Department of Computer Engineering

Academic Term: JAN-MAY 2022

Class: ***BE COMPUTERS***

Subject Name: ***CLOUD COMPUTING LABORATORY***

Subject Code: CSL803

Practical No:	**05**
Title:	**AWS IAM**
Date of Performance:	**09/02/22**
Date of Submission:	**11/04/2022**
Roll No:	**8626**
Name of the Student:	**Divita Phadakale**

Evaluation:

Sr. No	Rubric	Grade
1	On time submission(2)	
2	Preparedness(2)	
3	Output(2)	
4	Post Lab Questions (4)	
	TOTAL	

Signature of the Teacher:

Fr. Conceicao Rodrigues College Of Engineering

Cloud Computing Lab

Prof. Sunil Choudhary

Cloud Security AWS IAM

Introduction

Amazon Web Services (AWS) cloud provides a secure virtual platform where users can deploy their applications. Compared to an on-premises environment, AWS security provides a high level of data protection at a lower cost to its users. There are many types of security services, but Identity and Access Management (IAM) is one the most widely used. AWS IAM enables you to securely control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

Cloud security is the highest priority in AWS. When you host your environment in the cloud, you can be assured that it's hosted in a data center or in a network architecture that's built to meet the requirements of the most security-sensitive organization. Additionally, this high level of security is available on a pay-as-you-go basis, meaning there is really no upfront cost, and the cost for using the service is a lot cheaper compared to an on-premises environment.

There are many types of security services available but some of them are widely used by AWS, such as:

- IAM
- Key Management System (KMS)
- Cognito
- Web Access Firewall (WAF)

IAM

<u>What is IAM?</u>

AWS Identity and Access Management (IAM) is a web service for securely controlling access to AWS resources. It enables you to create and control

services for user authentication or limit access to a certain set of people who use your AWS resources.

Components Of IAM

Users

These are the people that will be interacting with your resources. In other words, anyone that you want to have the ability to log into the AWS console.

Groups

Groups are a collection of users. For example, you can organize your users who are in the business development team to a group named BusinessDev. By grouping all the users into a group you are able to assign group permissions, and therefore can only allow access to the resources needed by the group.

Roles

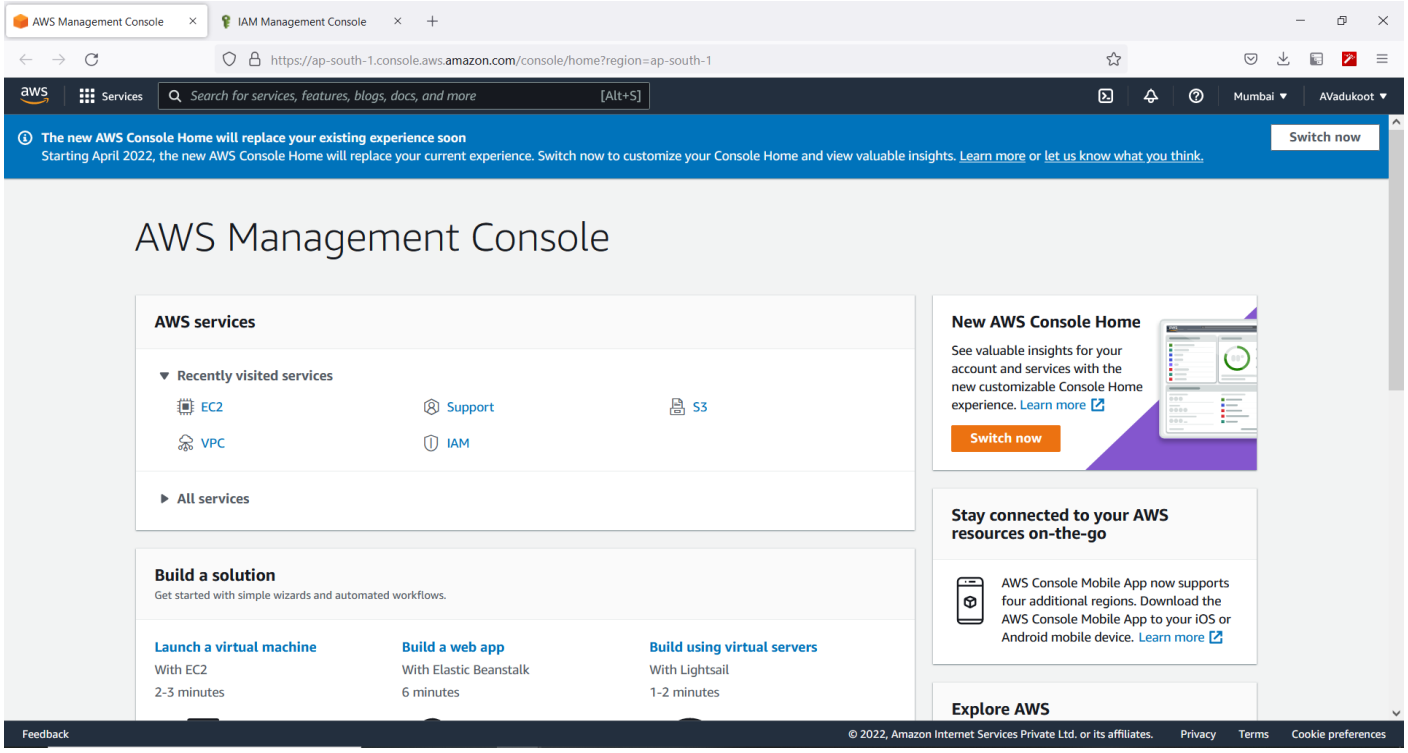
An IAM role defines a set of permissions that can be attributed to users, groups, or services such as EC2.

Policies

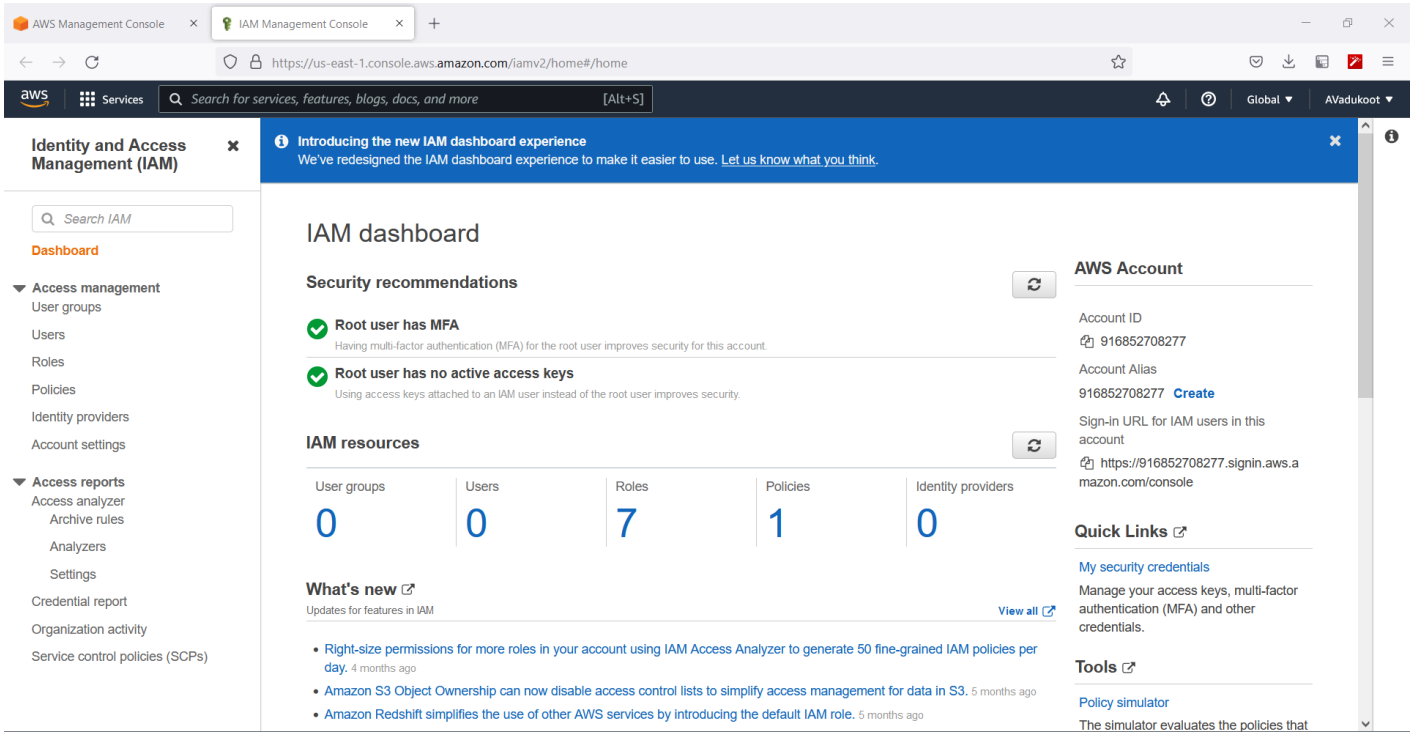
A policy is a document that defines one or more permissions.

