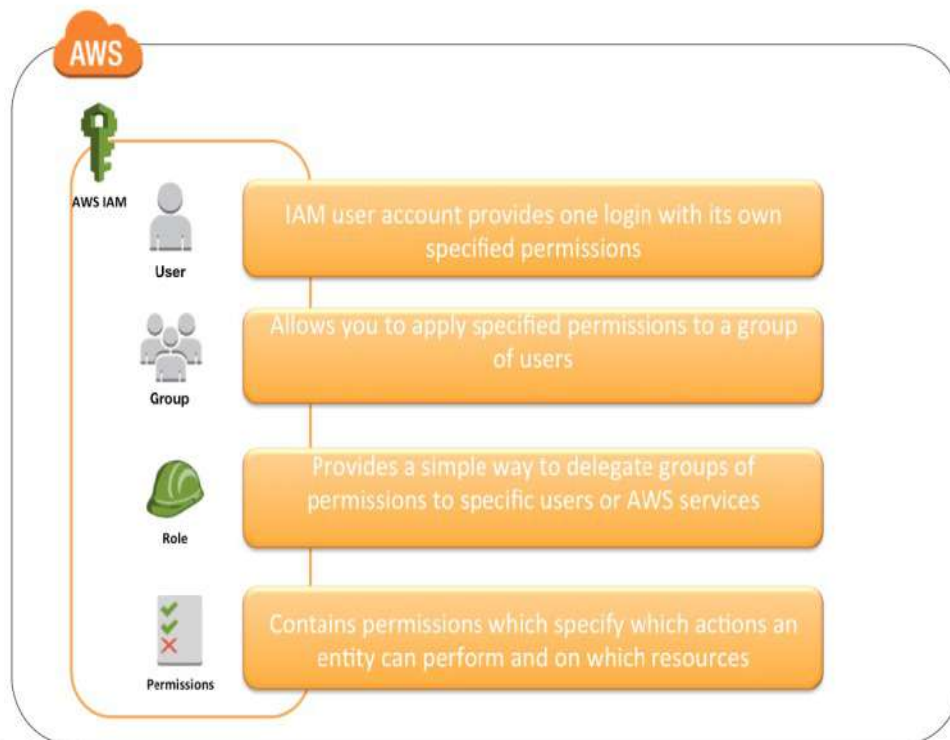
- Shared access to your AWS account
 - Grant other people permission to administer and use resources in your AWS account without having to share your password or access key.
- Granular permissions
 - Each user can be granted with different set granular permissions as required to perform their job
- Secure 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

AWS IAM Identities



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.

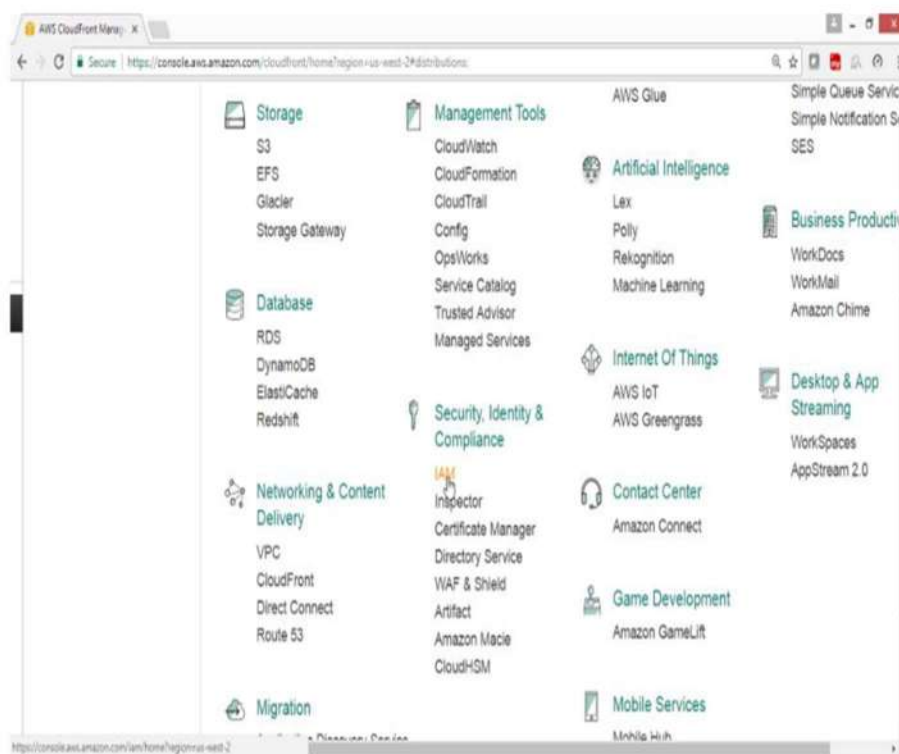
Users Login to sign-in page.

Deleting users and groups.

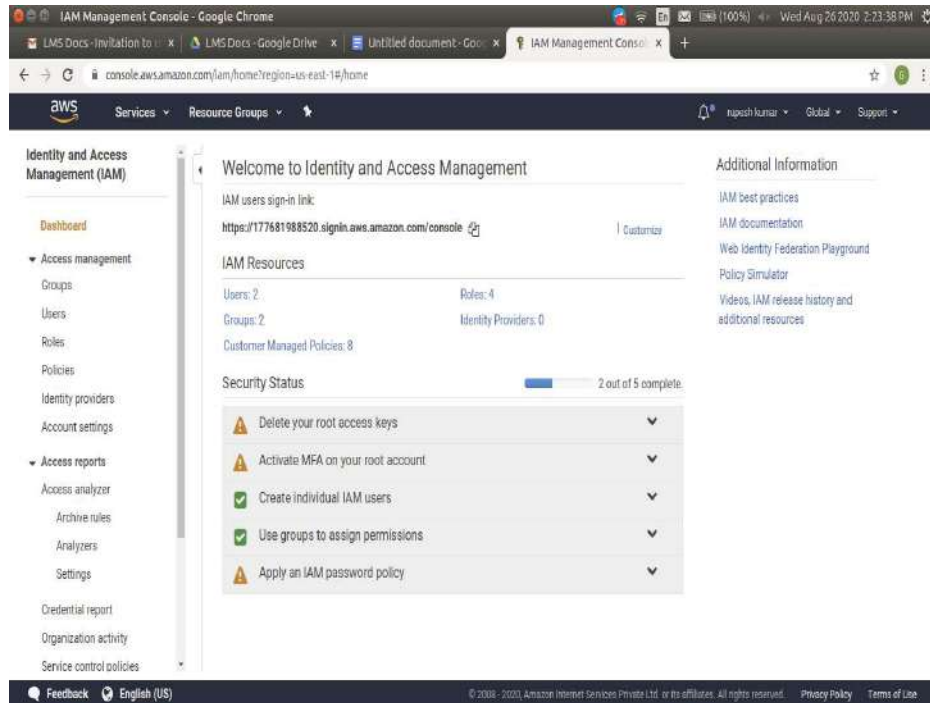
Creating an IAM role to login other users.

Open AWS console and select Security, Identity & Compliance

Click on **IAM** service

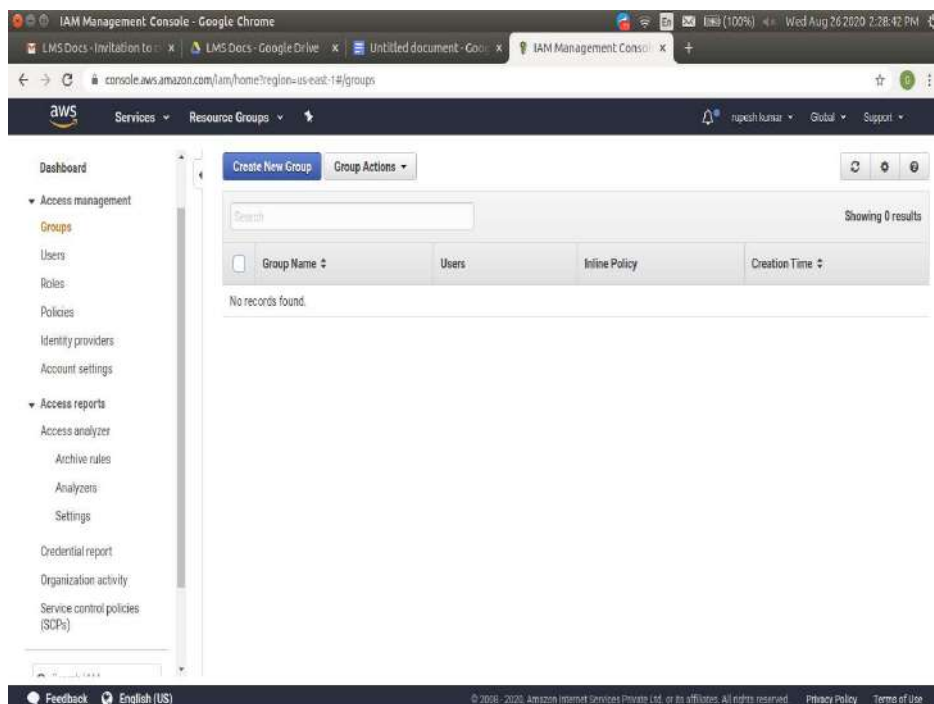


IAM Dashboard panel available



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

Set Group Name

Specify a group name. Group names can be edited any time.

