CLOUD COMPUTING LABORATORY- 10

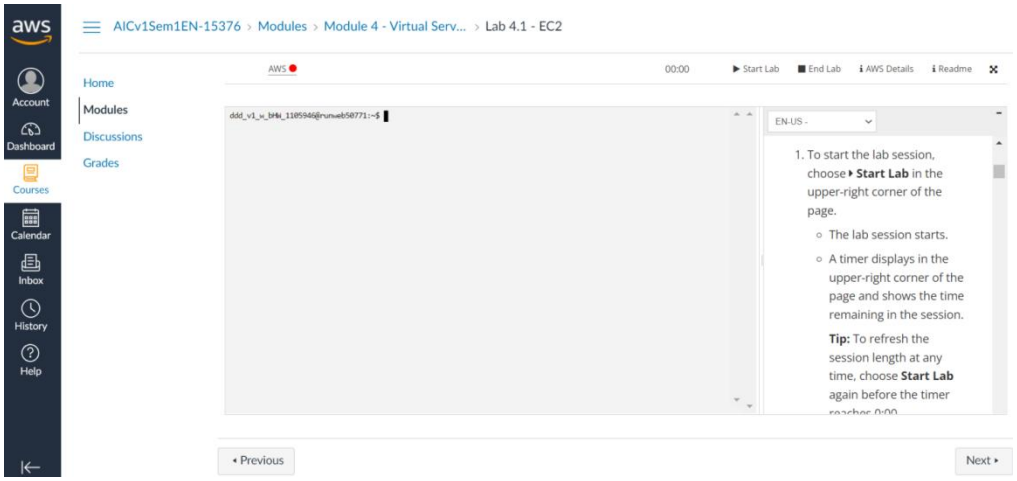
AWS ACADEMY LAB 07

Amazon Web Services

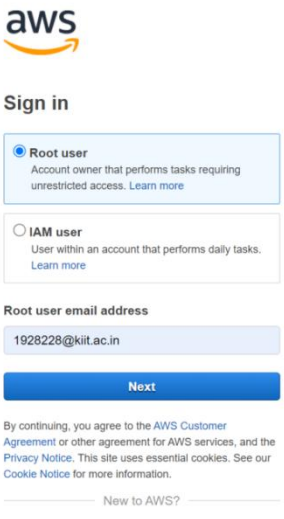
Name: Drishti.
Roll No: 1928228
Date: 27/03/2022

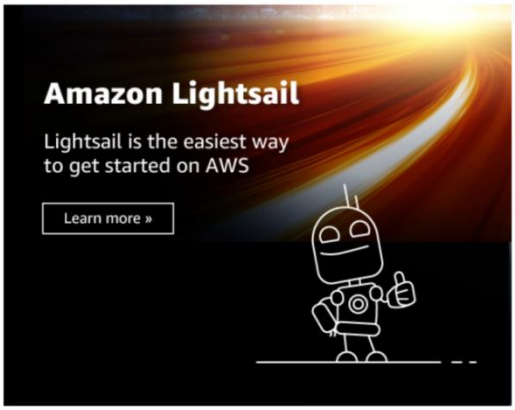
Aim: **Explored users, groups, and policies in the AWS Identity and Access Management (IAM) service.**
Time Duration: **Approximately 40 minutes.**
Requirements: **- AWS account (access to AWS console dashboard)**
- Internet connection

1. If we use AWS academy to log in, we go to LAB 7 and click on start lab, allowing the light beside AWS to turn green, before clicking on AWS on the left side, which automatically displays the AWS console dashboard.



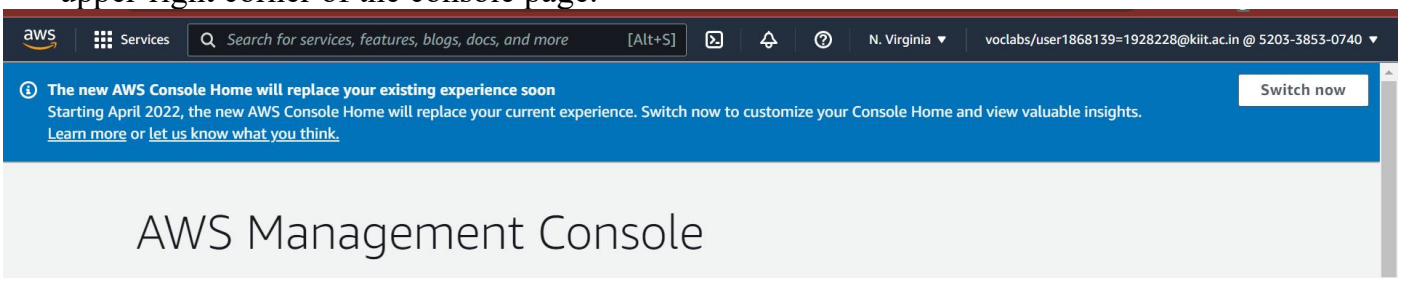
2. We go to https://aws.amazon.com , click on 'Sign in to Console', and login with our root account.



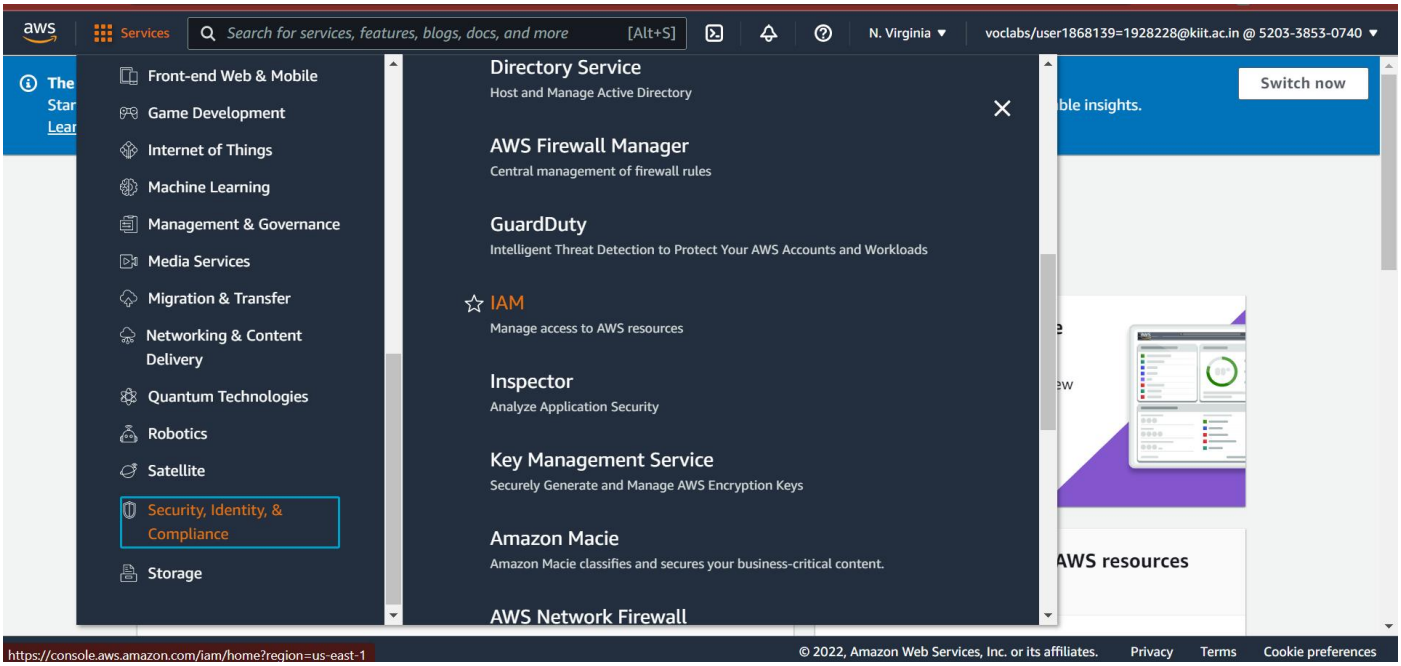


Explore the users and groups

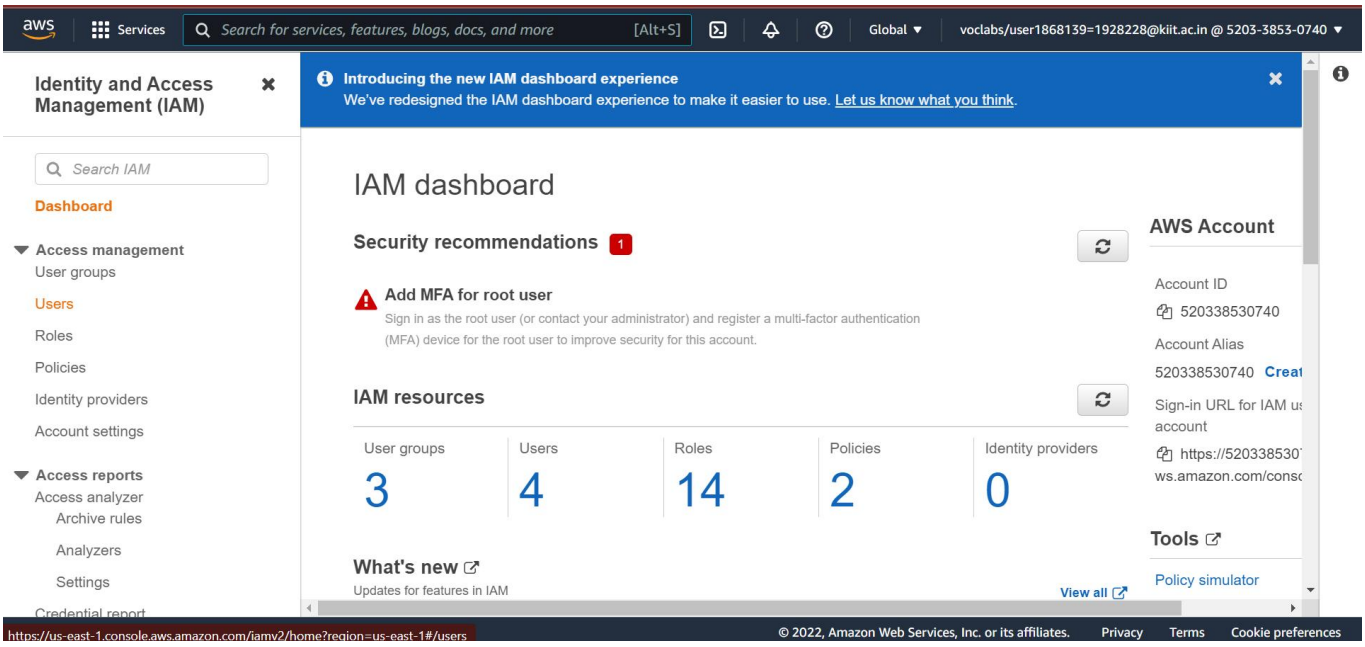
3. In this task, you will explore the users and groups that have already been created for you in IAM.
4. First, note the Region that you are in; for example, N. Virginia. The Region is displayed in the upper-right corner of the console page.