How to use IAM and create Users, assign User Groups, Roles

Step 1 : Go to the Services dropdown menu and search for IAM.



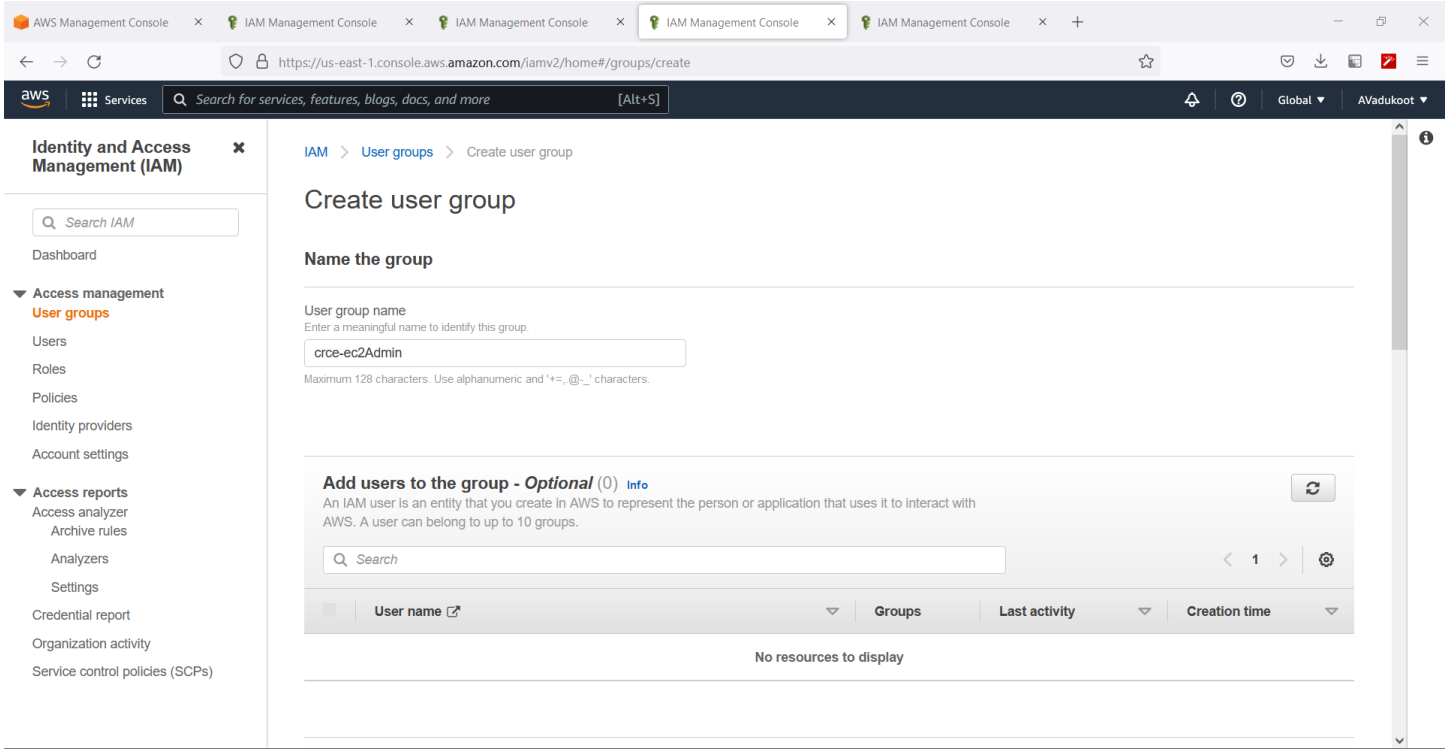
Step 2 :Click on IAM. You should be navigated to the IAM Dashboard.



In this section, before getting to creating users, AWS will prompt you to enable MFA (Multifactor Authentication) and ask you to delete active keys.

Step 3: Create IAM User Group

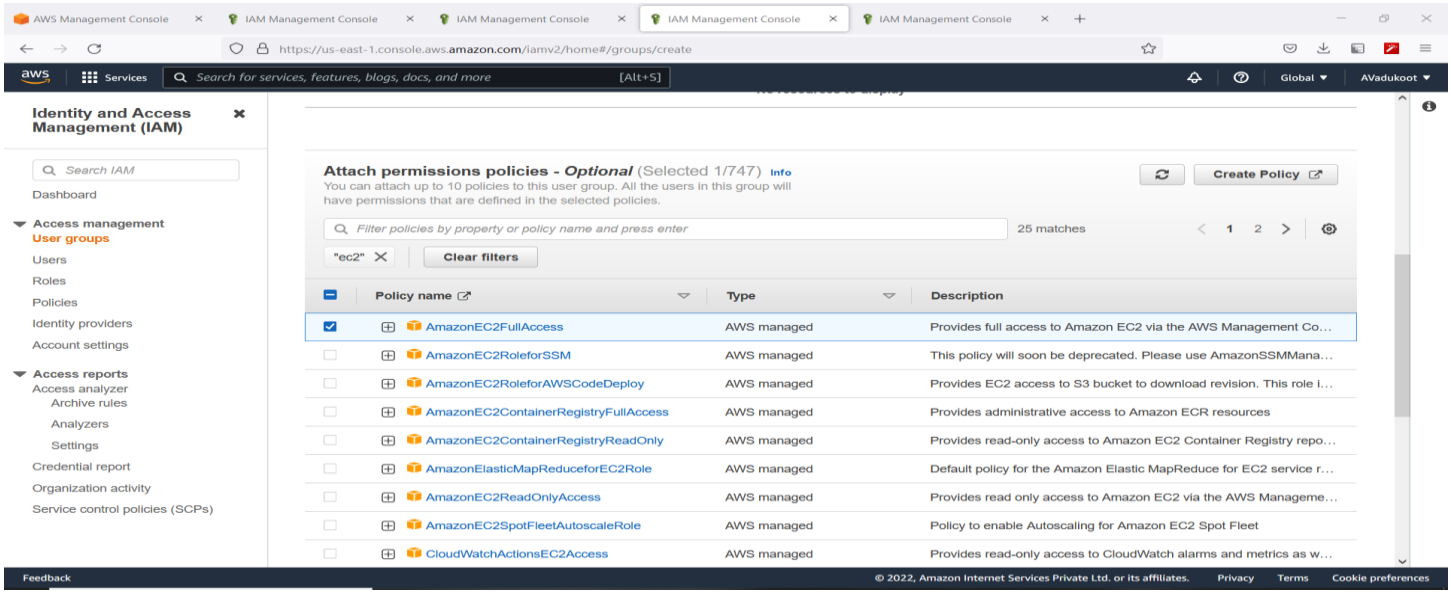
In the main IAM page, there exists a USER GROUP tab which enables the root user to view all the user groups and also create/delete user groups.

