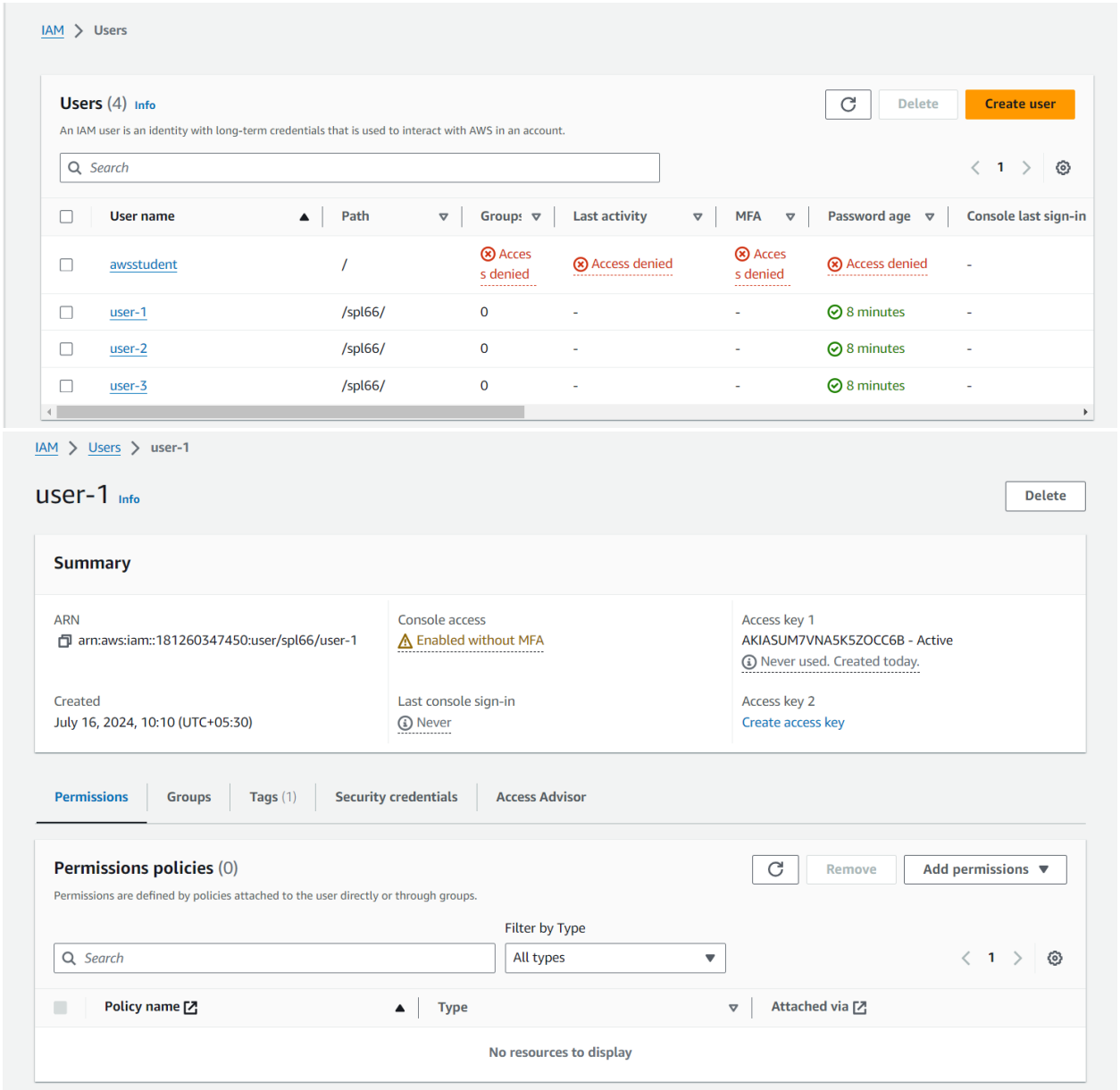
Cloud Computing – LAB-4

Ismail Basheer

2348521

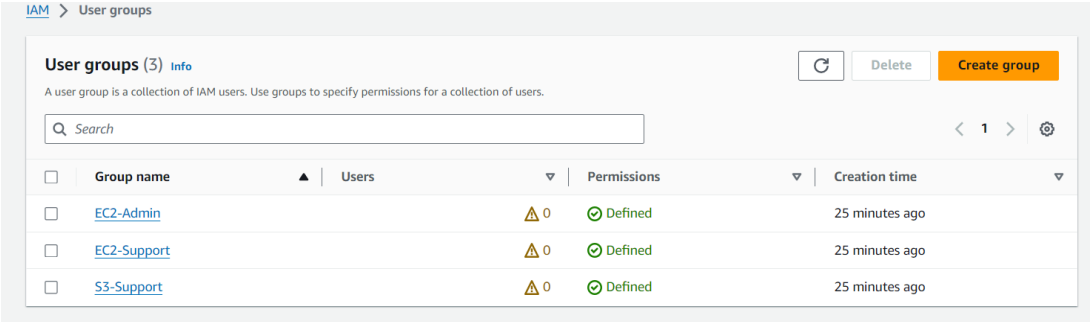
1. Exploring pre-created IAM Users and Groups

Viewing pre-created users

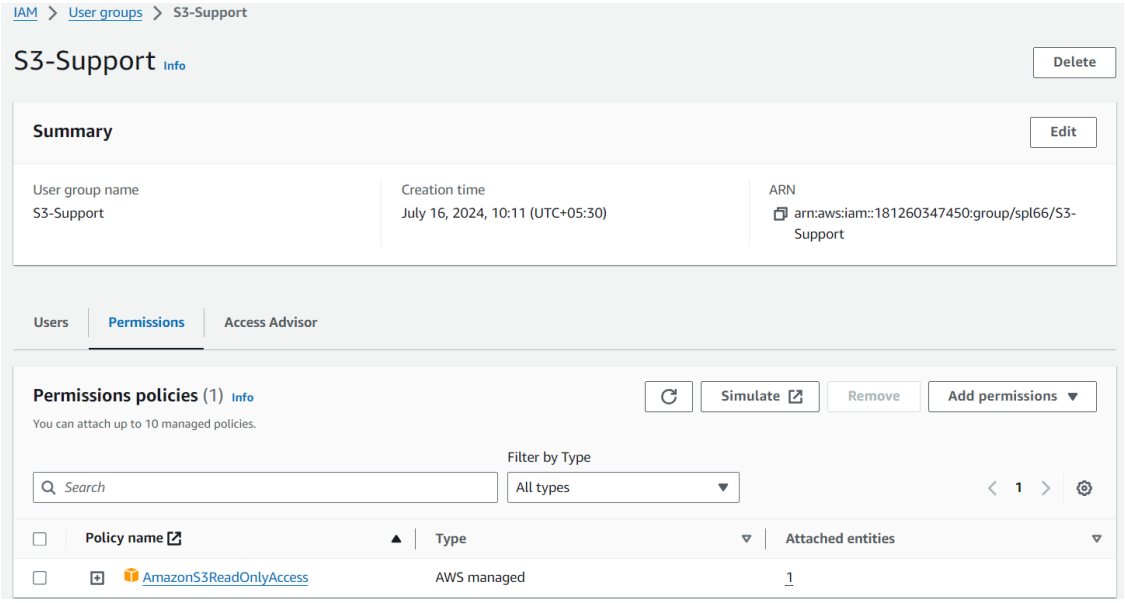


Inspecting IAM policies as applied to the pre-created groups

a) The pre-defined security groups



b) A policy defines what actions are allowed or denied for specific AWS resources. The S3-Support group has the **AmazonS3ReadOnlyAccess** policy attached.

