Name: Prasad Deshpande

Enrollment Number: 243341024

MSC(CS) Part I

Cloud Computing Practical Assignment No 6

Working and Implementation of Identity and Access Management (Using AWS).

Click on "Start Tab". When the message "Lab Status: Ready" appears, click "AWS" as shown in Fig 1

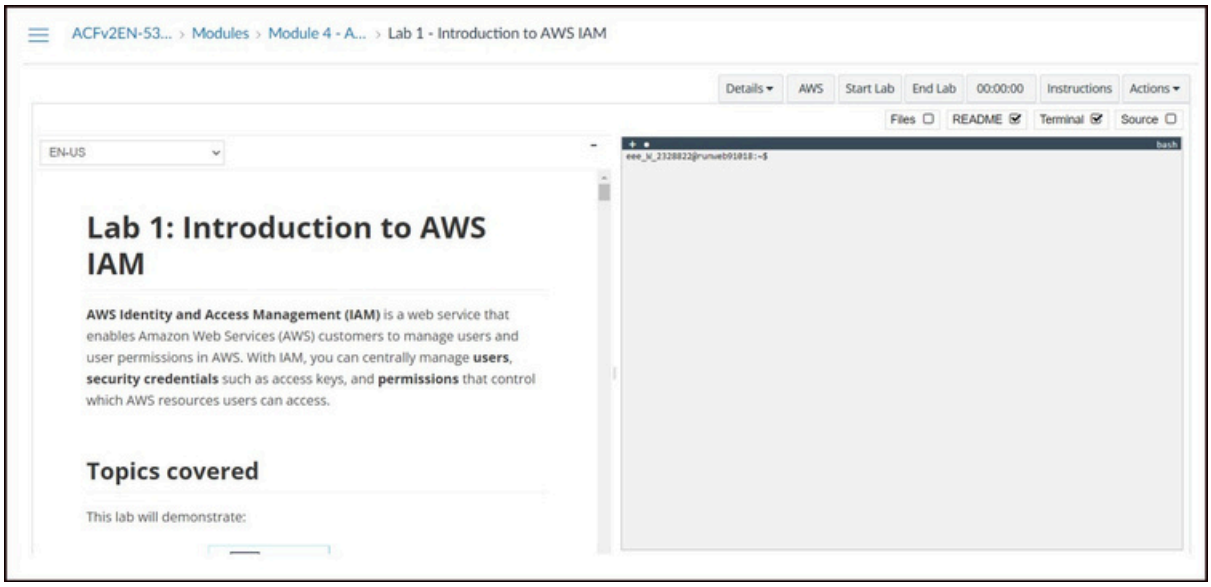

Fig 1

After clicking on “AWS” we get the console home as shown in Fig 2. Then click "View All Services".

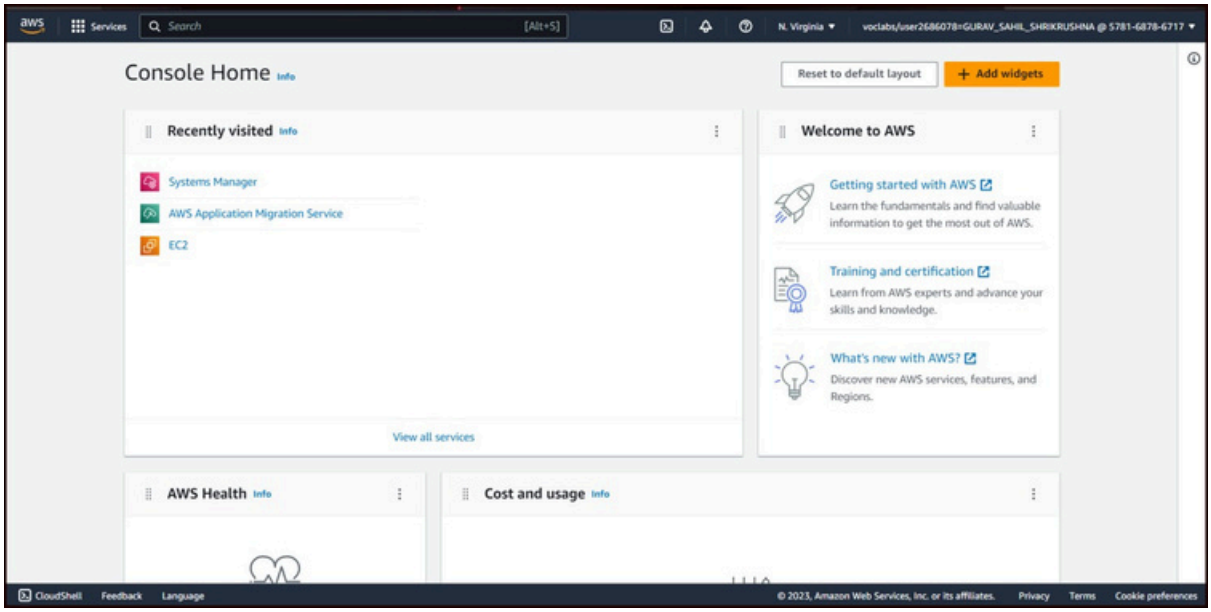

Fig 2

After clicking on “View All Services” we can see the services in Fig 3. In that select "IAM" service

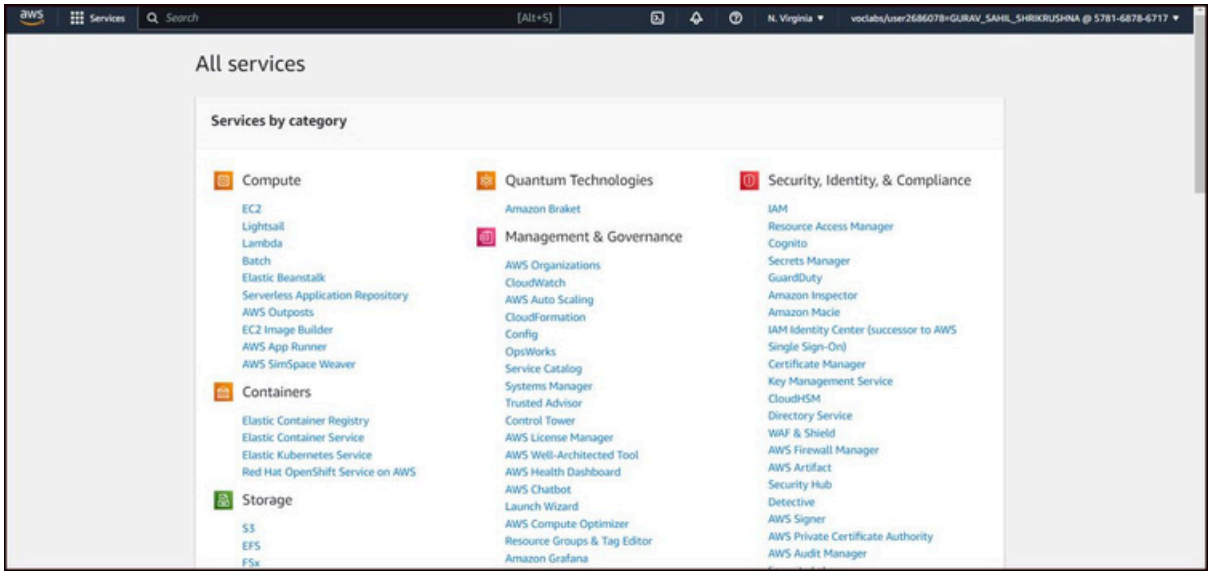

Fig 3

IAM Dashboard In Fig 4 we can see that there are already 3 groups and 4 users in IAM.

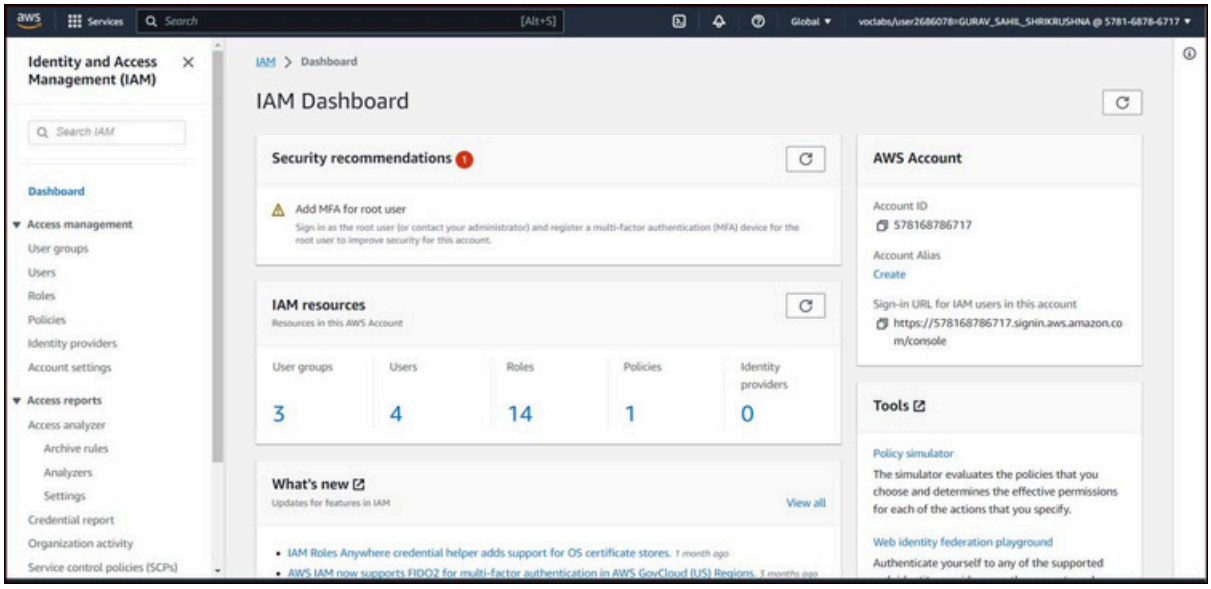

Fig 4

In the navigation pane on the left, select "Users" in which we can see that there are 4 users. The given user does not exist in any group we can see in Fig 5

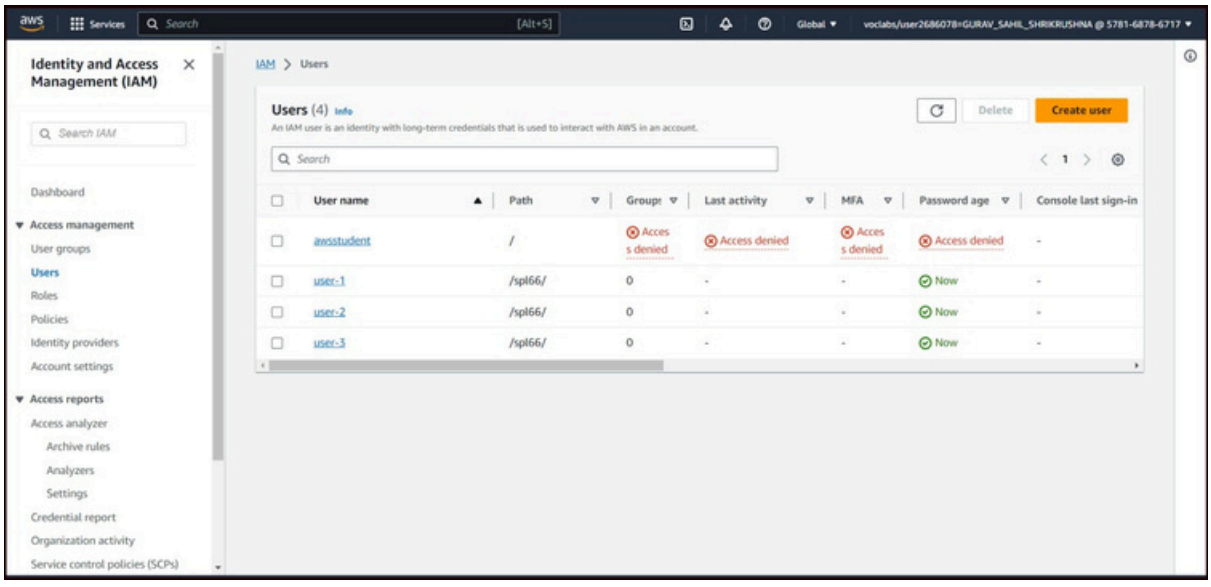

Fig 5

After clicking on “User-1” we can see the details regarding “User-1”. No permissions granted to "user-1" in "Permissions" tab that we can see in Fig 6

