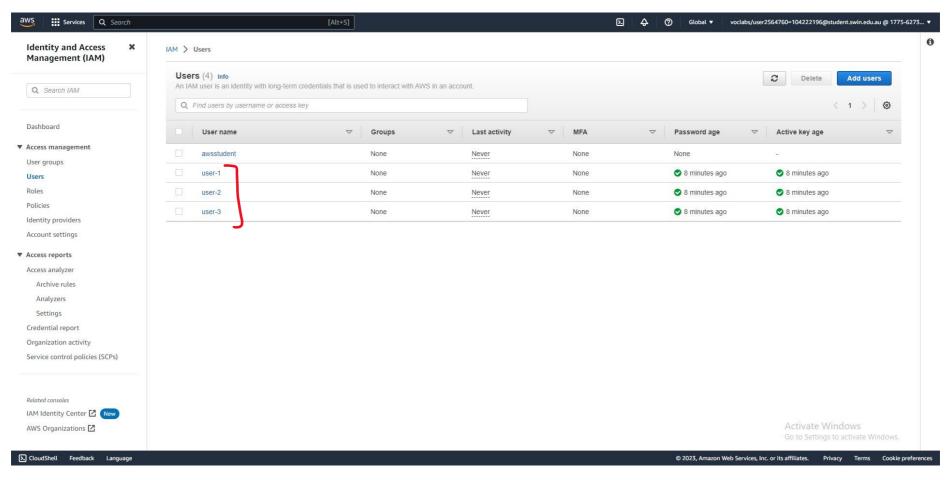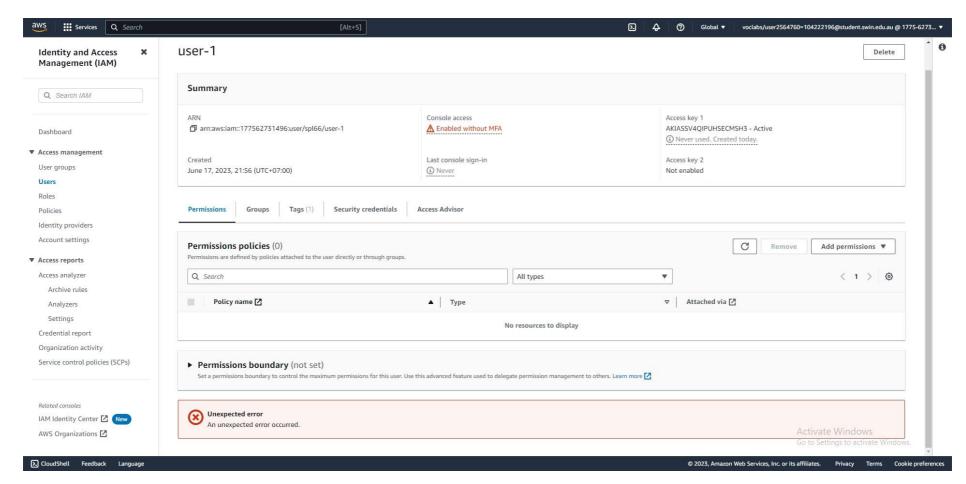Ta Quang Tung – 104222196