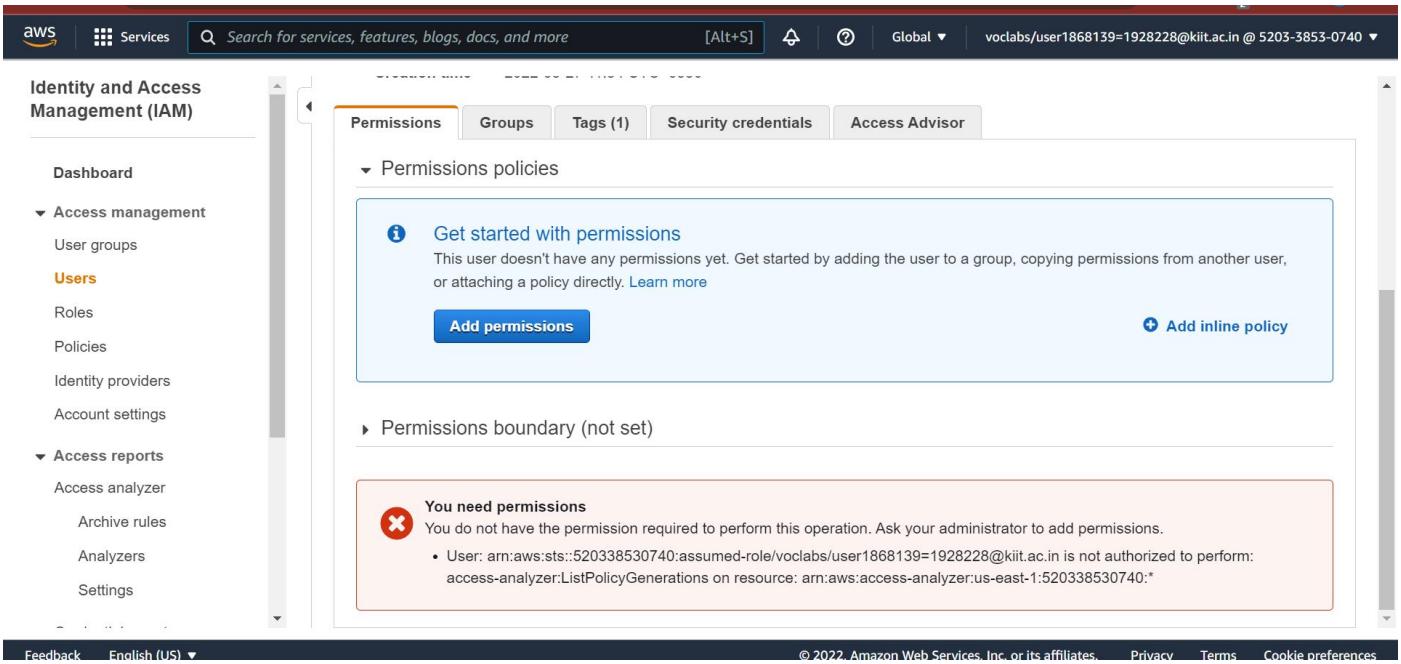
5. Choose the Services menu, locate the Security, Identity, & Compliance services, and choose IAM.



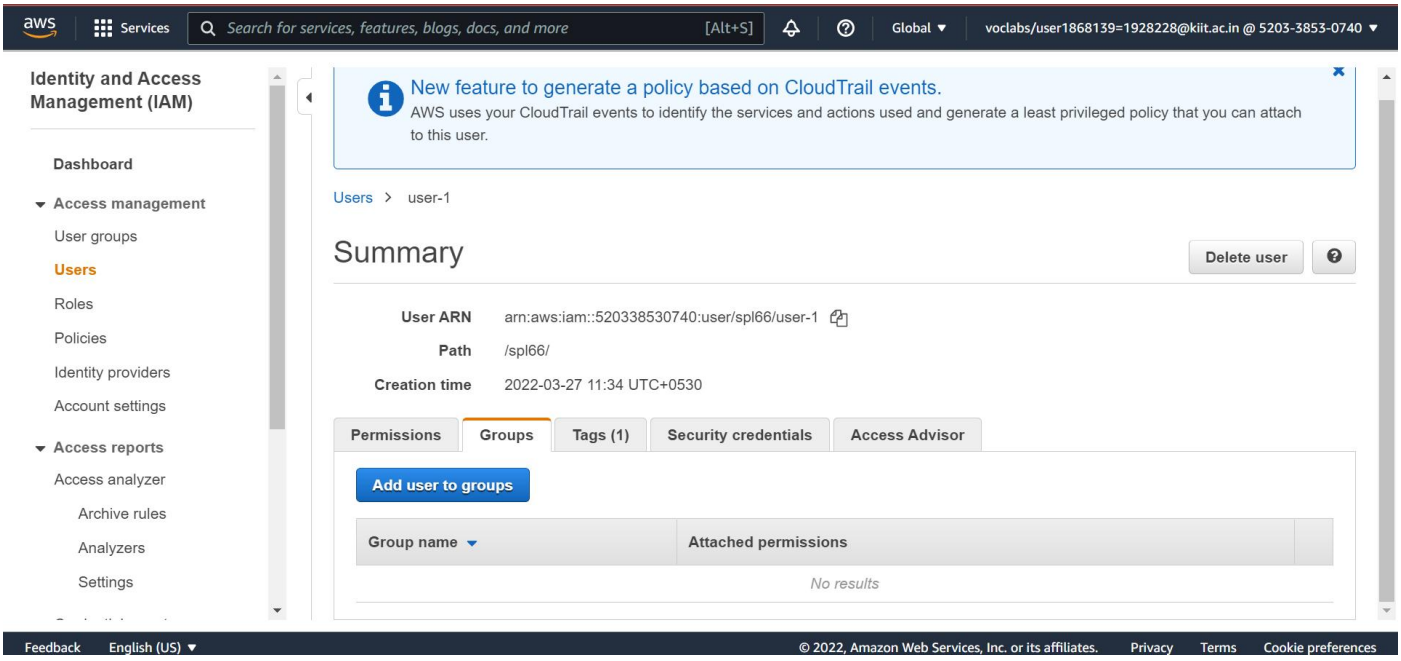
6. In the navigation pane on the left, choose Users.



7. The following IAM users have been created for you:
   a) user-1
   b) user-2
   c) user-3
8. Choose the name of user-1.
9. This brings you to a summary page for user-1. The Permissions tab will be displayed.

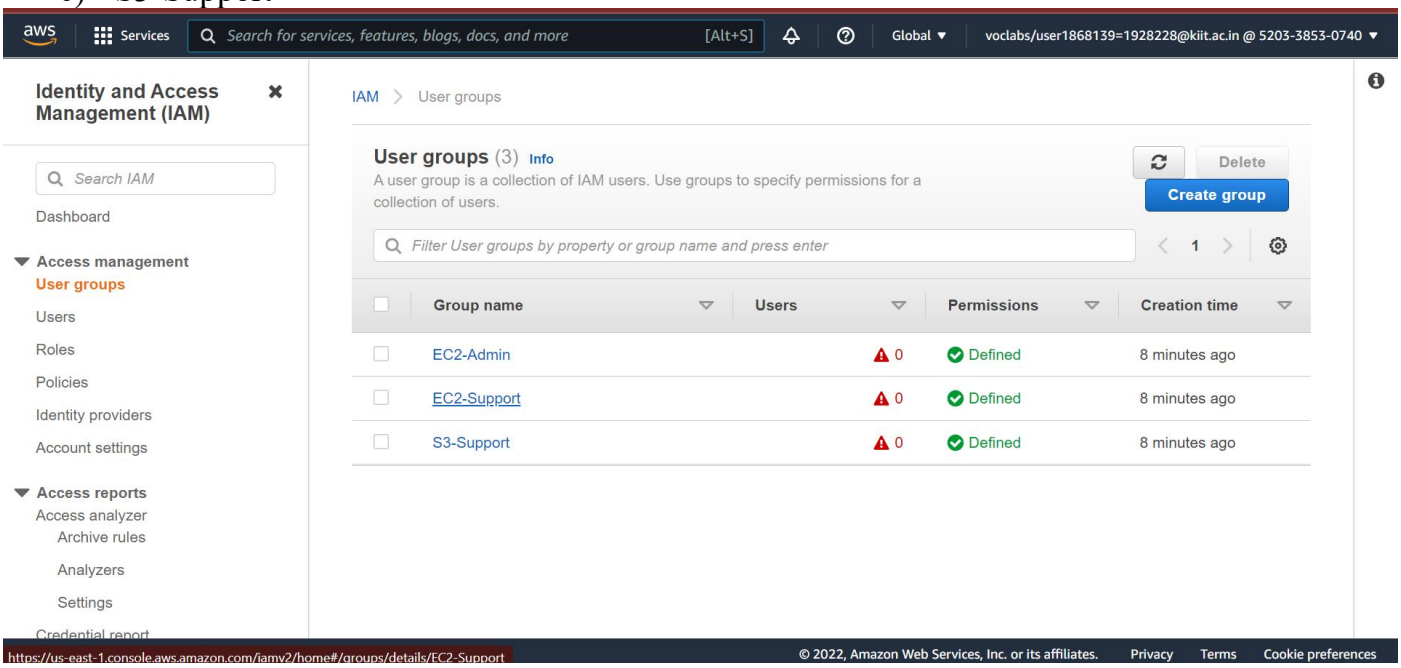


10. Notice that user-1 does not have any permissions.
11. Choose the Groups tab.
12. Notice that user-1 also is not a member of any groups.