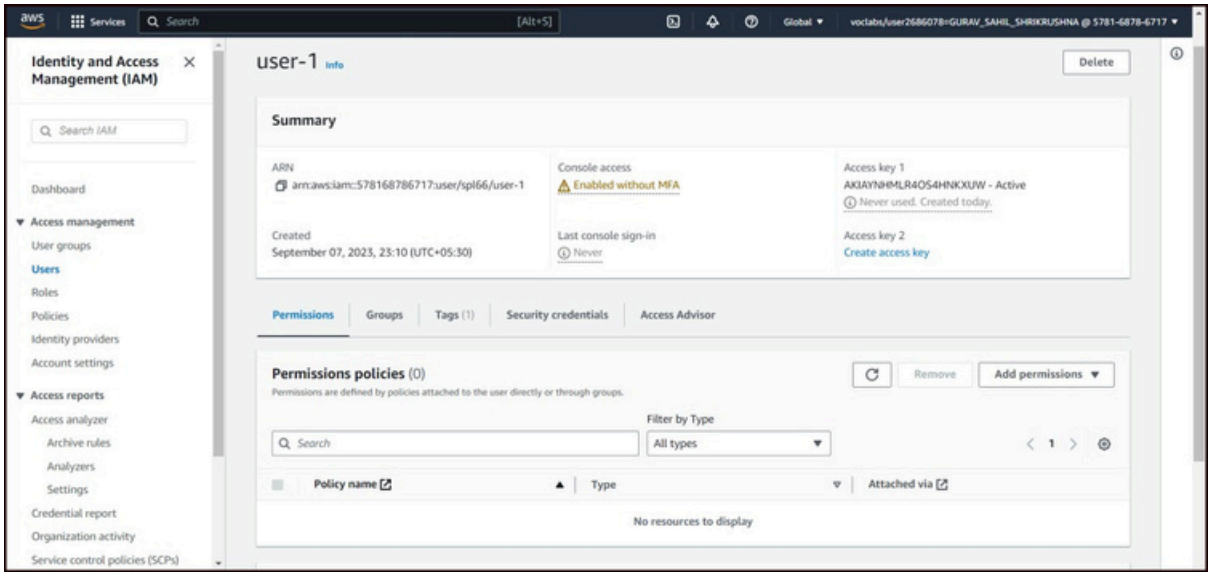

Fig 6

In Fig 7 "Groups" tab we can see that "user-1" does not exist in any group

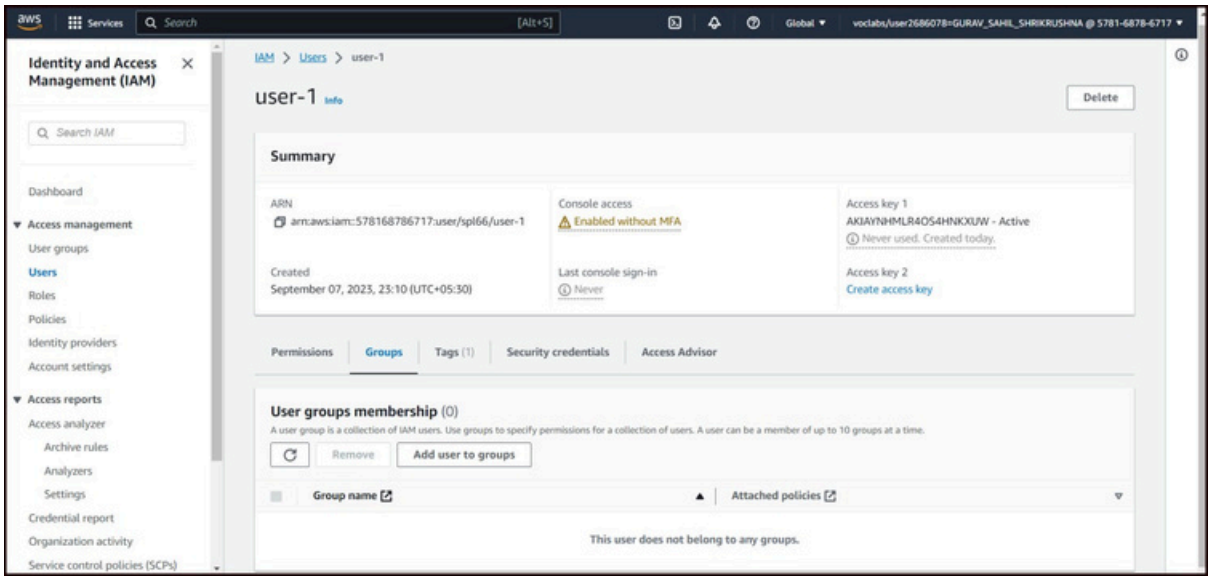

Fig 7

In the left side navigation pane, select "User Groups" in which we can see there are 3 groups. User does not exist in that groups we can see in Fig 8

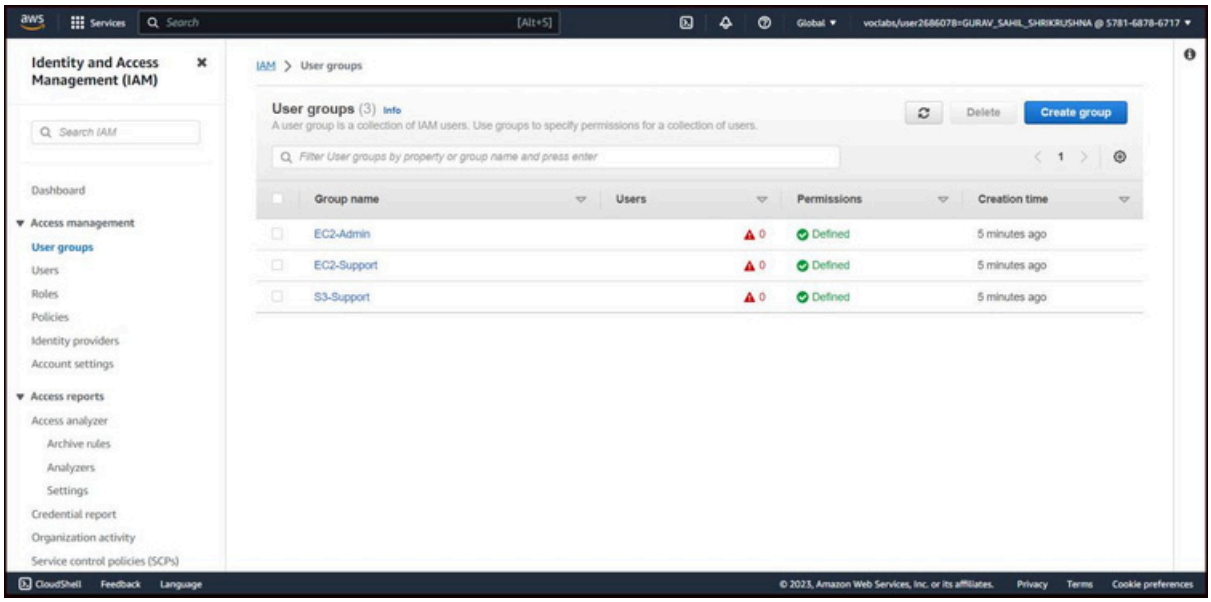

Fig 8

In Fig 9 we see that in "EC2-Support" select the "Permission " tag, select the plus (+) icon next to the "AmazonEC2ReadOnlyAccess" policy to view the policy details.

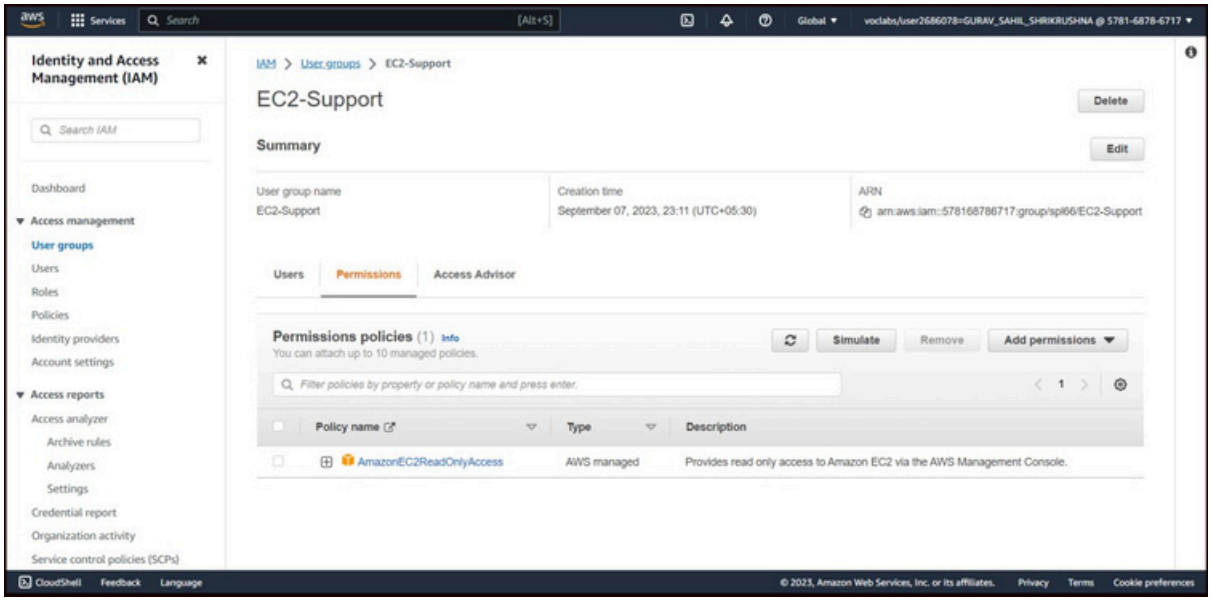

Fig 9

In Fig 10 we can see the "AmazonEC2ReadOnlyAccess" policy.

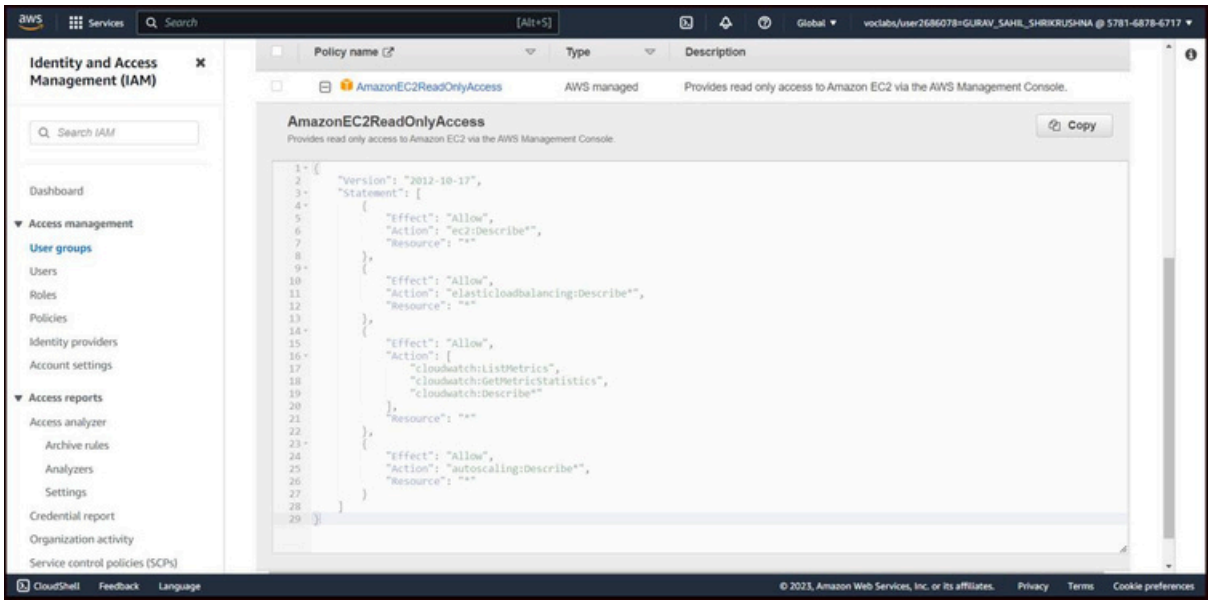

Fig 10

In Fig 11 we see that in "S3-Support" select the "Permission " tag, select the plus (+) icon next to the "AmazonS3ReadOnlyAccess" policy to view the policy details. we can see the "AmazonS3ReadOnlyAccess" policy