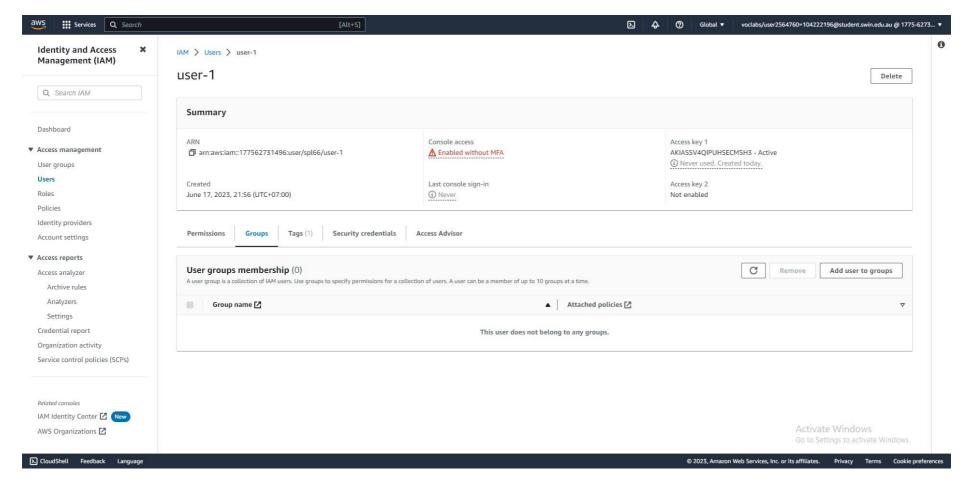COS20019 – Cloud Computing Architecture - Wk6: ACF Lab 1: Intro to AWS IAM
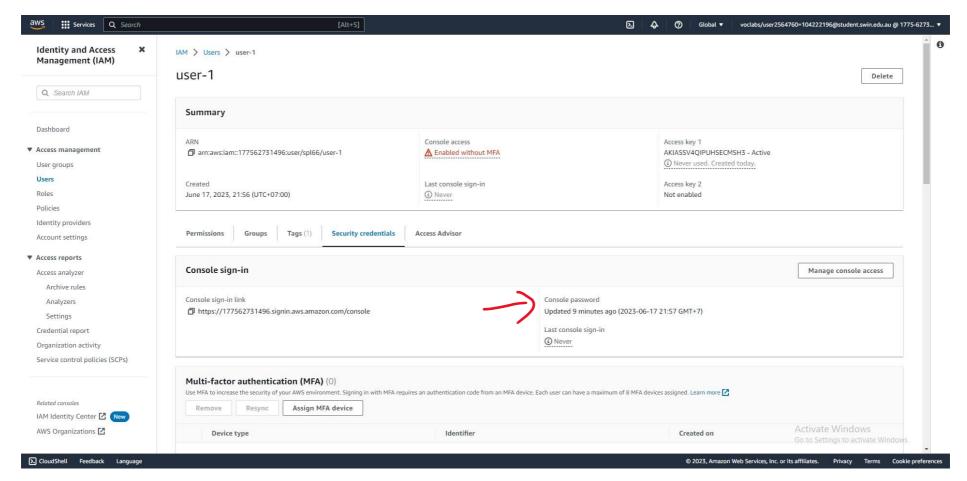
Task 1 - Explore the Users and Groups

Three IAM users (user-1 to user-3) have been created by the lab.
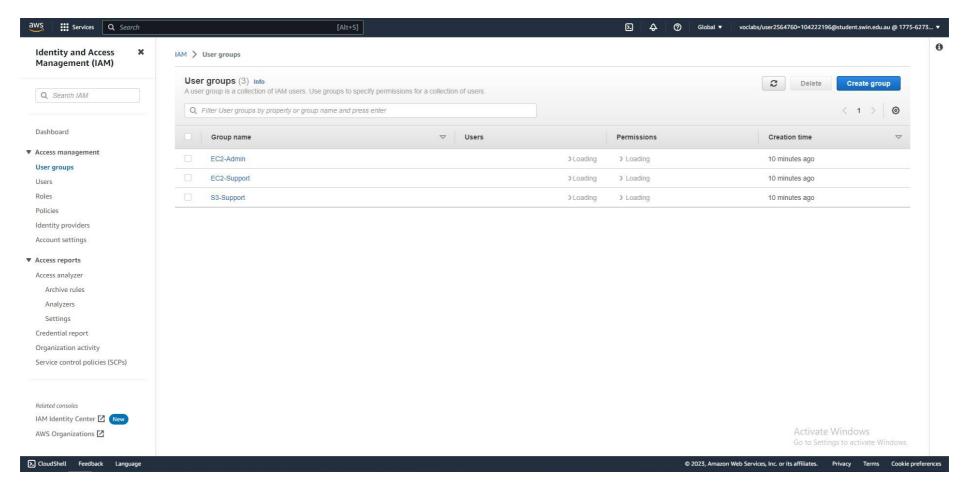
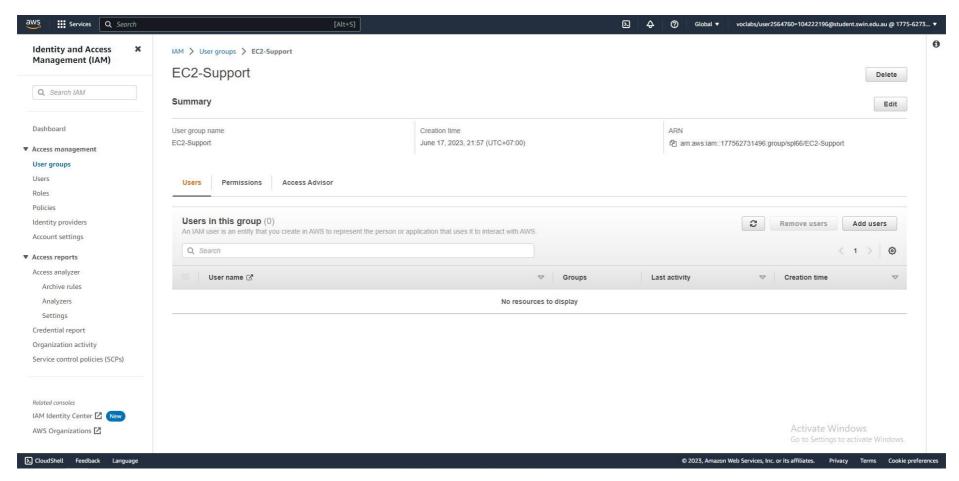The summary page for user-1. There are no permissions.