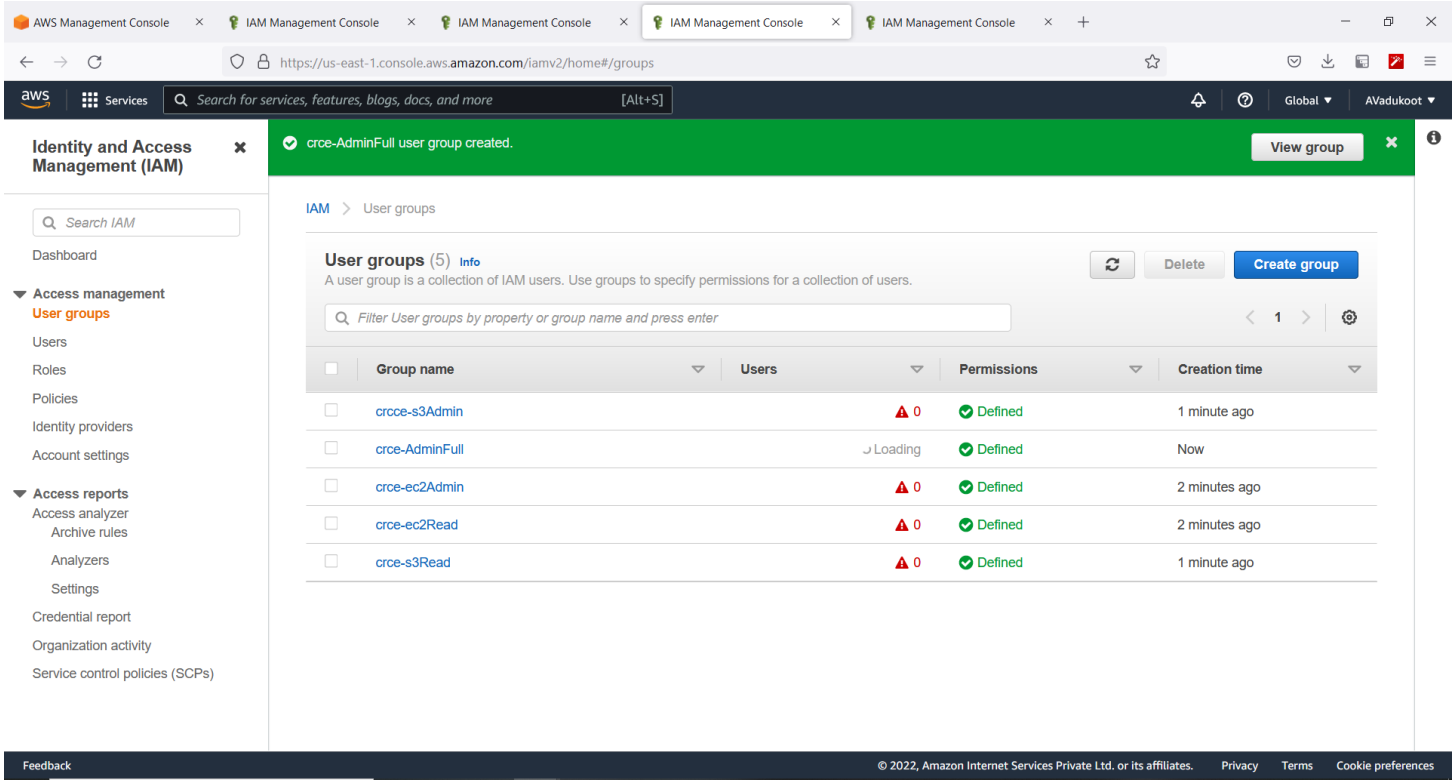


To create a new user group :

Root User has to mention the group name

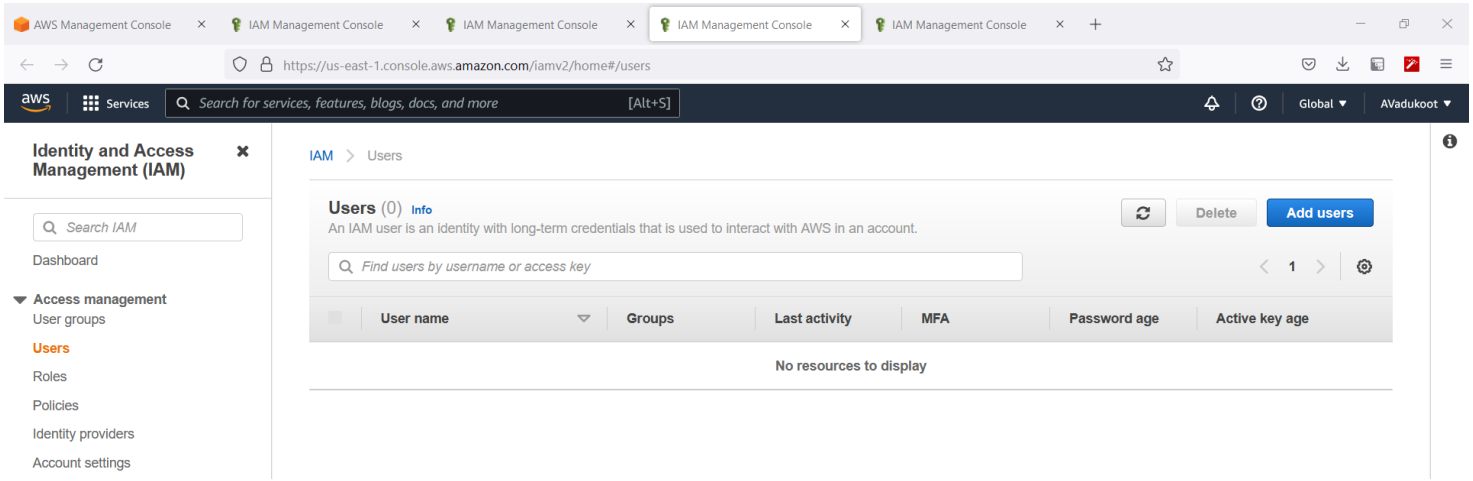
And Assign it specific Roles





Step 4 : Create IAM User

In the main IAM page, there exists a USER tab which enables the root user to view all the users and also create/delete users.

