AIM: To study and implement Identity and Access Management (IAM) practices on AWS/Azure cloud.

THEORY:

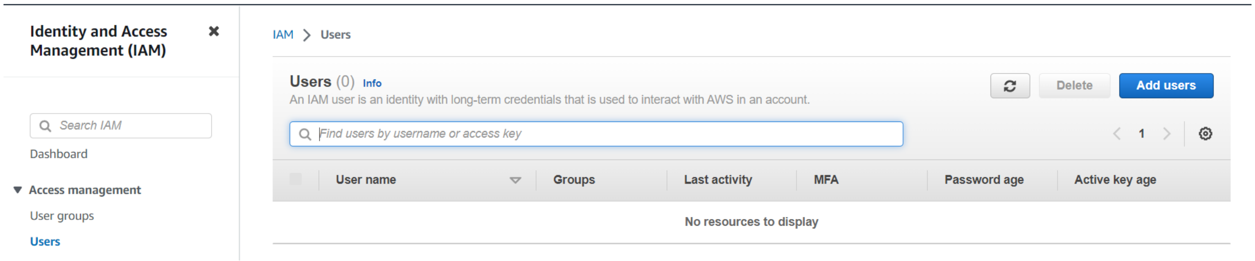
- AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users.
- The service is targeted at organizations with multiple users or systems that use AWS products such as Amazon EC2, Amazon RDS, and the AWS Management Console.
- With IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access.

Features of IAM:

- **Centralised control of your AWS account:** You can control creation, rotation, and cancellation of each user's security credentials. You can also control what data in the aws system users can access and how they can access.
- **Shared Access to your AWS account:** Users can share the resources for the collaborative projects.
- **Granular permissions:** It is used to set a permission that user can use a particular service but not other services.
- **Identity Federation:** An Identity Federation means that we can use Facebook, Active Directory, LinkedIn, etc with IAM. Users can log in to the AWS Console with same username and password as we log in with the Active Directory, Facebook, etc.
- **Multifactor Authentication:** An AWS provides multifactor authentication as we need to enter the username, password, and security check code to log in to the AWS Management Console.
- **Permissions based on Organizational groups:** Users can be restricted to the AWS access based on their job duties, for example, admin, developer, etc.

OUTPUT:

1. Click on Add user and add name of the user. Click on Next.



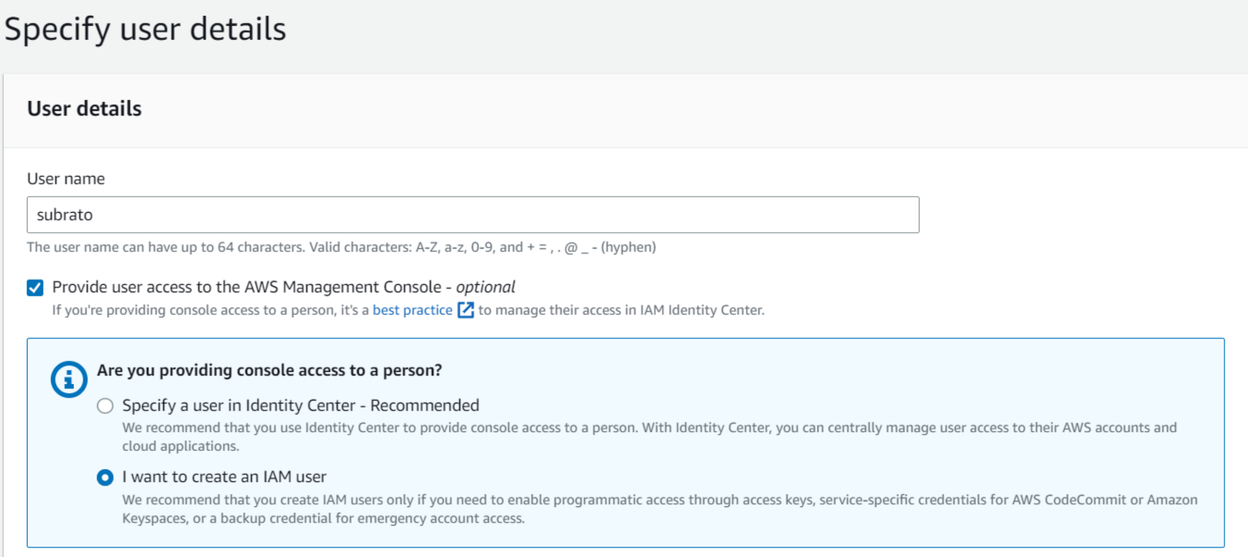
Users (0) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Find users by username or access key

