

Date: 17/2/2023

Roll No: 20BCE204

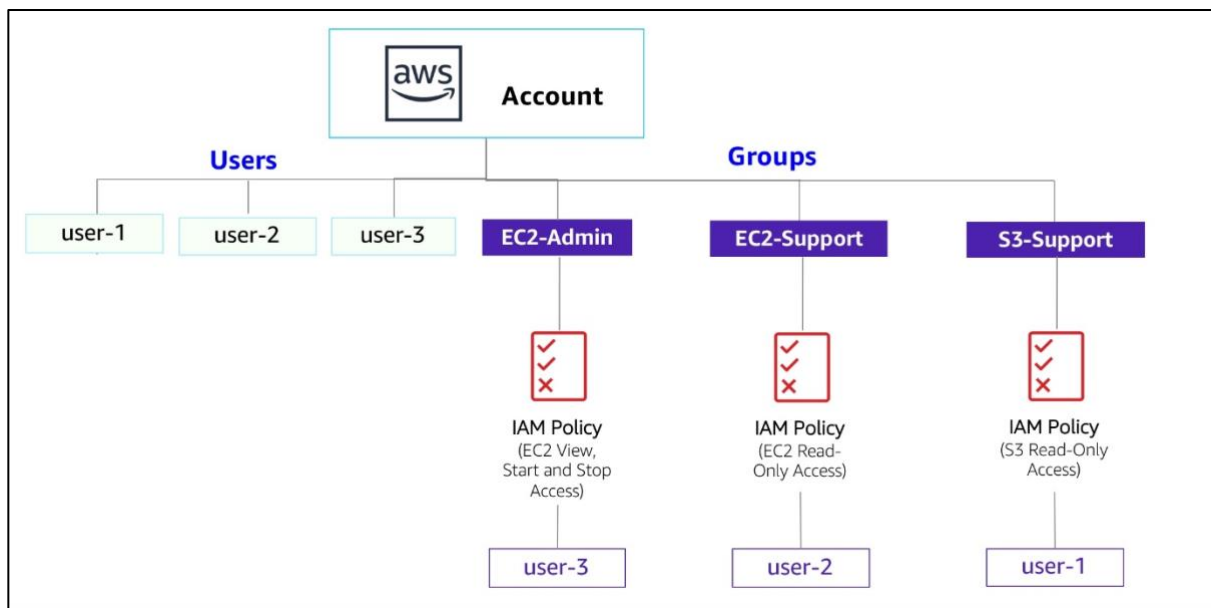
Subject: Cloud Computing

Practical: 2

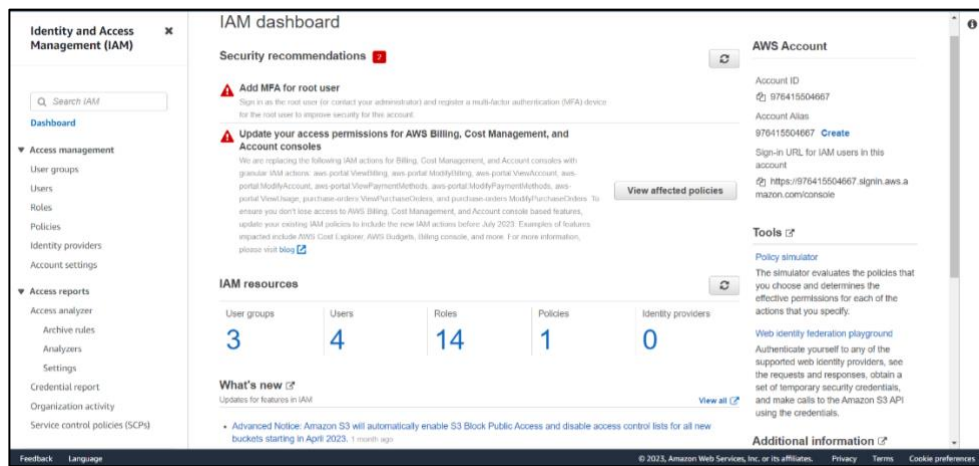
Aim: Working with an IaaS Cloud Computing: Using AWS (Amazon Web Services) to understating the following concept. Working with an IAM (Identity Access Management): AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

AWS Identity and Access Management (IAM) is a web service that enables Amazon Web Services (AWS) customers to manage users and user permissions in AWS. With IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access.

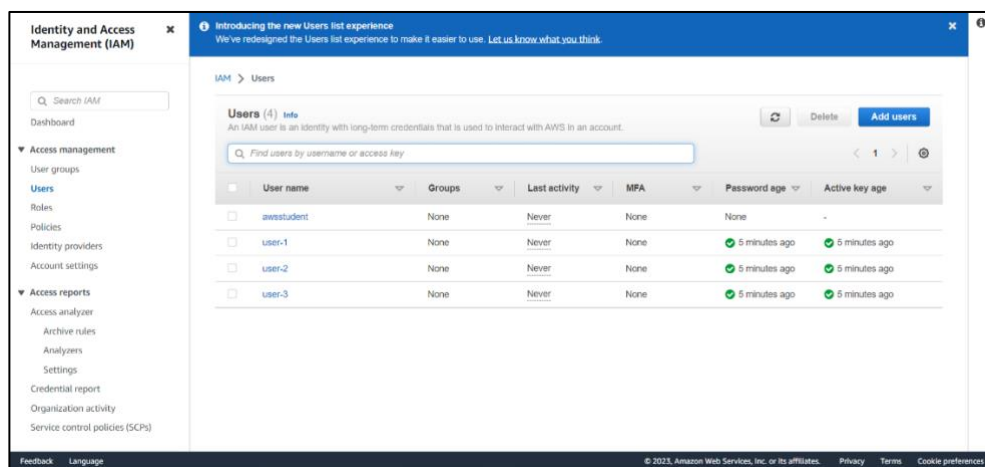
In this practical will be demostrating the below image in AWS IAM console. In this image we can see , we have 3 user and 3 user groups. The User Group are EC2-Admin, EC2-support and S3(simple Storage Service)-support. We will assign the role and responsibility to this user by assign them to this user group.