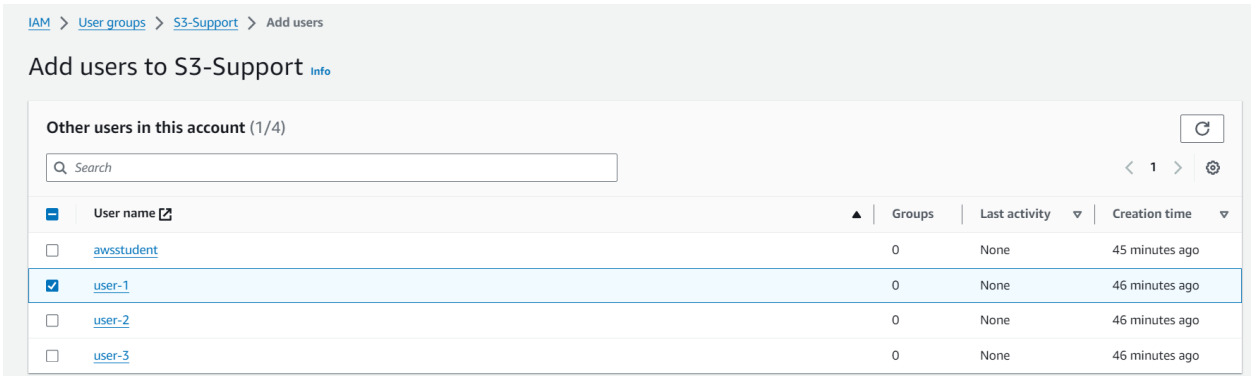


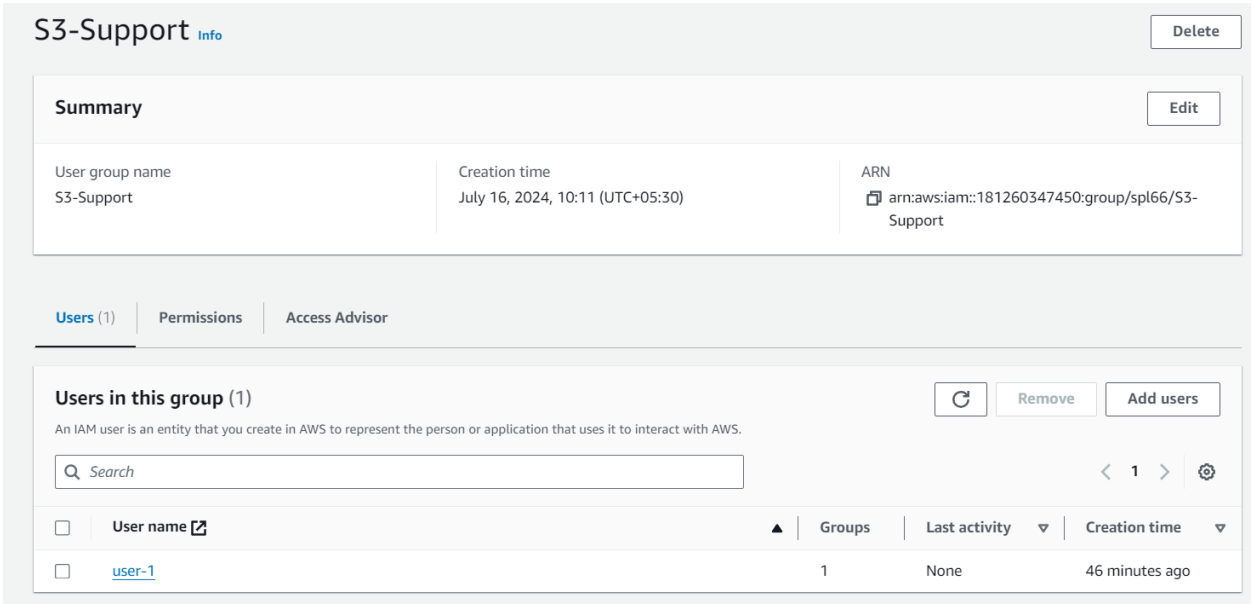
2. **Following a real-world scenario, adding users to groups with specific capabilities enabled.**