No resources to display

2. Write the **user name.** Select Provide uder access to AWS management. Click on I want to create an IAM user.



Specify user details

User details

User name: subrato

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☑ Provide user access to the AWS Management Console - *optional*

If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

Are you providing console access to a person?

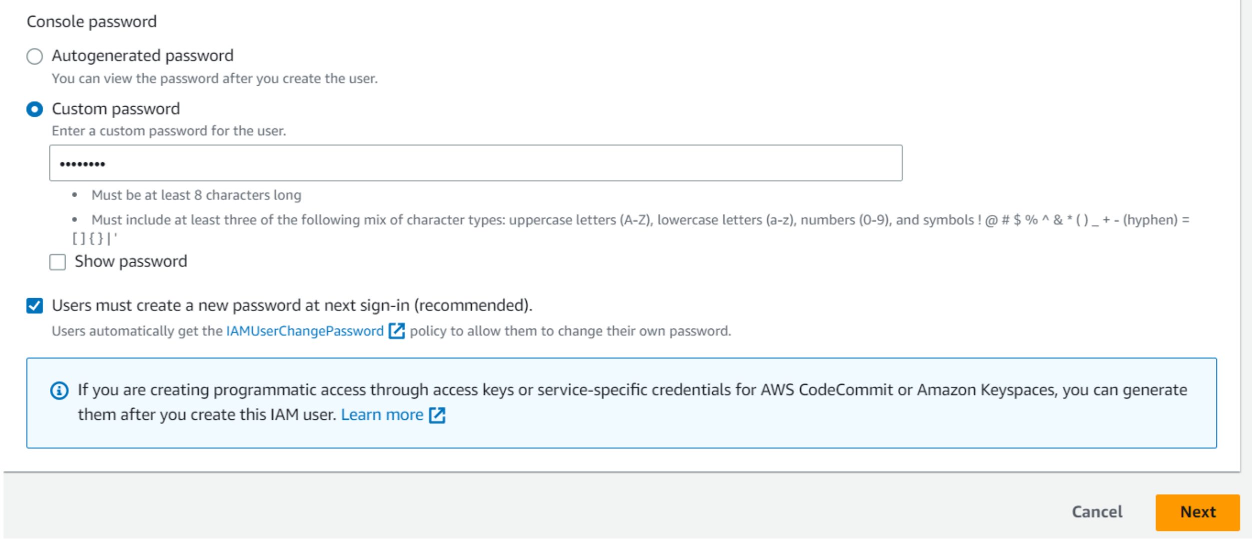
○ Specify a user in Identity Center - Recommended

We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

● I want to create an IAM user

We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

3. Enter custom password and click next. Finally Click on Next



Console password

○ Autogenerated password

You can view the password after you create the user.

● Custom password

Enter a custom password for the user.