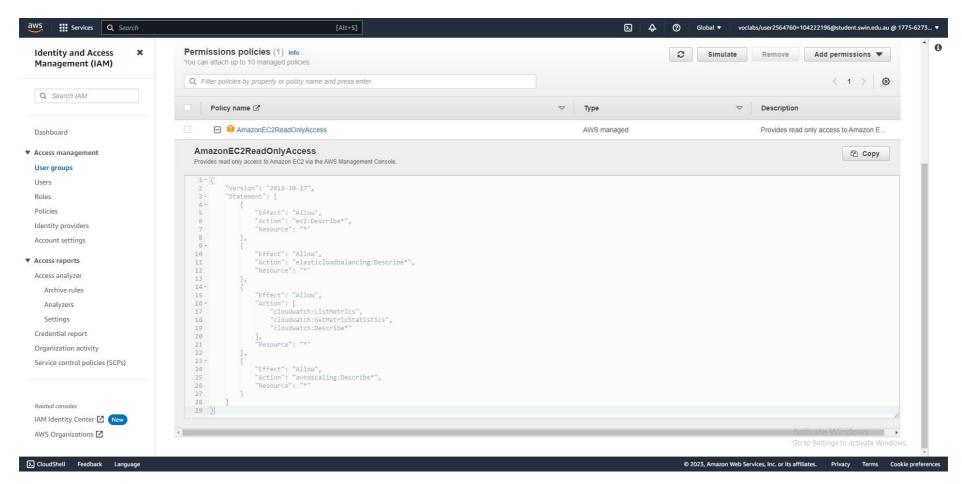The Groups tab for user-1, which is also empty.

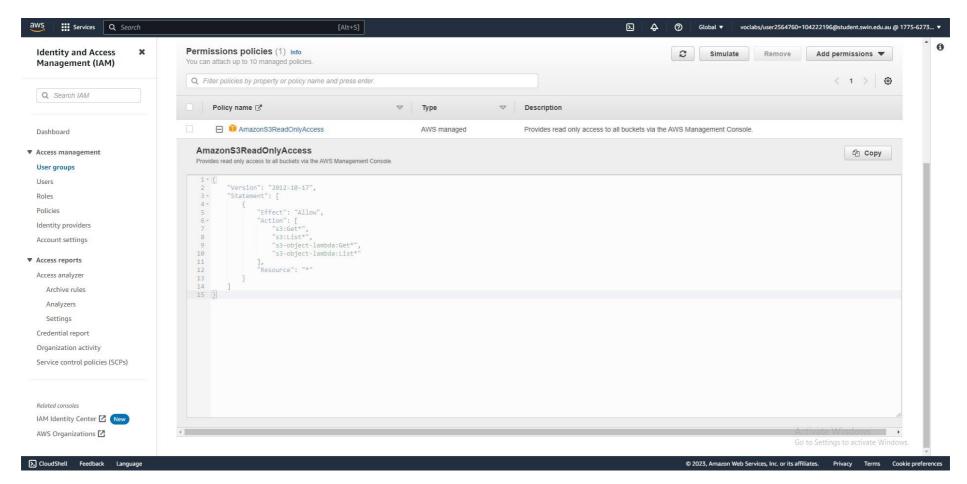In the security credentials tab, user-1 is assigned a console password.