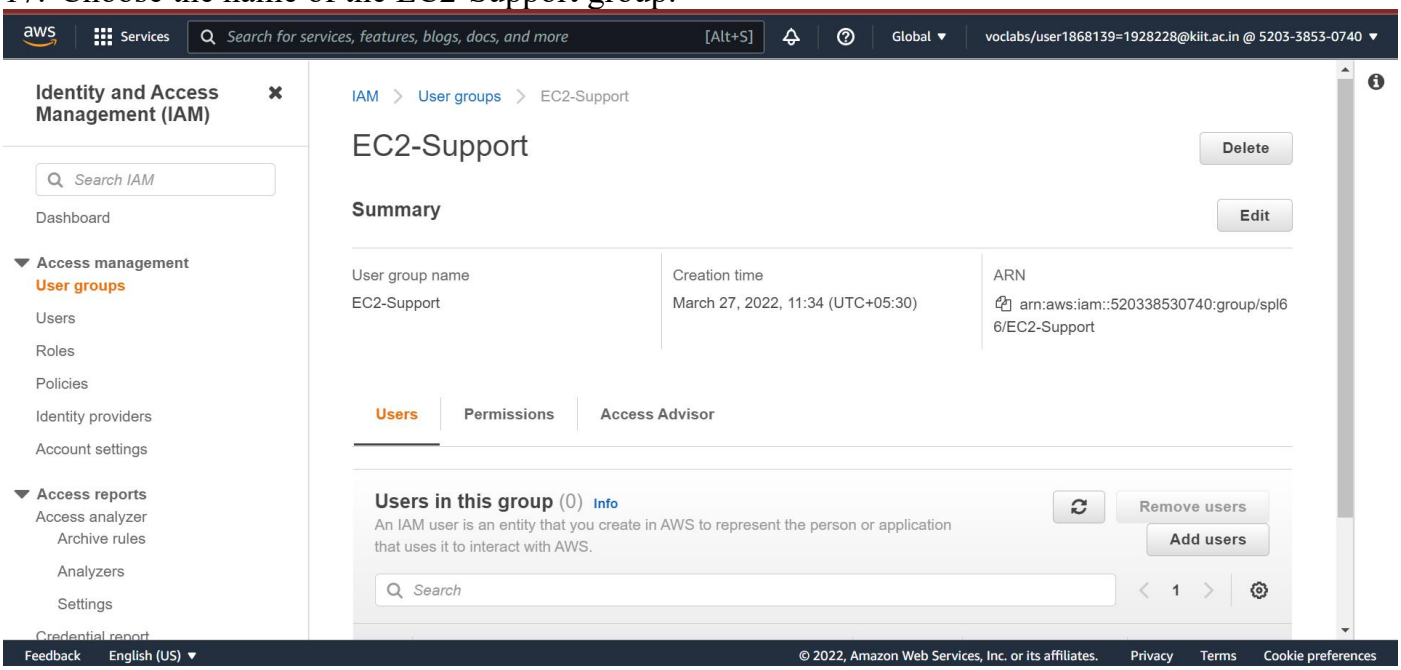


13. Choose the Security credentials tab.
14. Notice that user-1 is assigned a Console password. This allows the user to access the AWS Management Console.

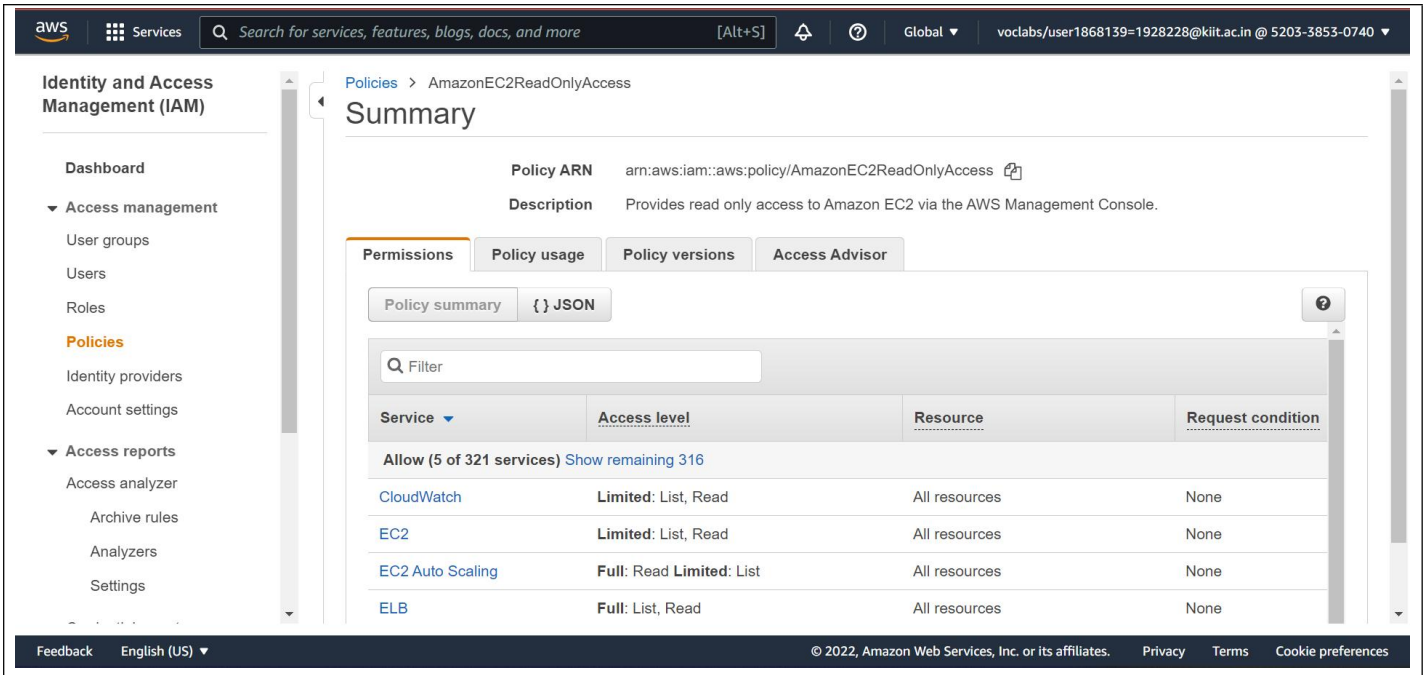
15. In the navigation pane on the left, choose User groups.
16. The following groups have already been created for you:
    a) EC2-Admin
    b) EC2-Support
    c) S3-Support



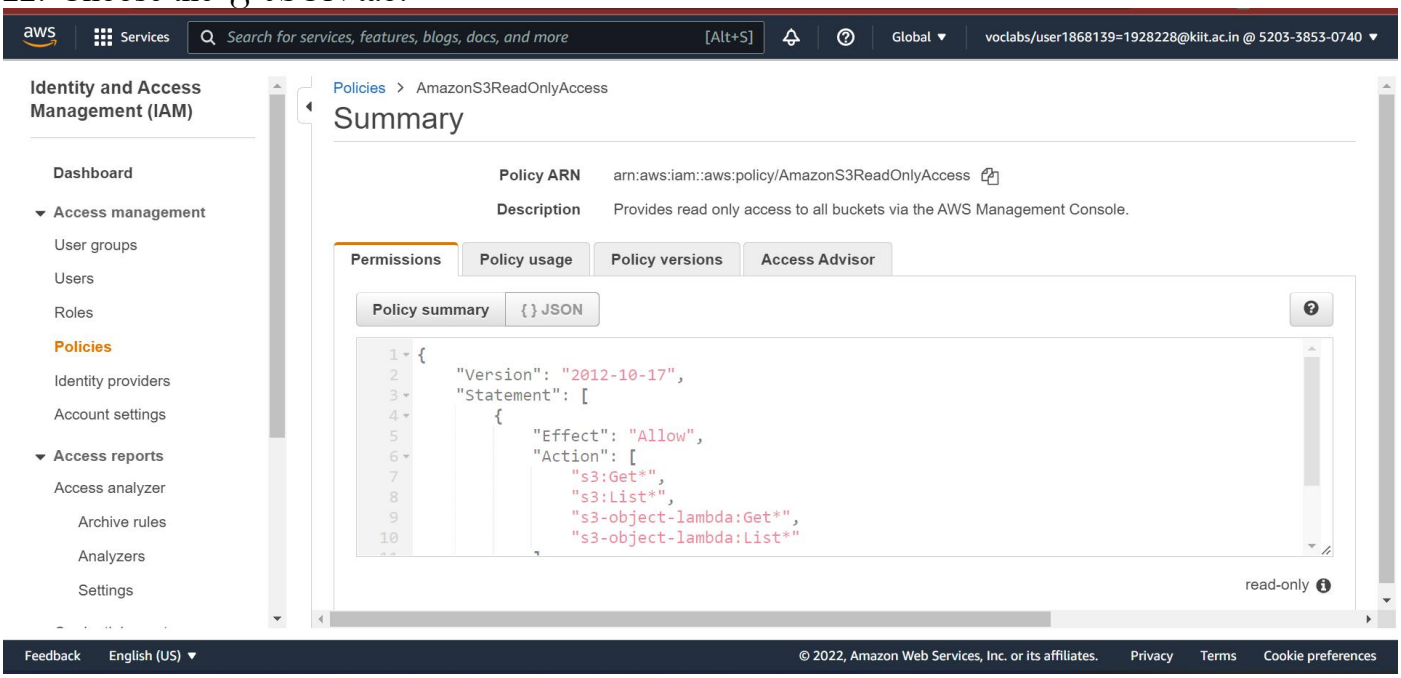
17. Choose the name of the EC2-Support group.