Group Name:

Example: Developers or Project Alpha
Maximum 128 characters

Cancel Next Step

In Filter type → EC2 Read Only access

Select check box for Amazon EC2 Read Only access

Click on Next Step button

Attach Policy

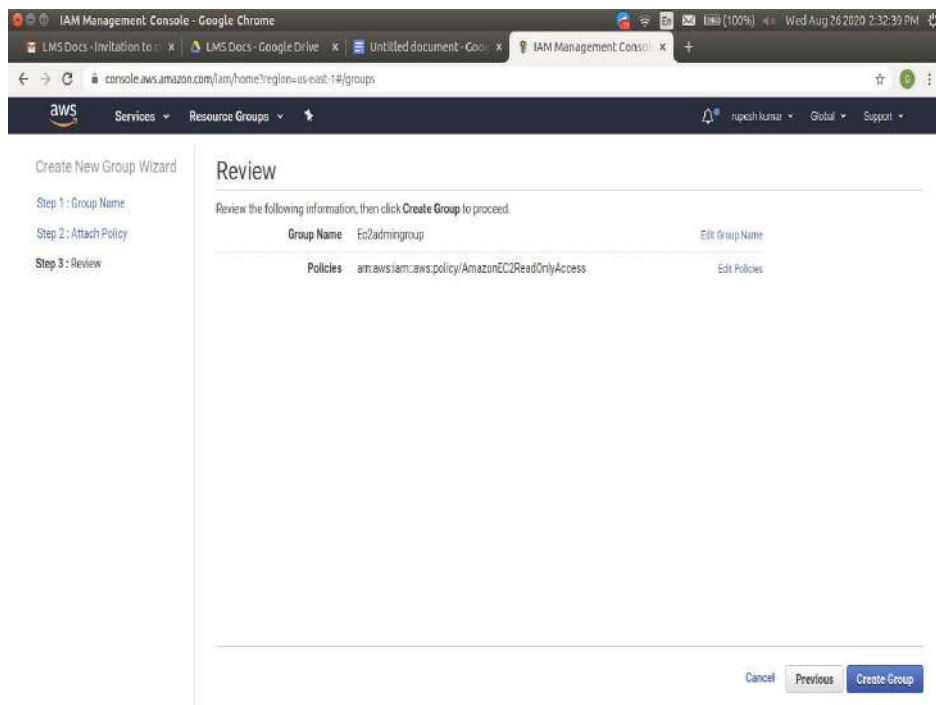
Select one or more policies to attach. Each group can have up to 10 policies attached.

Filter: Policy Type: Ec2read Showing 1 results

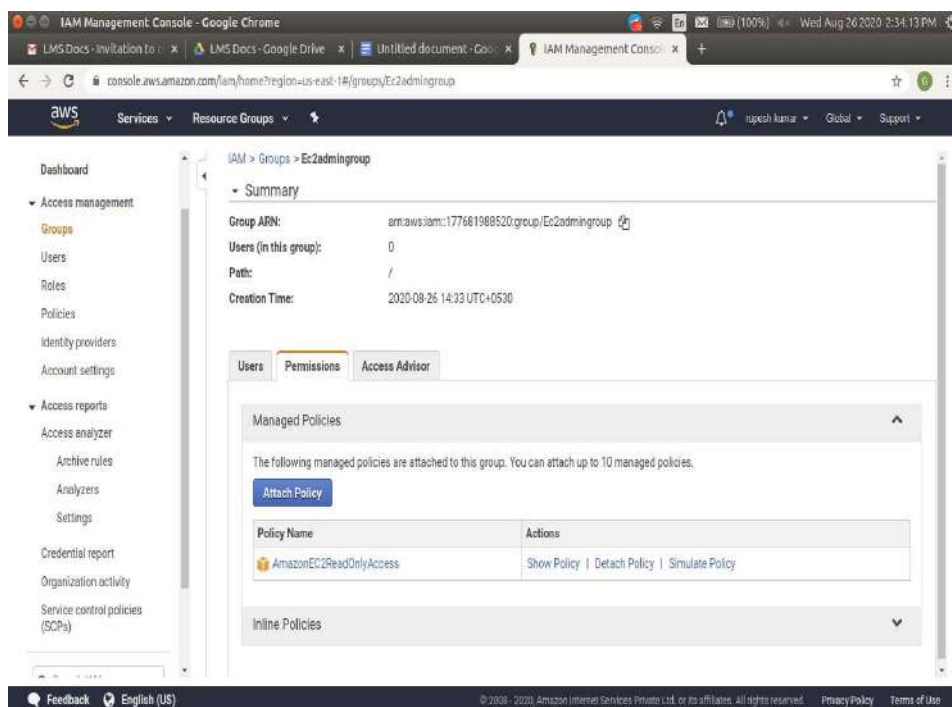
Policy Name	Attached Entities	Creation Time
<input checked="" type="checkbox"/> AmazonEC2ReadOnlyAccess	0	2015-02-07 09:10 UTC+0...