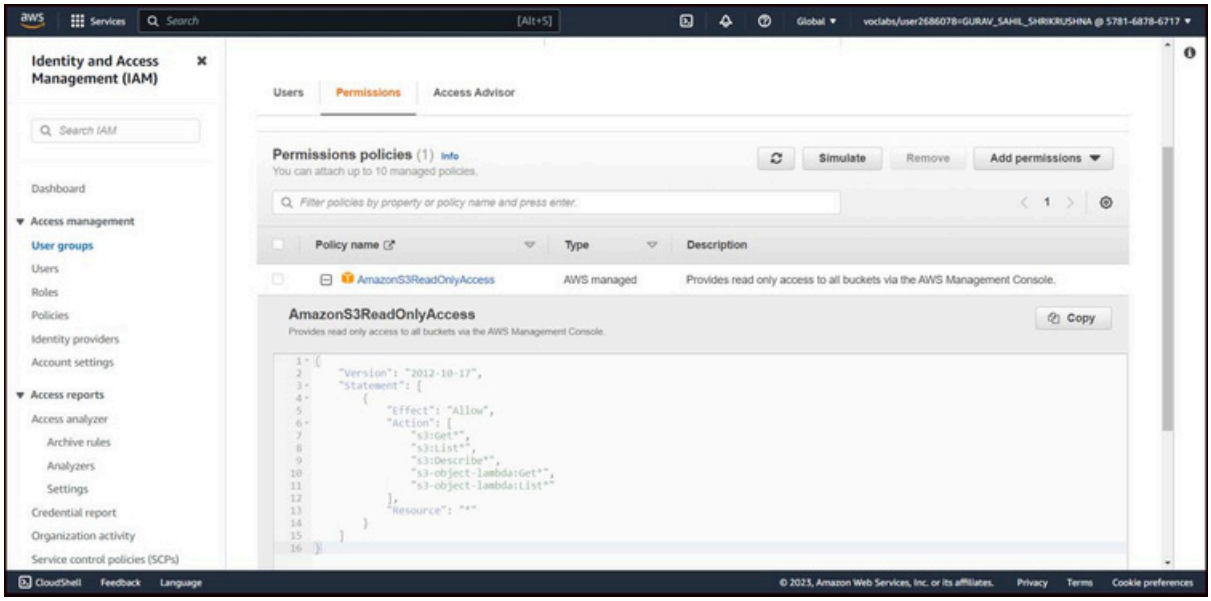

Fig 11

In Fig 11 we see that in "EC2-Admin-Policy" select the "Permission" tag, select the plus (+) icon next to the "EC2-Admin-Policy" policy to view the policy details. we can see the "EC2-Admin-Policy" policy

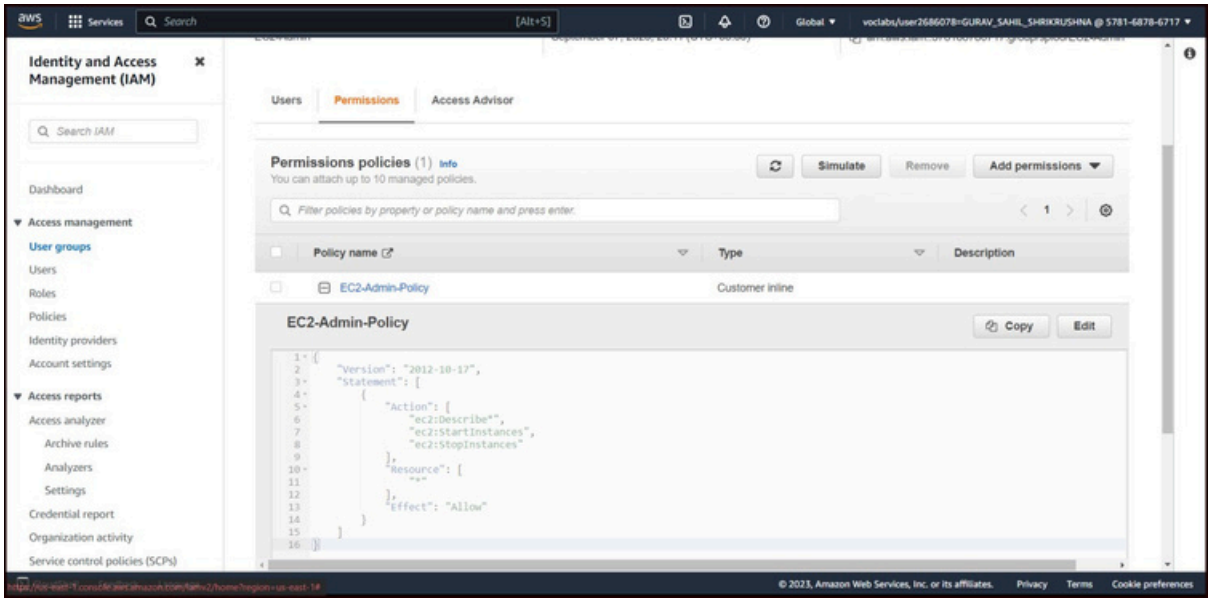

Fig 12

In Fig 13 we can see that there is no user in the group

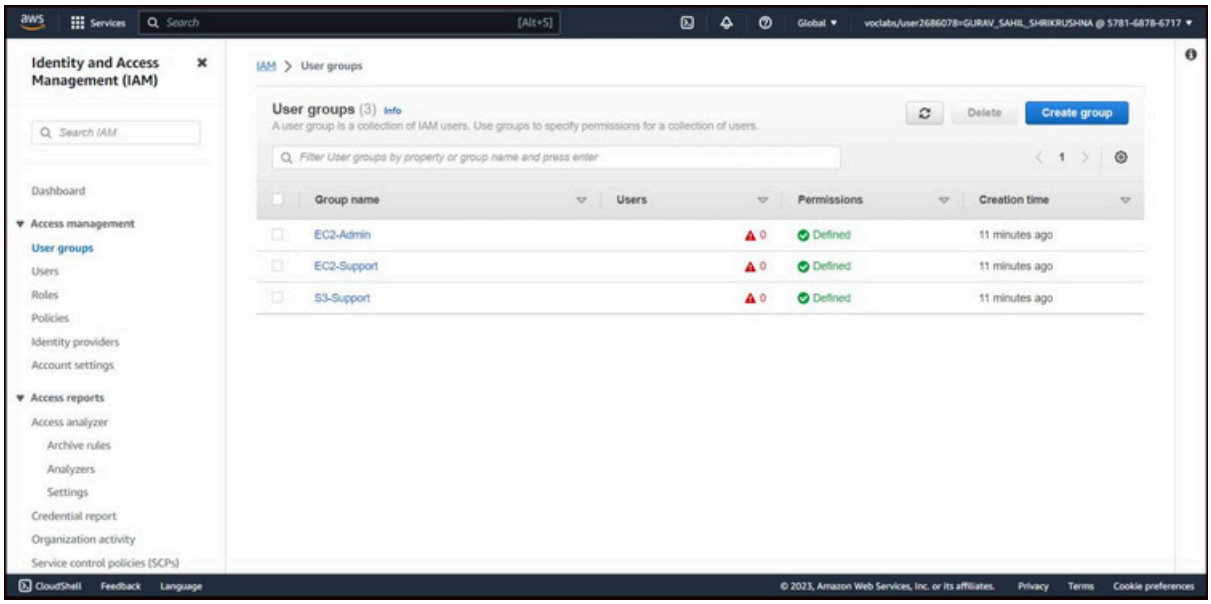

Fig 13

Select the "S3-Support" group in Fig 14, select "Add User" in it.

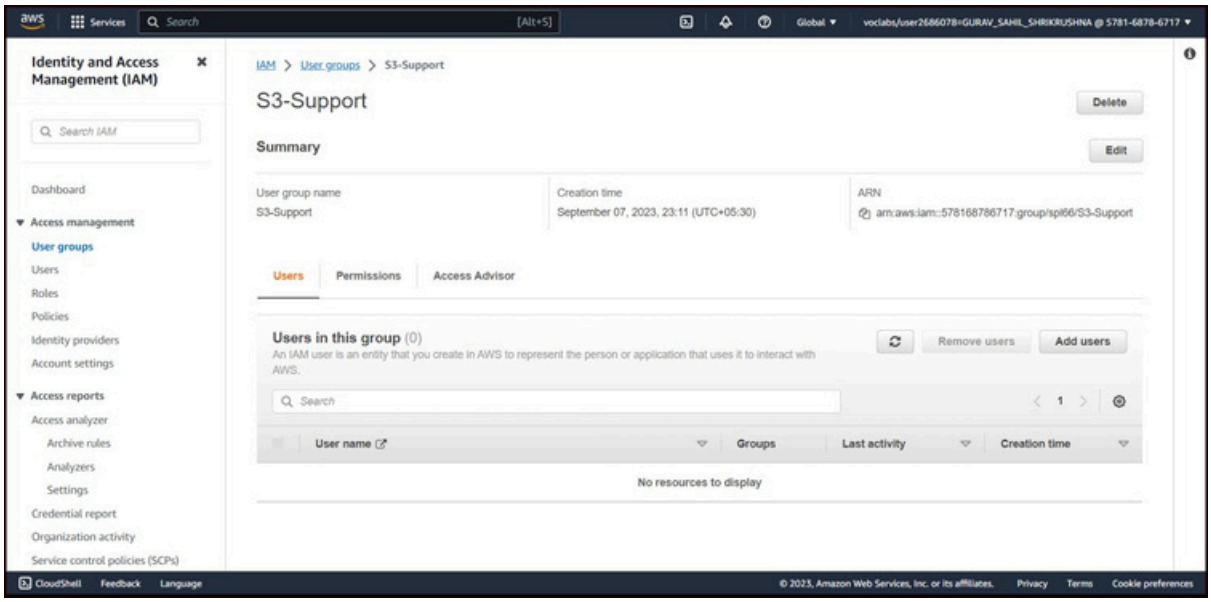

Fig 14

Add “user-1” to “S3-support”, then click “Add User” as shown in Fig 15.

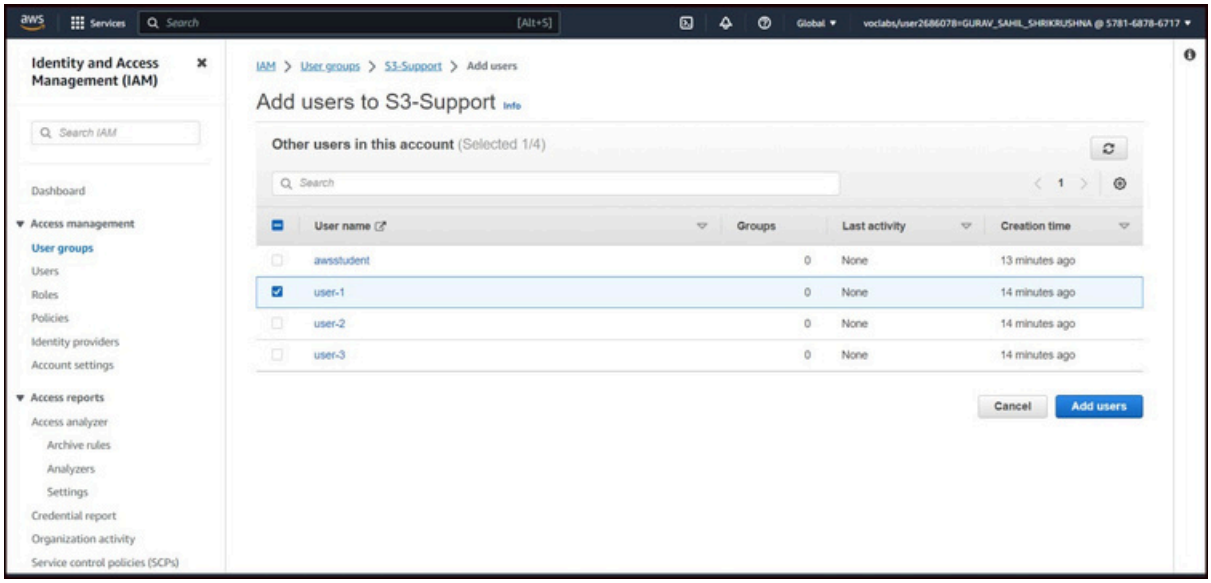

Fig 15

We can see in Fig 16 “user-1” is added in the group “S3-Support”