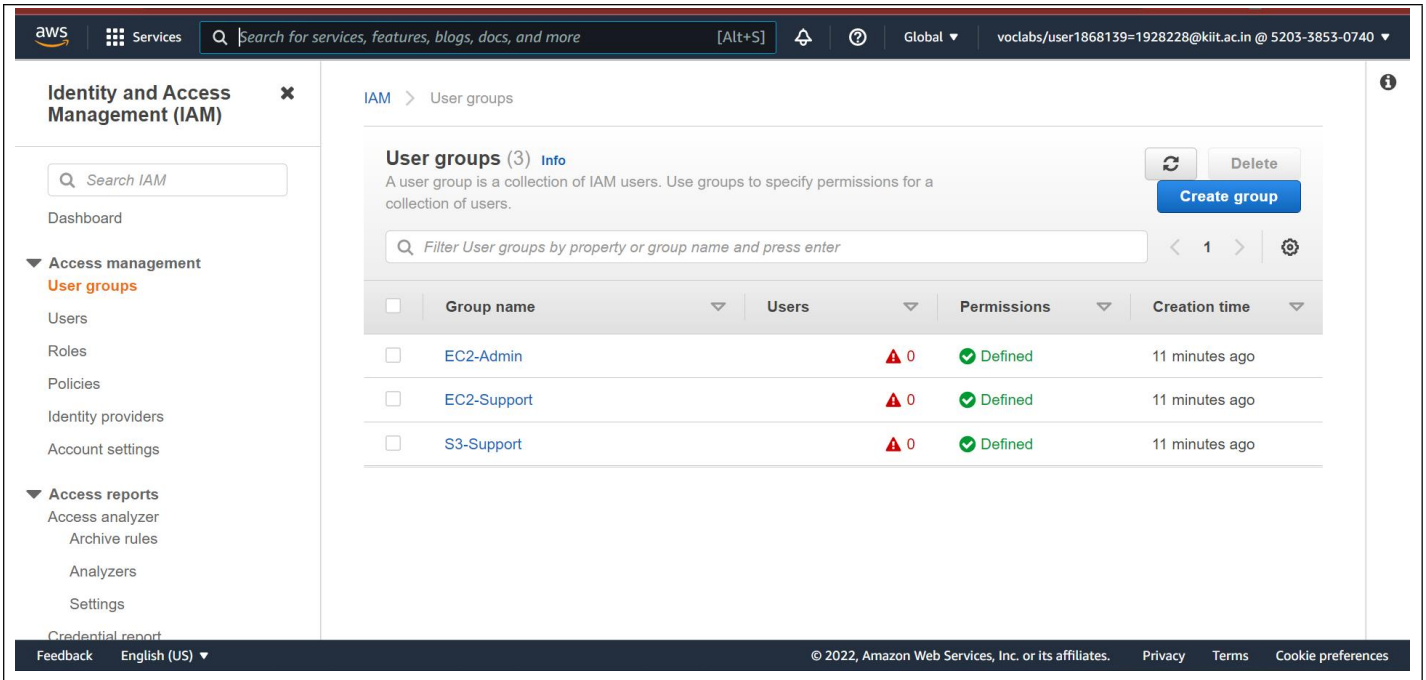
18. This brings you to the summary page for the EC2-Support group.
19. Choose the Permissions tab.
20. This group has a managed policy called AmazonEC2ReadOnlyAccess associated with it. Managed policies are prebuilt policies (built either by AWS or by your administrators) that can be attached to IAM users and groups. When the policy is updated, the changes to the policy are immediately applied against all users and groups that are attached to the policy.
21. Under Policy Name, choose the link for the AmazonEC2ReadOnlyAccess policy.



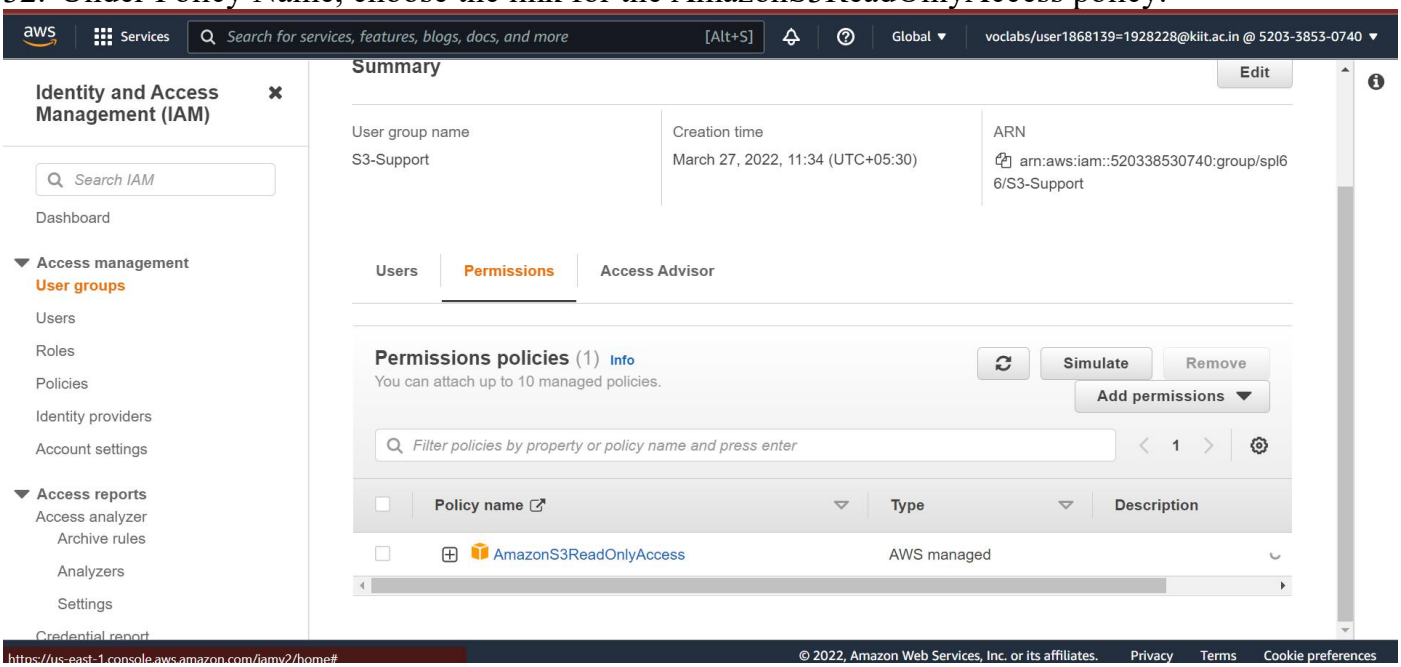
22. Choose the {} JSON tab.



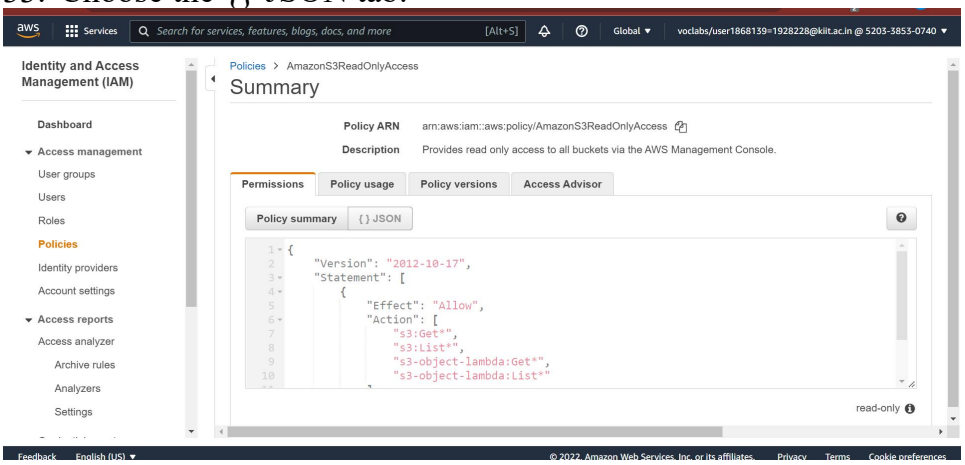
23. A policy defines what actions are allowed or denied for specific AWS resources. This policy is granting permission to List and Describe (view) information about Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing, Amazon CloudWatch, and Amazon EC2 Auto Scaling. This ability to view resources, but not modify them, is ideal for assigning to a support role.
24. Statements in an IAM policy have the following basic structure:
25. Effect says whether to Allow or Deny the permissions.
26. Action specifies the API calls that can be made against an AWS service (for example, cloudwatch:ListMetrics).
27. Resource defines the scope of entities covered by the policy rule (for example, a specific Amazon Simple Storage Service [Amazon S3] bucket or Amazon EC2 instance; an asterisk [*] means any resource).
28. In the navigation pane on the left, choose User groups.



