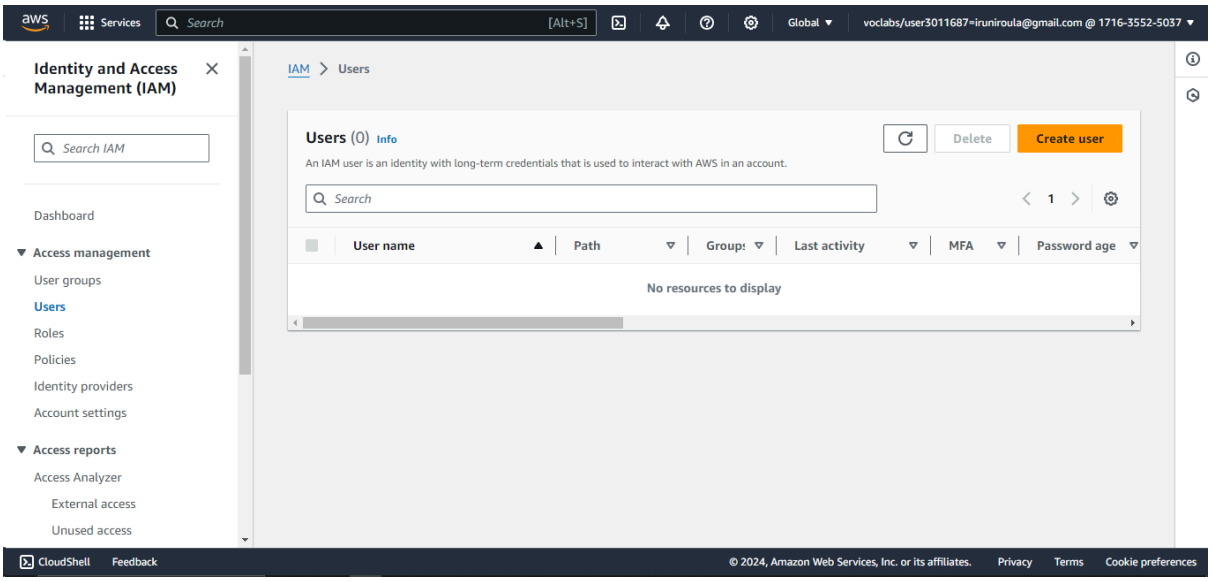
IAM Users and Roles Lab

Objective: To understand AWS Identity and Access Management (IAM) by creating and managing users, groups, and roles.

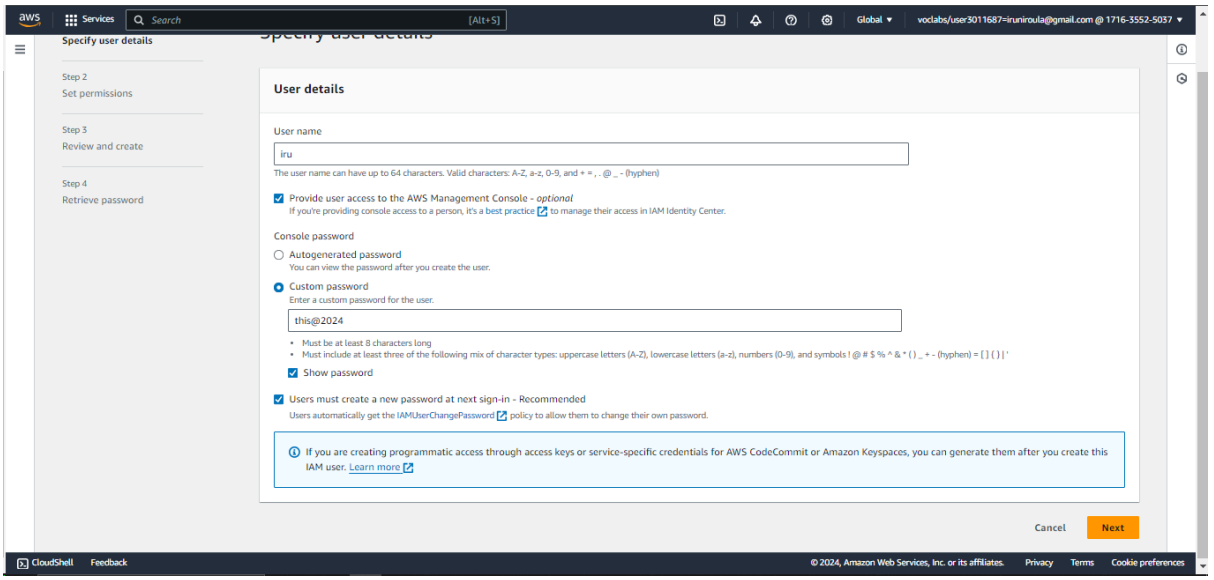
Approach: Students will create new IAM users, assign them to groups, and apply policies to manage permissions. The lab will also involve creating roles for AWS services and understanding the use of IAM roles for cross-service access.