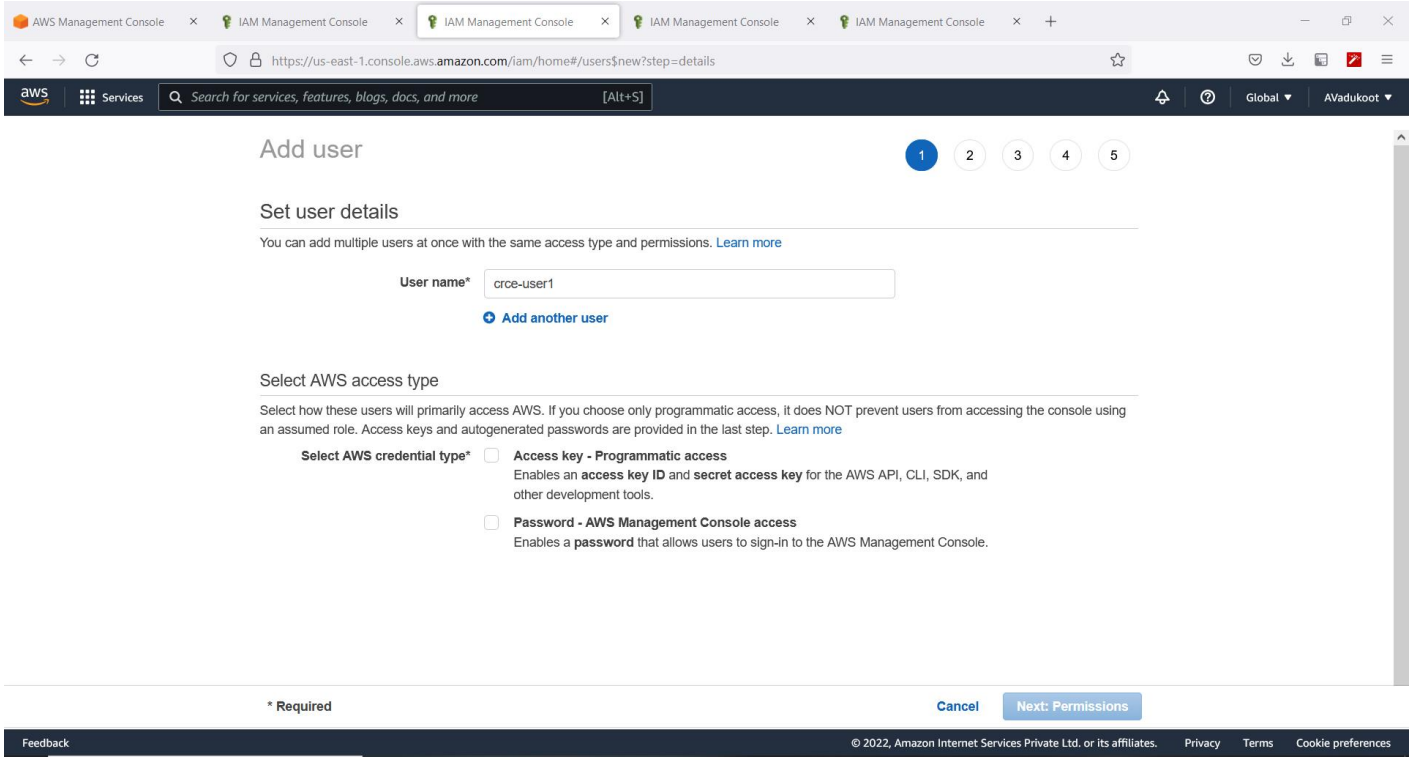


To create a new user:

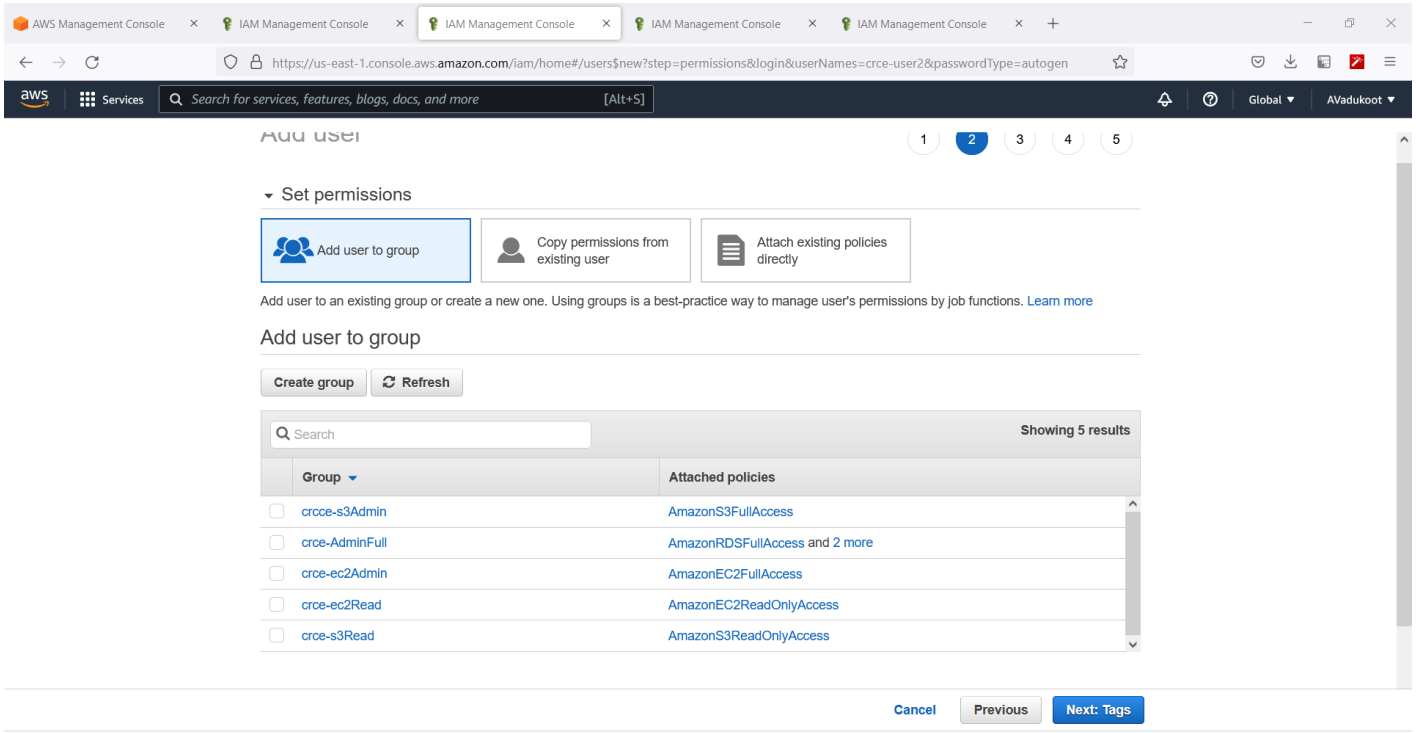
It will ask you to input User name

Ask you type of password for the user

And if the password has to be reset for every use.

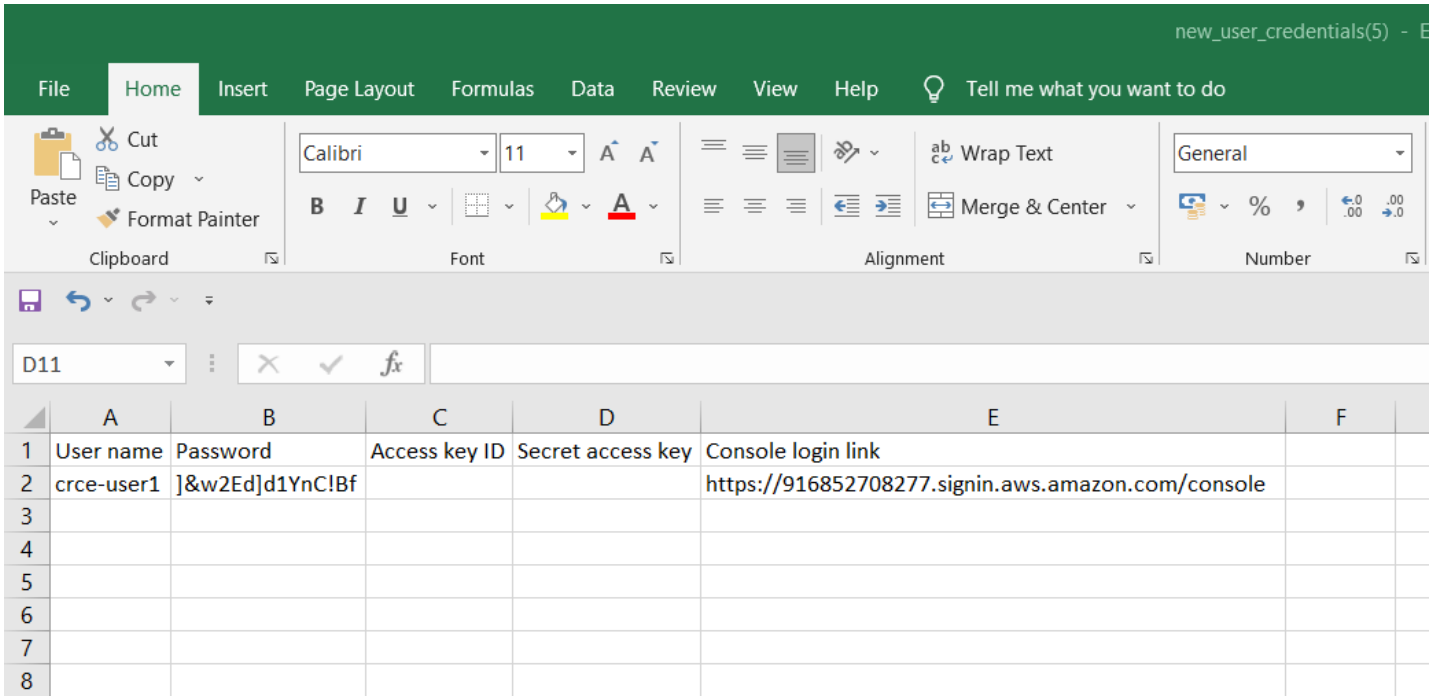


Then it will ask you to add the user to a user group or assign roles to the user.