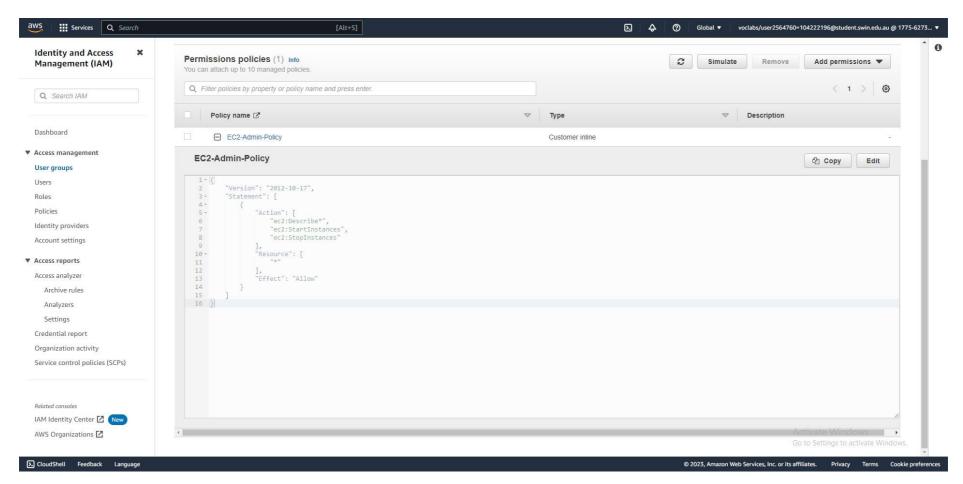The User groups page shows three groups created by the lab.

The summary page for EC2-Support group.

The Permissions tab for EC2-Support shows a managed policy named AmazonEC2ReadOnlyAccess.
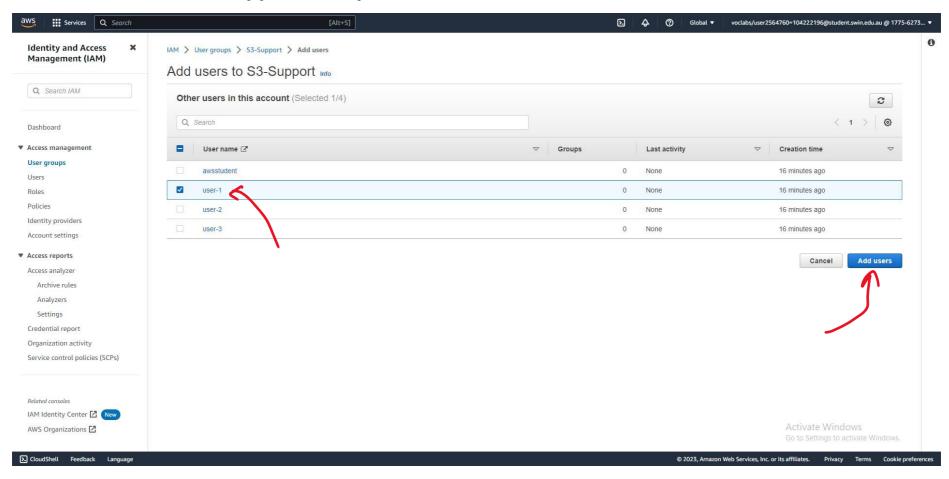
Identity and Access Management (IAM) ✕

Q Search IAM

Dashboard

▼ **Access management**
  User groups
  Users
  Roles
  Policies
  Identity providers
  Account settings

▼ **Access reports**
  Access analyzer
    Archive rules
    Analyzers
    Settings
  Credential report
  Organization activity
  Service control policies (SCPs)

Related consoles
IAM Identity Center ↗ New
AWS Organizations ↗

Permissions policies (1) Info
You can attach up to 10 managed policies.