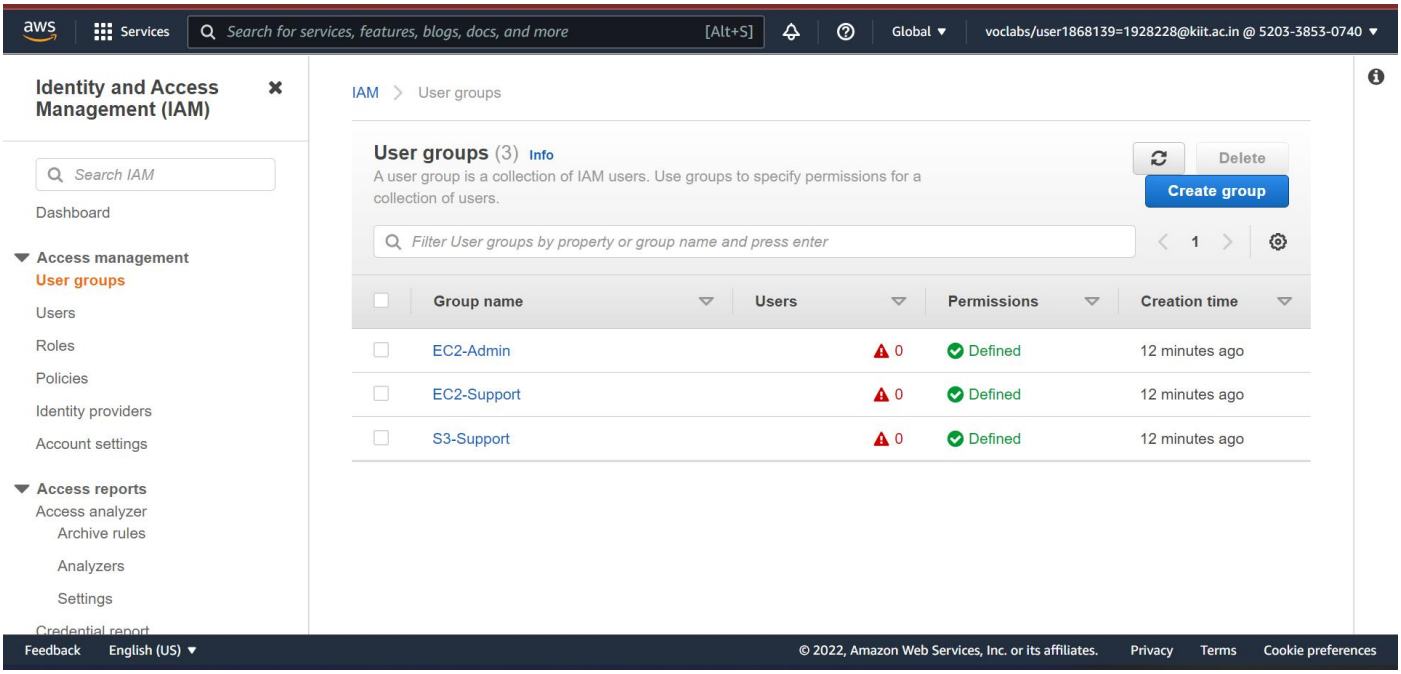
29. Choose the name of the S3-Support group.
30. Choose the Permissions tab.
31. The S3-Support group has the AmazonS3ReadOnlyAccess policy attached.
32. Under Policy Name, choose the link for the AmazonS3ReadOnlyAccess policy.



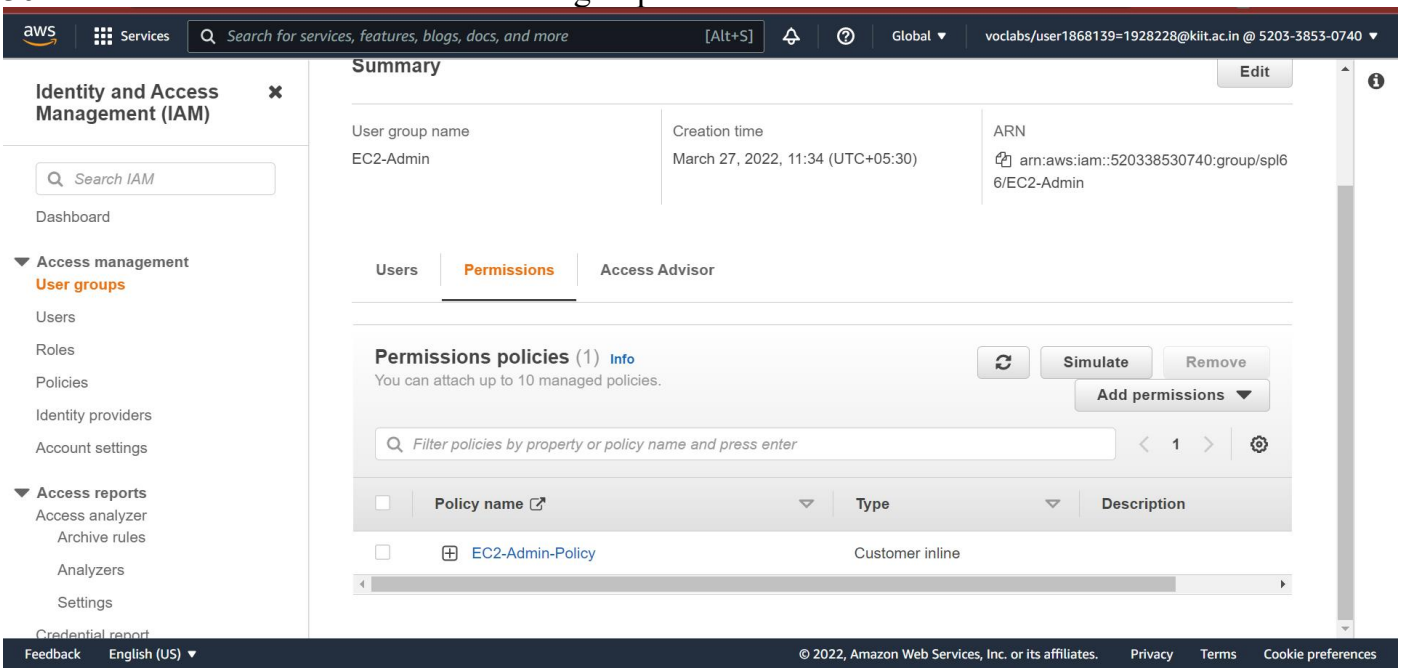
33. Choose the {} JSON tab.



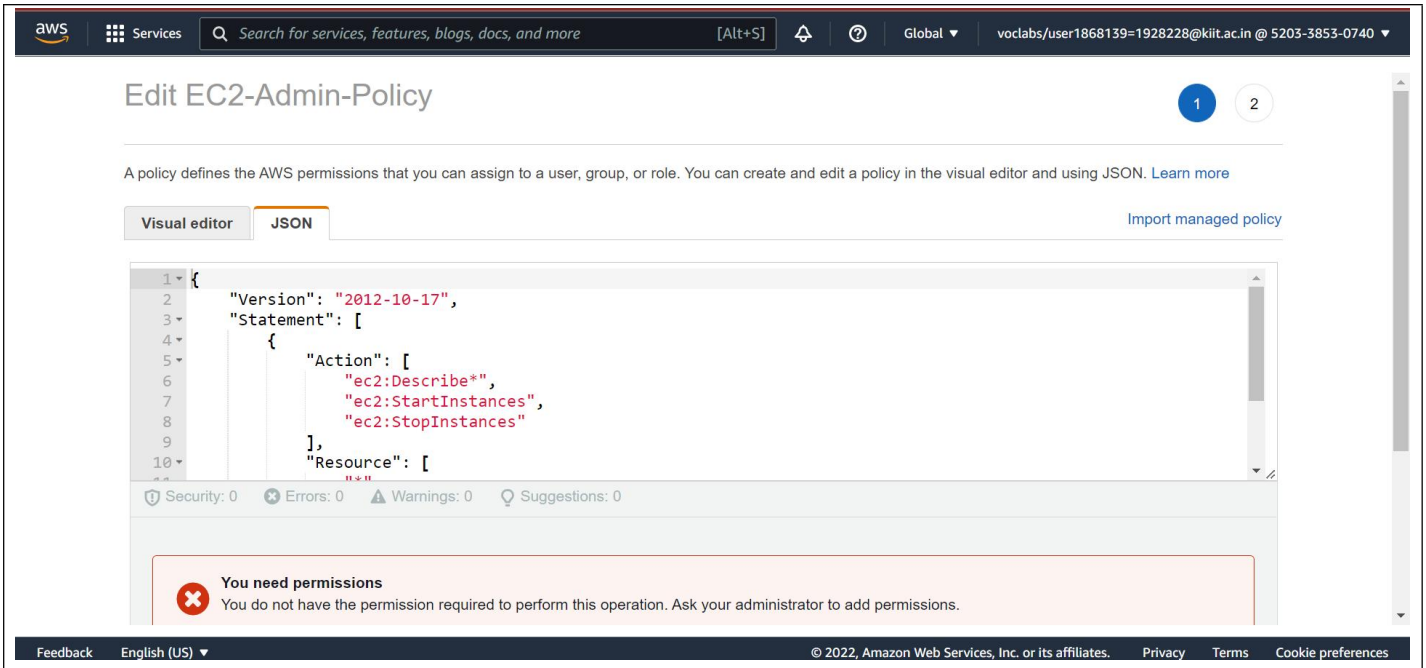
34. This policy has permissions to Get and List for all resources in Amazon S3.
35. In the navigation pane on the left, choose User groups.