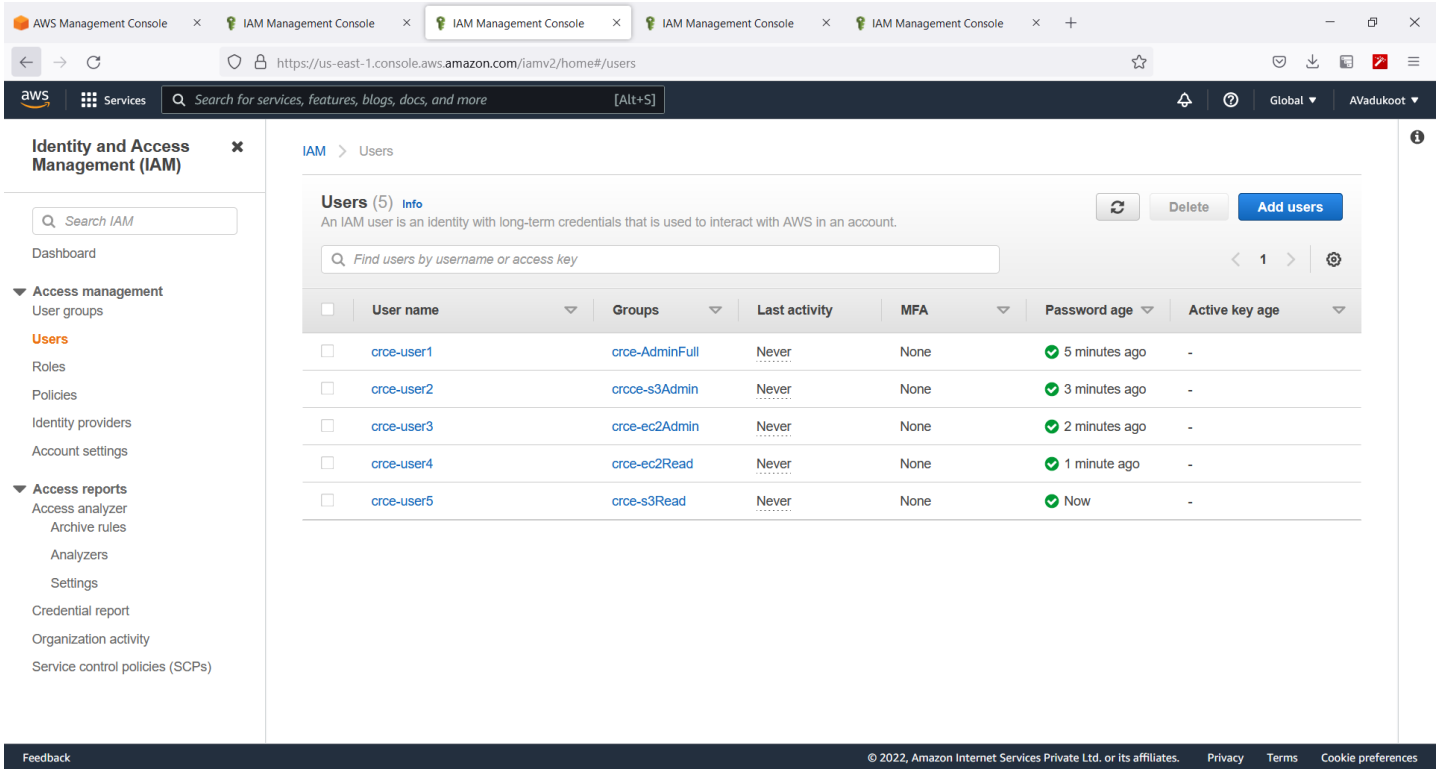
After that step, IAM prompt will give out the password and id of the user.

This can be downloaded or sent to mail for reference



	A	B	C	D	E	F
1	User name	Password	Access key ID	Secret access key	Console login link	
2	crce-user1	]&w2Ed]d1YnC!Bf			https://916852708277.signin.aws.amazon.com/console	
3						
4						
5						
6						
7						
8						

In this way you can create multiple users and assign them different Roles or put them in different User Groups.



The users above have these permissions

Crce-user1 – S3FullAccess

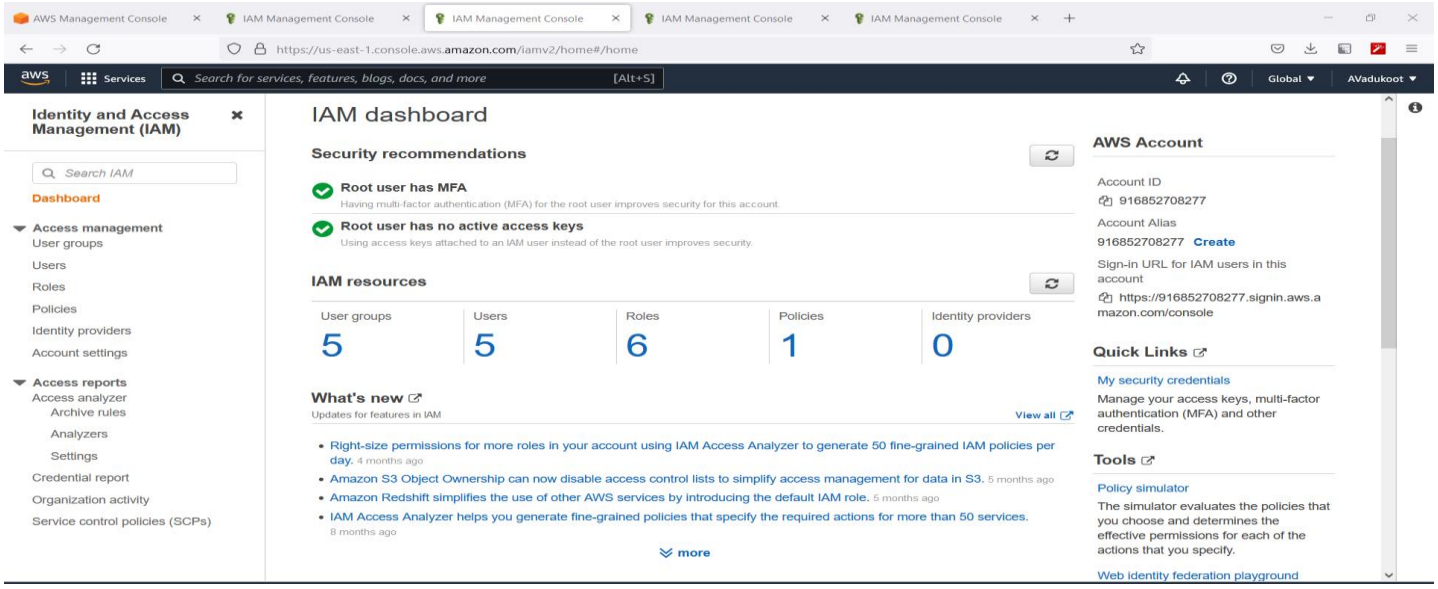
Crce-user2 – FullAccess (RDS,EC2,S3)