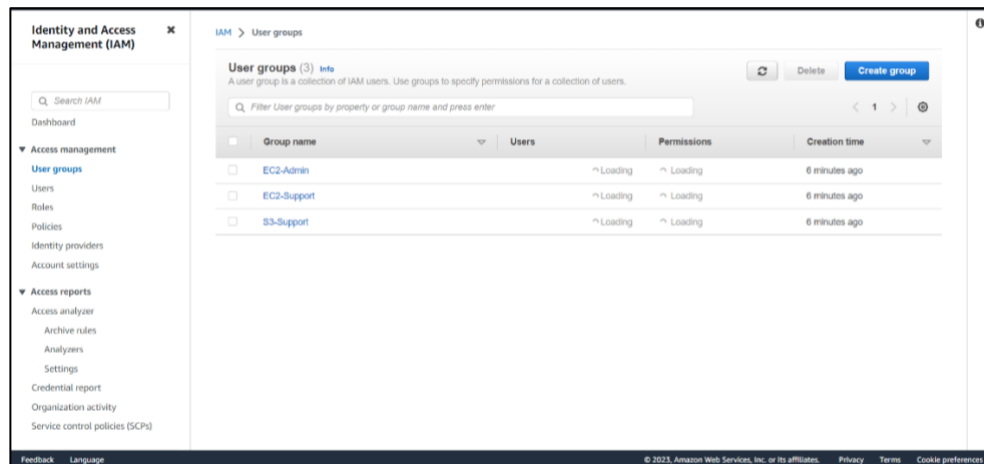
- ⇒ Now lets start the Lab, by access the IAM console.
- ⇒ Below we can see the dashbord of IAM console. The sign in url for different user is shown on right side and other services of IAM console is shown in left navigation panel.



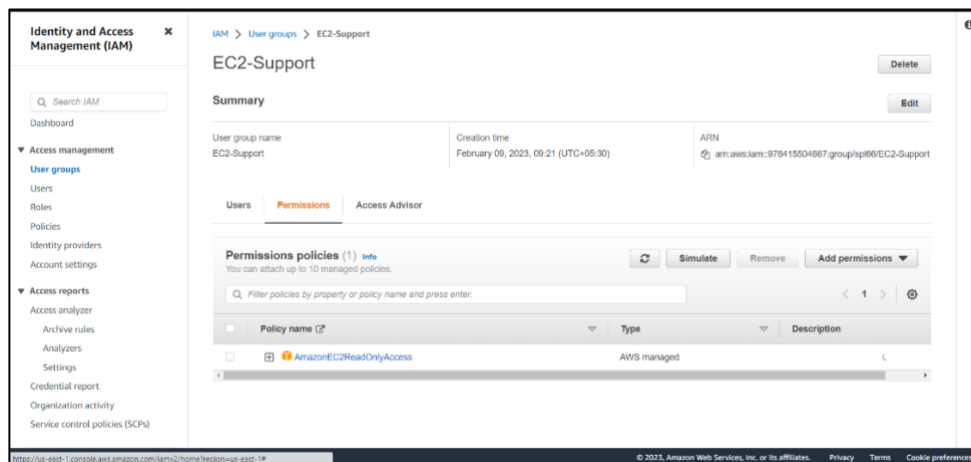
⇒ On clicking the **Users**, we will be able to see all the users and other information about the user. We can also see which group is/are assign to a particular user.



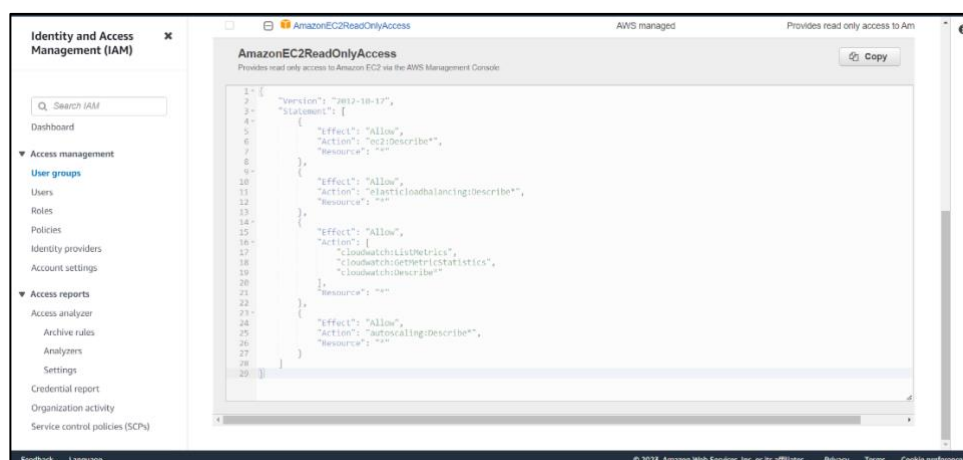
⇒ On clicking **User Groups**, we will be able to see all the group and other information about that group like number users in that group.



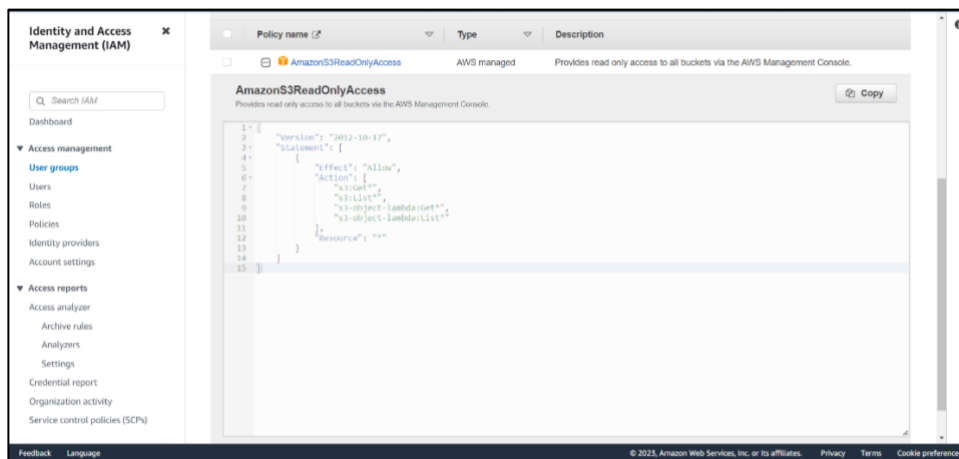
⇒ When we open the **EC2-Support**, we will be able to see the policy name under permission tab(AmazonEC2ReadOnlyAccess)