36. Choose the name of the EC2-Admin group.



37. Choose the Permissions tab.
38. This group is different from the other two. Instead of a managed policy, the group has an inline policy, which is a policy assigned to just one user or group. Inline policies are typically used to apply permissions for specific situations.
39. Under Policy Name, choose the name of the EC2-Admin-Policy policy.
40. Choose the JSON tab.



41. This policy grants permission to Describe information about Amazon EC2 instances, and also the ability to Start and Stop instances.
42. At the bottom of the screen, choose Cancel to close the policy.

Business scenario

For the remainder of this lab, you will work with these users and groups to enable permissions that support the following business scenario.

Your company is growing its use of AWS services, and is using many Amazon EC2 instances and Amazon S3 buckets. You want to give access to new staff depending upon their job function, as indicated in the following table:

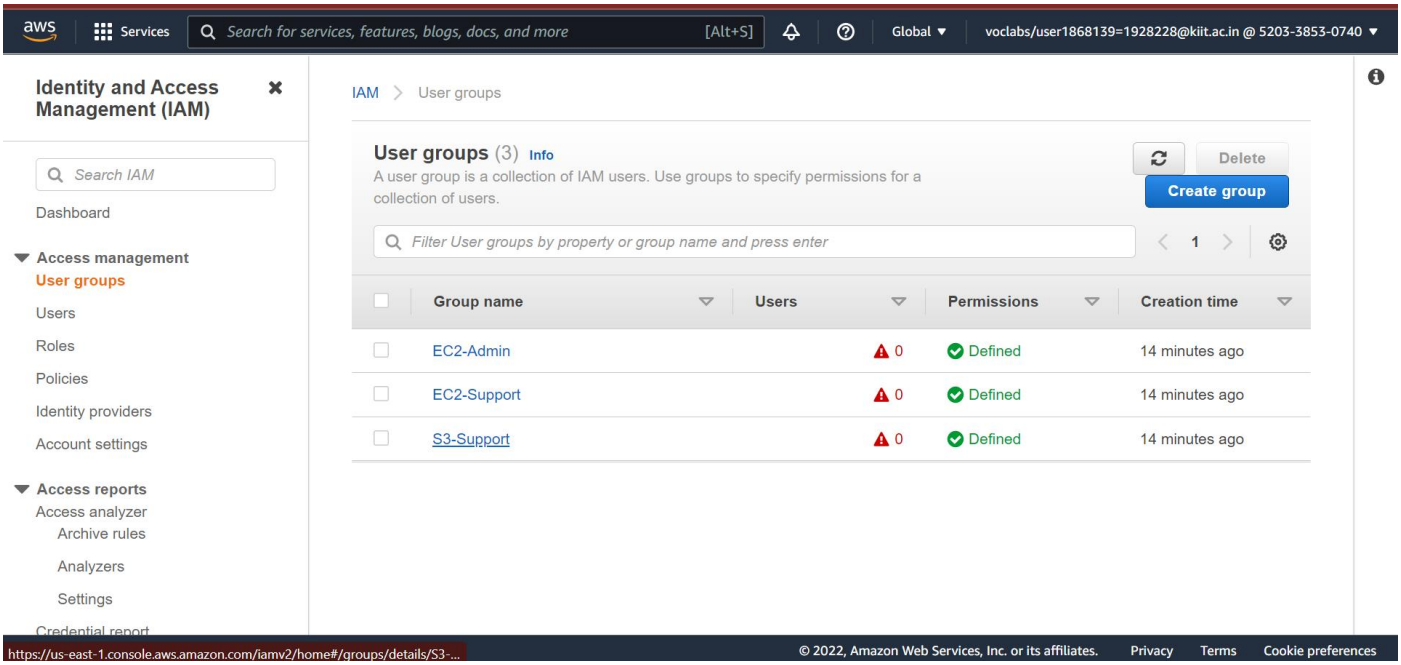
User	In Group	Permissions
user-1	S3-Support	Read-only access to Amazon S3
user-2	EC2-Support	Read-only access to Amazon EC2
user-3	EC2-Admin	View, Start, and Stop Amazon EC2 instances

Add users to groups

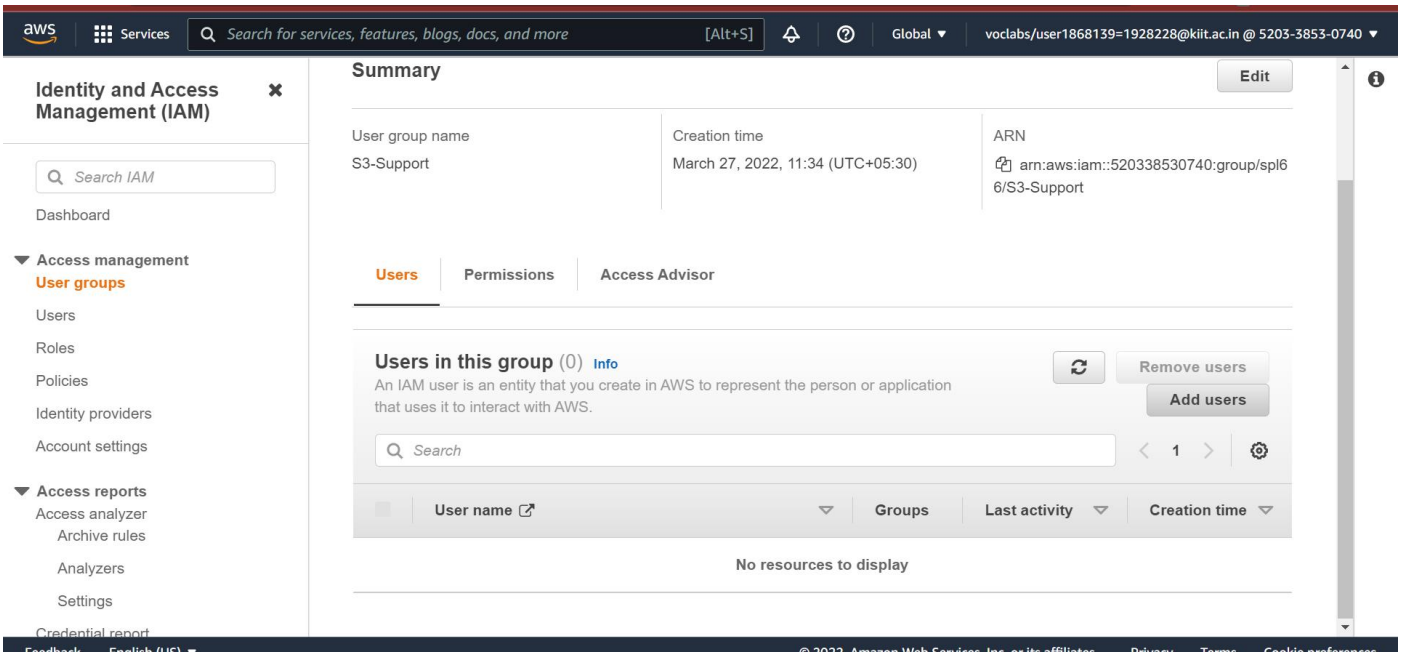
43. You have recently hired user-1 into a role where they will provide support for Amazon S3. You will add them to the S3-Support group so that they inherit the necessary permissions via the attached AmazonS3ReadOnlyAccess policy.
44. Ignore any "not authorized" errors that appear during this task. They are caused by your lab account having limited permissions and will not impact your ability to complete the lab.

Add user-1 to the S3-Support group

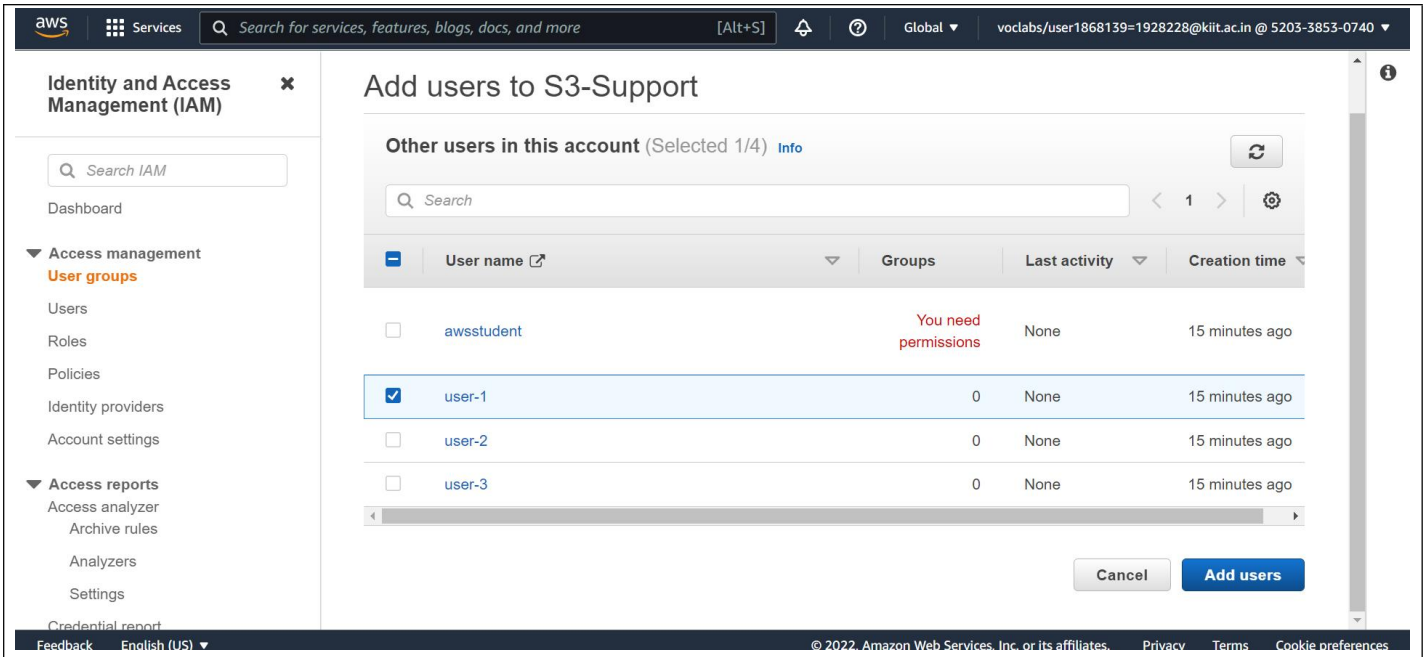
45. In the left navigation pane, choose User groups.
46. Choose the name of the S3-Support group.