[Simulate] [Remove] [Add permissions ▼]

Q Filter policies by property or policy name and press enter.

< 1 > ⚙

☐	Policy name ↗	Type	Description
☐	⊟ 📦 AmazonS3ReadOnlyAccess	AWS managed	Provides read only access to all buckets via the AWS Management Console.

AmazonS3ReadOnlyAccess
Provides read only access to all buckets via the AWS Management Console.

[📋 Copy]

```
1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Effect": "Allow",
6              "Action": [
7                  "s3:Get*",
8                  "s3:List*",
9                  "s3-object-lambda:Get*",
10                 "s3-object-lambda:List*"
11             ],
12             "Resource": "*"
13         }
14     ]
15 }
```

Activate Windows
Go to Settings to activate Windows.

S3-Support group has a managed policy named AmazonS3ReadOnlyAccess.

Identity and Access Management (IAM) ✕

Search IAM

Dashboard

▼ Access management
   User groups
   Users
   Roles
   Policies
   Identity providers
   Account settings

▼ Access reports
   Access analyzer
     Archive rules
     Analyzers
     Settings
   Credential report
   Organization activity
   Service control policies (SCPs)

Related consoles

IAM Identity Center 🔗 **New**

AWS Organizations 🔗

Permissions policies (1)   Info
You can attach up to 10 managed policies.

Simulate   Remove   Add permissions ▼

Filter policies by property or policy name and press enter.

☐	Policy name 🔗	Type	Description
☐	⊟ EC2-Admin-Policy	Customer inline	-

EC2-Admin-Policy

Copy   Edit

```
1   {
2       "Version": "2012-10-17",
3       "Statement": [
4           {
5               "Action": [
6                   "ec2:Describe*",
7                   "ec2:StartInstances",
8                   "ec2:StopInstances"
9               ],
10              "Resource": [
11                  "*"
12              ],
13              "Effect": "Allow"
14          }
15      ]
16  }
```

Activate Windows
Go to Settings to activate Windows.

EC2-Admin has an inline policy named EC2-Admin-Policy.

Task 2 - Add Users to Groups

Add user-1 to the S3-Support Group

In the Users tab for S3-Support, select user-1 and click add users.

user-1 has been successfully added to S3-Support group.
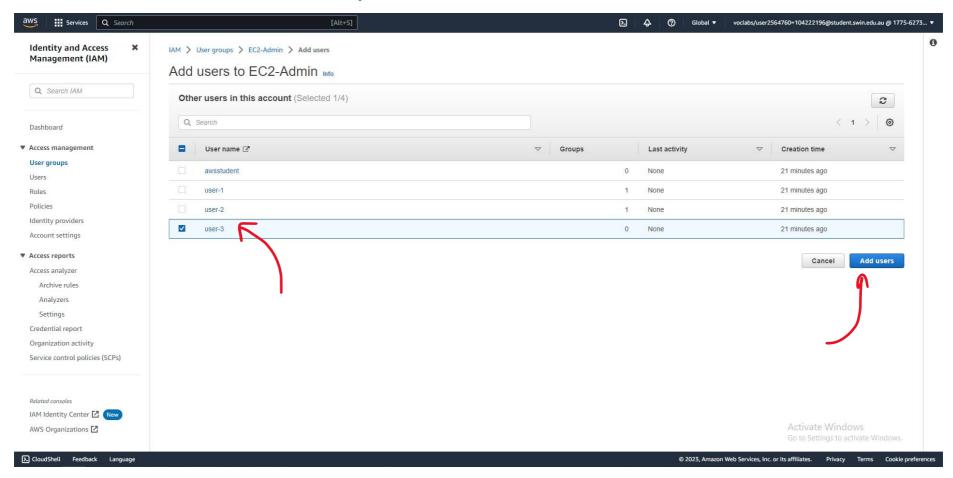
Add user-2 to the EC2-Support Group