Cancel Previous Next Step

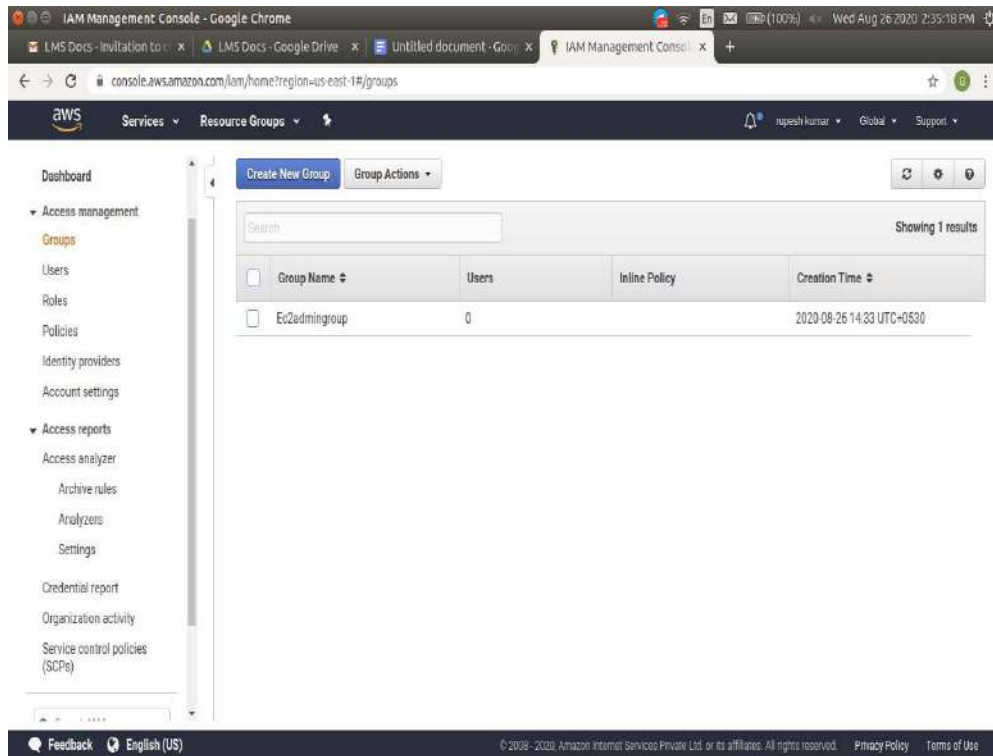
Click on Create Group



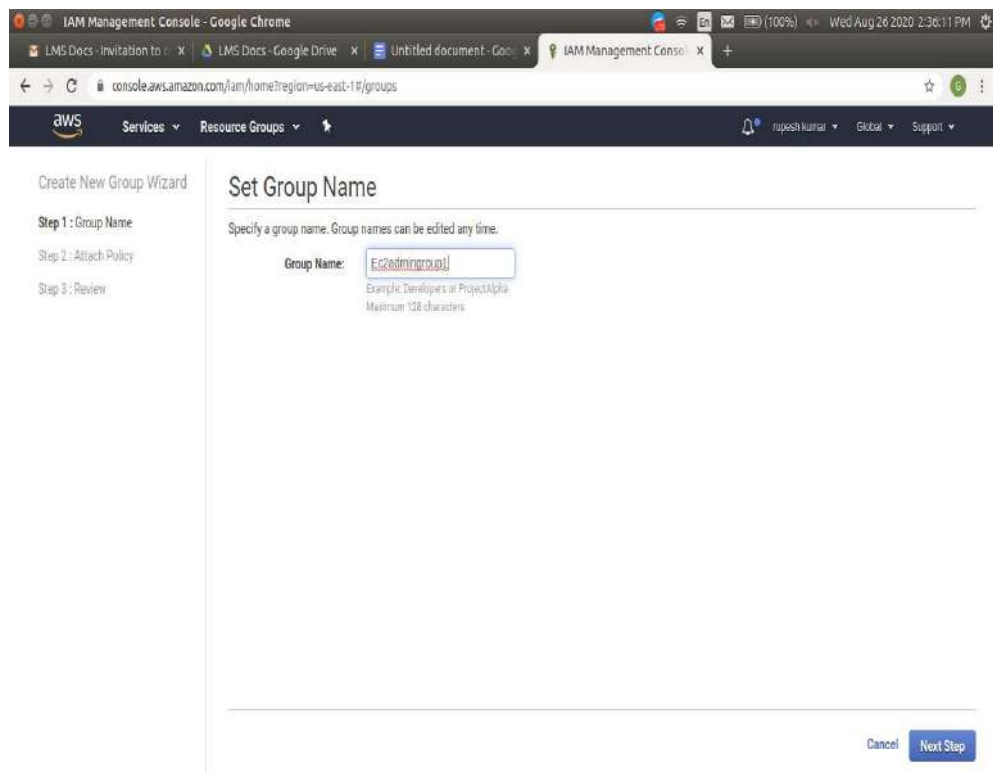
Verify Group EC2admingroup got created with Amazon EC2ReadOnlyAccess