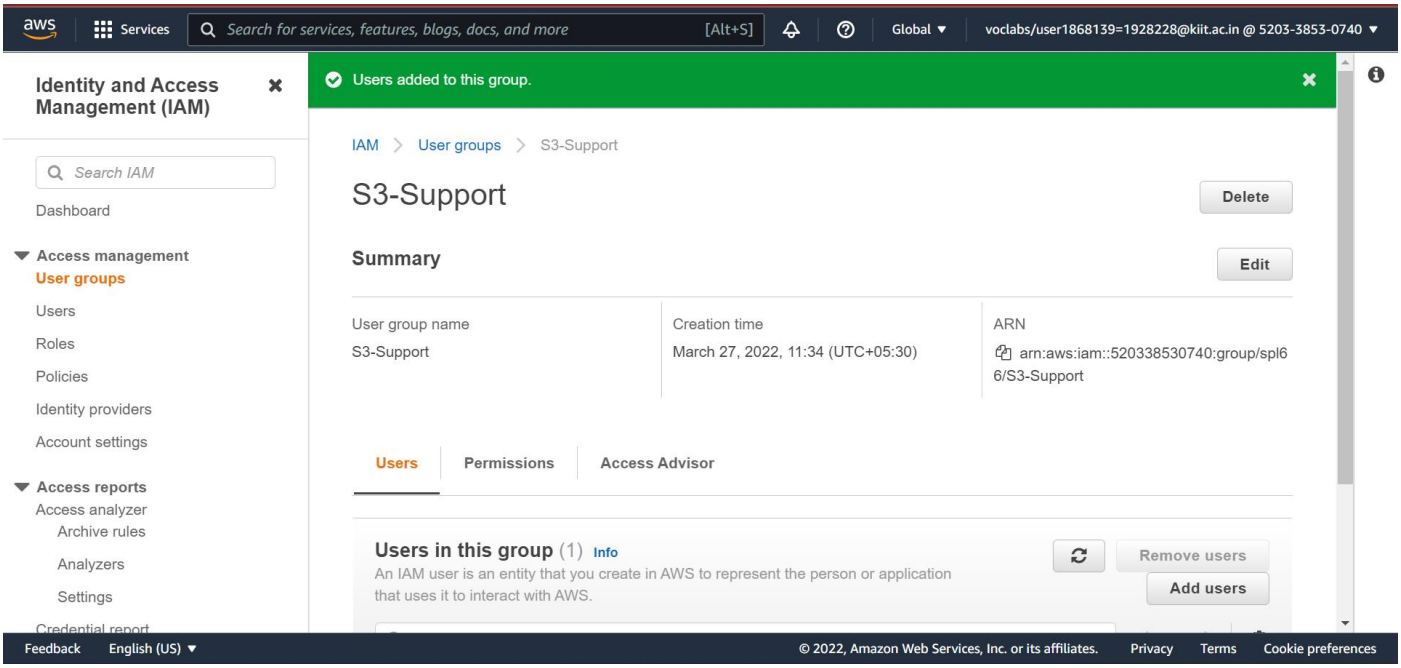


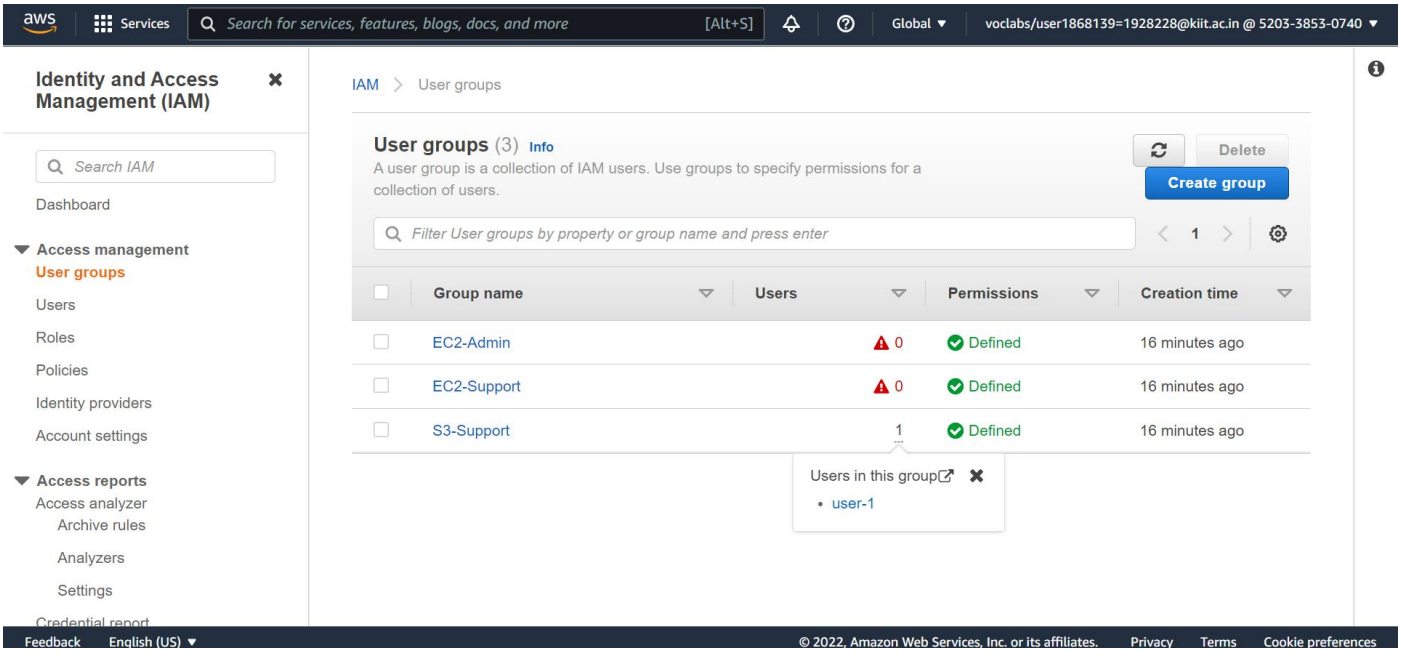
47. On the Users tab, choose Add users.
48. Select user-1, and choose Add users.



49. On the Users tab, notice that user-1 has been added to the group.

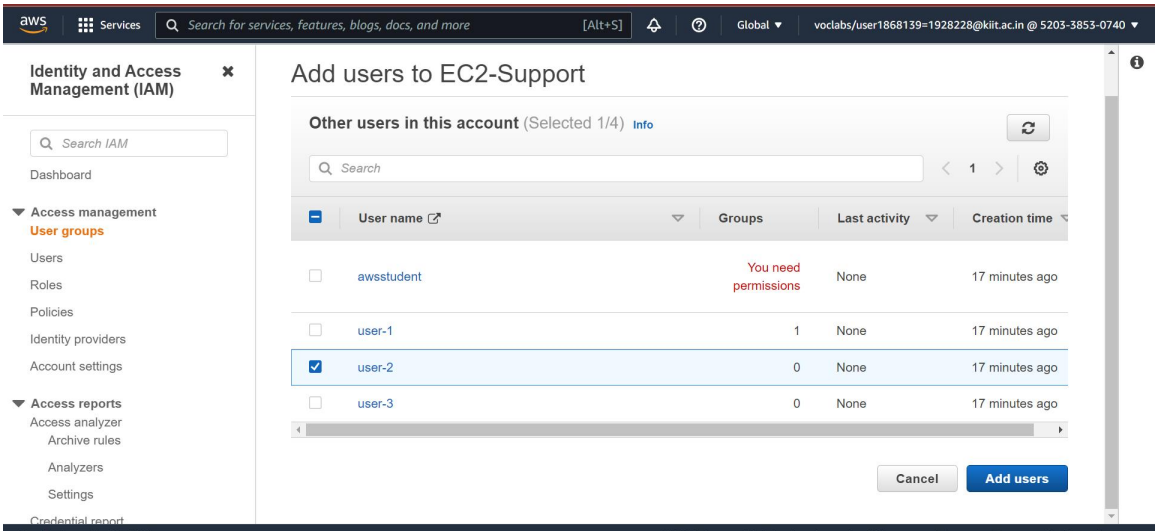

Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
voclabs/user1868139=1928228@kiit.ac.in @ 5203-3853-0740
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Add users to S3-Support
Other users in this account (Selected 1/4) Info
Search
1
User name
Groups
Last activity
Creation time
awsstudent
You need permissions
None
15 minutes ago
user-1
0
None
15 minutes ago
user-2
0
None
15 minutes ago
user-3
0
None
15 minutes ago
Cancel
Add users
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