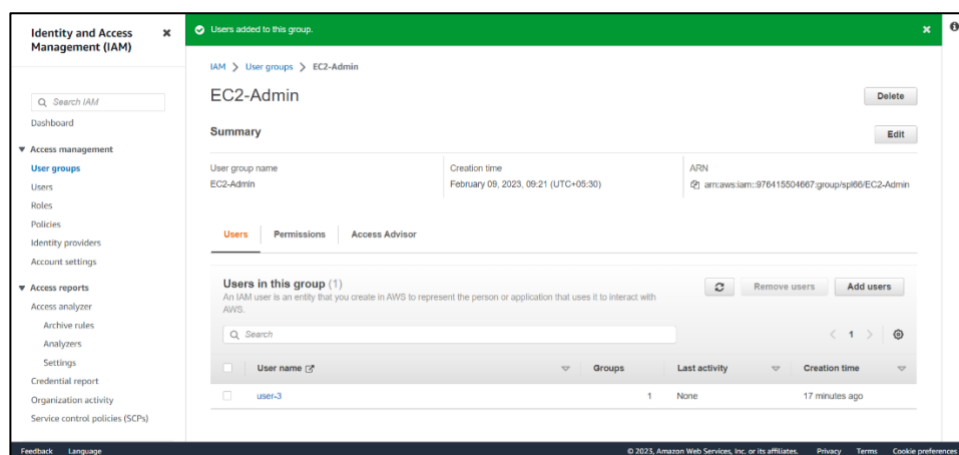
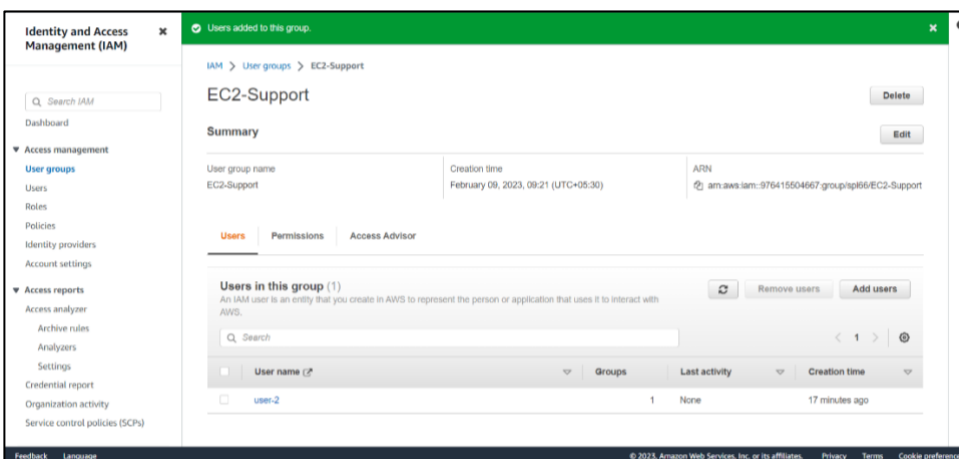
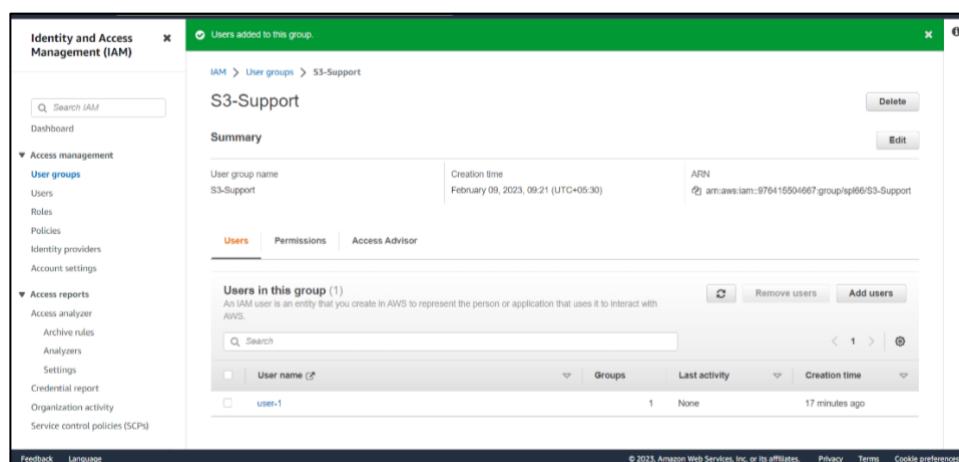
⇒ On clicking the **AmazonEC2ReadOnlyAccess** policy we will be able to see Policy in JSON format



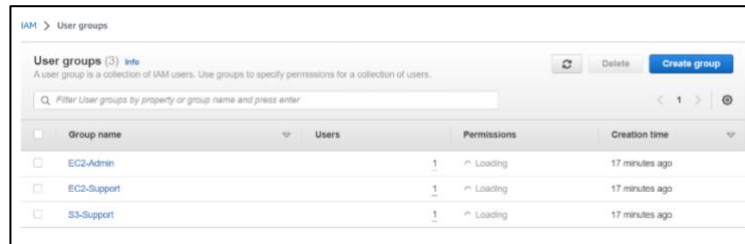
⇒ In the same way we can see the policy For S3-Support named as AmazonS3ReadOnlyAccess inside the permission tab of S3-Support.