Now again create Another Group
Click on Create Group



Give Group Name → EC2admingroup1
Click on Next Step button

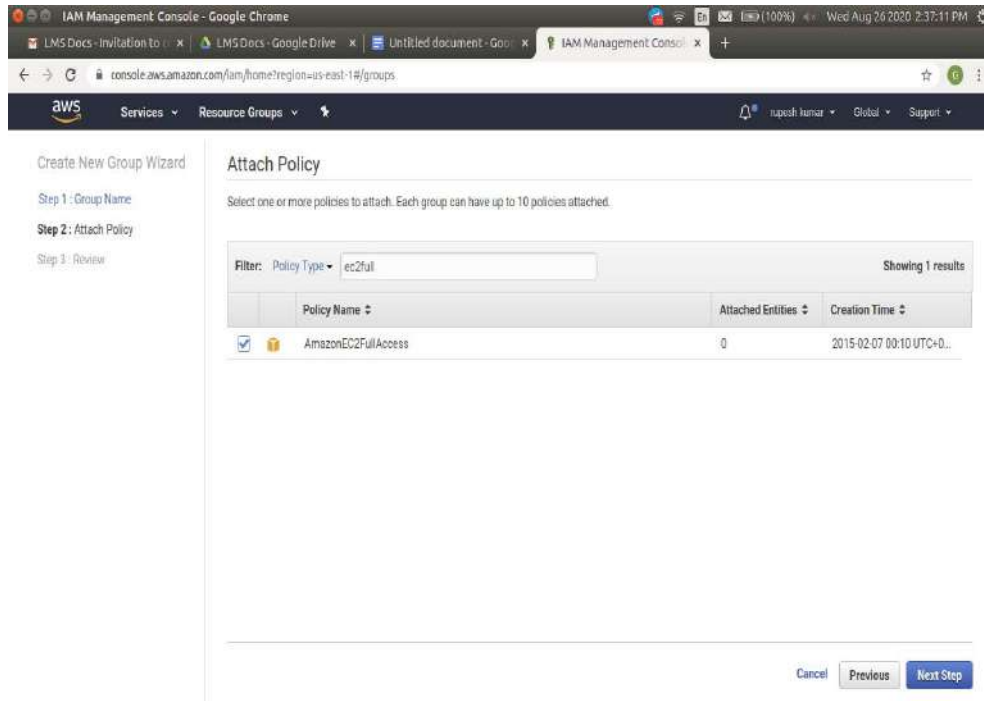




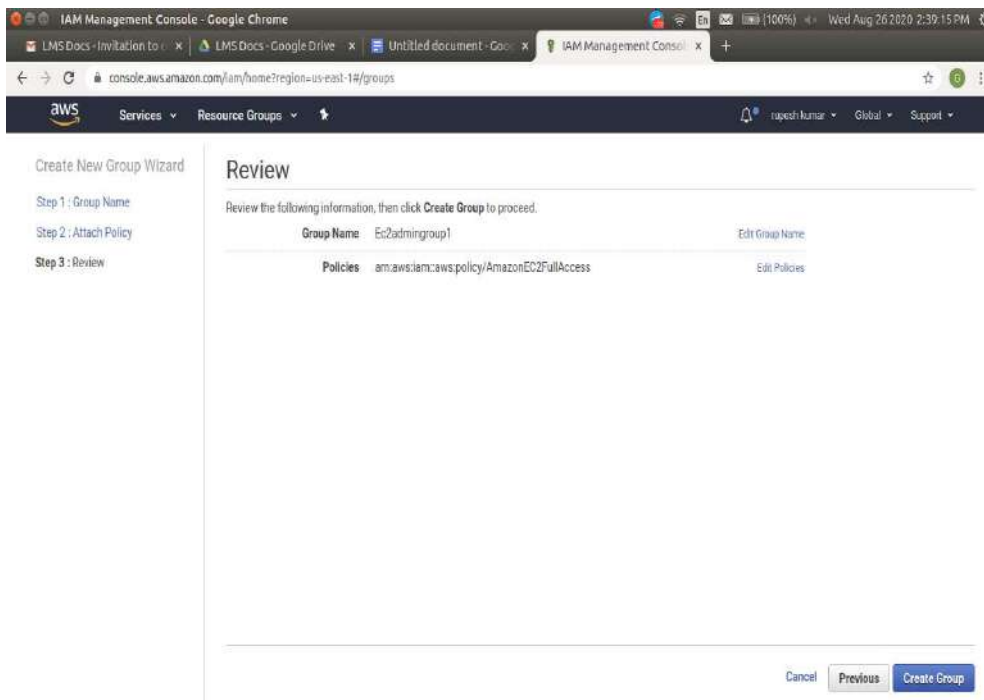
In Filter type → EC2FullAccess

Select check box for AmazonEC2FullAccess

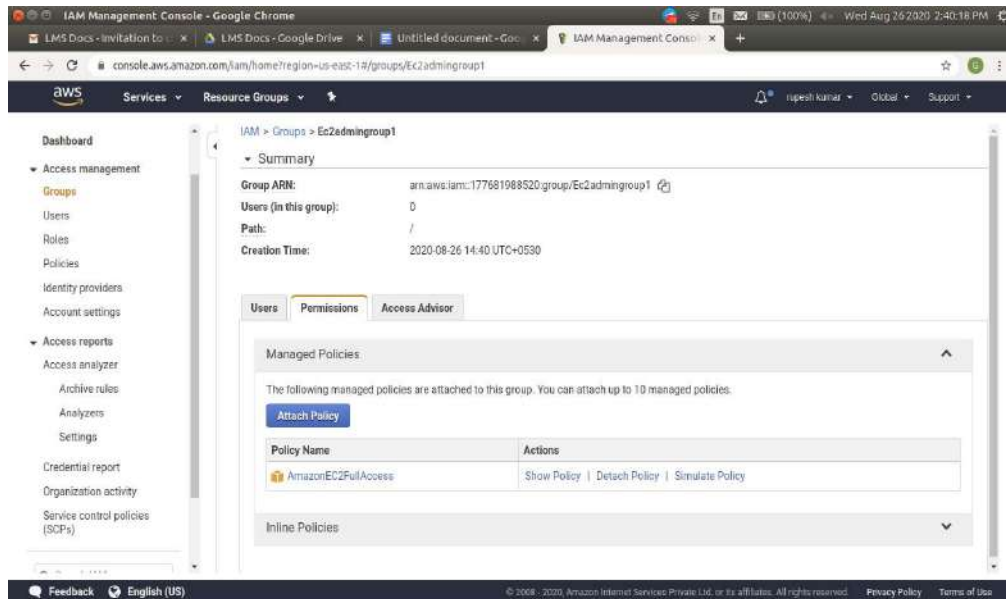
Click on Next Step button



Click on Create Group



Verify Group EC2admingroup1 got created with AmazonEC2FullAccess



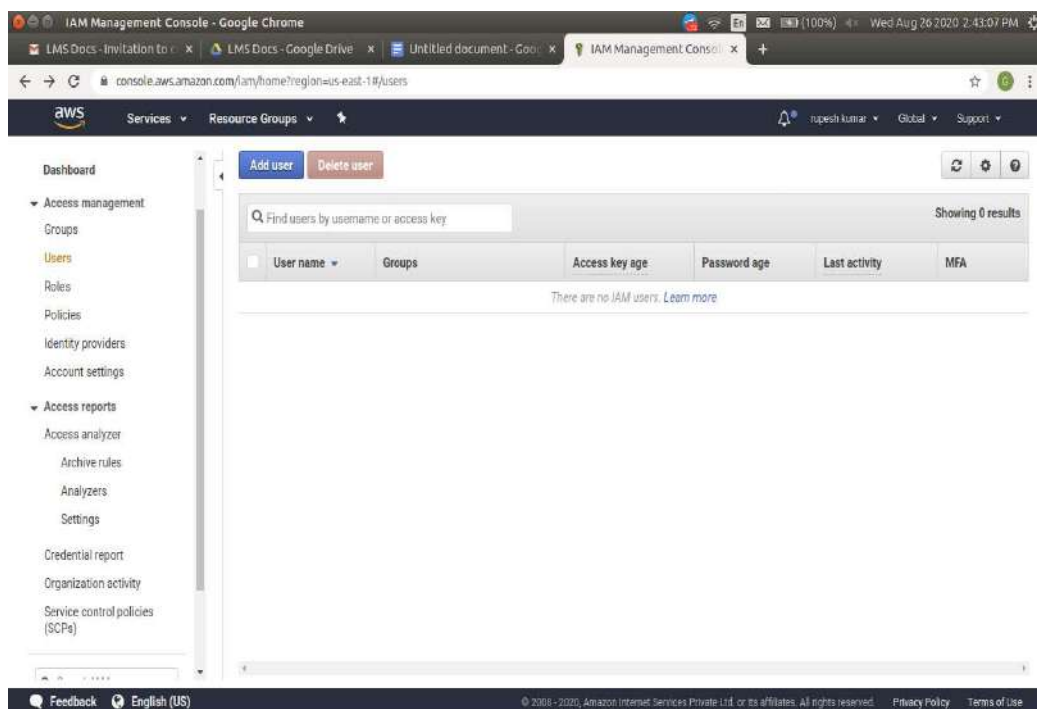
Create user **ram** join to EC2admingroup1

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



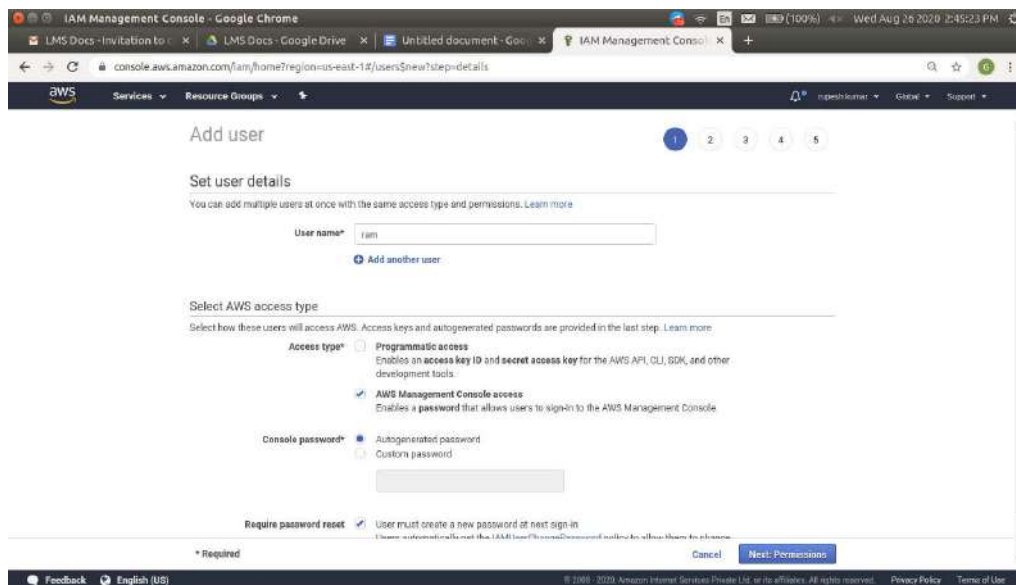
1. Scenario

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

For username → **ram**

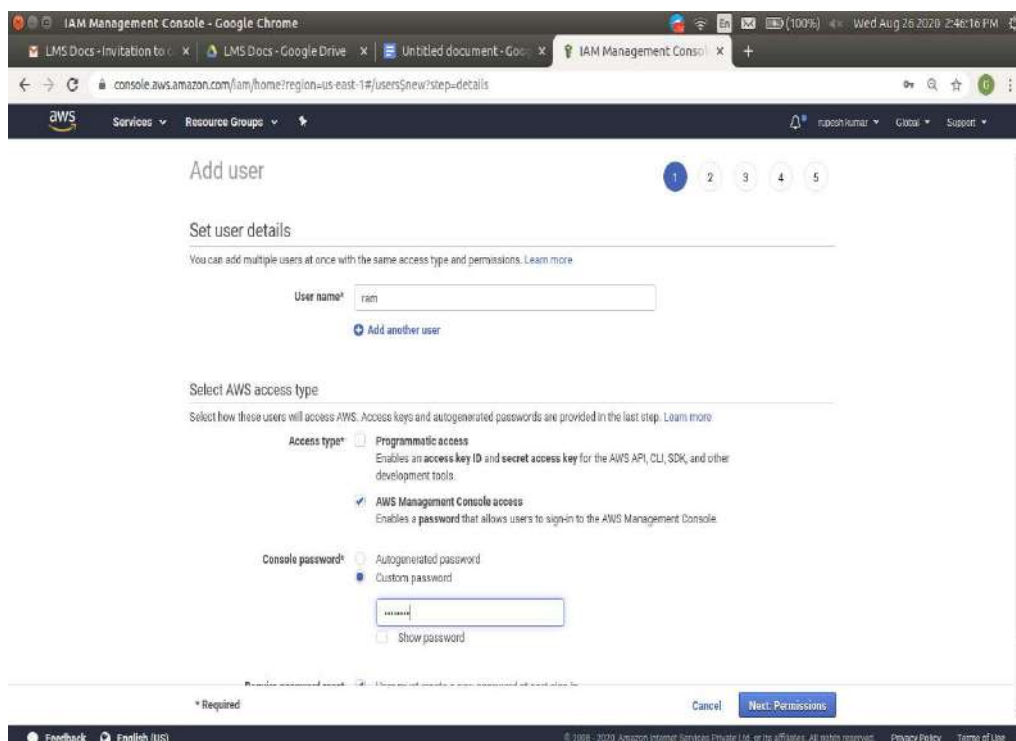
For Access type → **AWS Management Console access**