Crce-user3 – EC2FullAccess

Crce-user4 – EC2ReadOnly

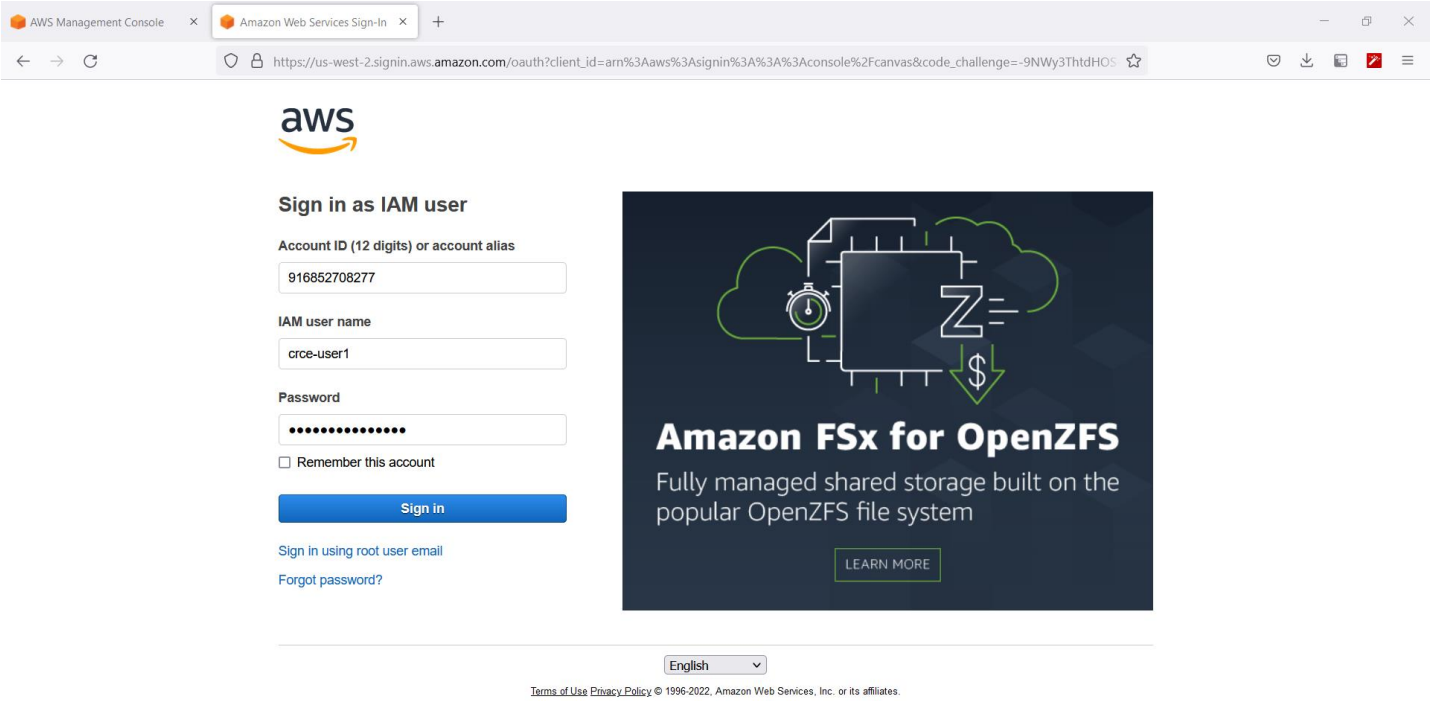
Crce-user5 – S3ReadOnly

After creation of Users and Groups , the Main IAM Dashboard will appear like this



Step 5: Now that created Users have been assigned to specific User Groups, let us sign in as the user and check what permissions it has.

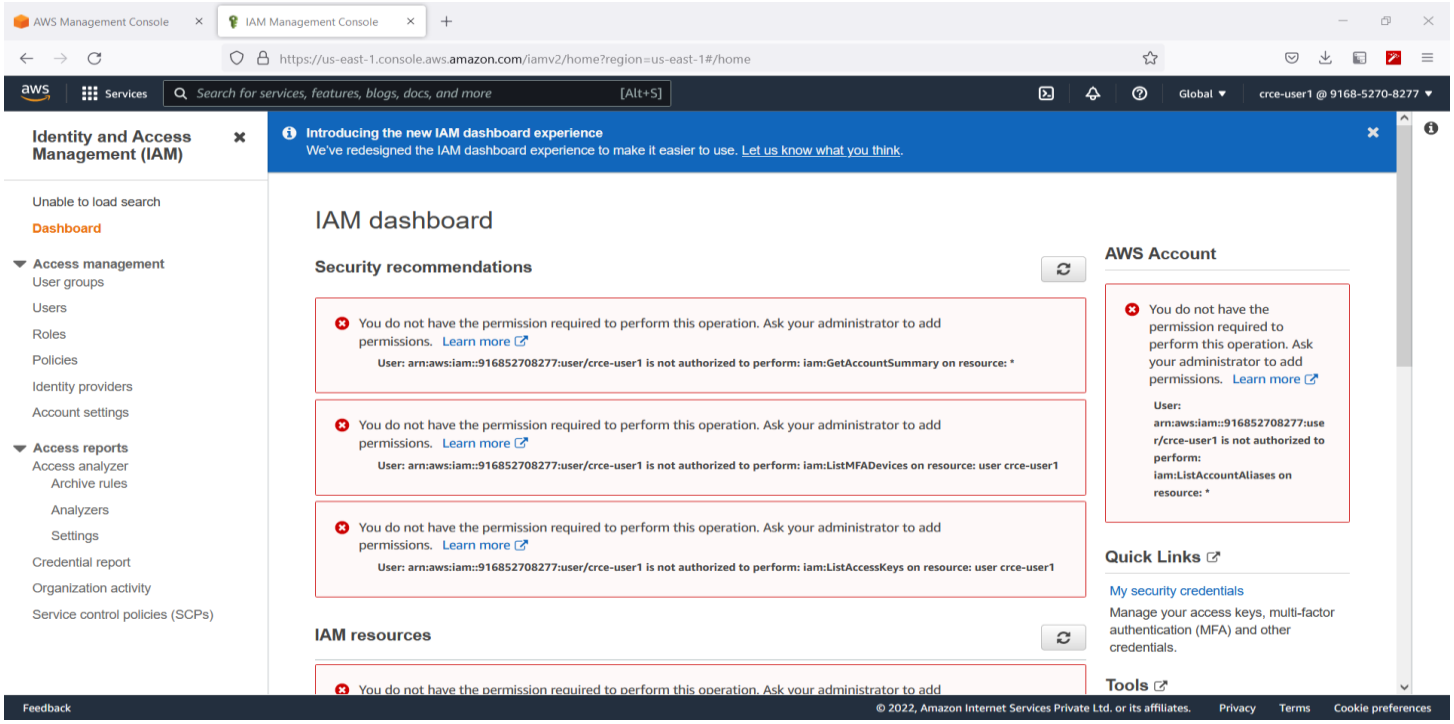
The root user has a code , called the Account ID , which all users must have to sign in