⇒ Now we will assign the user a User group. We can do this by going inside user group and click on add user inside the users tab. Below shown how we have added user-1 to S3-Support, user-2 to EC2-Support and user-3 to EC2-Admin



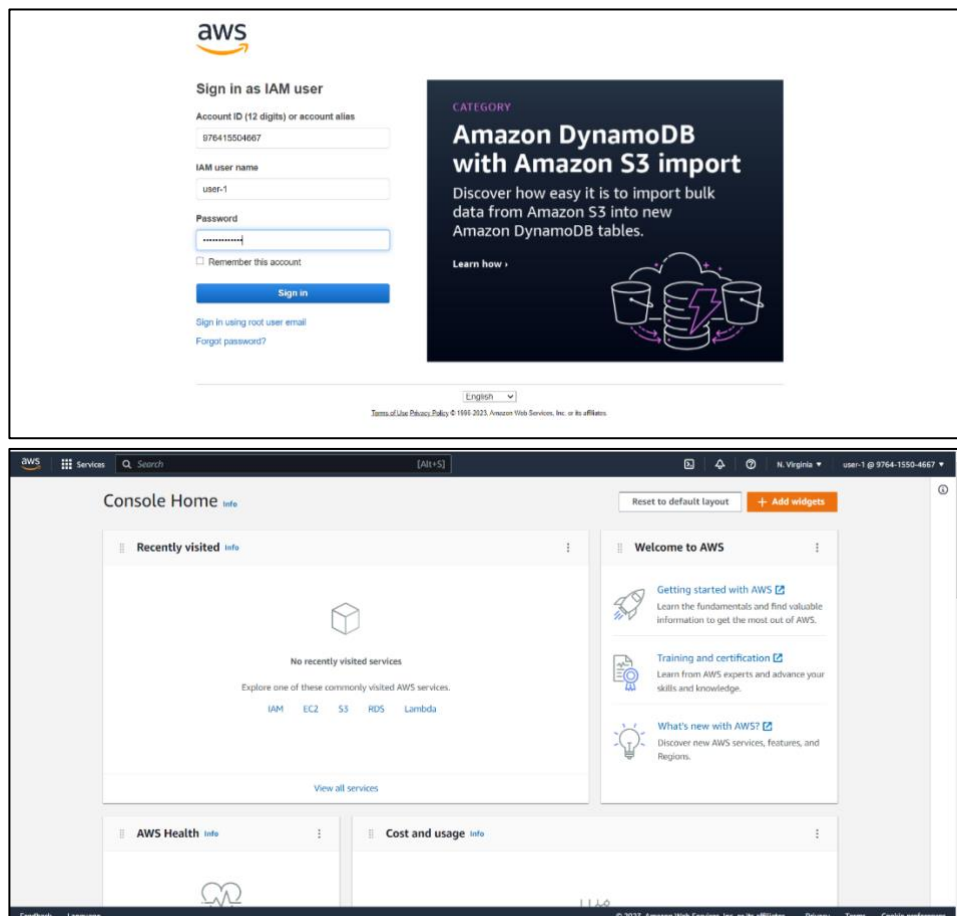
⇒ As we can see now that every group has 1 user. This user will follow the policy assign by the User Group



The screenshot shows the 'User groups' page in the AWS IAM console. It lists three user groups: EC2-Admin, EC2-Support, and S3-Support. Each group has 1 user assigned. The permissions for each group are listed as 'Loading'. The creation time for all groups is '17 minutes ago'.

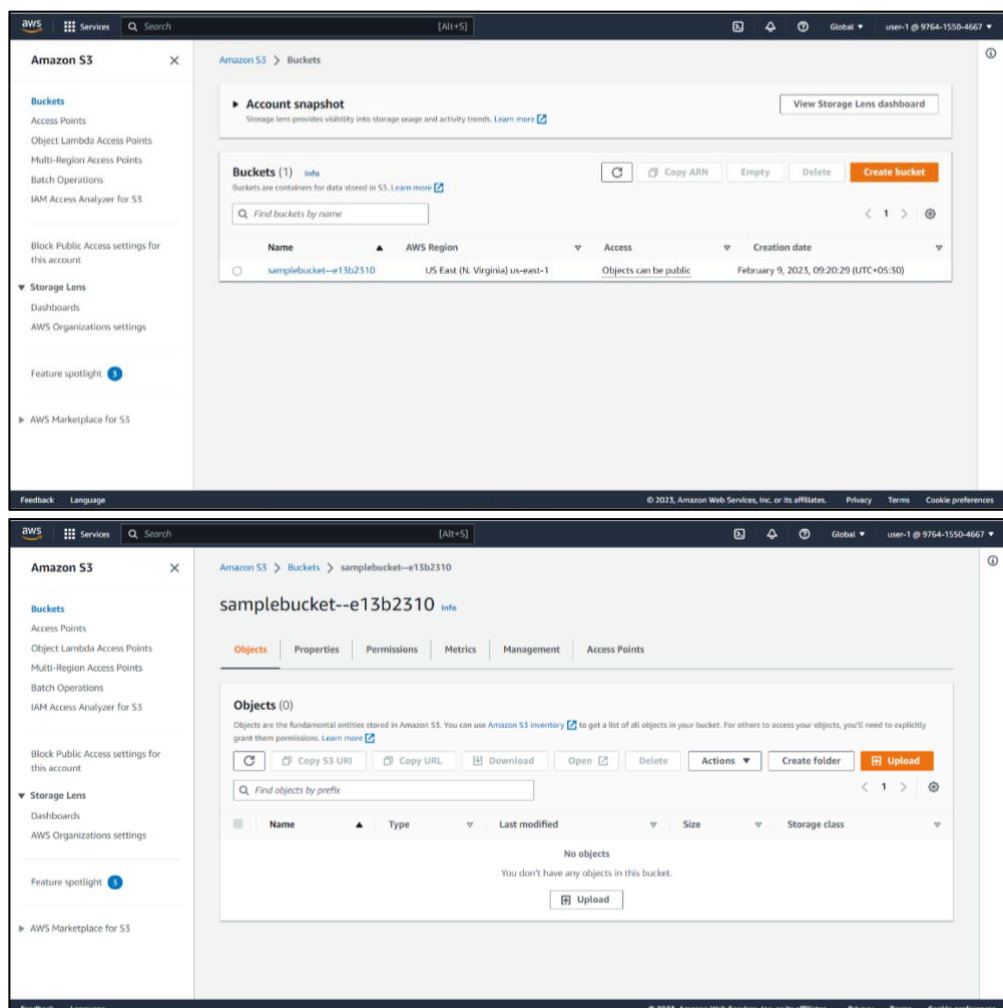
| Group name | Users | Permissions | Creation time |
|-------------|-------|-------------|----------------|
| EC2-Admin | 1 | Loading | 17 minutes ago |
| EC2-Support | 1 | Loading | 17 minutes ago |
| S3-Support | 1 | Loading | 17 minutes ago |

⇒ Now let's sign in to user-1 by using the URL available on right side of the IAM dashboard. Now we can see the dashboard of user-1 below.