Drag down

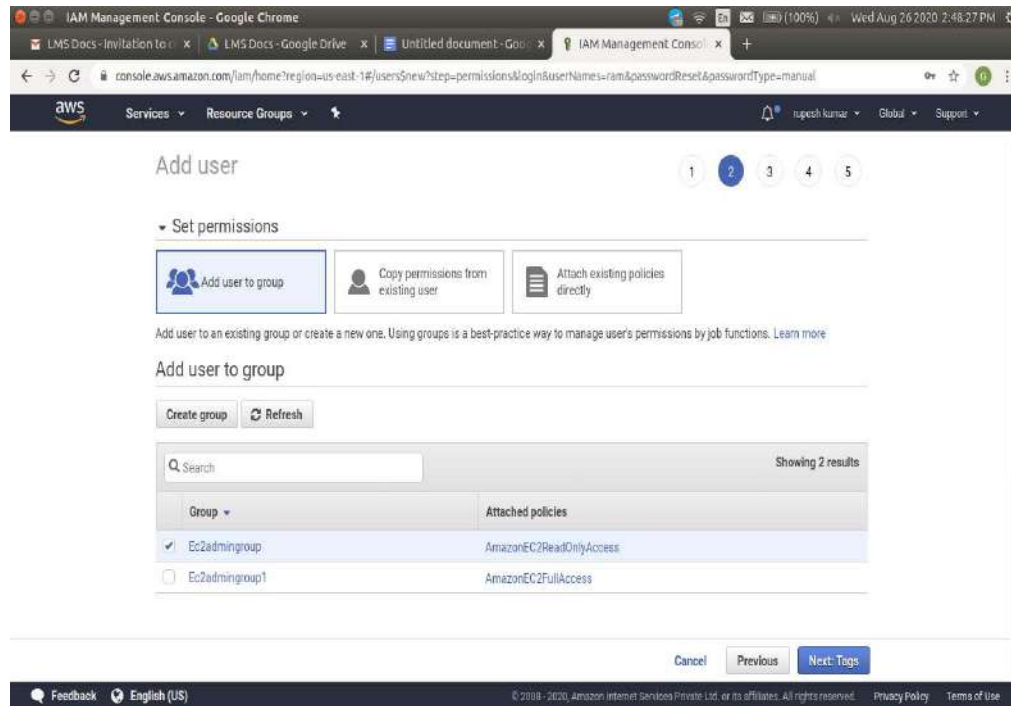


For Console password → *********

Click on Next Permission button



Under Group column, Select EC2admingroup
Click on Next Review



Add user

1 2 3 4 5

Set permissions

☒ Add user to group ☐ Copy permissions from existing user ☐ Attach existing policies directly

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Add user to group

Create group Refresh

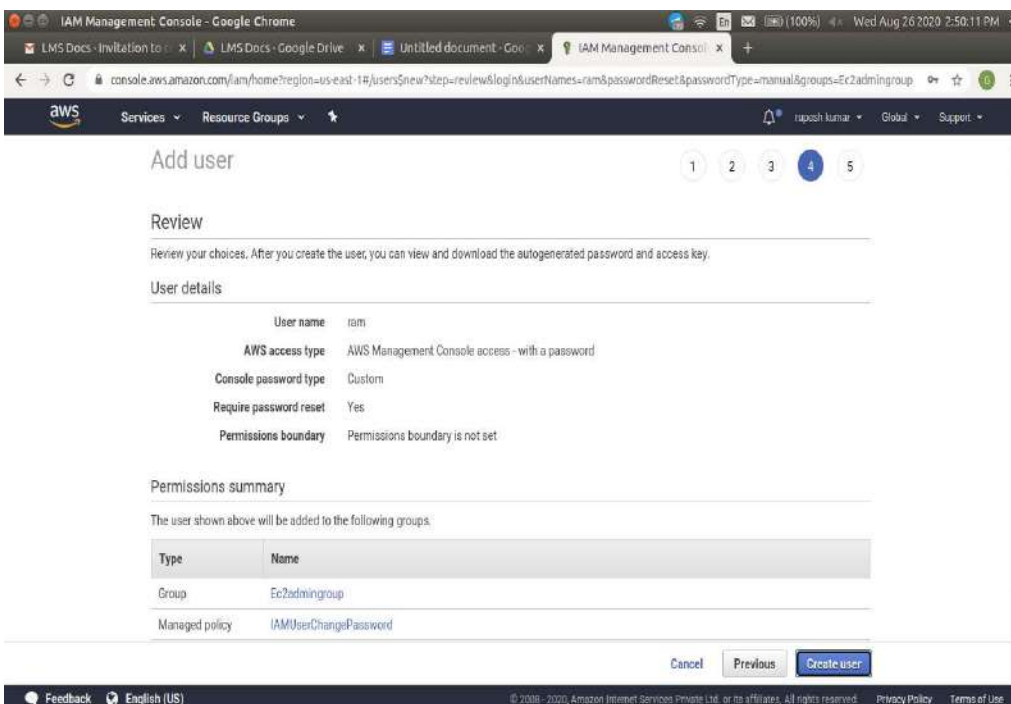
Search Showing 2 results

Group	Attached policies
<input checked="" type="checkbox"/> Ec2admingroup	AmazonEC2ReadOnlyAccess
<input type="checkbox"/> Ec2admingroup1	AmazonEC2FullAccess

Cancel Previous **Next: Tags**

Feedback English (US) © 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Verify users details
Click on Create user button



Add user

1 2 3 4 5

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	ram
AWS access type	AWS Management Console access - with a password
Console password type	Custom
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Permissions summary

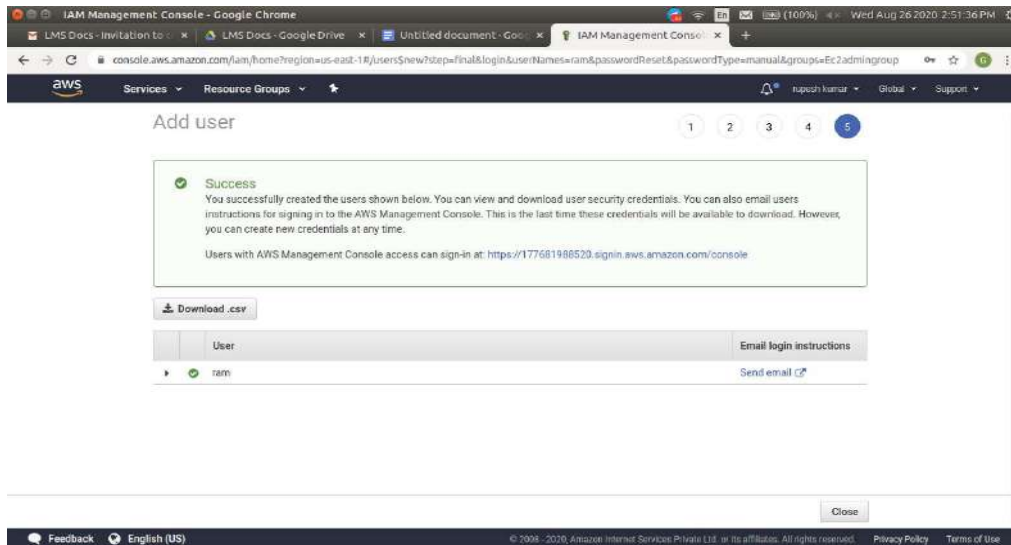
The user shown above will be added to the following groups.

Type	Name
Group	Ec2admingroup
Managed policy	IAMUserChangePassword

Cancel Previous **Create user**

Feedback English (US) © 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Click on close button



2. Scenario

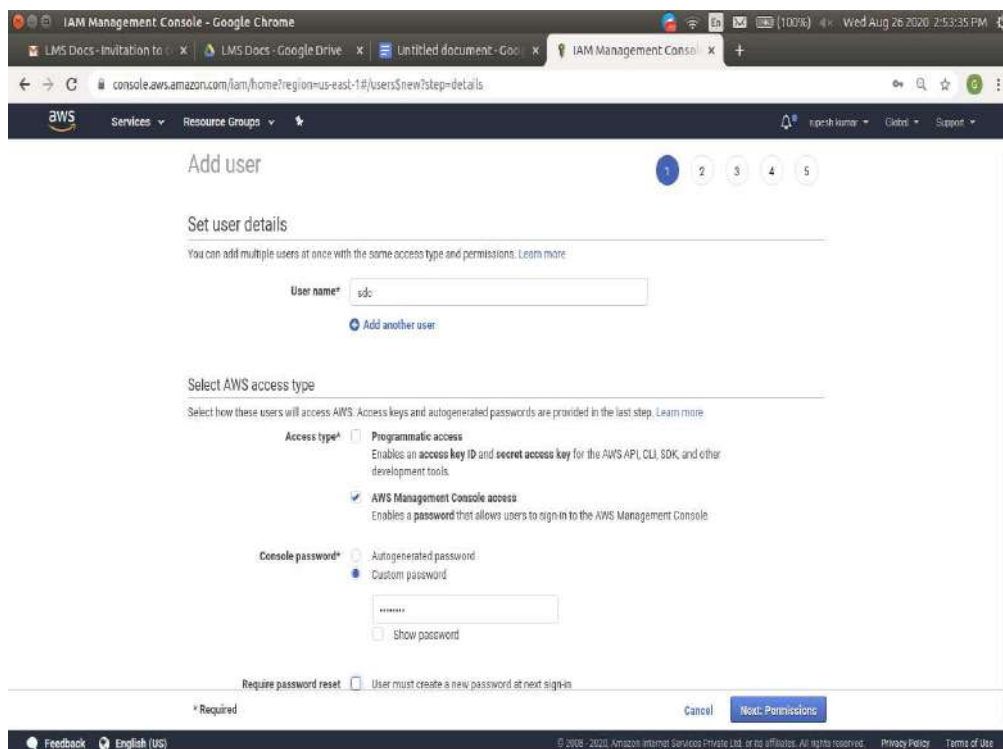
Create user **sdc** to **EC2admingroup1**