••••••••

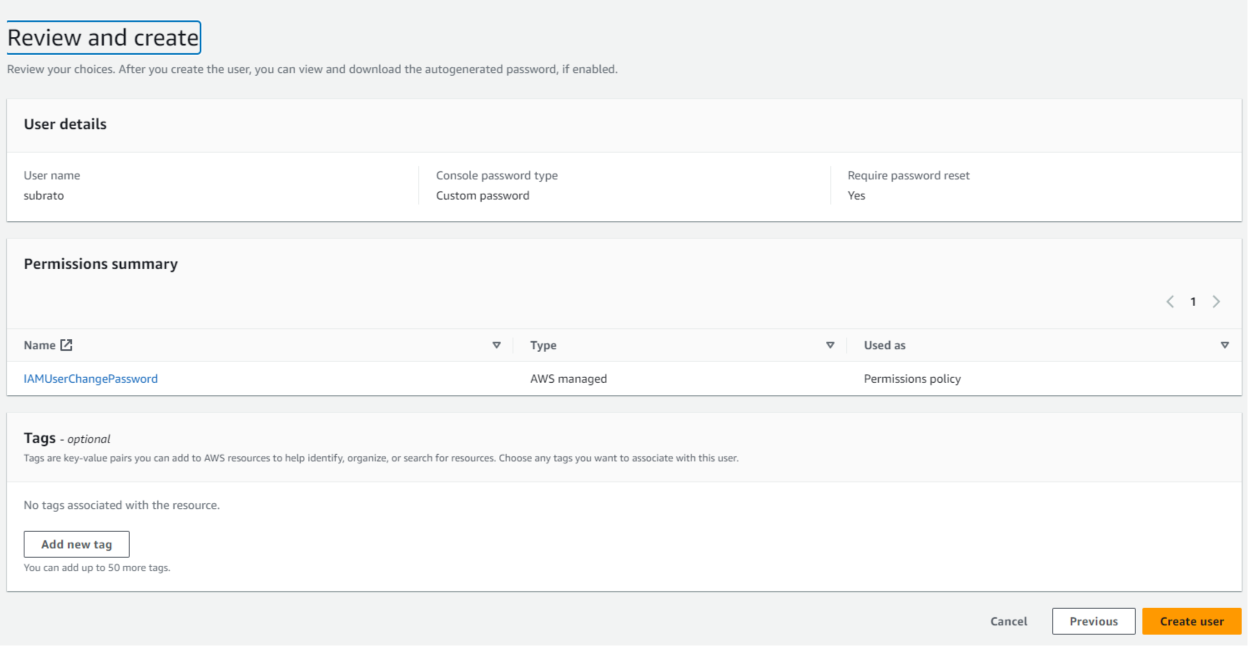
- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

□ Show password

☑ Users must create a new password at next sign-in (recommended).

Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more



Review and create

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

User details

User name	Console password type	Require password reset
subrato	Custom password	Yes

Permissions summary

Name	Type	Used as
IAMUserChangePassword	AWS managed	Permissions policy

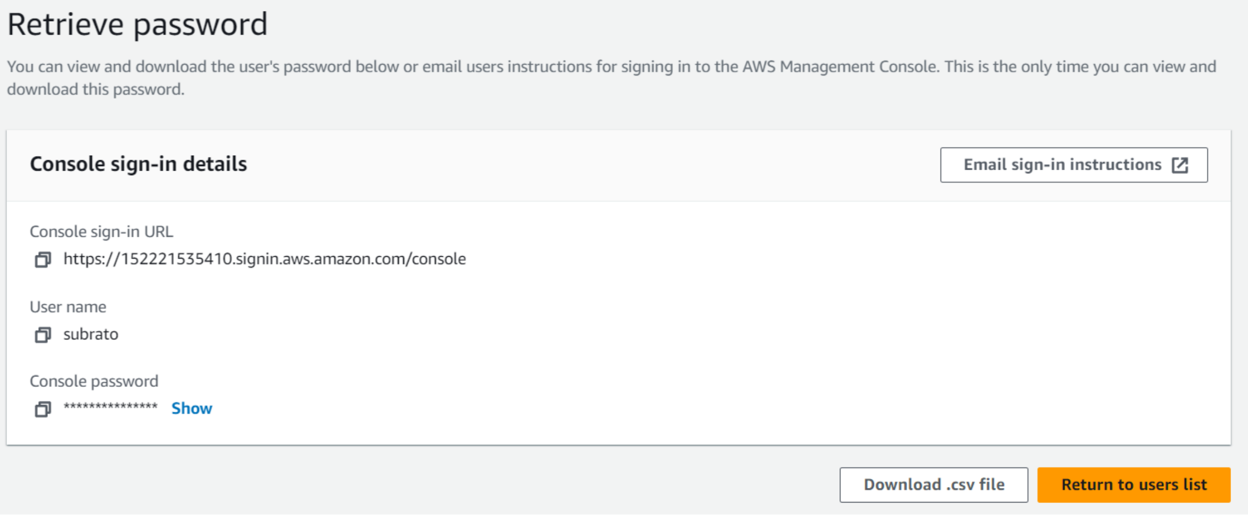
Tags - *optional*

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

You can add up to 50 more tags.