Goal: Students will learn about user and permission management in AWS, the importance of roles for security and best practices for IAM.

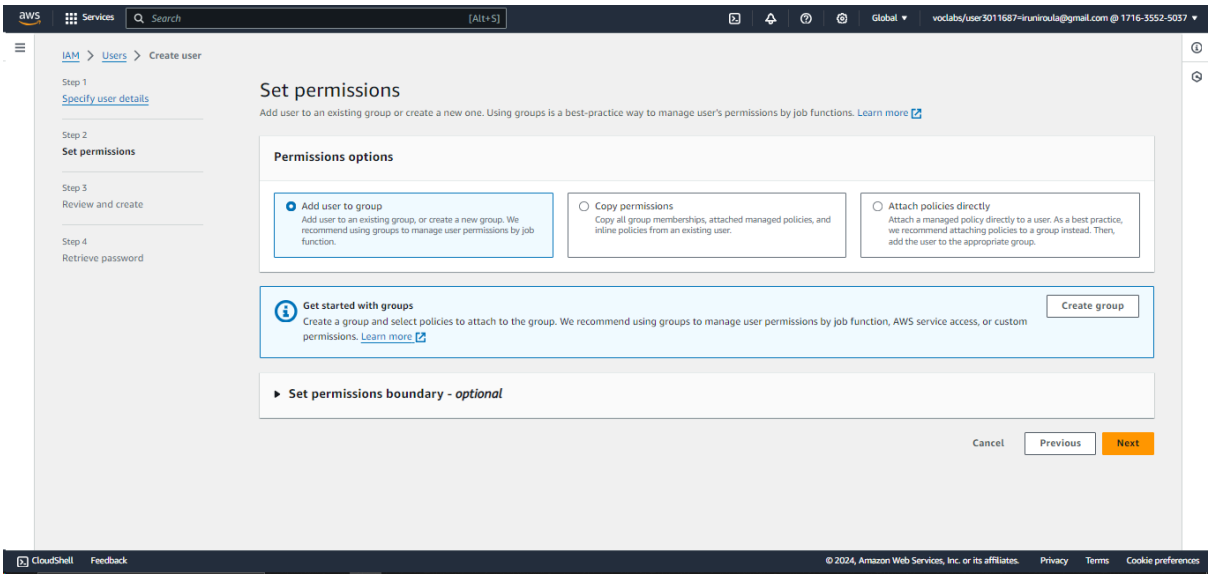
Create a new IAM User Group

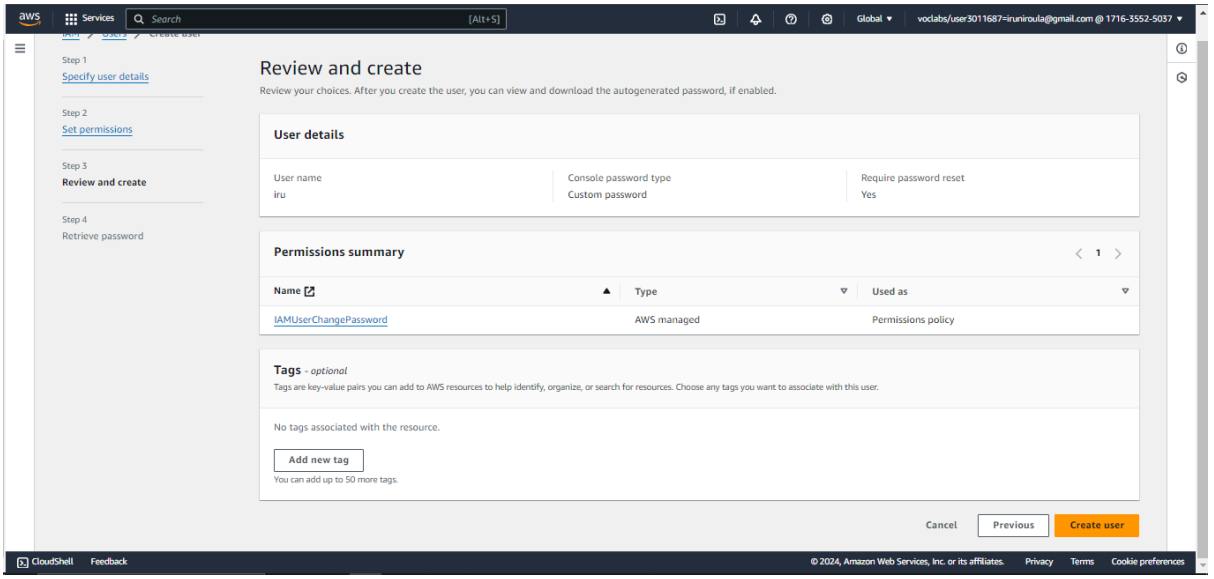