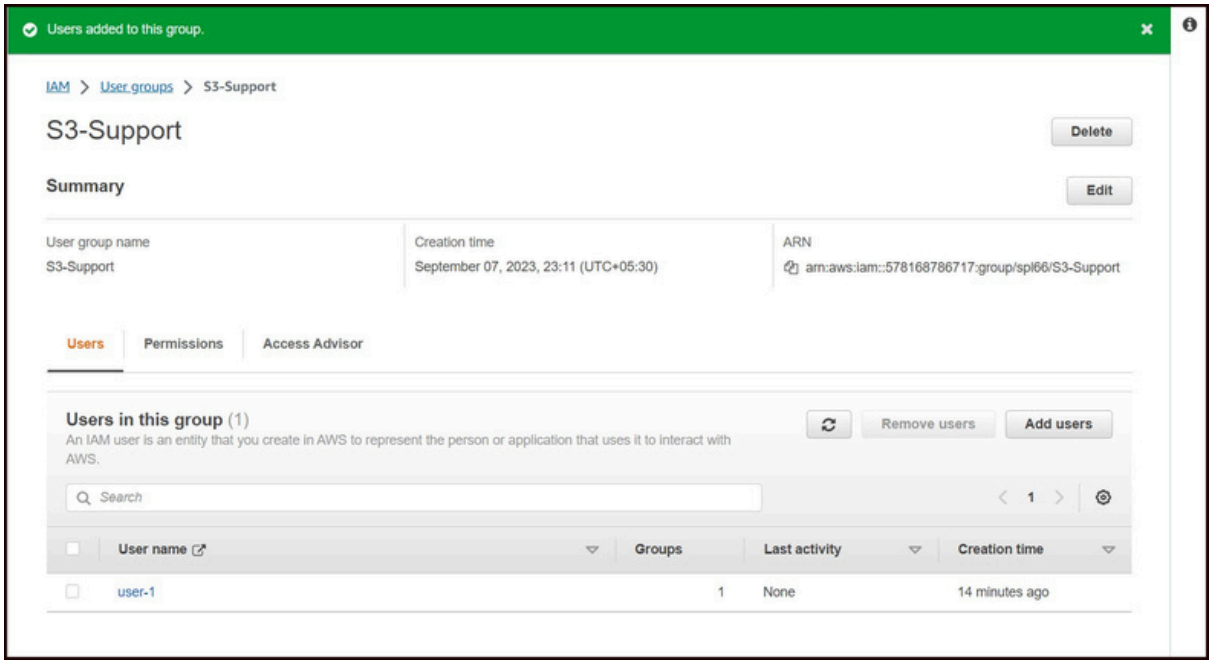

Fig 16

Select the "EC2-Support" group in Fig 17, select "Add User" in it.

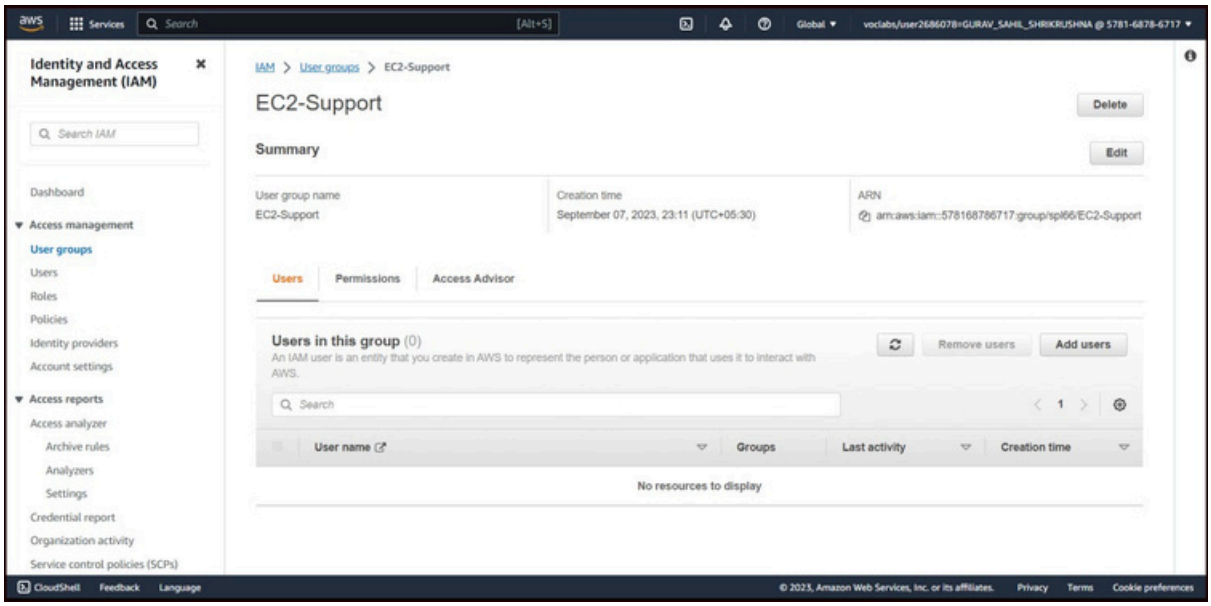

Fig 17

Add “user-2” to “EC2-Support”, then click “Add User” as shown in Fig 18.

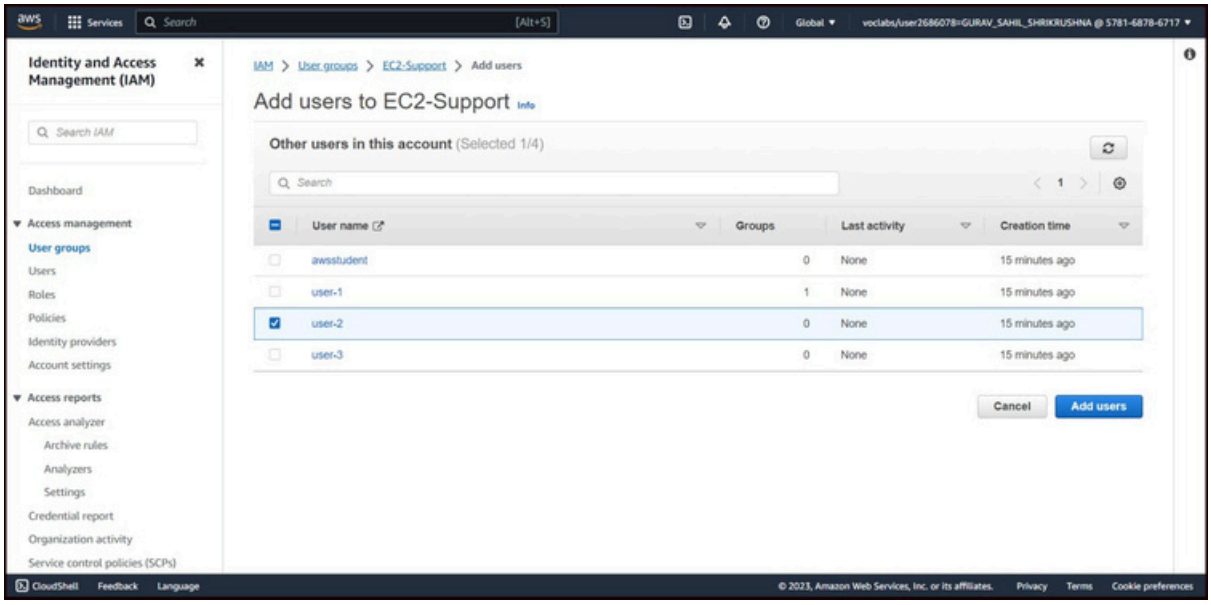

Fig 18

We can see in Fig 19 “user-2” is added in the group “EC2-Support”

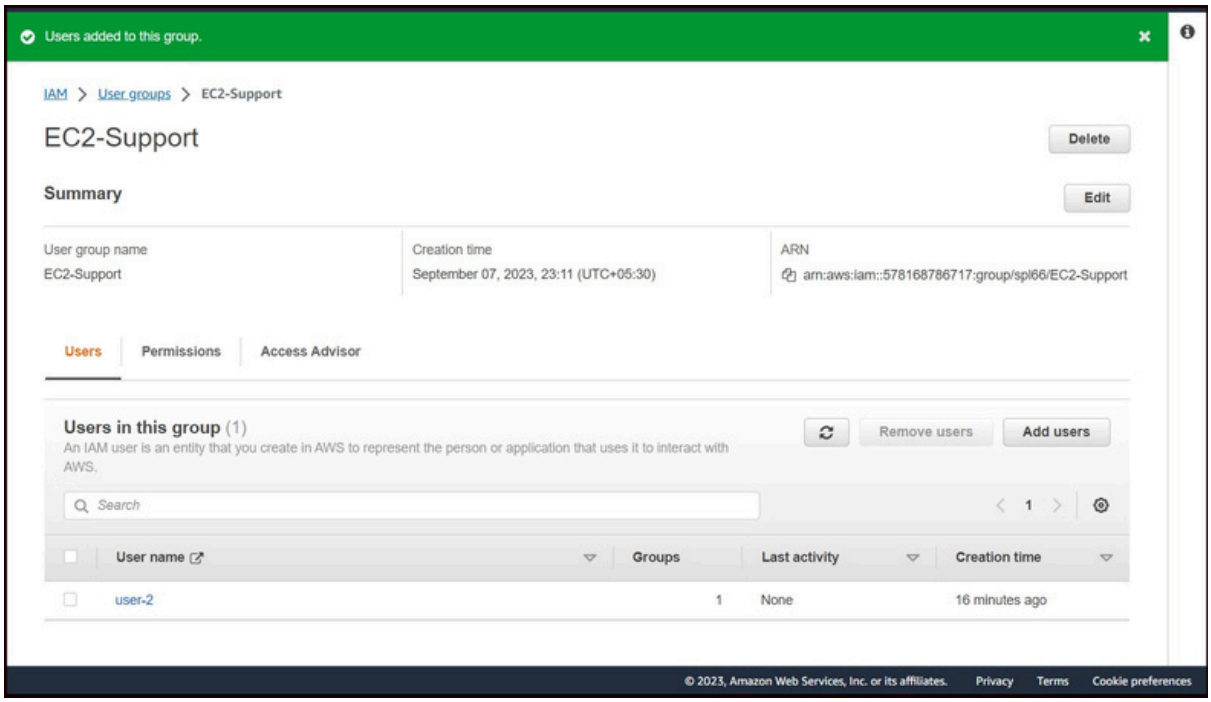

Fig 19

Select the "EC2-Admin" group in Fig 20, select "Add User" in it.