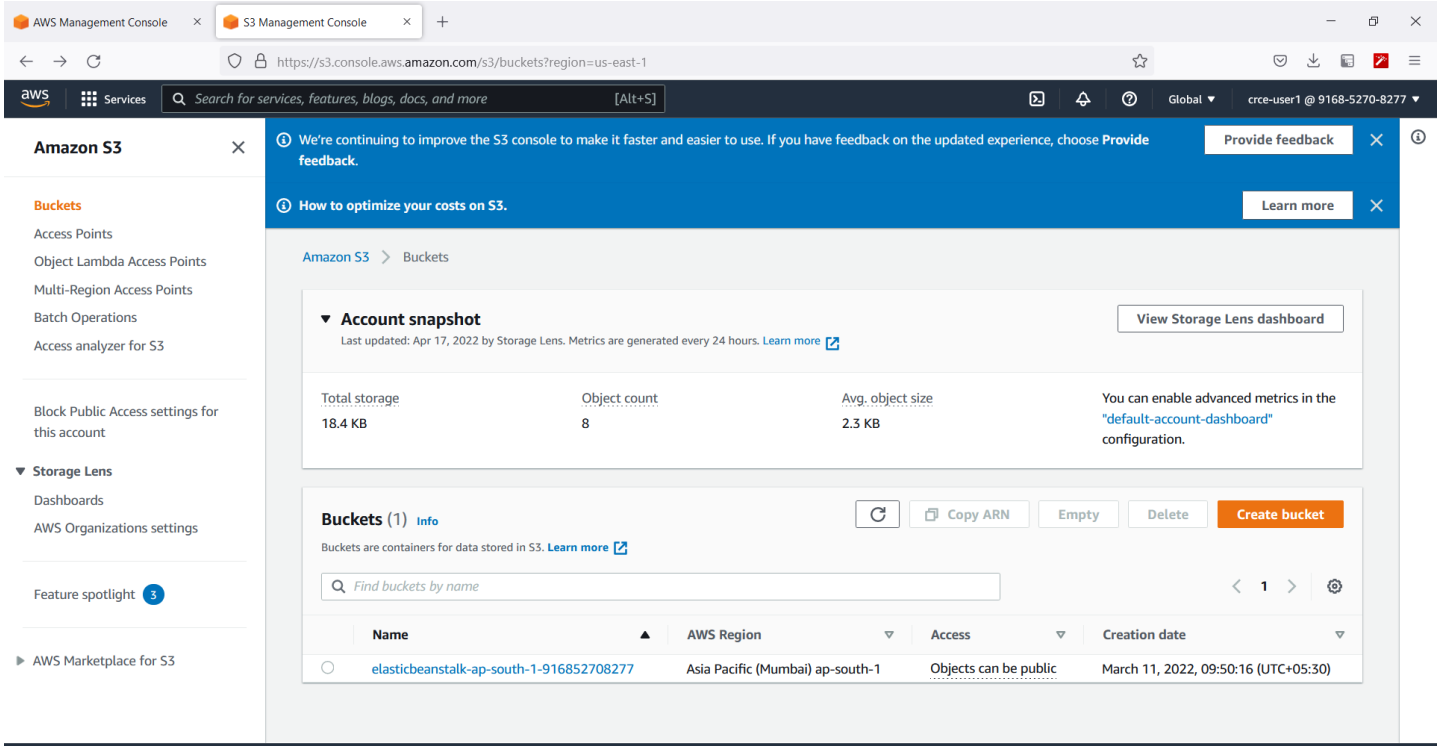
This specific user, crce-user1, has full access for S3 buckets

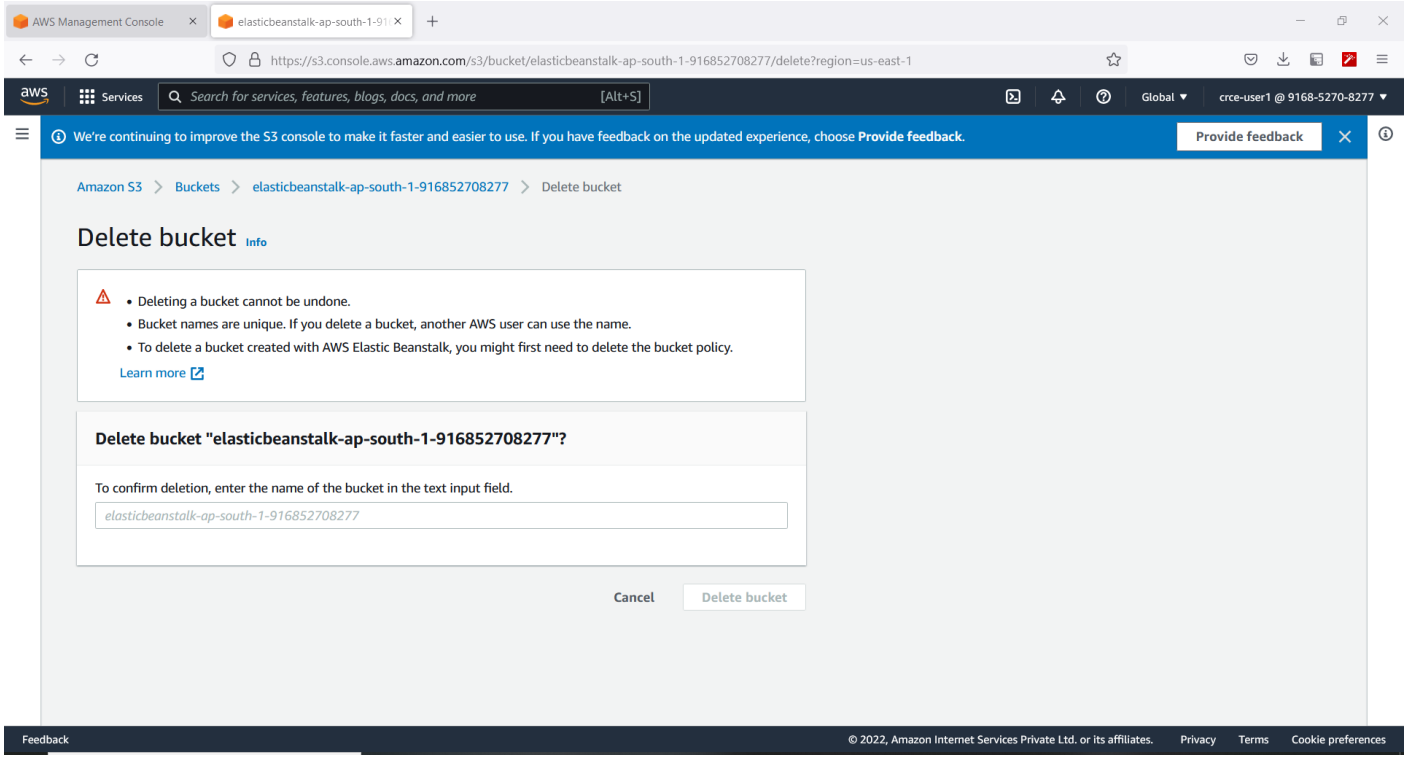
This should allow crce-user1 to handle only S3 bucket services and no other services.

IAM service (used by Root user) is not allowed to be used by crce-user1



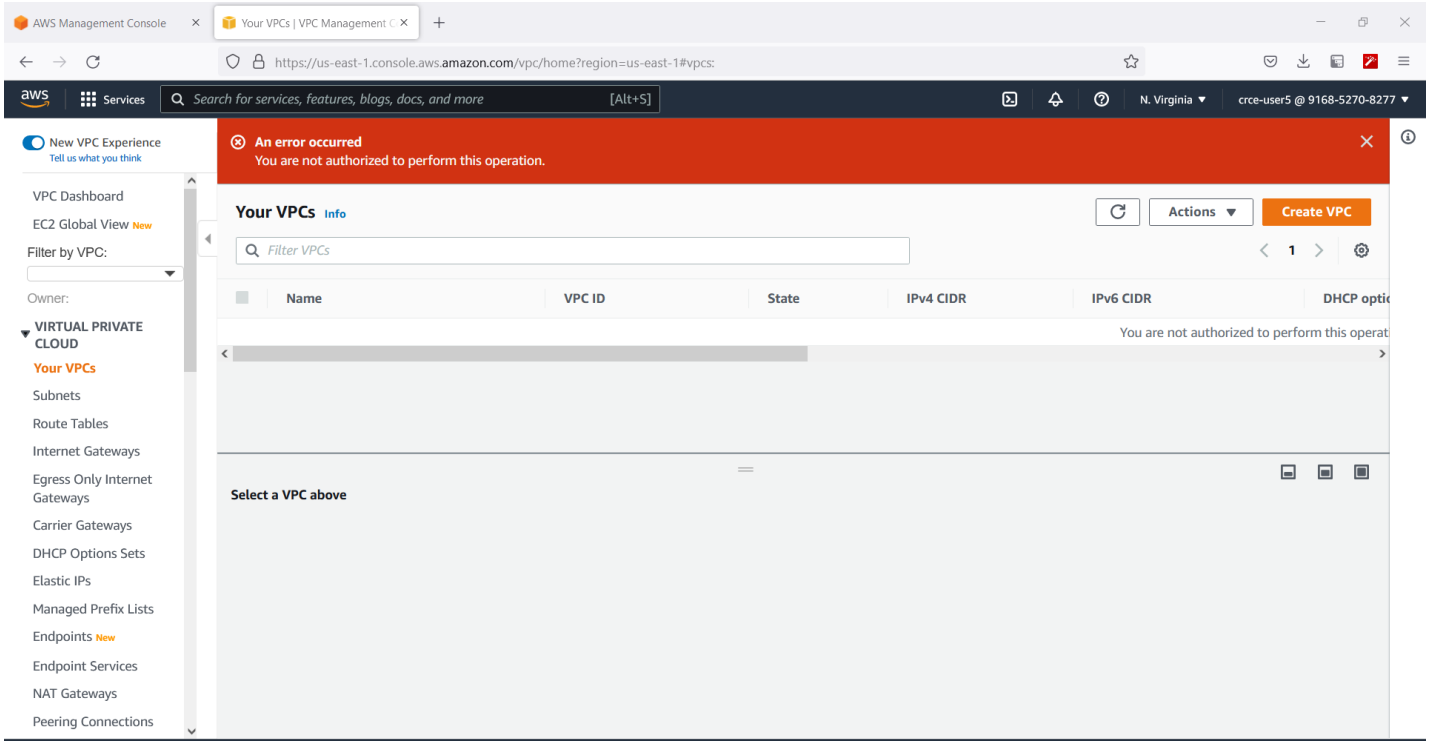
But it is able to freely use S3 buckets service