5. After creating a user, you get .csv file which contains the password of the user you created. You can download it if needed.



Retrieve password

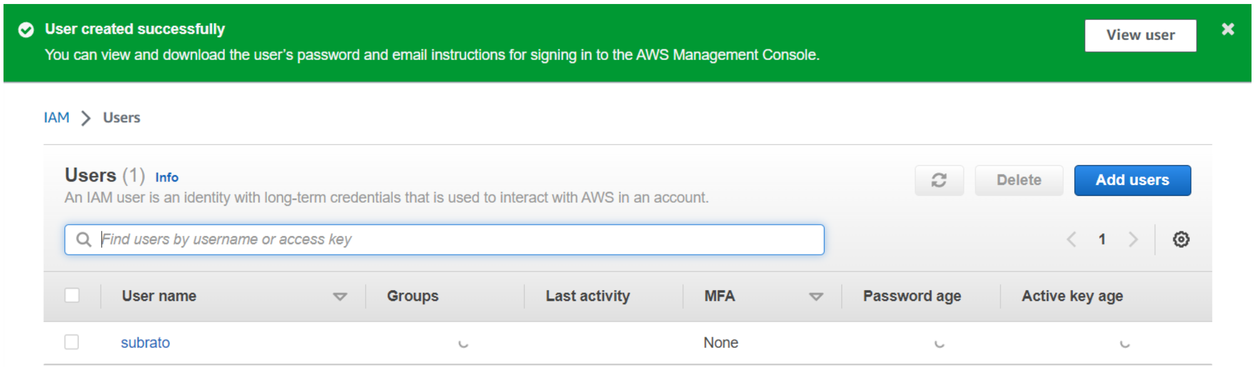
You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

Console sign-in URL
https://152221535410.signin.aws.amazon.com/console

User name
subrato

Console password
*************** Show



User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

IAM > Users

Users (1) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

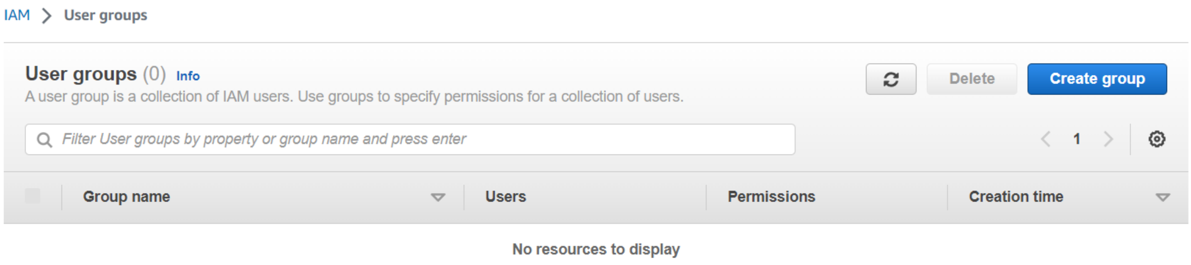
Find users by username or access key

User name	Groups	Last activity	MFA	Password age	Active key age
subrato			None		

User has been created successfully.

Create IAM Groups:

1. In user group, click on Create group.


IAM > User groups
Delete
Create group
Info
Filter User groups by property or group name and press enter
1