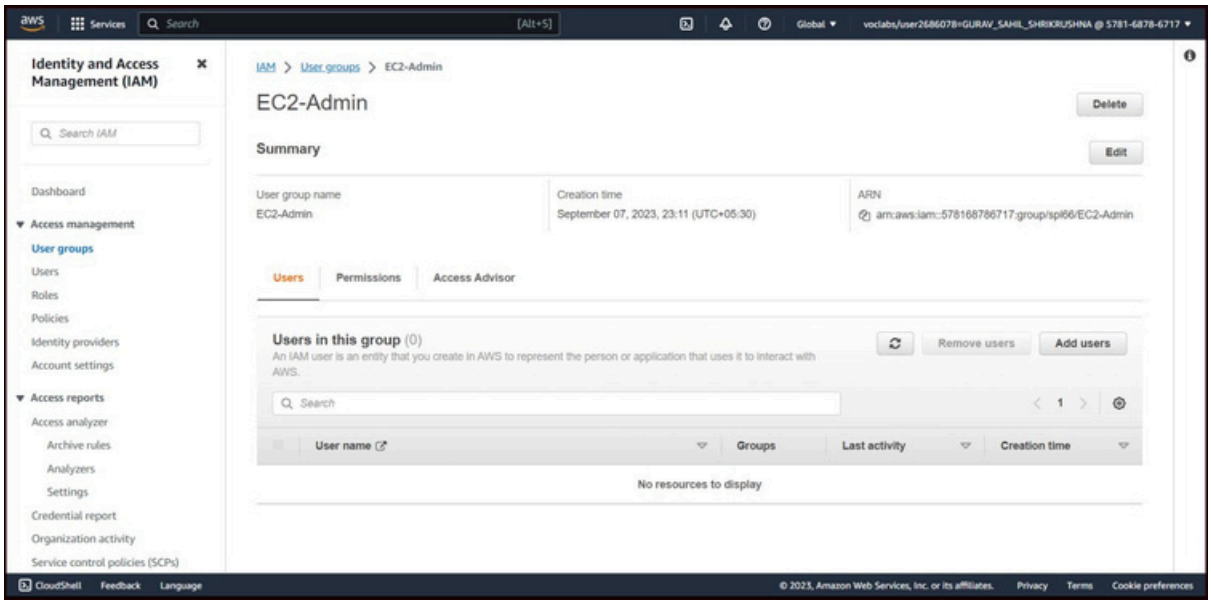

Fig 20

Add “user-3” to “EC2-Admin”, then click “Add User” as shown in Fig 21

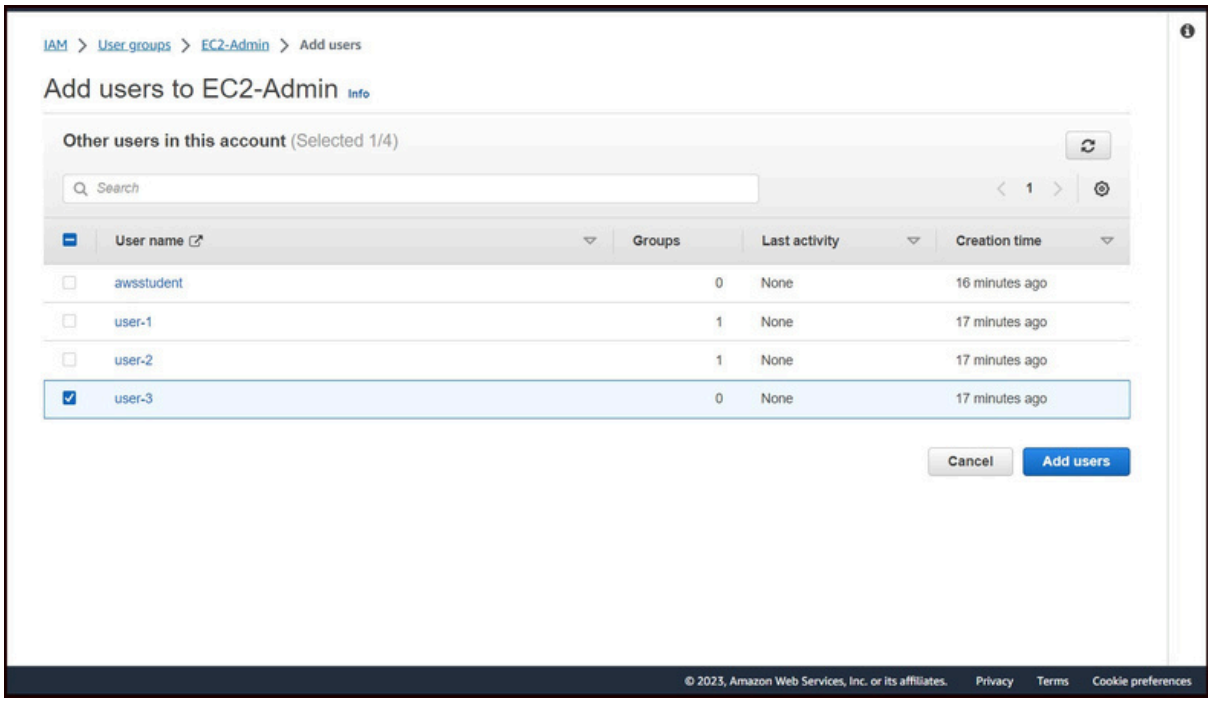

Fig 21

We can see in Fig 22 “user-3” is added in the group “EC2-Admin”.

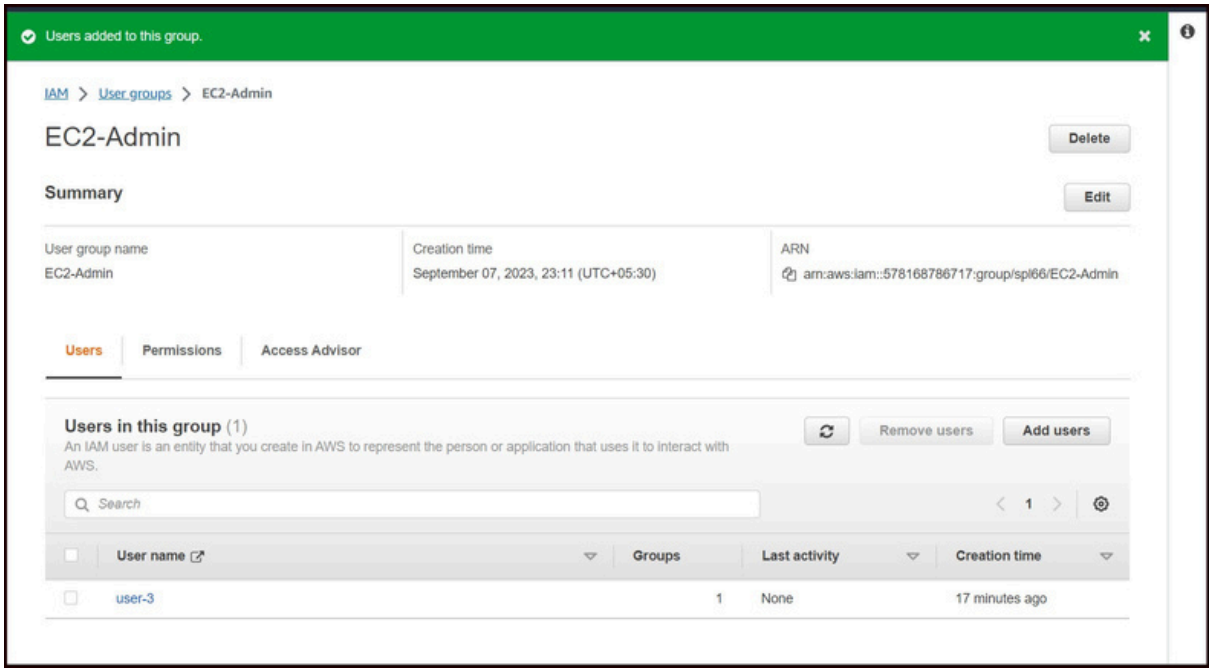

Fig 22

In Fig 23 we can see that each group has one user

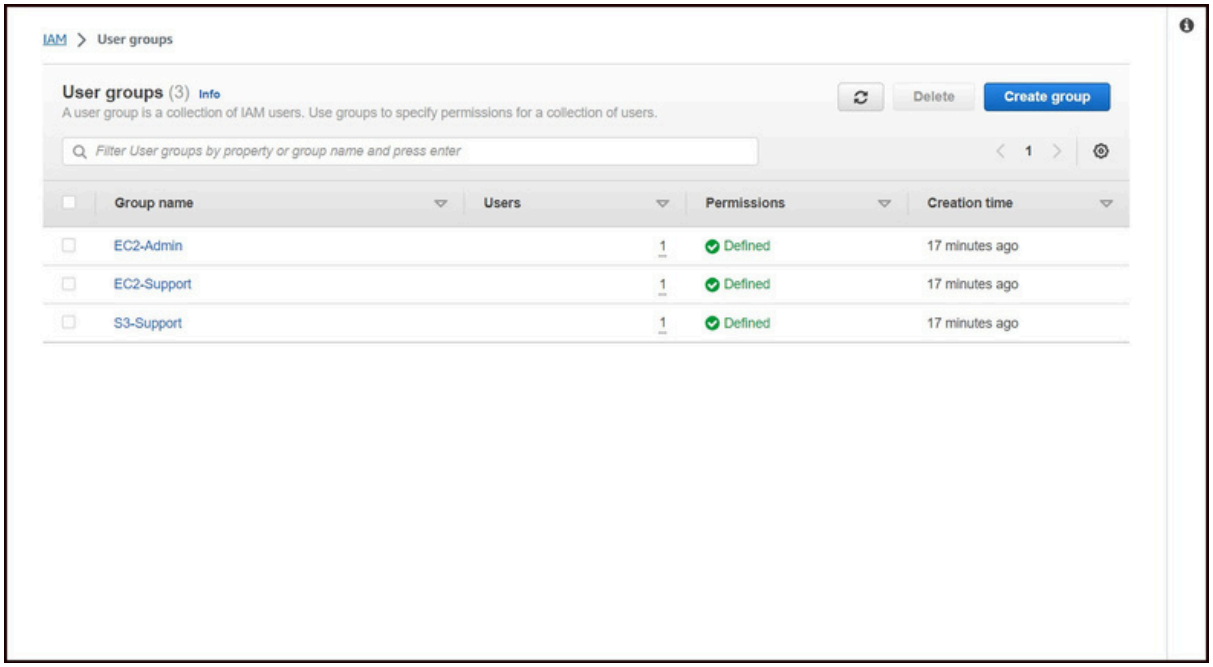

Fig 23

In the navigation pane on the left, select Dashboard. The IAM users sign-in link is then displayed on the right. We can see in Fig 24 Copy that sign-in URL for IAM users in this account into a incognito tab

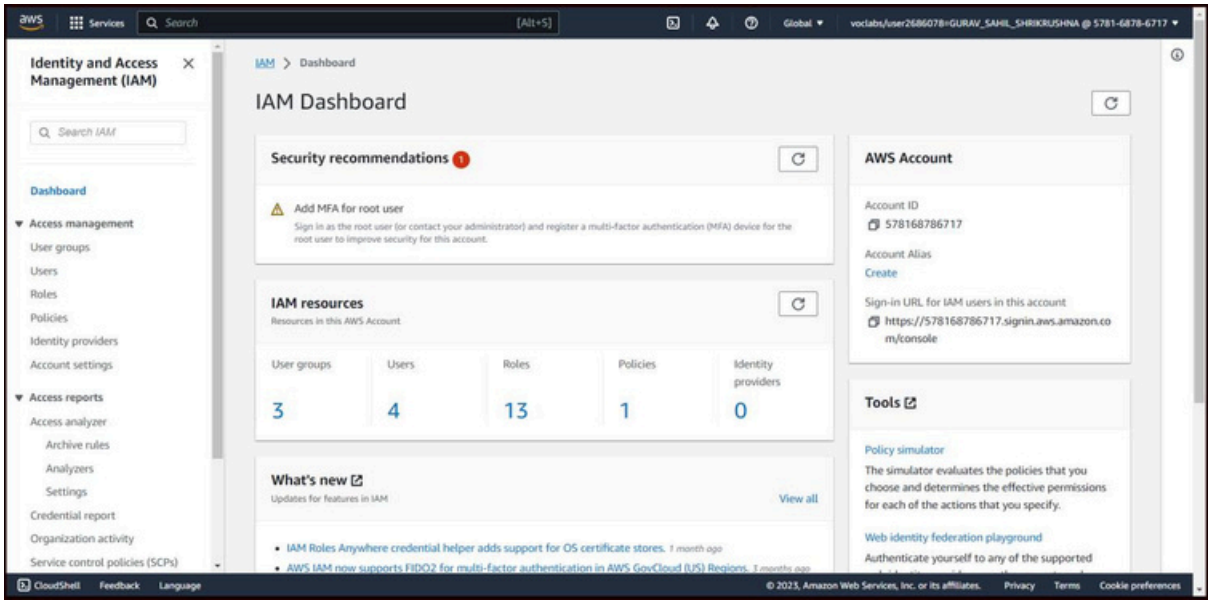

Fig 24

For the sign in IAM user name is “user-1” and password is “Lab-Password1” then click on “Sign in” button.