Inserting user details

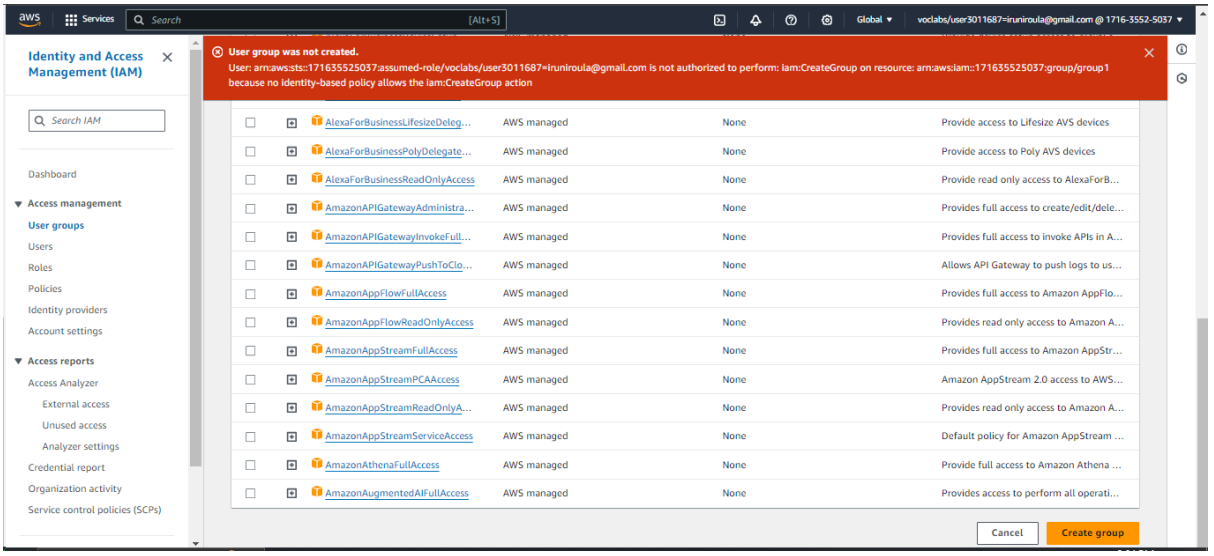


Setting Permissions

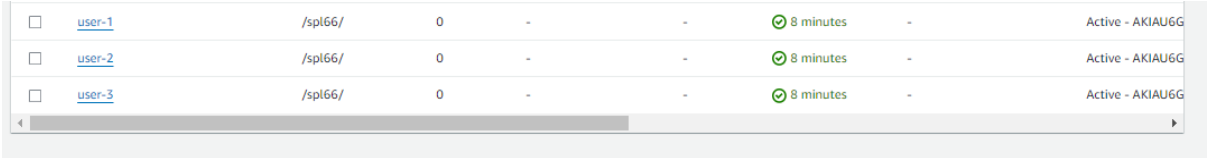




We are not authorized to create users or user groups. Therefore the rest of the actions are performed using AWS Cloud Foundations Lab