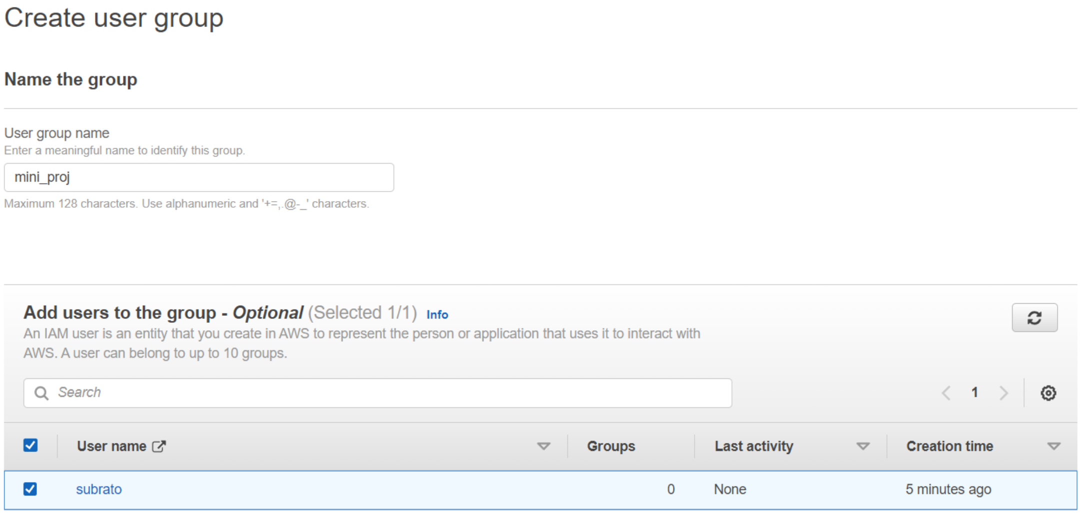
User groups (0)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Group name	Users	Permissions	Creation time

No resources to display

2. Enter a unique user group name and select user which you created to add in group.



Create user group

Name the group

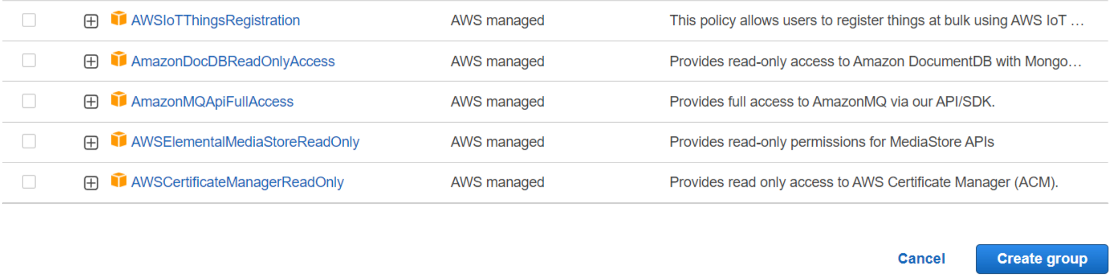
User group name
Enter a meaningful name to identify this group.
mini_proj
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Add users to the group - *Optional* (Selected 1/1)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user can belong to up to 10 groups.

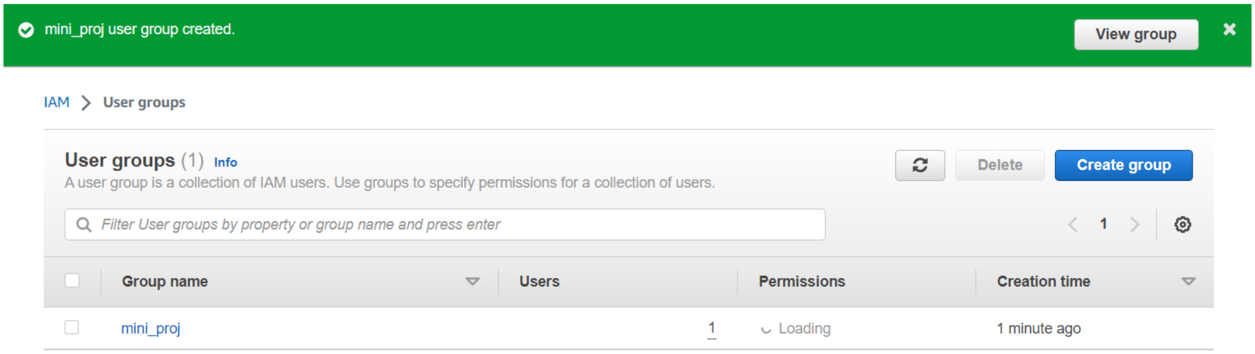
☑	User name	Groups	Last activity	Creation time
☑	subrato	0	None	5 minutes ago

You can attach permission policies if needed. Click on the create group button.