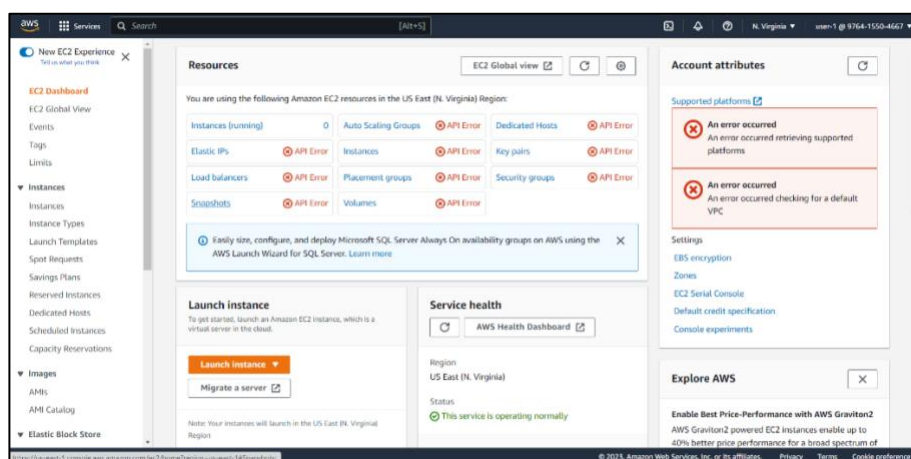


The top screenshot shows the 'Sign in as IAM user' page. It includes fields for Account ID (976415504667), IAM user name (user-1), and Password. A 'Sign in' button is present. To the right is a promotional banner for 'Amazon DynamoDB with Amazon S3 import'. Below the sign-in page is the 'Console Home' page, which displays 'Recently visited' services (IAM, EC2, S3, RDS, Lambda), 'AWS Health', and 'Cost and usage' sections.

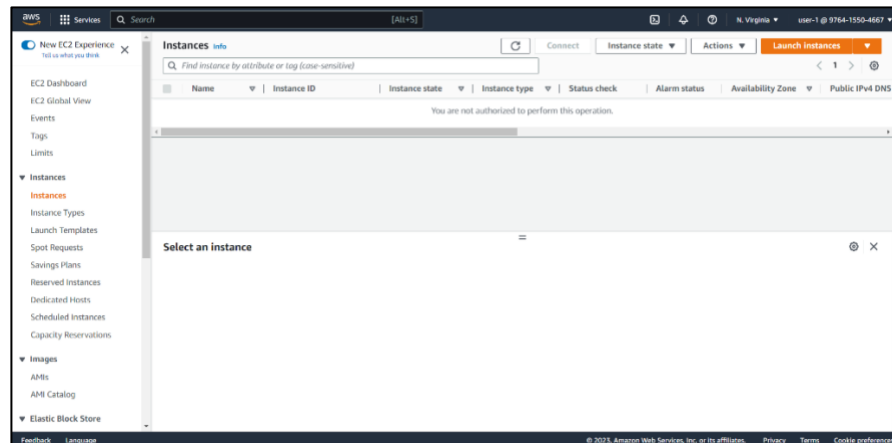
- ⇒ As we have assigned S3-Support to user, let's try to access the S3 Bucket.
- ⇒ We can click on S3 from the services available on top left corner of dashboard of user-1
- ⇒ As we can see a sample bucket. Opening this sample bucket we get option and rights to upload files.
- ⇒ User-1 is given rights of read and write of S3 bucket by S3-Support.



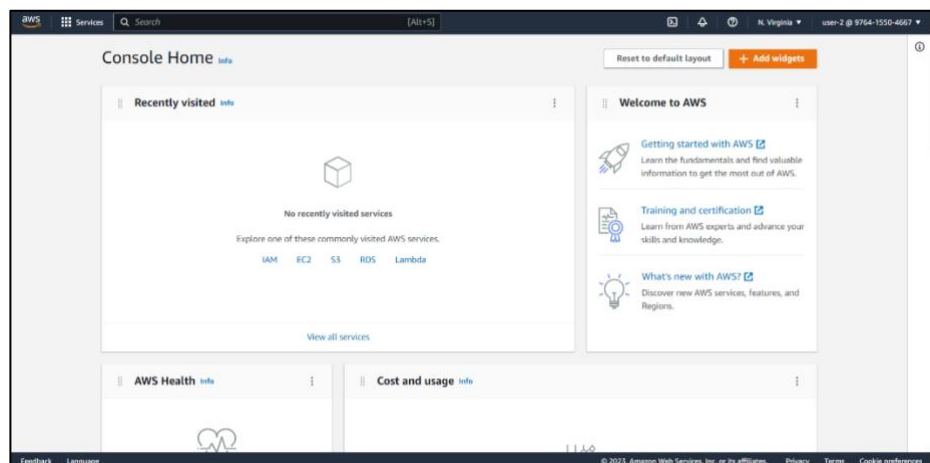
- ⇒ Now let's try to access the EC2
- ⇒ To access EC2, we will go to EC2 from the services button shown on top left corner.
- ⇒ Below is the EC2 Dashboard