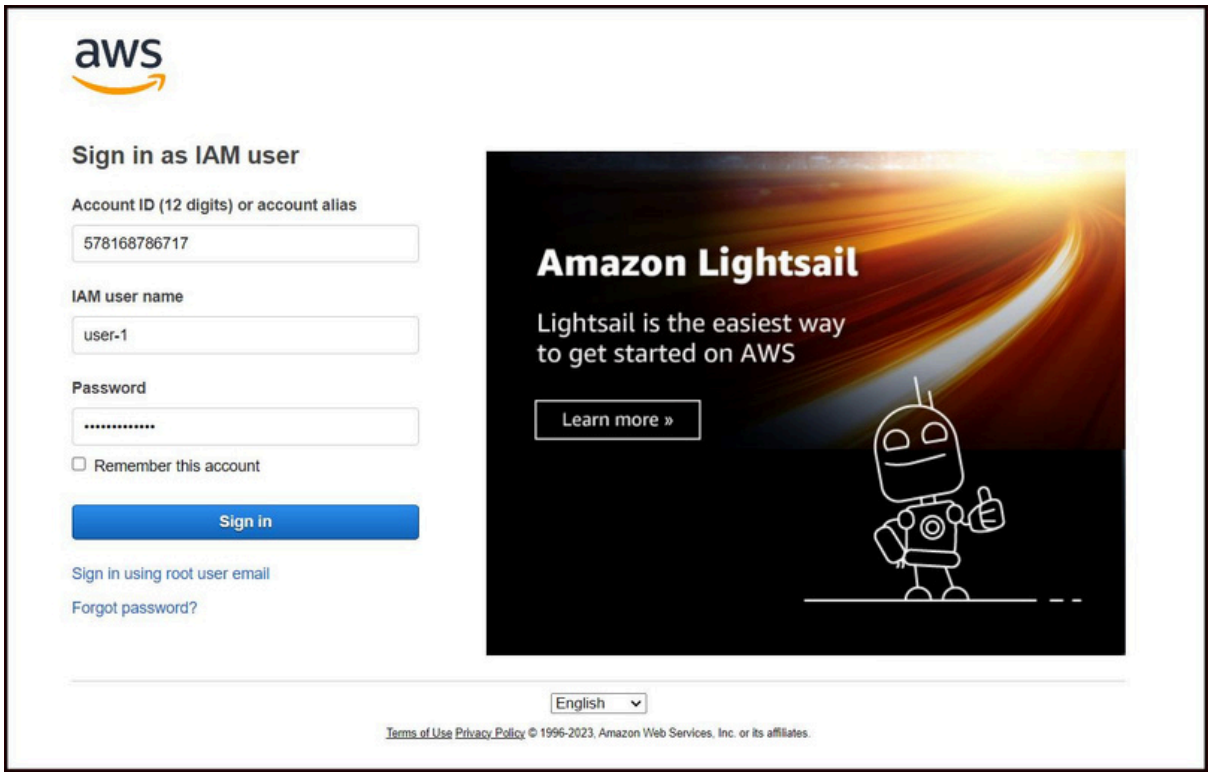

Fig 25

Click "View all services" in Figure 26 and then select the S3 service

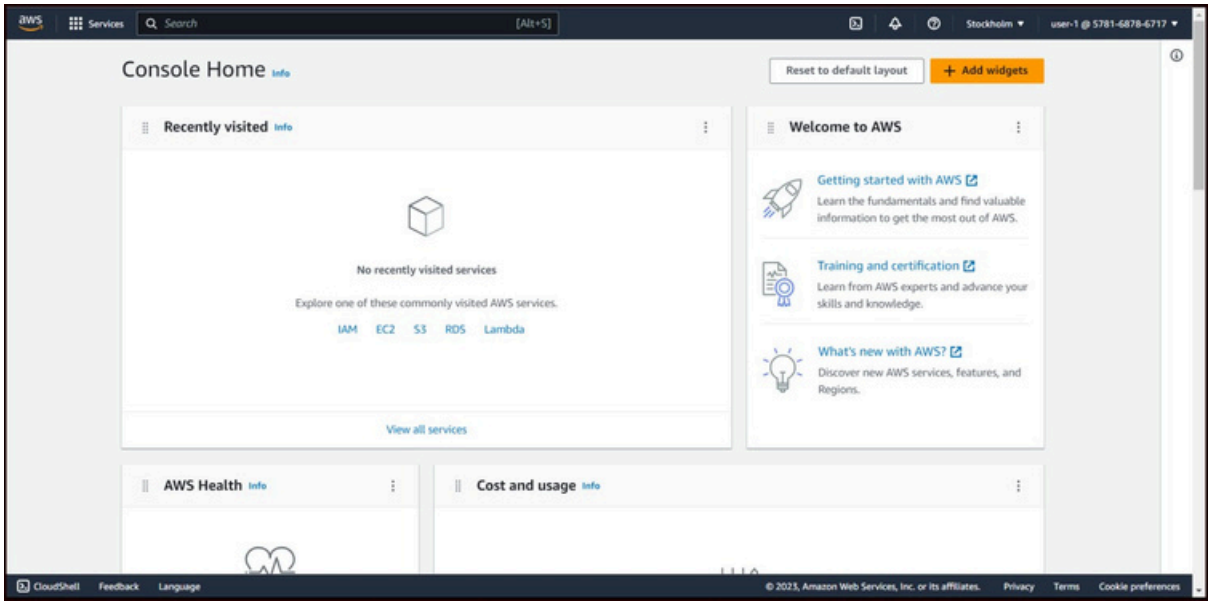

Fig 26

We can see in Fig 27 that we have granted permission to user-1 for the S3 bucket.

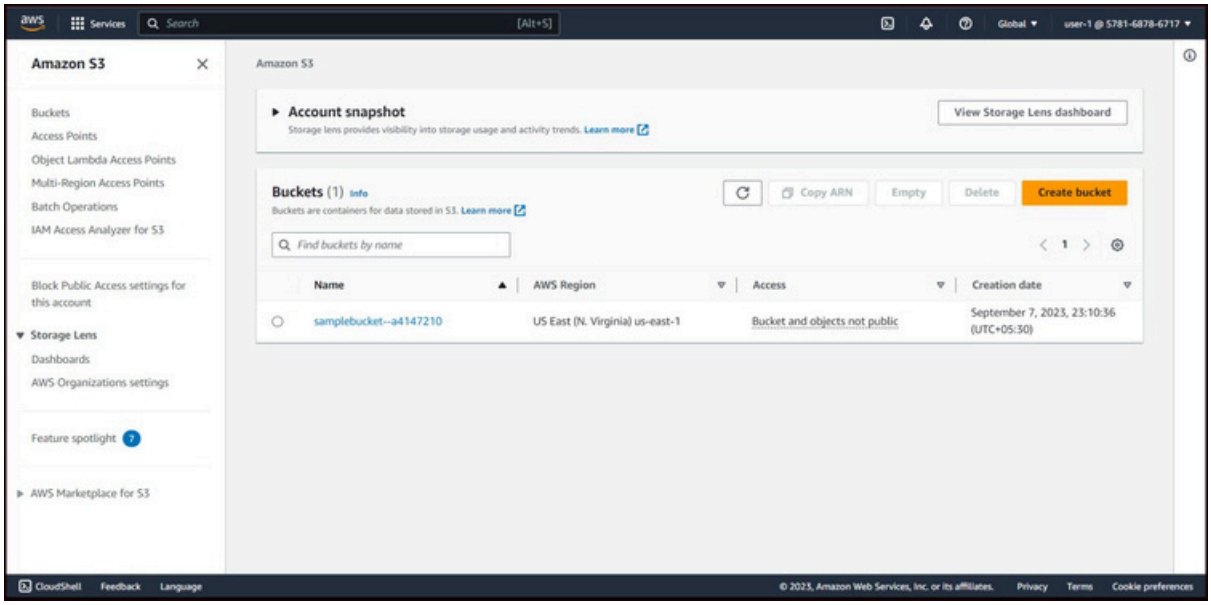

Fig 27

For User1 we allow only S3 bucket service so User1 has not given any other permission for other services so we will get error for other services that we can see in Fig 28 and Fig 29

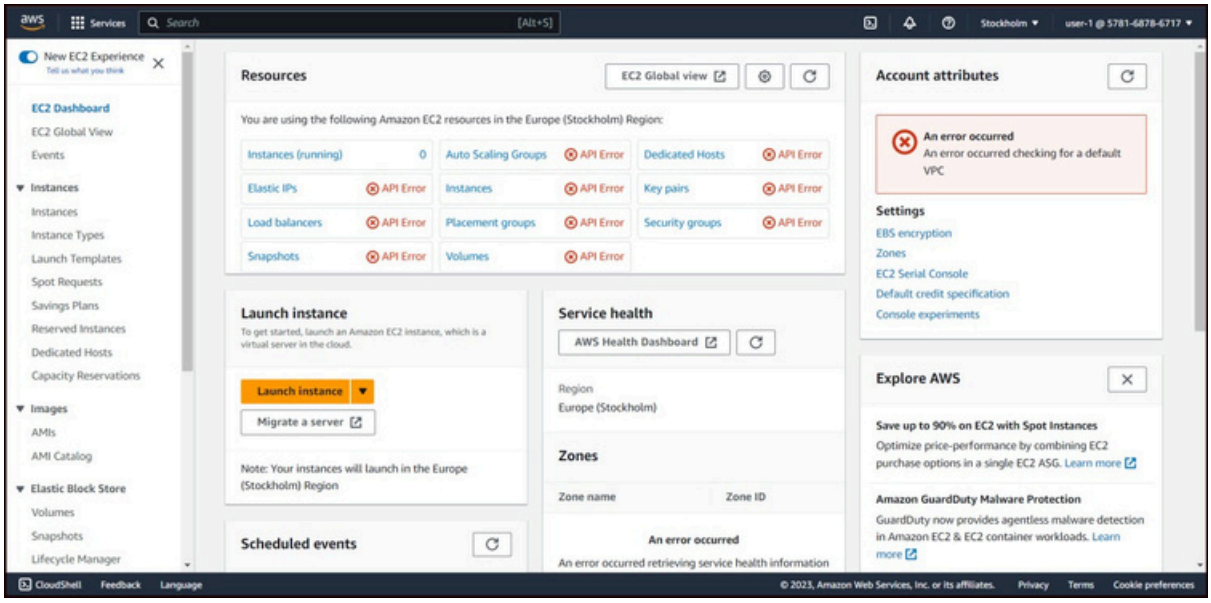

Fig 28

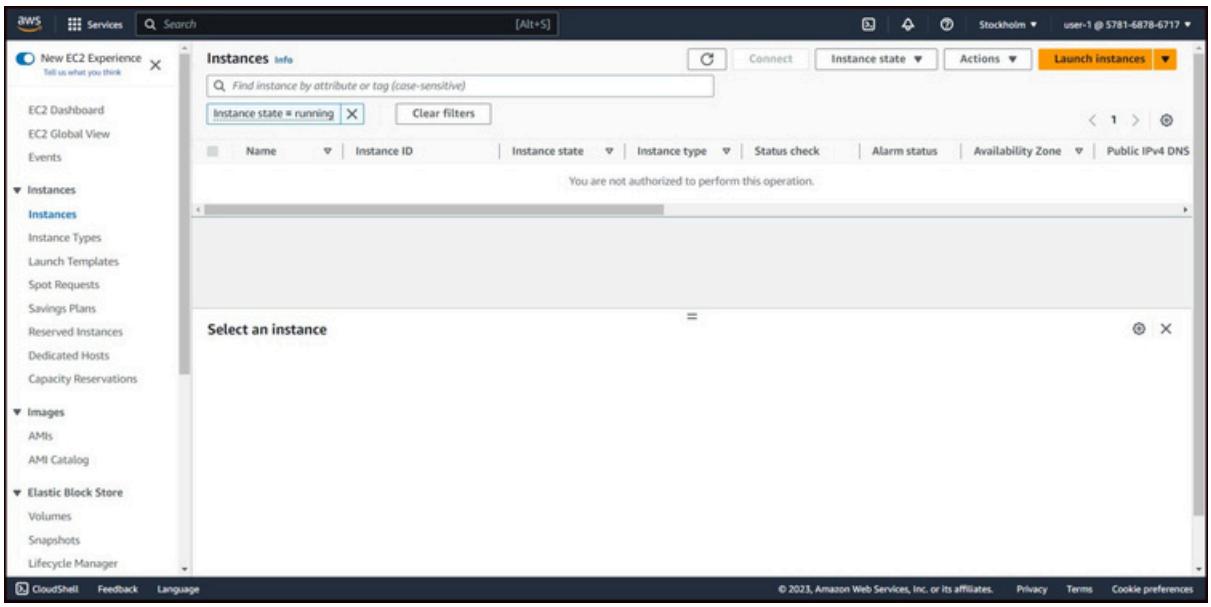

Fig 29

Then Sign out the user-1 as shown in Fig 30

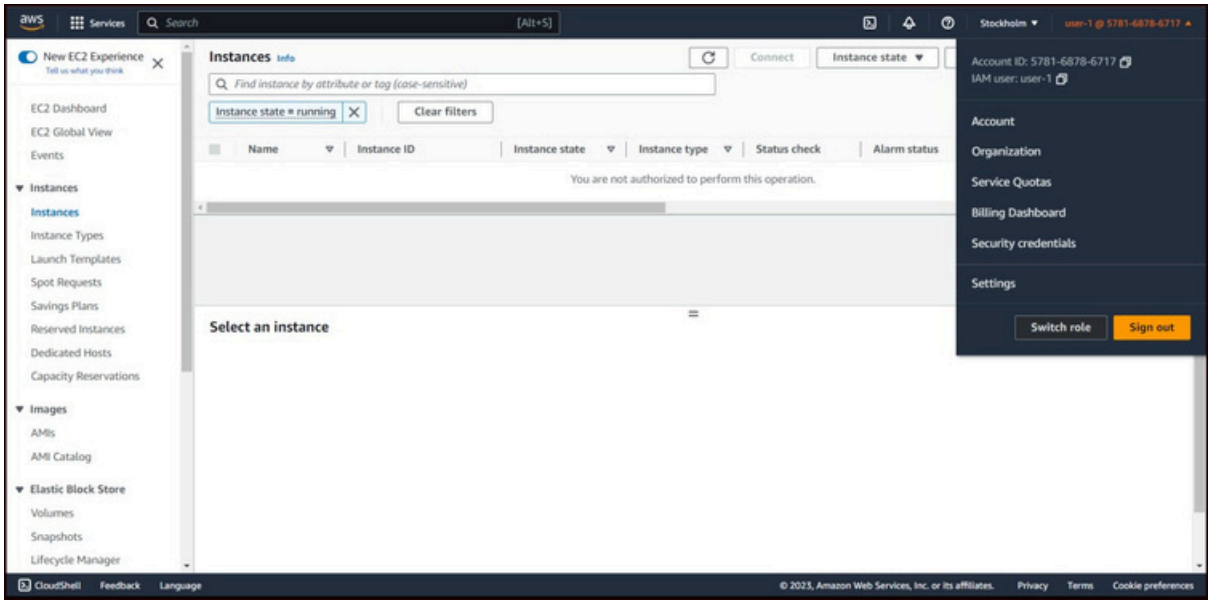

Fig 30

For the sign in IAM user name is “user-2” and password is “Lab-Password2” then click on “Sign in” button.