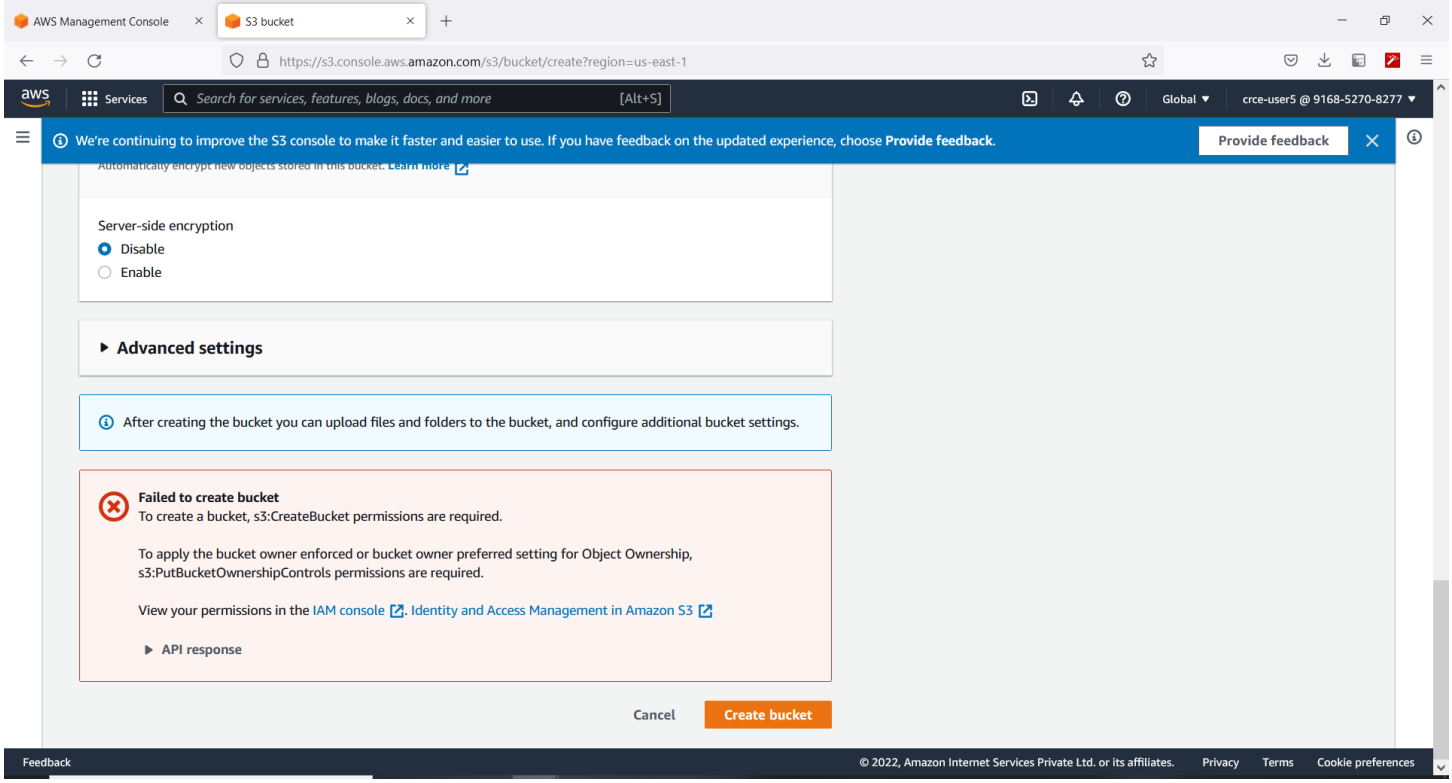


Now for example : crce-user5, has been given peprmission to only get S3ReadAccess

So, it is not able to use the VPC Services and Functions



Also, not able to create/delete buckets



Conclusion:

The main feature of IAM is that it allows you to create separate usernames and passwords for individual users or resources and delegate access. Restrictions can be applied to requests. For example, you can allow the user to download information, but deny the user the ability to update information through the policies. IAM supports MFA, in which users provide their username and password plus a one-time password from their phone—a randomly generated number used as an additional authentication factor. The IAM password policy allows you to reset a password or rotate passwords remotely. You can also set rules, such as how a user should pick a password or how many attempts a user may make to provide a password before being denied access.

Post Lab Questions:

Q1. What is AWS Identity and Access Management (IAM)?

AWS Identity and Access Management (IAM) is a web service for securely controlling access to AWS resources. It enables you to create and control services for user authentication or limit access to a certain set of people who use your AWS resources.

Components Of IAM

Users

These are the people that will be interacting with your resources. In other words, anyone that you want to have the ability to log into the AWS console.

Groups

Groups are a collection of users. For example, you can organize your users who are in the business development team to a group named BusinessDev. By grouping all the users into a group you are able to assign group permissions, and therefore can only allow access to the resources needed by the group.

Roles

An IAM role defines a set of permissions that can be attributed to users, groups, or services such as EC2.

Policies

A policy is a document that defines one or more permissions.

Q2. What problems does IAM solve?

- management pains
- streamline provisioning and de-provisioning
- boost user productivity
- lowering costs
- reducing demands on IT
- providing the enterprise with comprehensive data to assist in complying with regulatory standards.

Q3. How are IAM users managed?

The IAM workflow includes the following six elements:

1. A principal is an entity that can perform actions on an AWS resource. A user, a role or an application can be a principal.

2. Authentication is the process of confirming the identity of the principal trying to access an AWS product. The principal must provide its credentials or required keys for authentication.
3. Request: A principal sends a request to AWS specifying the action and which resource should perform it.
4. Authorization: By default, all resources are denied. IAM authorizes a request only if all parts of the request are allowed by a matching policy. After authenticating and authorizing the request, AWS approves the action.
5. Actions are used to view, create, edit or delete a resource.
6. Resources: A set of actions can be performed on a resource related to your AWS account.

Q4. What kinds of security credentials can IAM users have?

Cloud security is the highest priority in AWS. When you host your environment in the cloud, you can be assured that it's hosted in a data center or in a network architecture that's built to meet the requirements of the most security-sensitive organization. Additionally, this high level of security is available on a pay-as-you-go basis, meaning there is really no upfront cost, and the cost for using the service is a lot cheaper compared to an on-premises environment.

There are many types of security services available but some of them are widely used by AWS, such as:

- IAM
- Key Management System (KMS)
- Cognito
- Web Access Firewall (WAF)

We shall deal with IAM in this tutorial.

IAM enables you to manage access to AWS services and resources in a very secure manner. With IAM you can create groups and allow those users or groups to access some servers, or you can deny them access to the service.