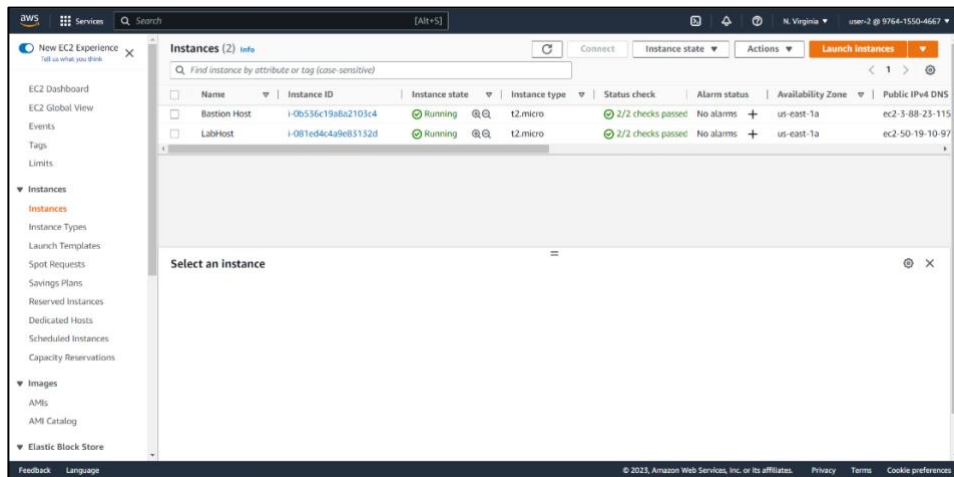
- ⇒ Now going to Instances inside the EC2-Dashboard. As we see there is no instance of EC2 listed.
- ⇒ This is because user-1 has the right only for S3 bucket from S3-support and not for EC2



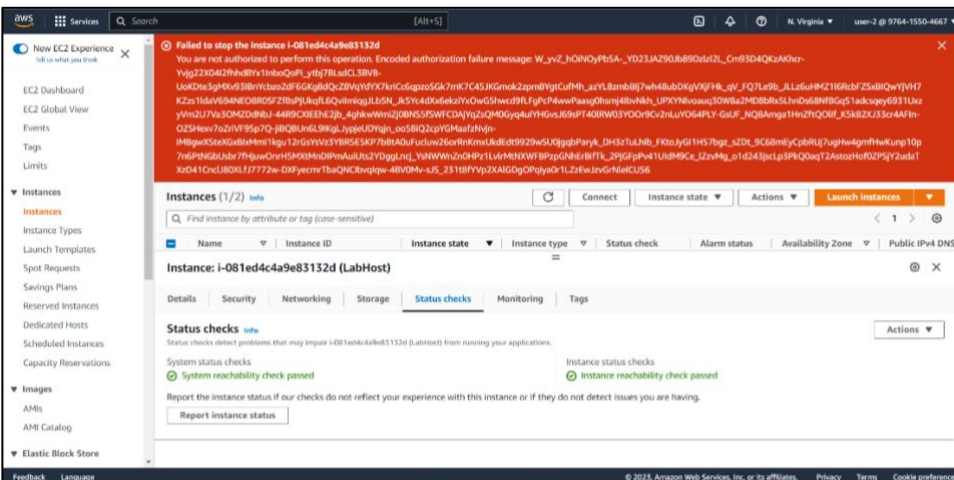
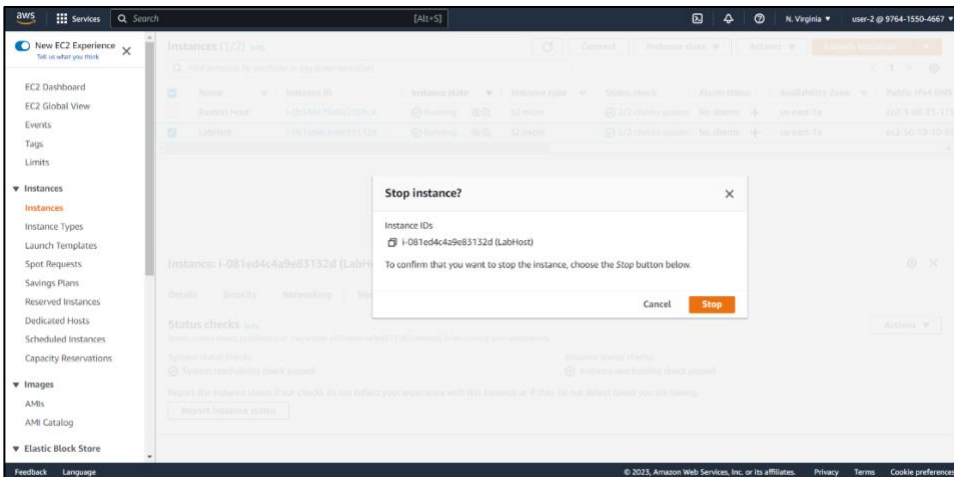
- ⇒ Now lets login into user-2, and see the EC2 rights given by EC2-support by opening the EC2 Dashboard



- ⇒ Now we see instance of EC2 in the Instances. We have listed two instance of EC2.
- ⇒ We can see the additional information about the instance like id of instance, instance status, instance type and etc.
- ⇒ To get more details of the instances we can open the instances by clicking on instance