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

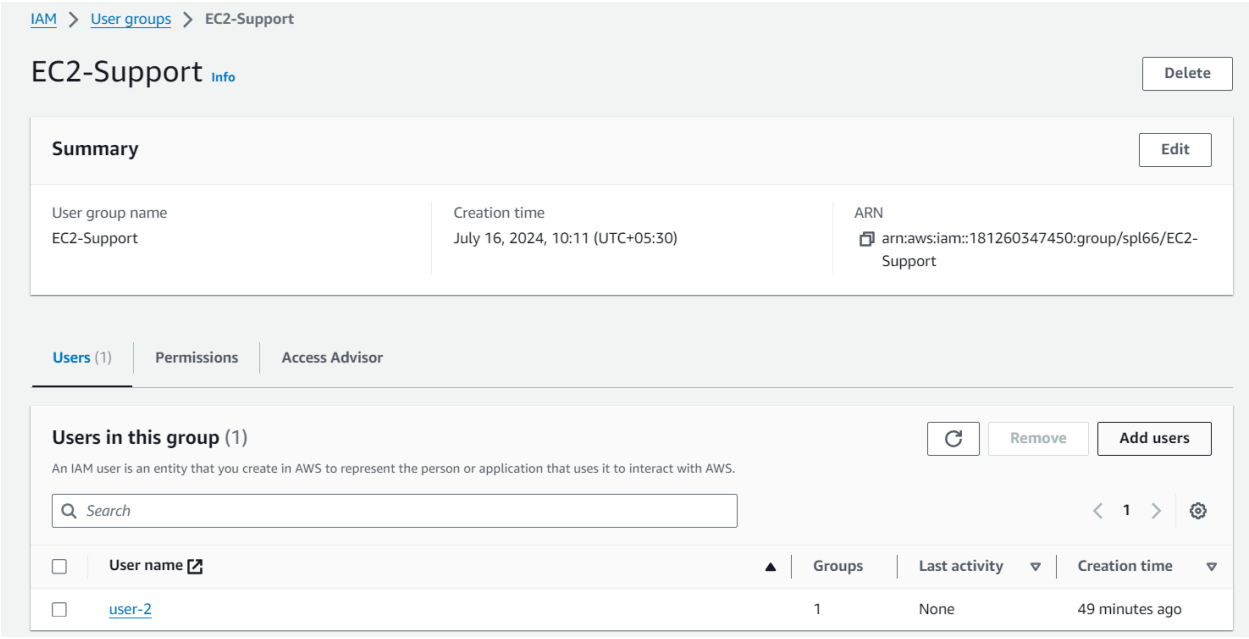
Real-world scenario

a) Add user1 to the S3 support group

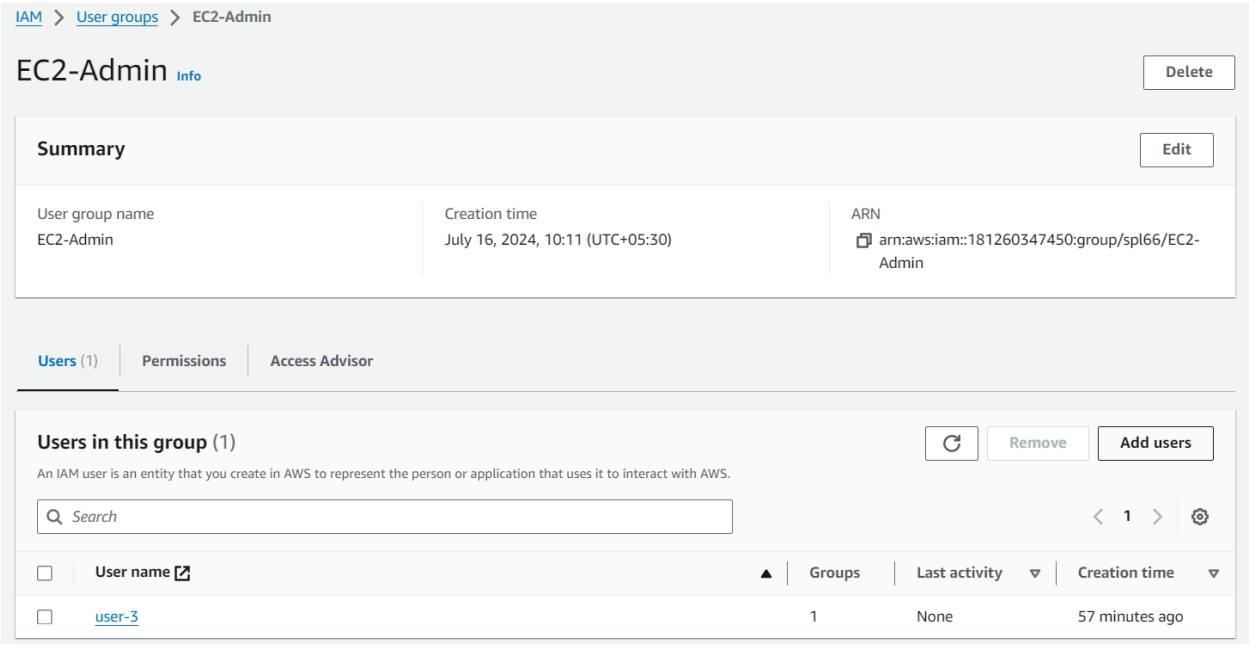




b) Add user 2 to the EC2 support group

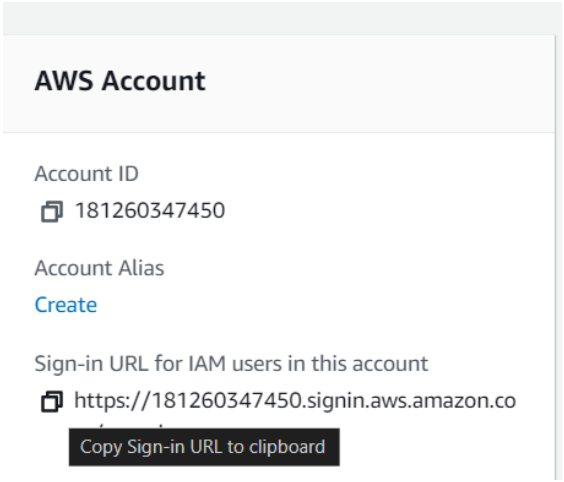


c) Add user 3 to the EC2 admin group