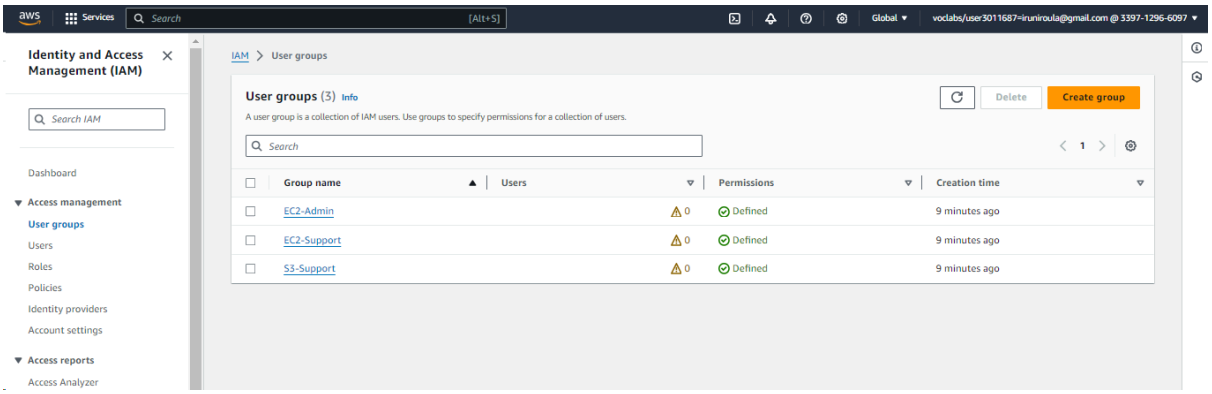


The following three users are created by default

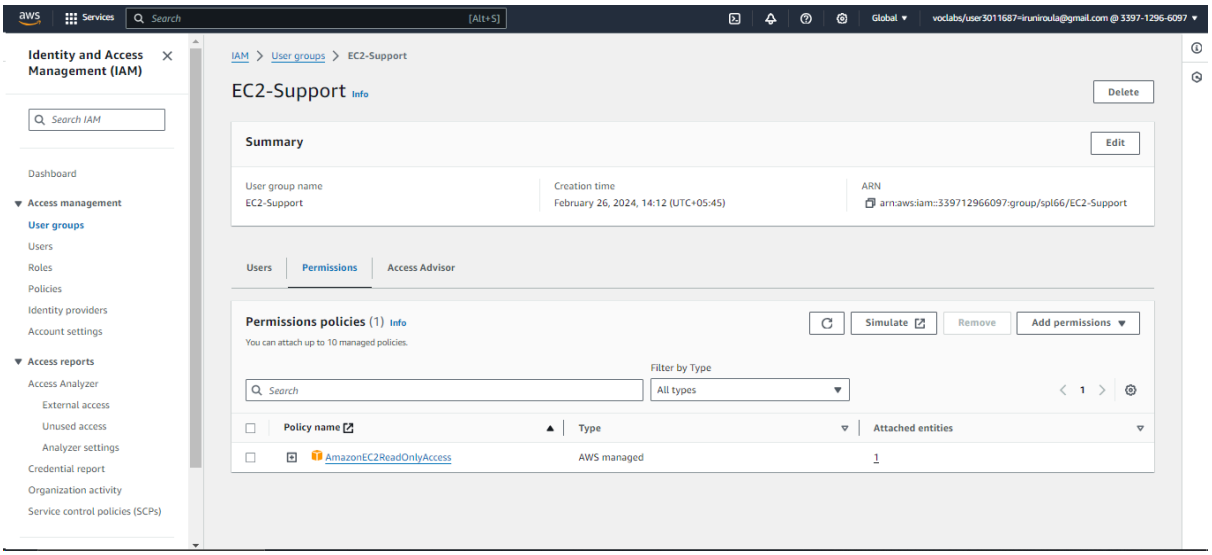


user-1	/spl66/	0	-	-	8 minutes	-	Active - AKIAU6G
user-2	/spl66/	0	-	-	8 minutes	-	Active - AKIAU6G
user-3	/spl66/	0	-	-	8 minutes	-	Active - AKIAU6G