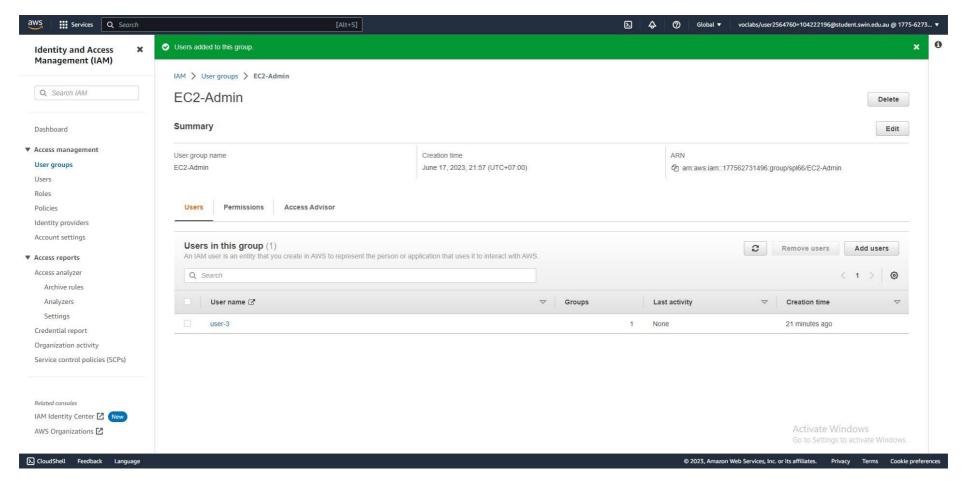In the Users tab for EC2-Support, select user-2 and click add users.

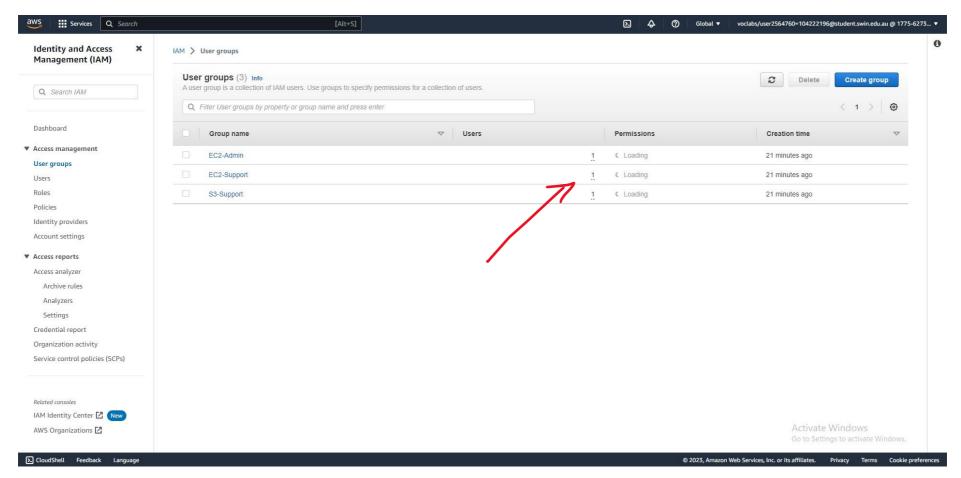user-2 has been successfully added to EC2-Support group.