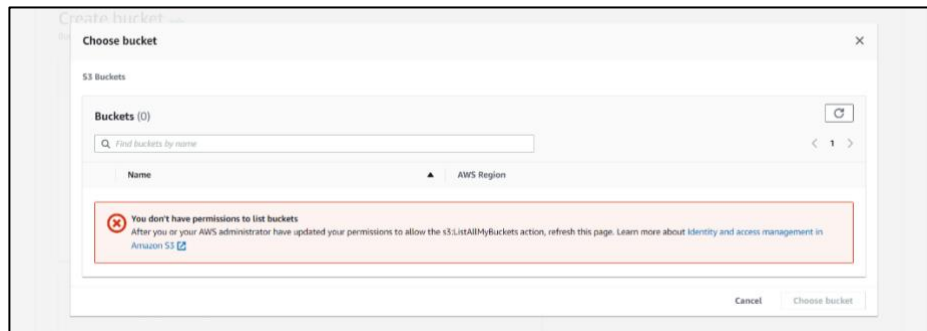
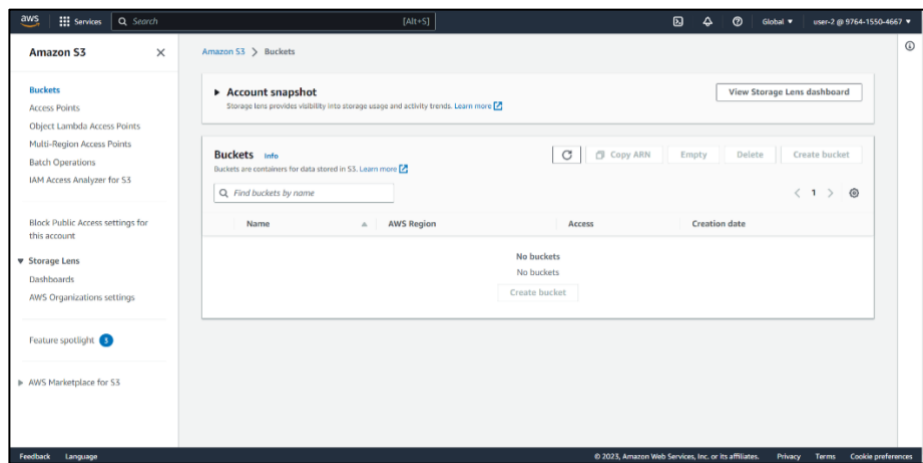
⇒ Now lets **stop** the LabHost instance by clicking on instance state on top right corner



⇒ On stopping we get an error of *“fail to stop the instance”*.

⇒ This is because user-2 has only right of reading the EC2 instance but not the write rights of modification rights

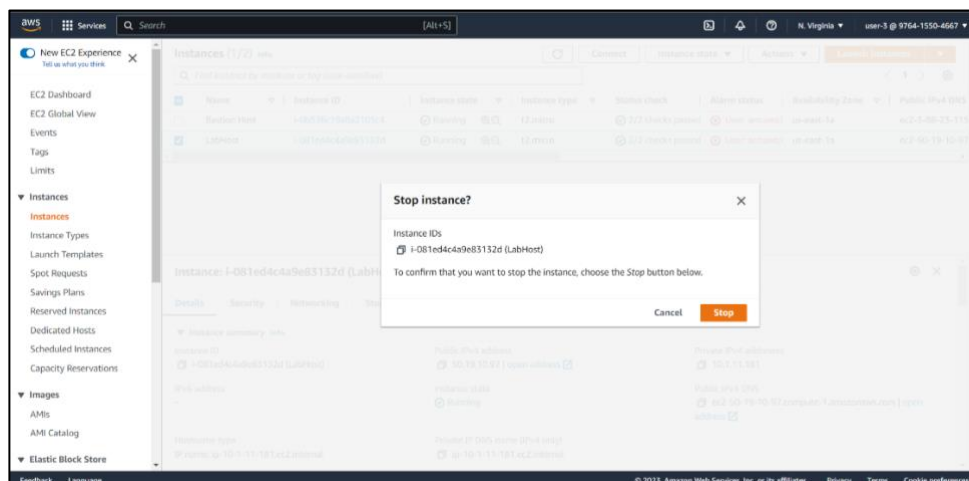
⇒ Now lets try to access S3 bucket from user-2



⇒ As we can see that we have got an error of “*you don’t have permissions to list bucket*”, this tells us that user-2 don’t have any rights of read or write of S3-bucket.

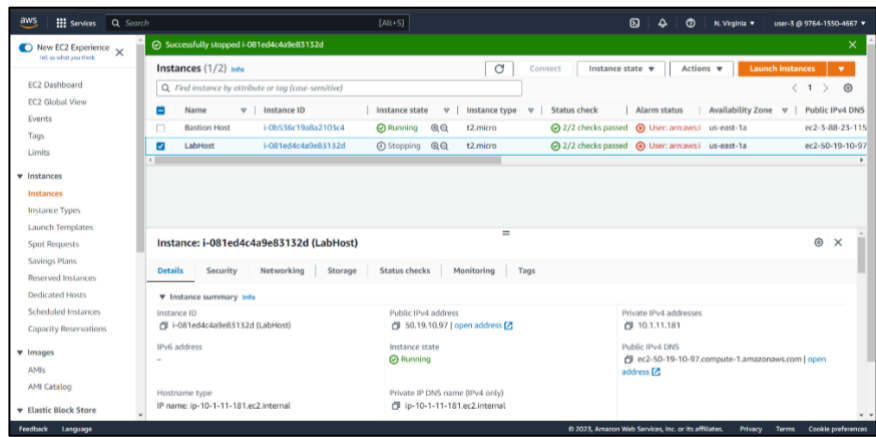
⇒ Now lets login in user-3 and see what all rights are given to user-3 by EC2-Admin.

⇒ We will try to stop the LabHost instance now from user-3 and see what happens.