Select user

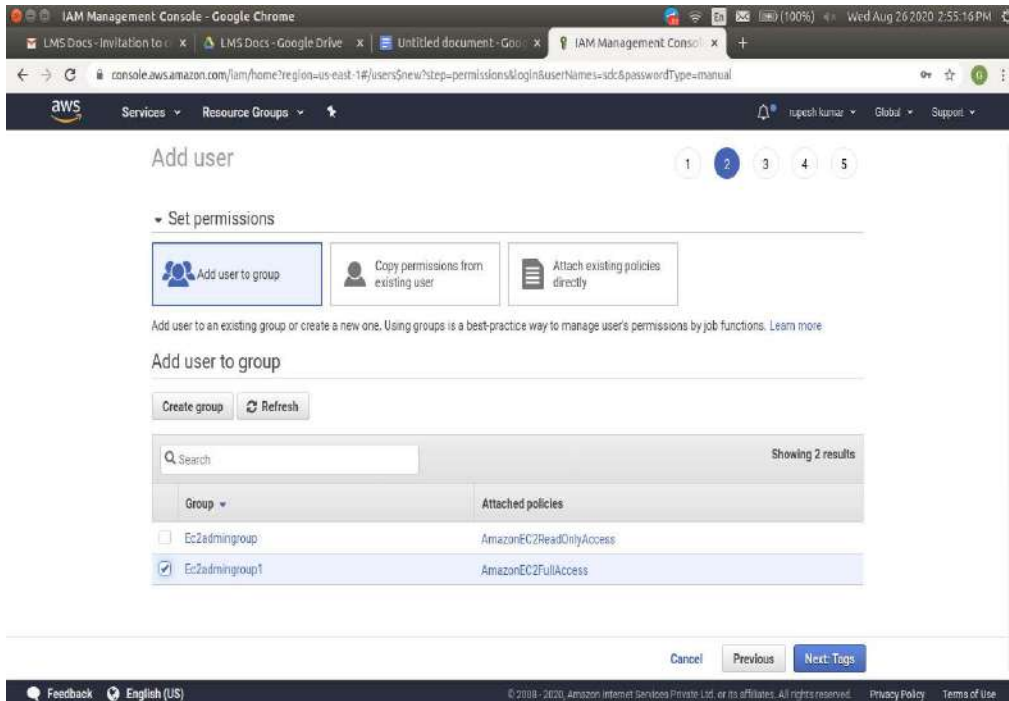
Click on Add user button

For Console password → *****

Click on Next Permission button



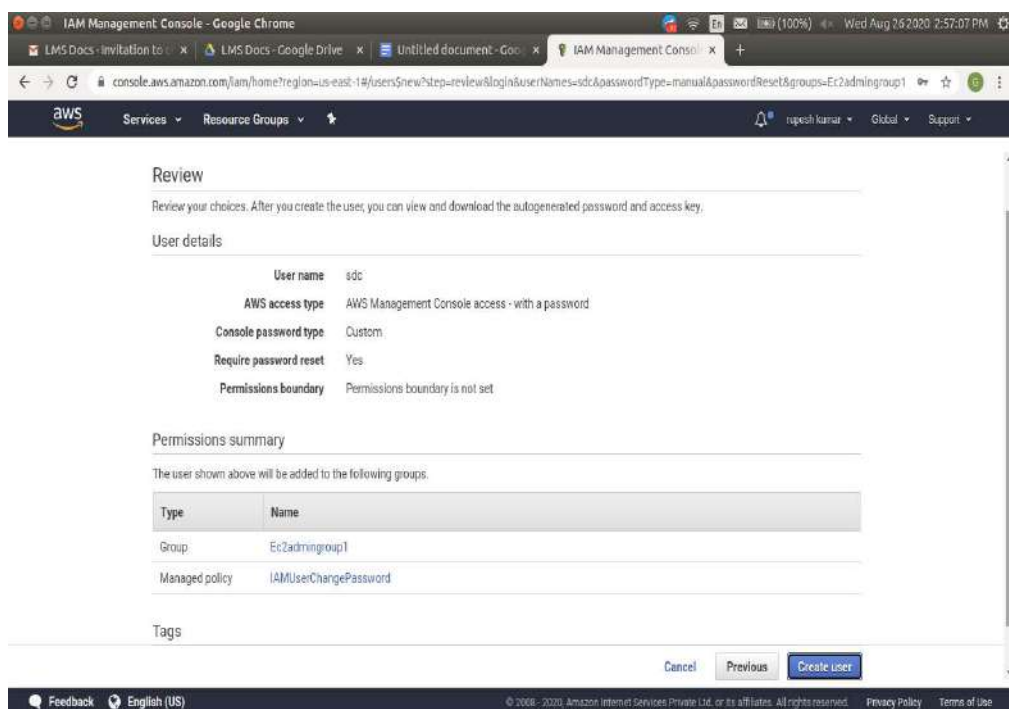
Under Group column, Select EC2admingroup1
Click on Next Review



The screenshot shows the 'Add user' page in the AWS IAM Management Console. The 'Set permissions' section is active, and the 'Add user to group' option is selected. A table lists available groups, with 'EC2admingroup1' selected. The 'Next: Tags' button is visible at the bottom right.

Group	Attached policies
<input type="checkbox"/> EC2admingroup	AmazonEC2ReadOnlyAccess
<input checked="" type="checkbox"/> EC2admingroup1	AmazonEC2FullAccess

Verify users details
Click on Create user button

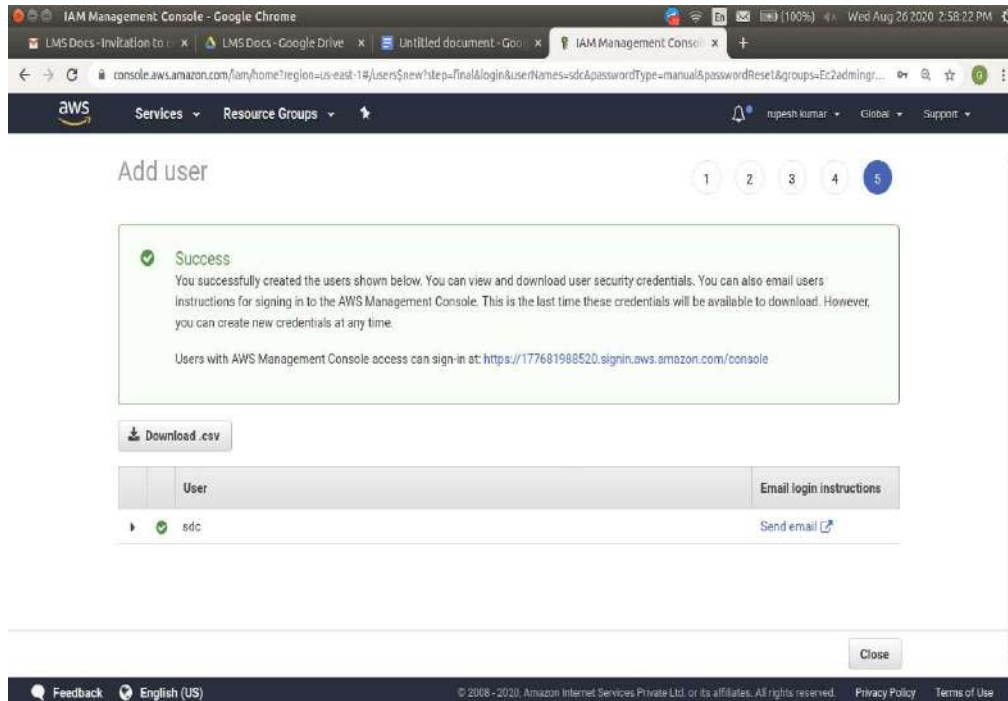


The screenshot shows the 'Review' page in the AWS IAM Management Console. It displays the user details and permissions summary. The 'Create user' button is visible at the bottom right.