Add user-3 to the EC2-Admin Group

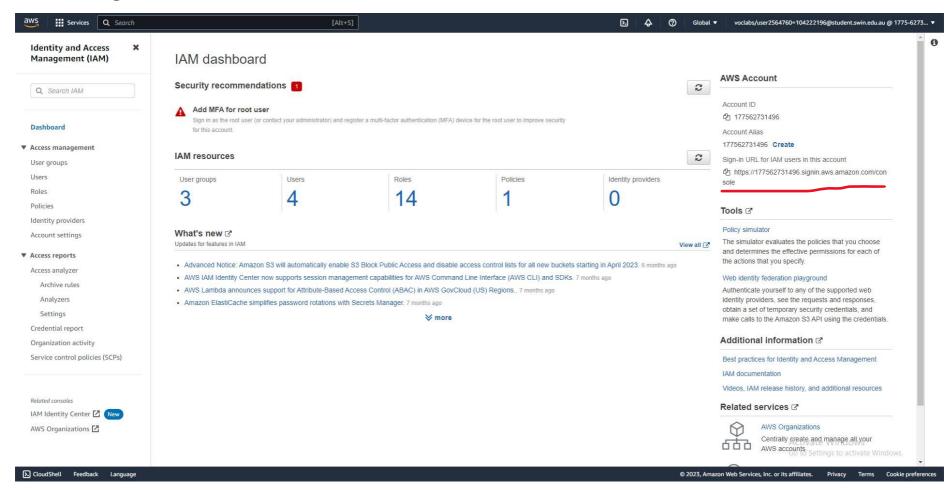In the Users tab for EC2-Admin, select user-3 and click add users.

user-3 has been successfully added to EC2-Admin group.

In the User groups panel, each group now has a user.

Task 3 - Sign-In and Test Users

In the IAM dashboard, copy and paste the sign-in URL for IAM users into an incognito tab.

Logging in as the user-1.

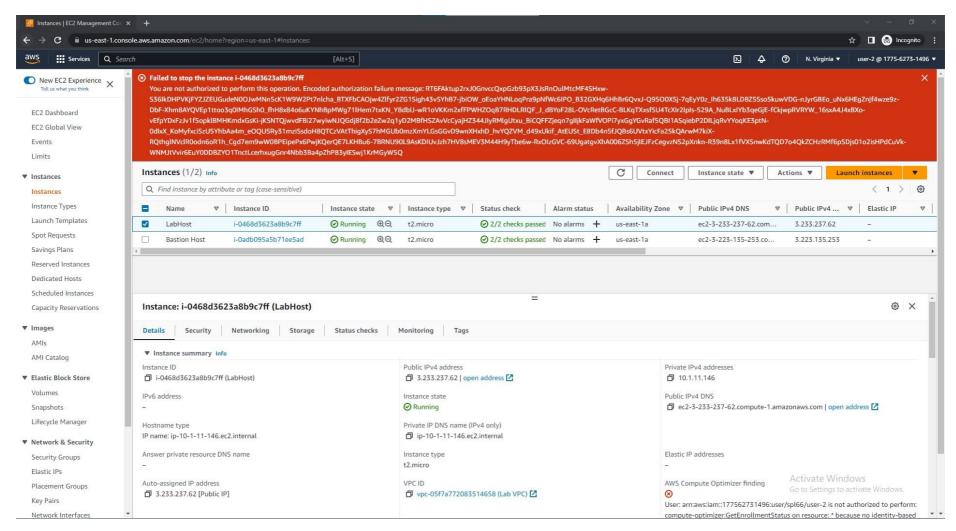user-1 can view the S3 bucket, which contains no content.