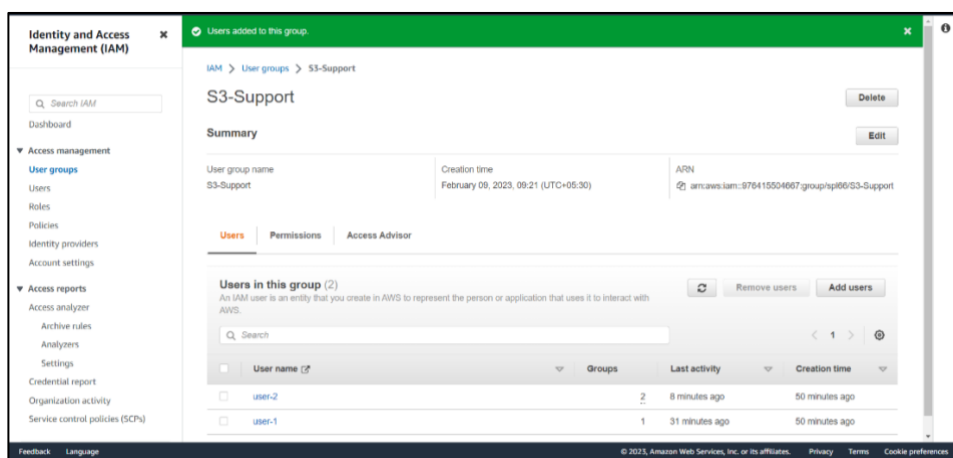


⇒ As we can see that we are able to stop the LabHost instance from user-3

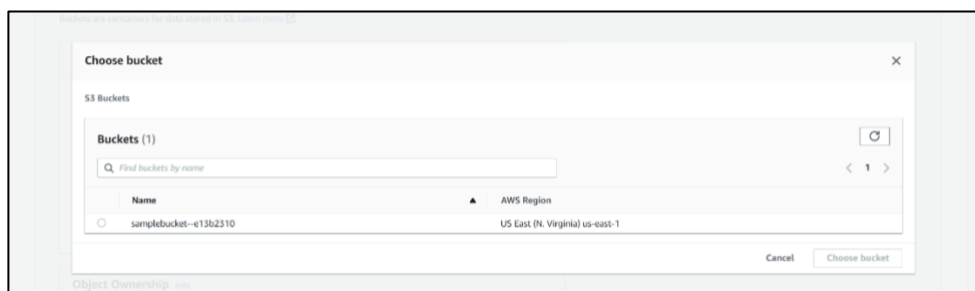
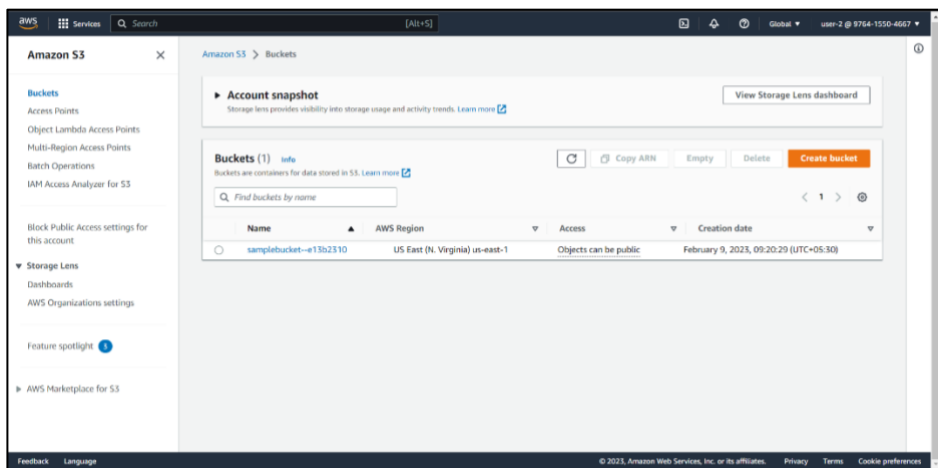
⇒ This is because EC2-Admin has given all rights of EC2 to user-3, that is why user-3 can read, write and modify the EC2 instance.



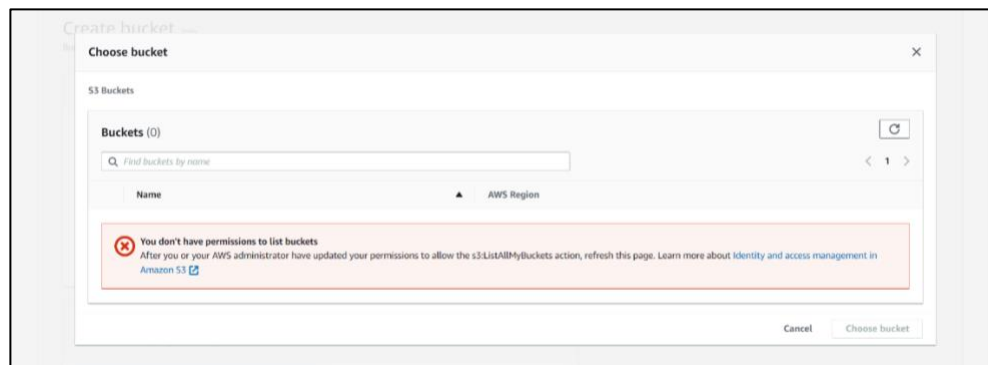
⇒ Now add user-2 to S3-support, to see whether we are able to list the S3 bucket inside the user-2, which we were not able to do before



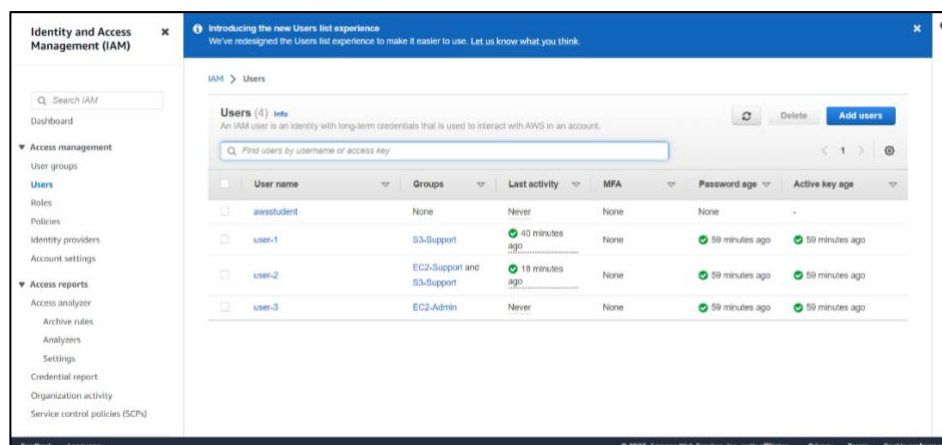
⇒ As we can see, we are able to list the bucket inside user-2.



- ⇒ Now if we try to access the bucket from user-3 which is having the rights given by EC2-Admin.
- ⇒ Than we can see we are not able to list the bucket inside user-3 because of no rights of S3 bucket.



- ⇒ Final configuration of users after our lab is as below.



Conclusion:

In this practical I have learnt about Identity Access Management in AWS cloud. I have learnt how to assign different roles to different users and how to create user groups and policies. I have successfully allocated allocated various user to various user groups and verified the same.