Field	Value
User name	sdcc
AWS access type	AWS Management Console access - with a password
Console password type	Custom
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Type	Name
Group	EC2admingroup1
Managed policy	IAMUserChangePassword

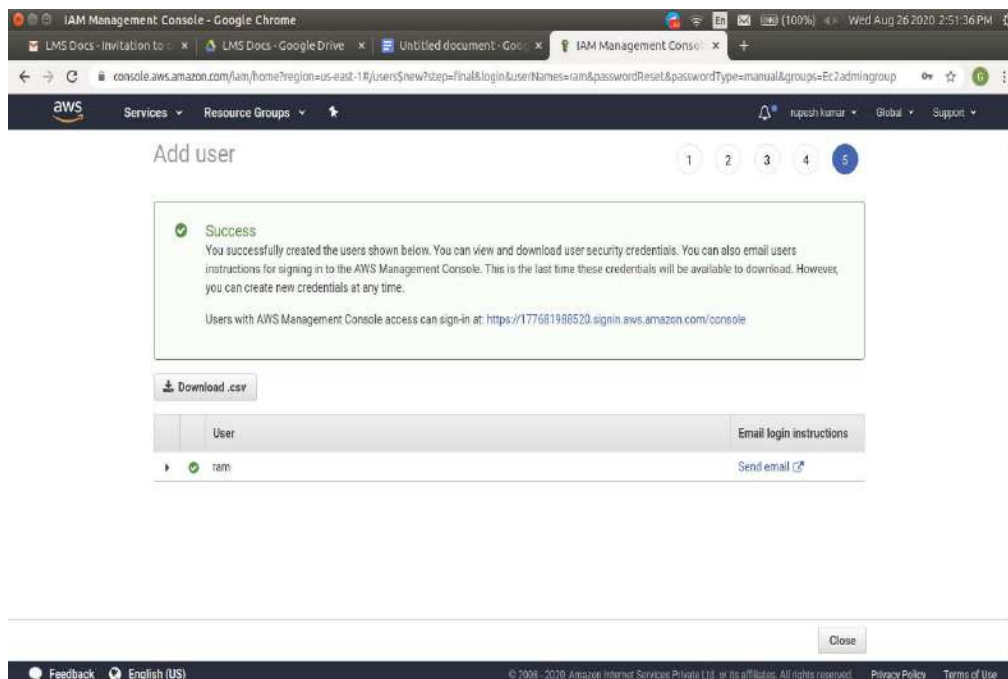
Click on close button



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

Amazon Web Services Sign-in - Google Chrome

Amazon Web Services Sign-in

us-east-1:signin.aws.amazon.com/console?SignatureVersion=4&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAJMOATPLHVSJ563XQ&X-Amz-...

aws

Sign in as IAM user

Account ID (12 digits) or account alias

177681988520

IAM user name

ram

Password

Sign in

Sign in using root user email

Forgot password?

Amazon Elasticsearch Service

Gain actionable insights from your log data in real-time, and get enterprise-grade security at no additional cost

aws

English

Terms of Use Privacy Policy © 1996-2020, Amazon Web Services, Inc. or its affiliates

User **ram** is not having **Ec2FullAccess**

Click on EC2 verify the access

AWS Management Console - Google Chrome

AWS Management Console

console.aws.amazon.com/console/home?region=us-east-1

aws

Services Resource Groups

ram @ 1776-8198-8520

My Account

My Organization

My Service Quotas

My Billing Dashboard

Orders and Invoices

My Security Credentials

Switch Role

Sign Out

AWS services

Find Services

You can enter names, keywords or acronyms.

Example: Relational Database Service, database, RDS

Recently visited services

IAM

EFS

EC2

AWS Cost Explorer

All services

Build a solution

Stay connected on-the-go

Explore

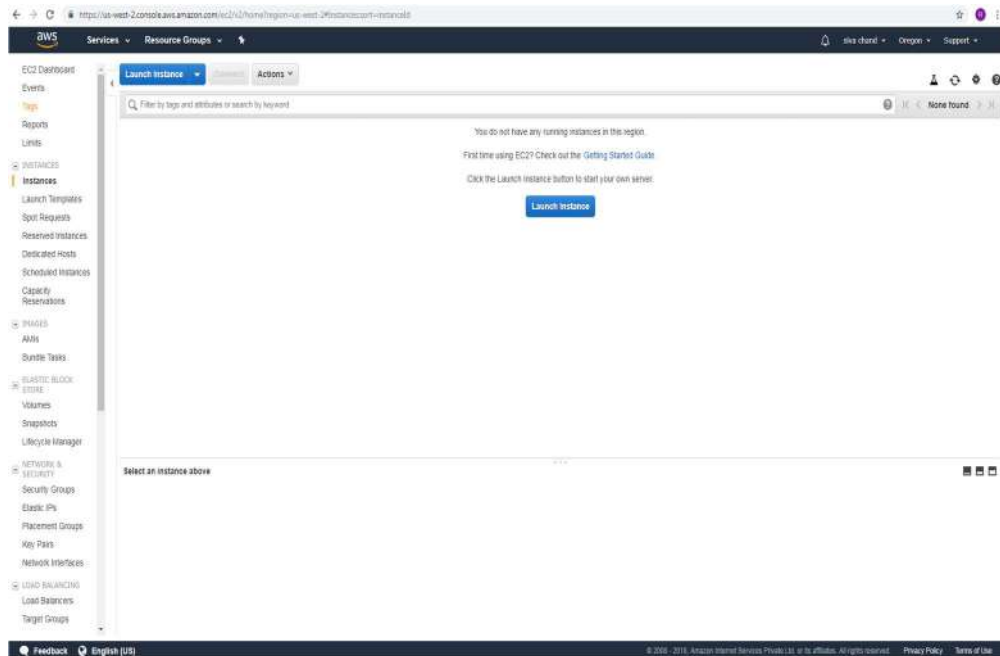
Get Up to 40% Better Price Performance in Amazon EC2

Amazon EC2 M6g, C6g, and R6g instances provide the best price performance for cloud native workloads in Amazon EC2. Learn more