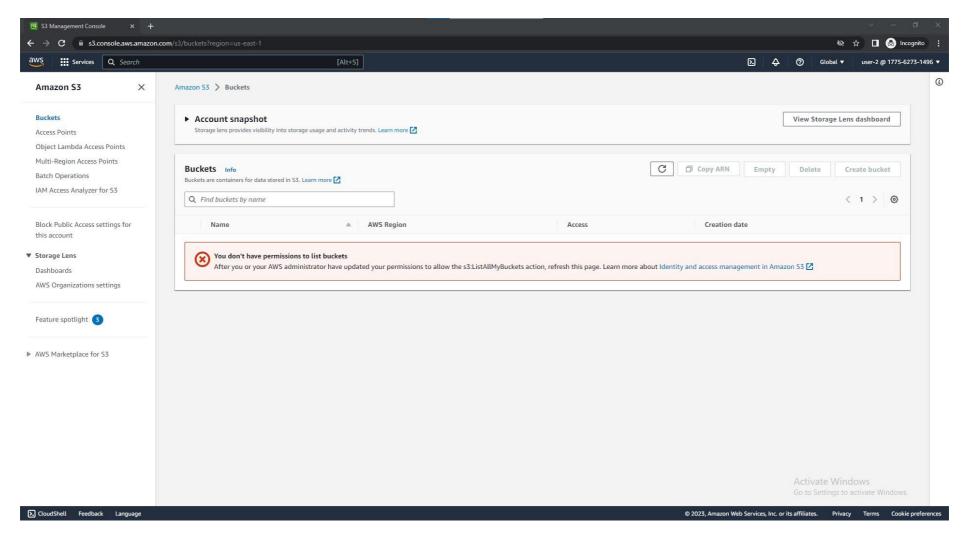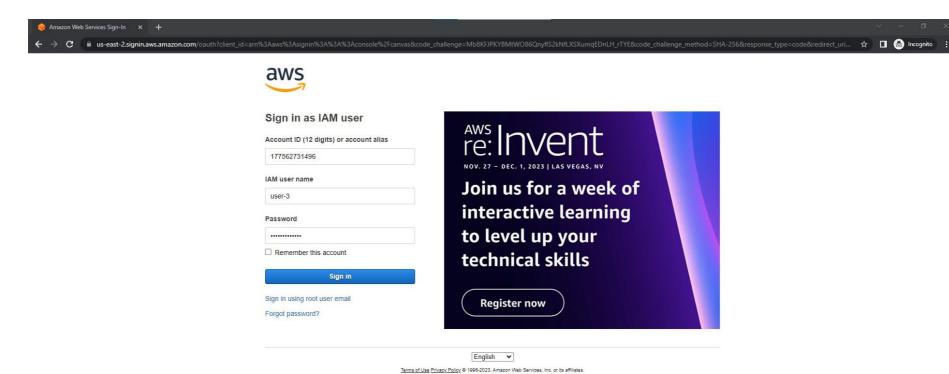user-1 cannot view the EC2 instances since they are not authorized.

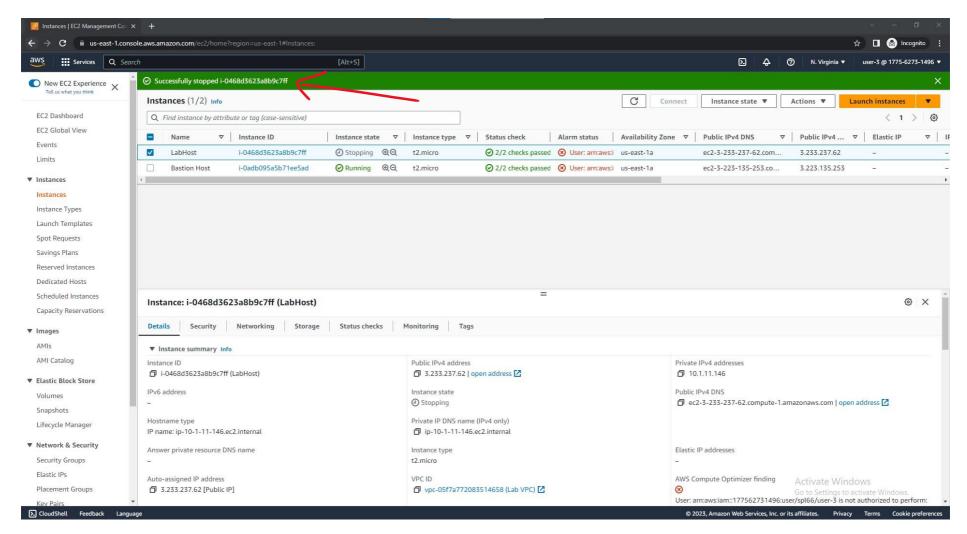After signing out, log in again as user-2.

user-2 is able to view the instances; however, they cannot stop them since they are not authorized.

user-2 does not have permission to view S3 buckets.

After signing out, log back in as user-3.

user-3 has permission to stop the EC2 instance.