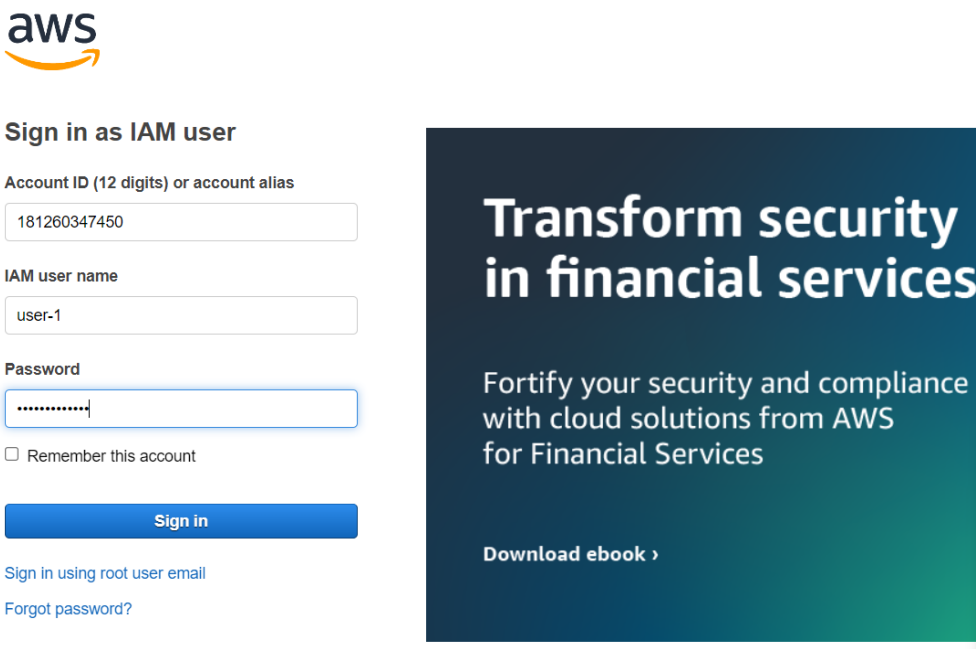


4. Locating and using the **IAM sign-in URL**

a) Copy Sign-in URL from the dashboard

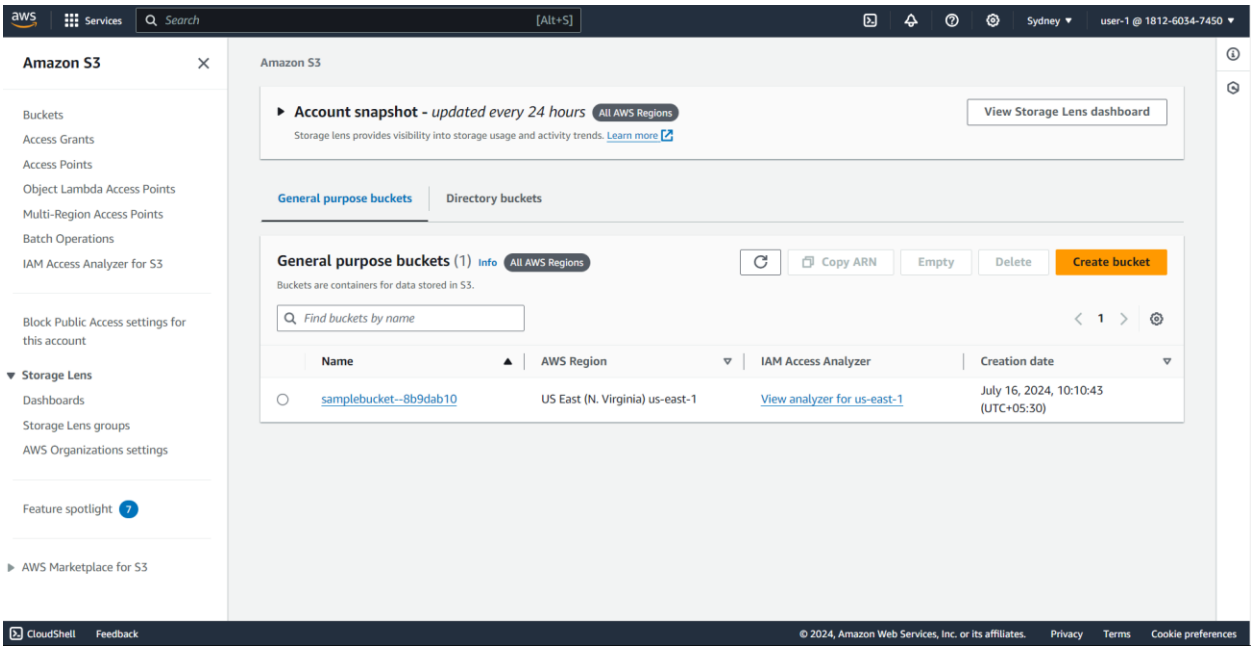


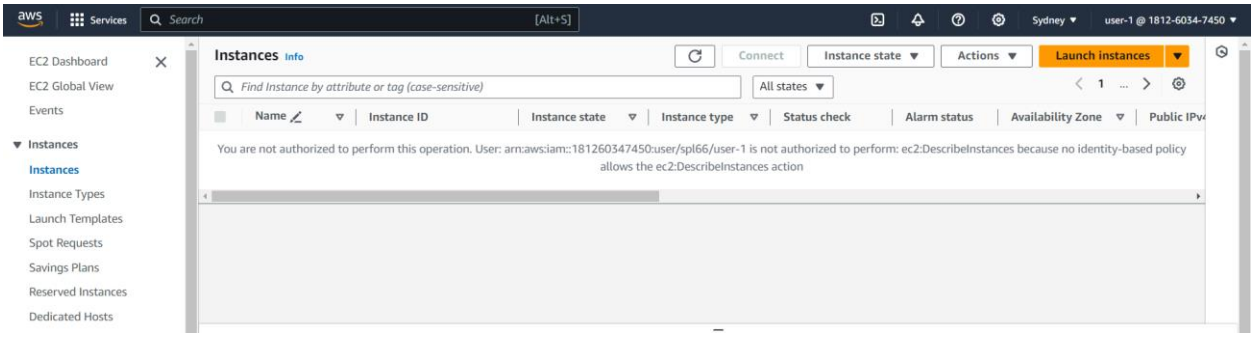
b) Opening the link in an incognito window and logging in as **user-1**



5. Experimenting with the effects of policies on service access

a) **User-1** has been hired to the S3 support group and hence has access to the S3 buckets but **can't access the EC2 instances** as **user-2** has been hired as EC2 support.





b) Logging in as user-2 gives us access to the instance as the user has been hired as the EC2 support group