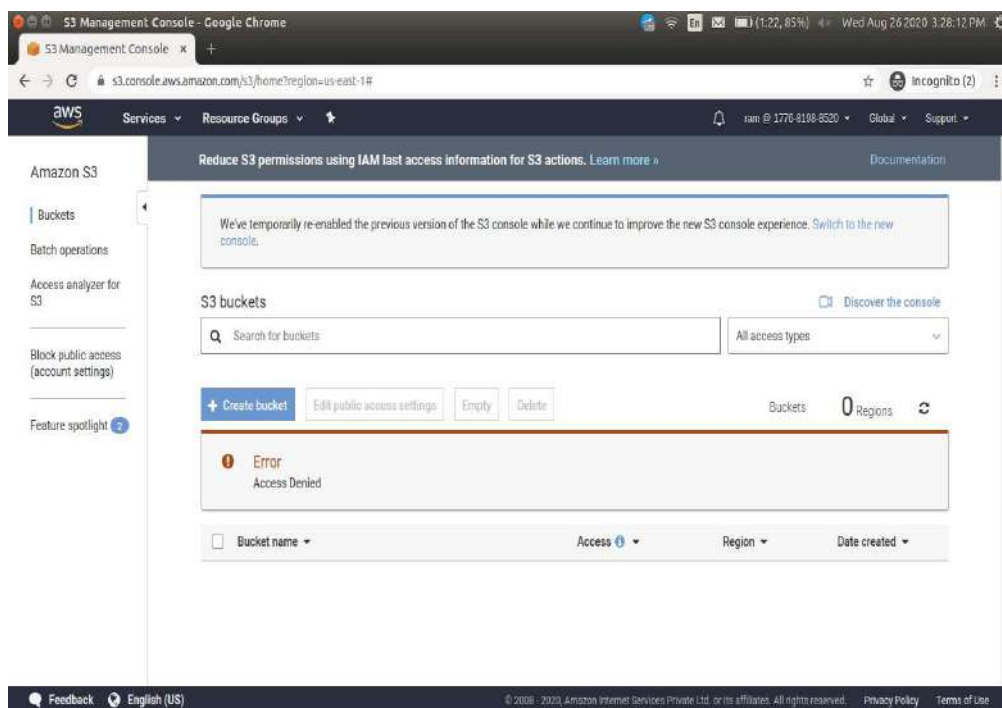
Join Other ML Experts

Verification

Click on EC2 verify the access

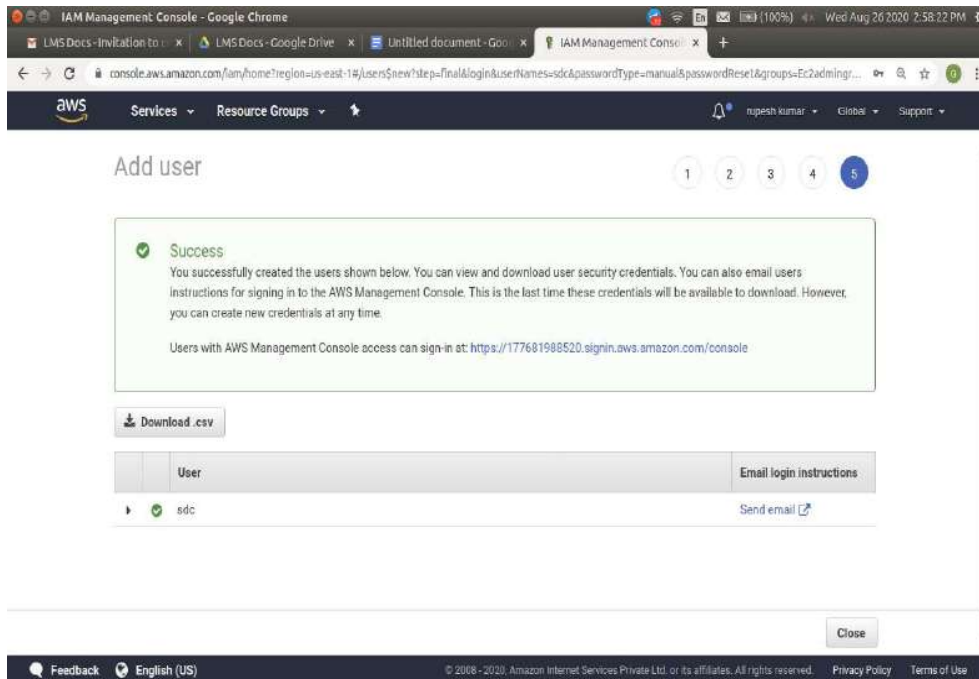


Click on S3 verify the access



To verify whether users can access particular Service

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

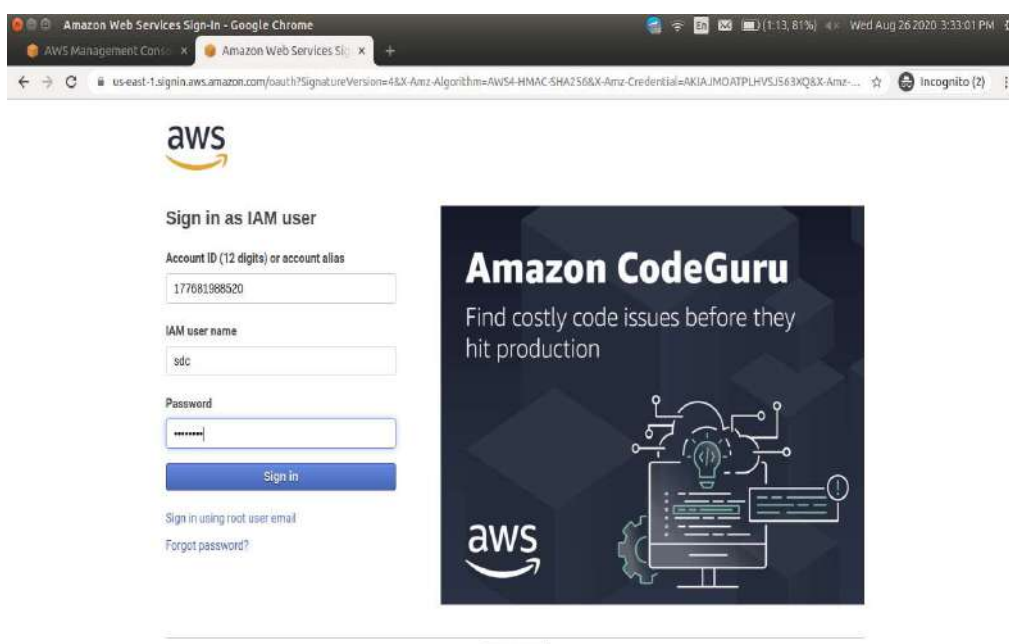


Provide the following url in Browser

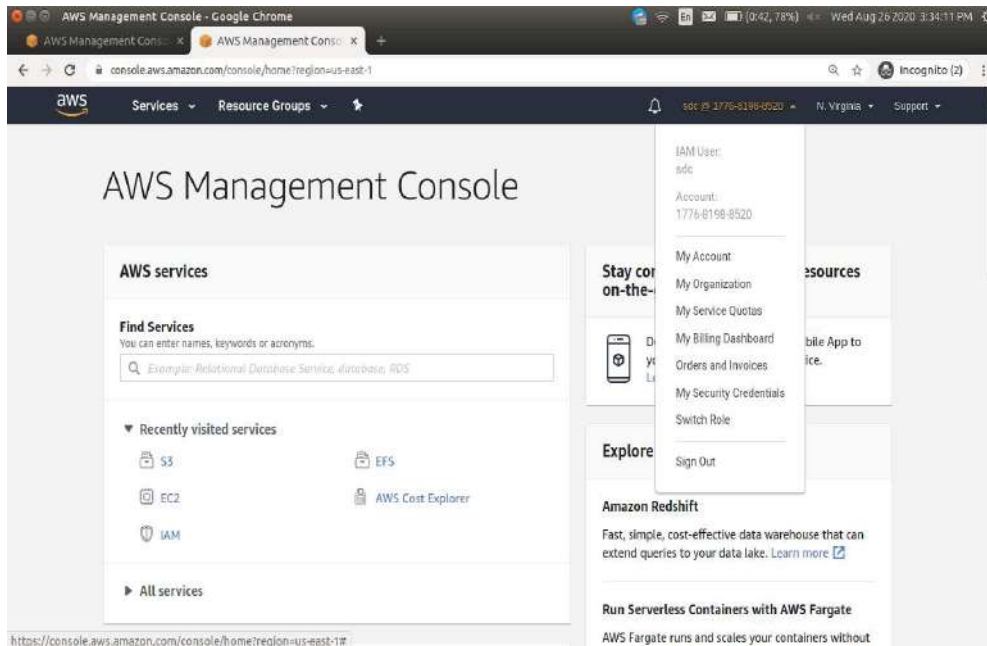
<https://177681988520.signin.aws.amazon.com/console>

Click on Sign in button

Now login as sd user

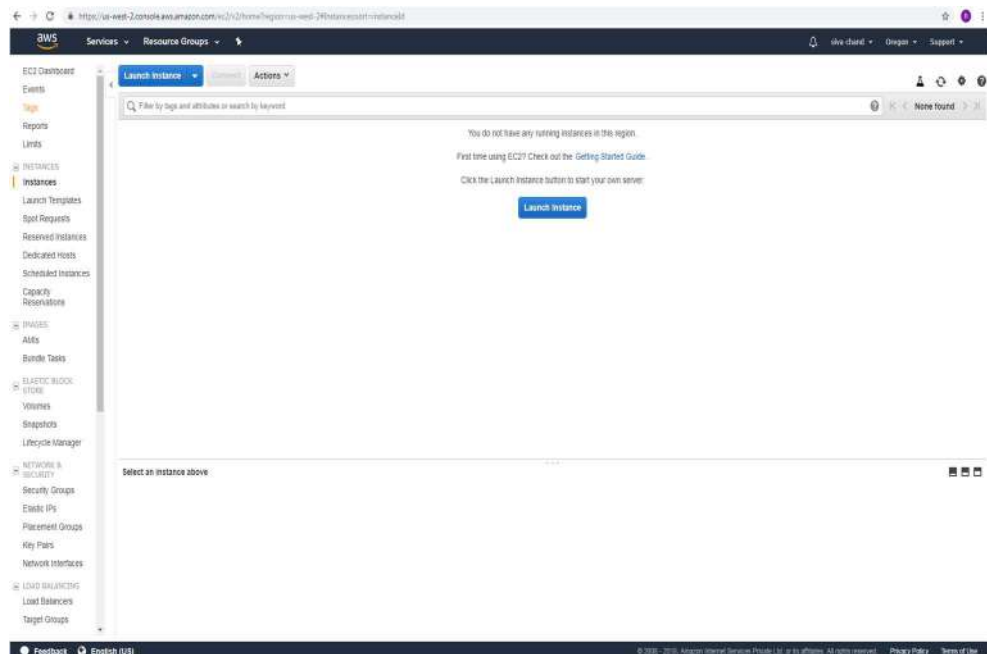


Verify user had successfully logged in



Verification

Click on EC2 verify the access



Click on S3 verify the access