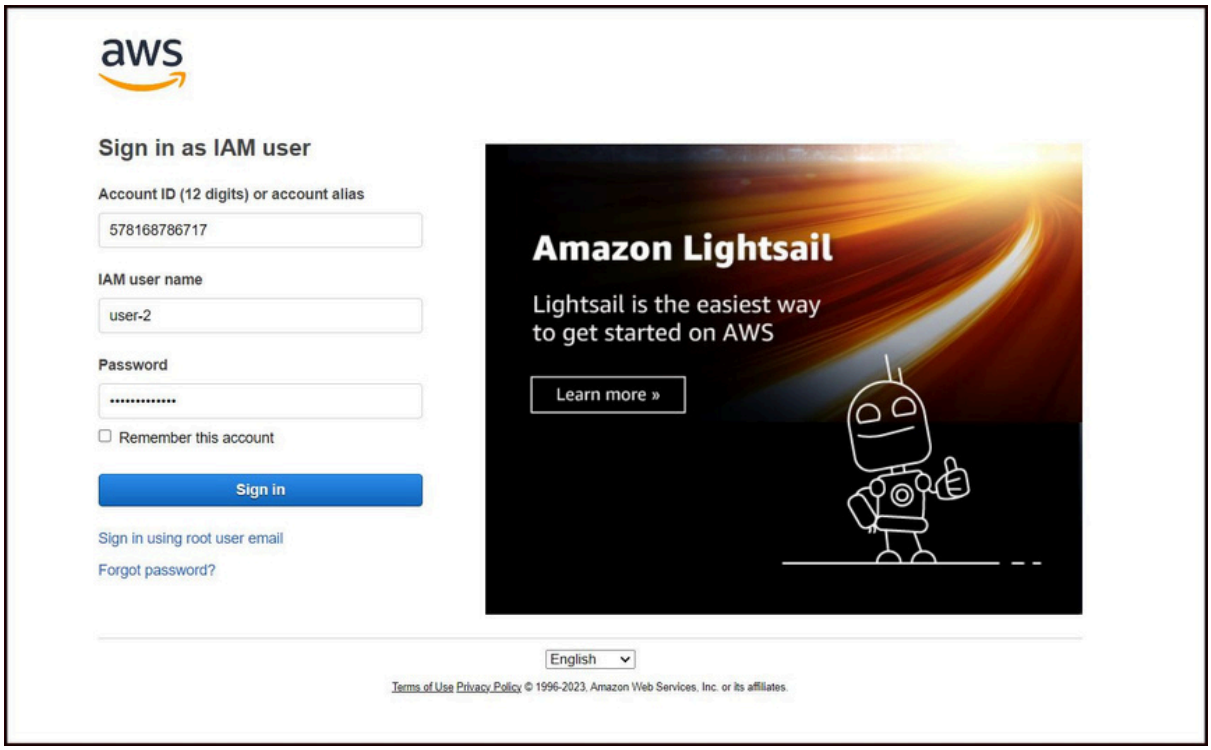

Fig 31

For user-2 we have not provided "S3" service so we have not seen the bucket in Fig 32

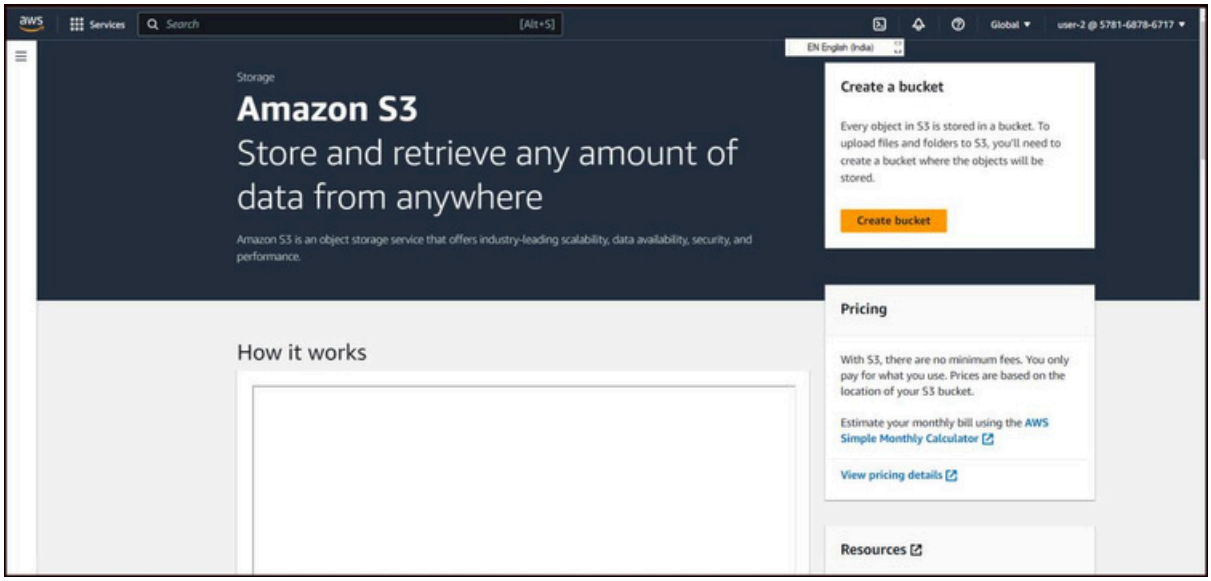

Fig 32

For user-2 we provide read access only so other operations such as terminating or stopping the instance are not performed by user-2 in Fig 33.

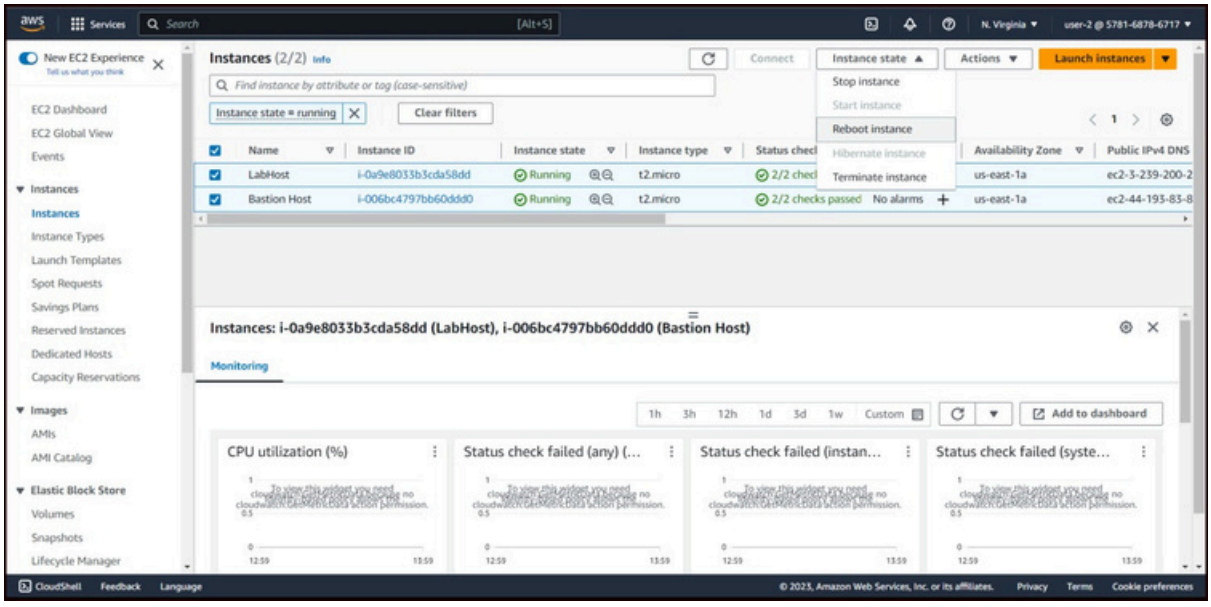

Fig 33

If user-2 tries to stop or terminate the instance we will get the error similar to the Fig 34

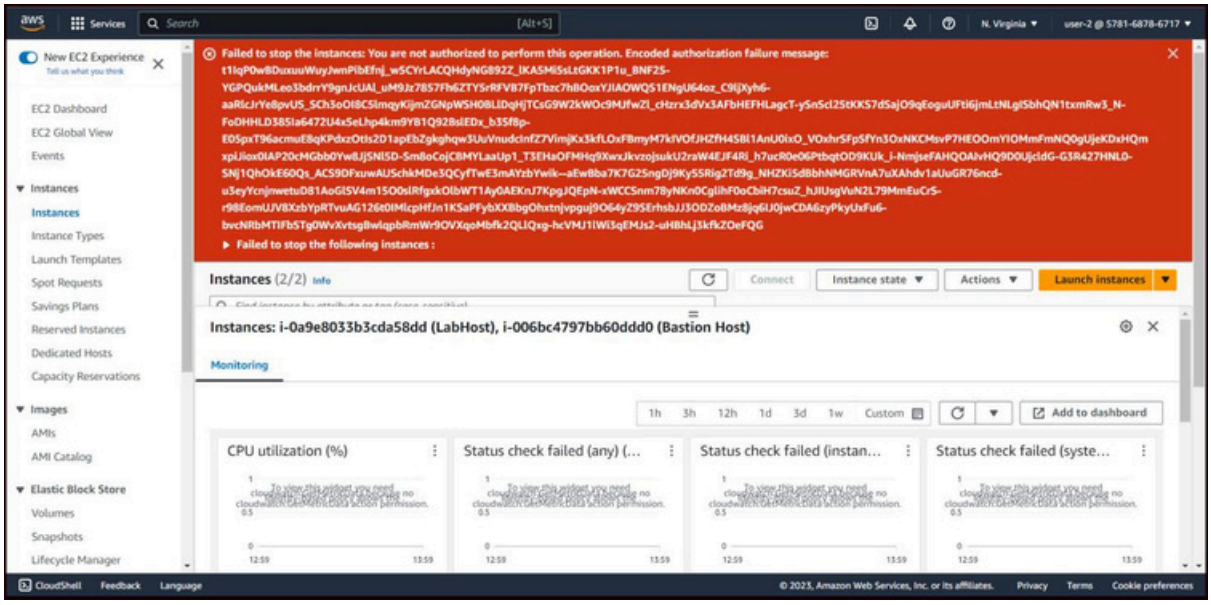

Fig 34

Then Sign out the user-2 as shown in Fig 35

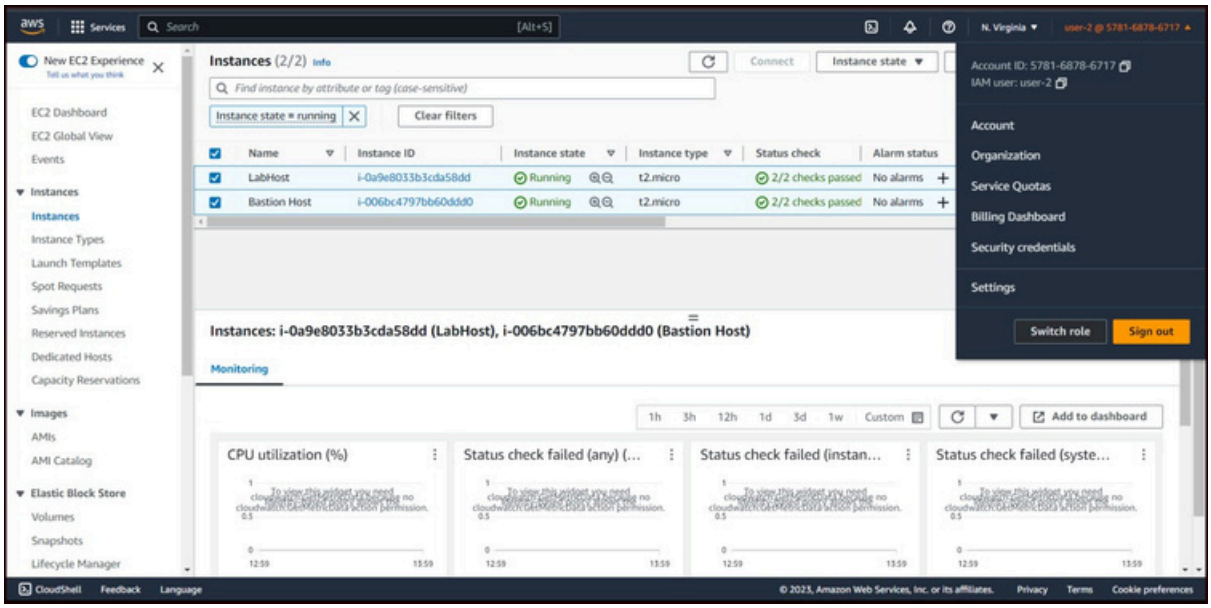

Fig 35

For the sign in IAM user name is “user-3” and password is “Lab-Password3” then click on “Sign in” button.