The following three user groups are created by default



Permission for EC2-Support Group

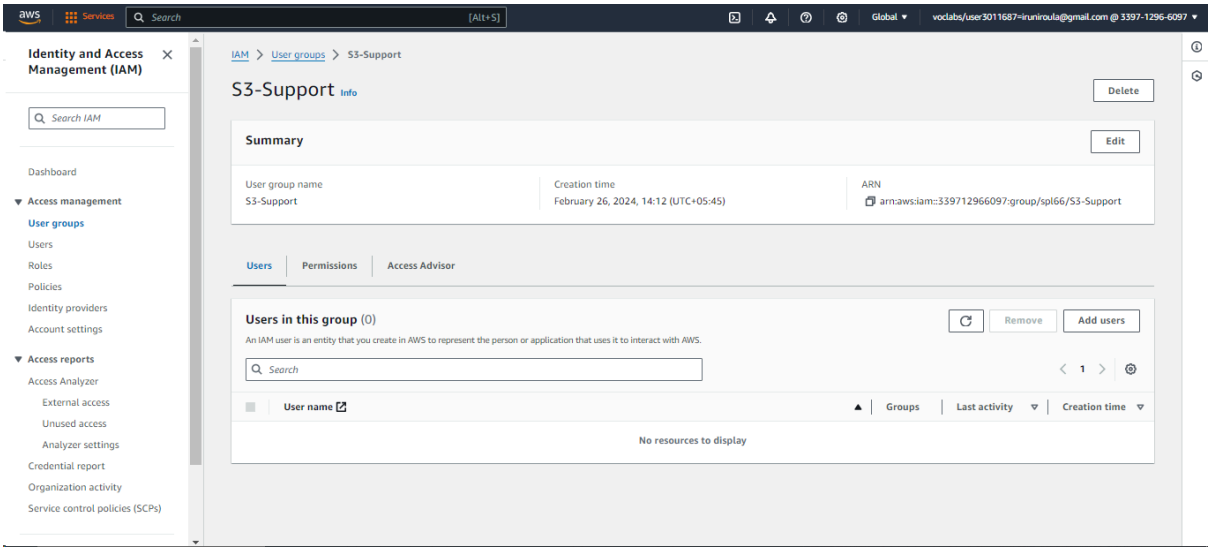


JSON Written Policy

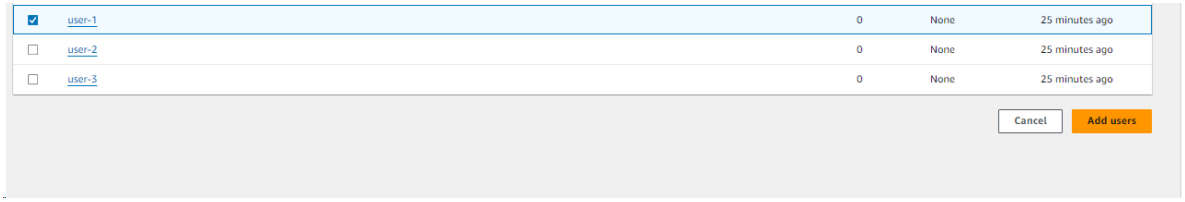
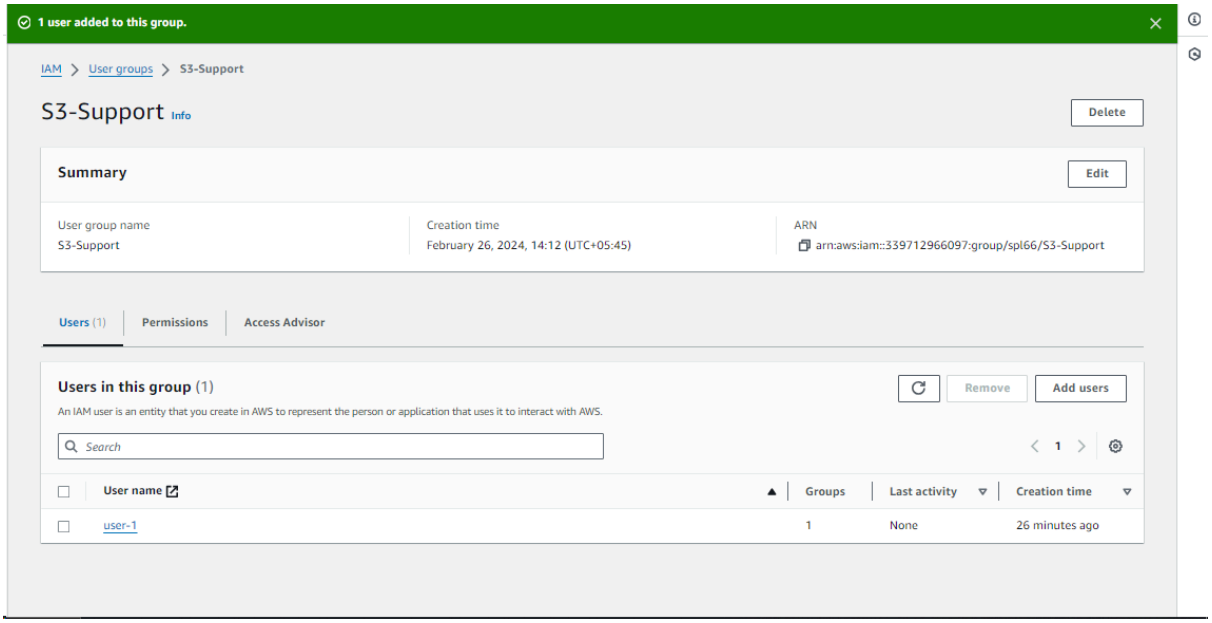
The following users need to be set to respective user groups

User	In Group	Permissions
user-1	S3-Support	Read-Only access to Amazon S3
user-2	EC2-Support	Read-Only access to Amazon EC2
user-3	EC2-Admin	View, Start and Stop Amazon EC2 instances

Adding users to the user group



Selecting user 1



User added to the user group