□	⊞ AWSIoTThingsRegistration	AWS managed	This policy allows users to register things at bulk using AWS IoT …
□	⊞ AmazonDocDBReadOnlyAccess	AWS managed	Provides read-only access to Amazon DocumentDB with Mongo…
□	⊞ AmazonMQApiFullAccess	AWS managed	Provides full access to AmazonMQ via our API/SDK.
□	⊞ AWSElementalMediaStoreReadOnly	AWS managed	Provides read-only permissions for MediaStore APIs
□	⊞ AWSCertificateManagerReadOnly	AWS managed	Provides read only access to AWS Certificate Manager (ACM).

3. IAM User Group is created successfully with the user you just created.


View group
IAM > User groups
Delete
Create group
Info
Filter User groups by property or group name and press enter
1

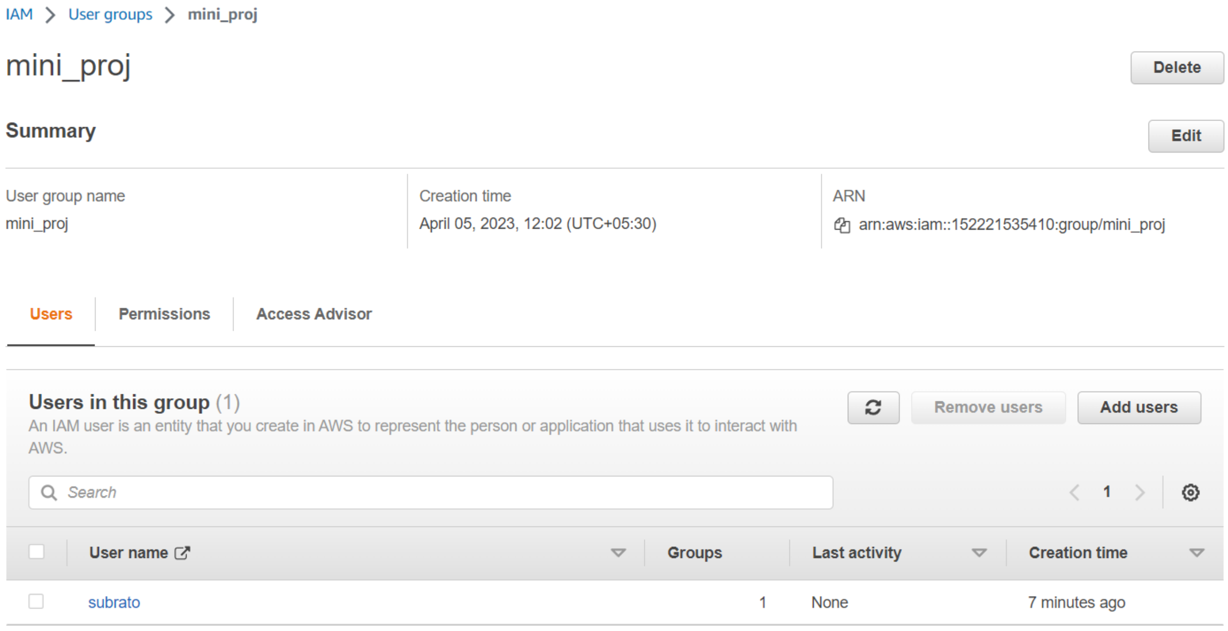
mini_proj user group created.

User groups (1)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

□	Group name	Users	Permissions	Creation time
□	mini_proj	1	Loading	1 minute ago

4. You can check for the summary of the user group that you have created.



IAM > User groups > mini_proj

mini_proj

Delete

Summary

Edit

User group name: mini_proj

Creation time: April 05, 2023, 12:02 (UTC+05:30)

ARN: arn:aws:iam::152221535410:group/mini_proj

Users | Permissions | Access Advisor

Users in this group (1)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Remove users | Add users

Search

1

□	User name	Groups	Last activity	Creation time
□	subrato	1	None	7 minutes ago

CONCLUSION:

We have studied and implemented IAM. We also created an IAM user and an user group.