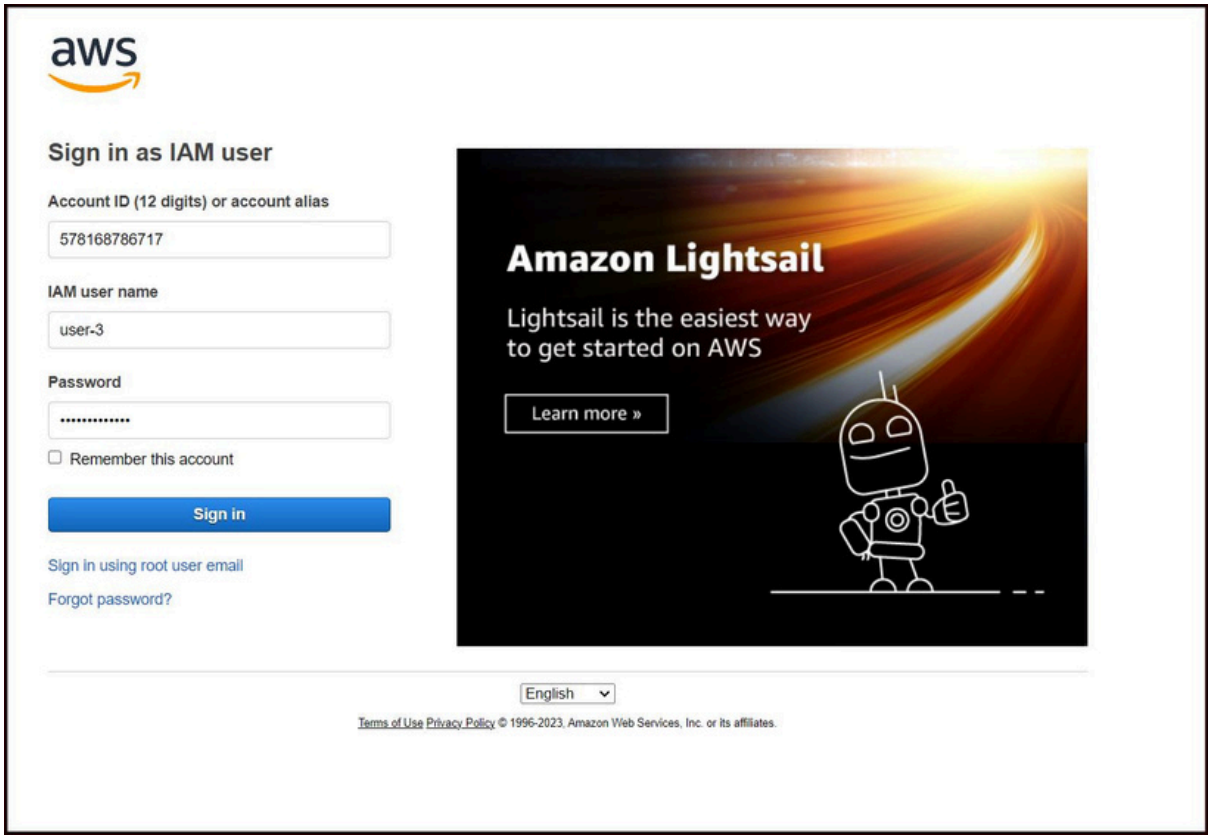

Fig 36

For user-3 we provide read-write access so that other operations such as terminating or stopping the instance are performed by user-3 in Fig 37.

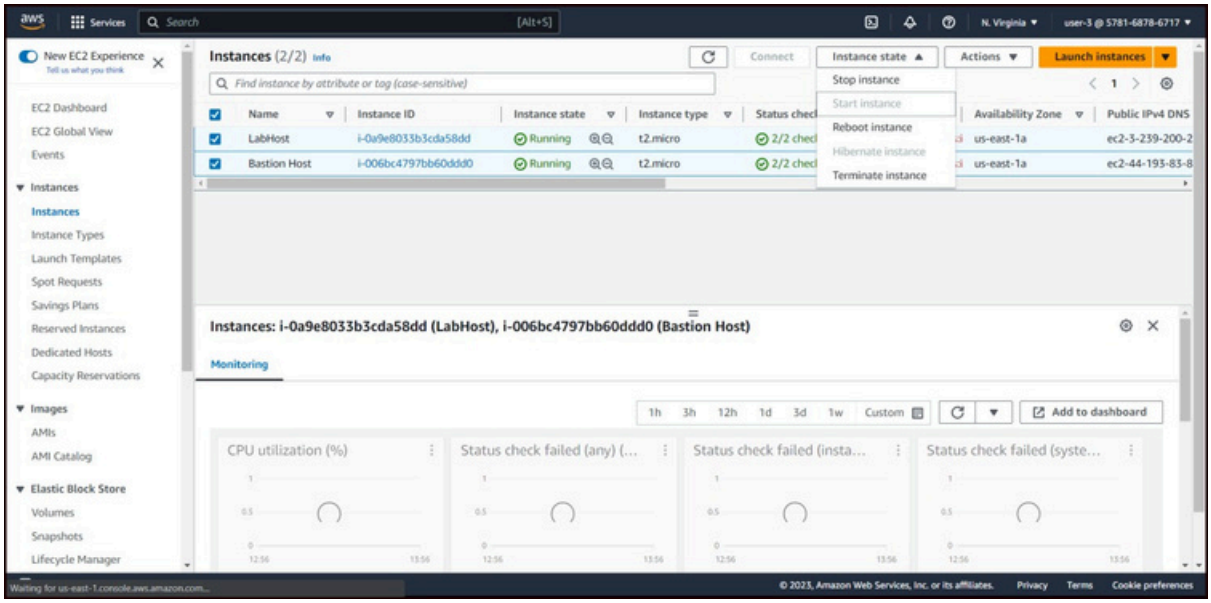

Fig 37

User-3 can execute the Stop and Terminate Instance operation. In Fig 38, we can see that the instance has been successfully stopped.

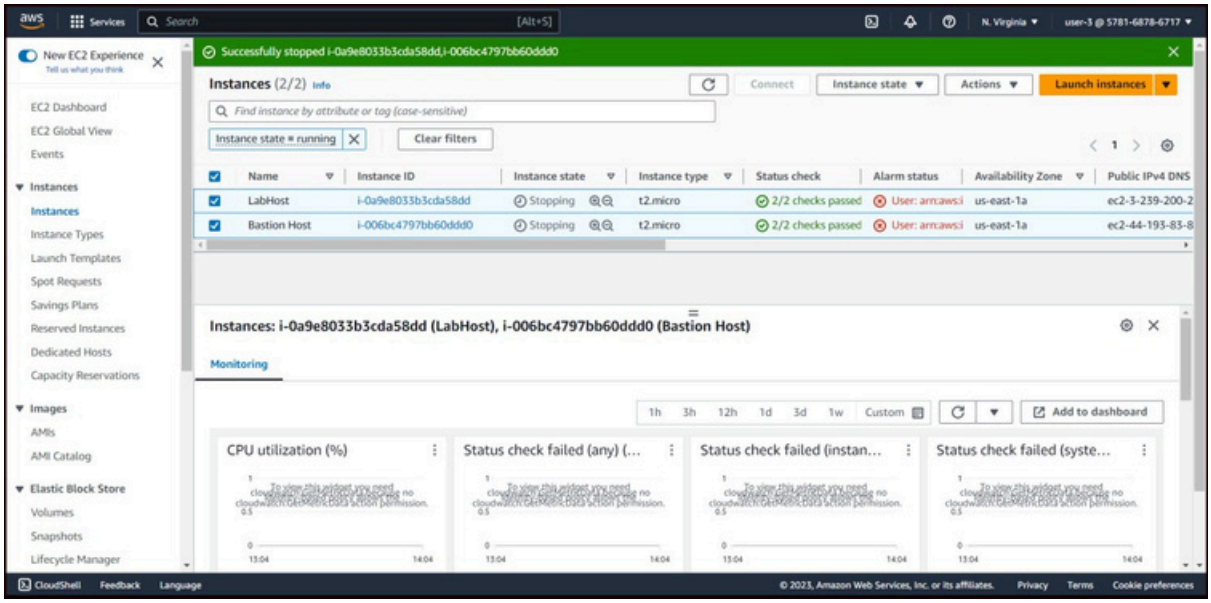

Fig 38

Then Sign out the user-23 as shown in Fig 39

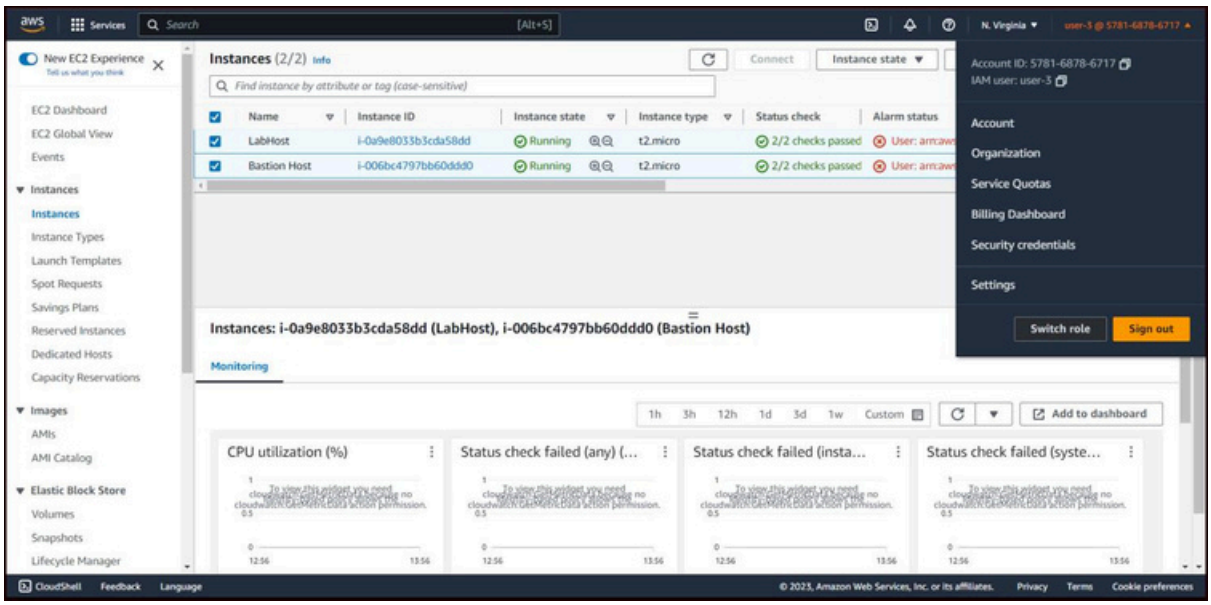

Fig 39