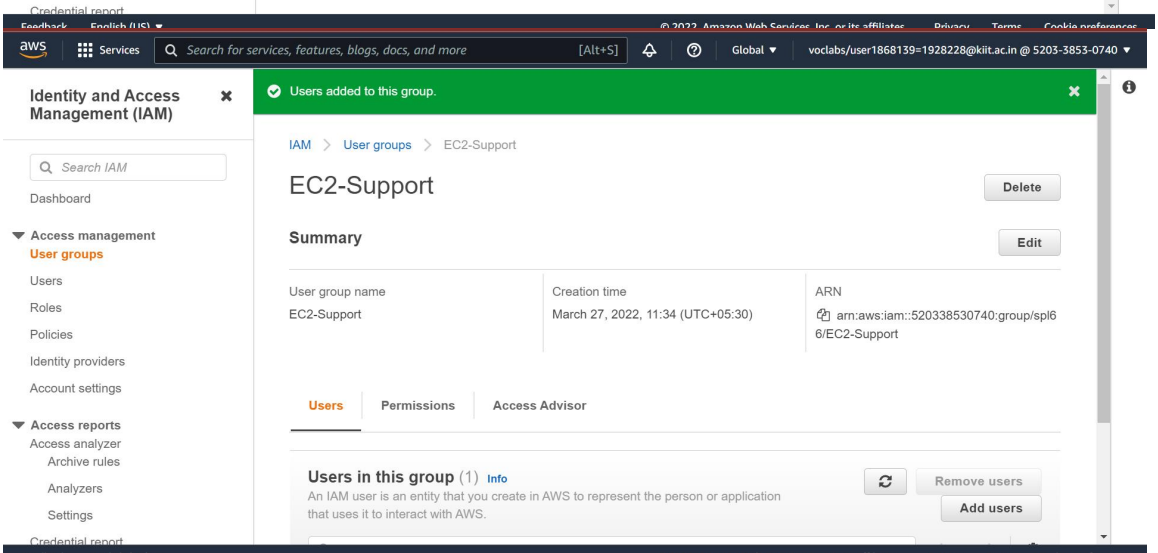

Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
voclabs/user1868139=1928228@kiit.ac.in @ 5203-3853-0740
Identity and Access Management (IAM)
Users added to this group.
IAM > User groups > S3-Support
S3-Support
Delete
Summary
Edit
User group name
S3-Support
Creation time
March 27, 2022, 11:34 (UTC+05:30)
ARN
arn:aws:iam::520338530740:group/spl66/S3-Support
Users
Permissions
Access Advisor
Users in this group (1) Info
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.
Remove users
Add users
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

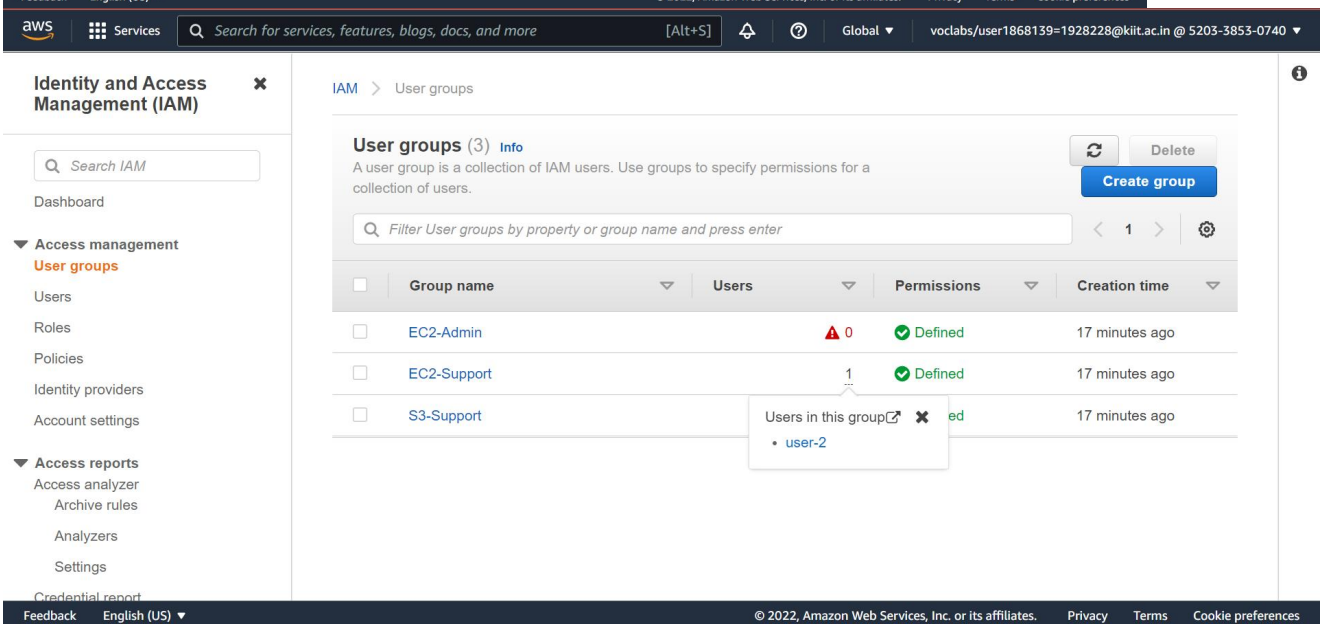

Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
voclabs/user1868139=1928228@kiit.ac.in @ 5203-3853-0740
Identity and Access Management (IAM)
IAM > User groups
User groups (3) Info
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.
Delete
Create group
Filter User groups by property or group name and press enter
1
Group name
Users
Permissions
Creation time
EC2-Admin
0
Defined
16 minutes ago
EC2-Support
0
Defined
16 minutes ago
S3-Support
1
Defined
16 minutes ago
Users in this group
user-1
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Add user-2 to the EC2-Support group

50. You have hired user-2 into a role where they will provide support for Amazon EC2. You will add them to the EC2-Support group so that they inherit the necessary permissions via the attached AmazonEC2ReadOnlyAccess policy.
51. Use what you learned from the previous steps to add user-2 to the EC2-Support group.
52. user-2 should now be part of the EC2-Support group.

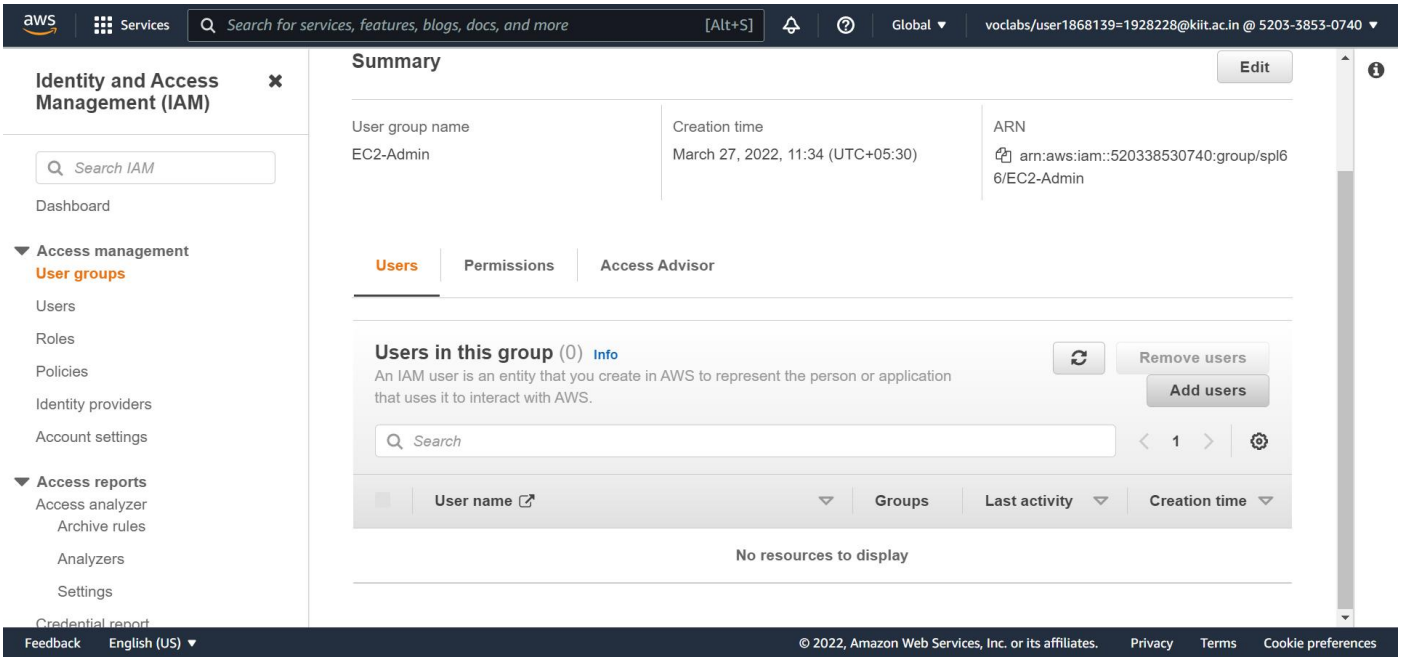




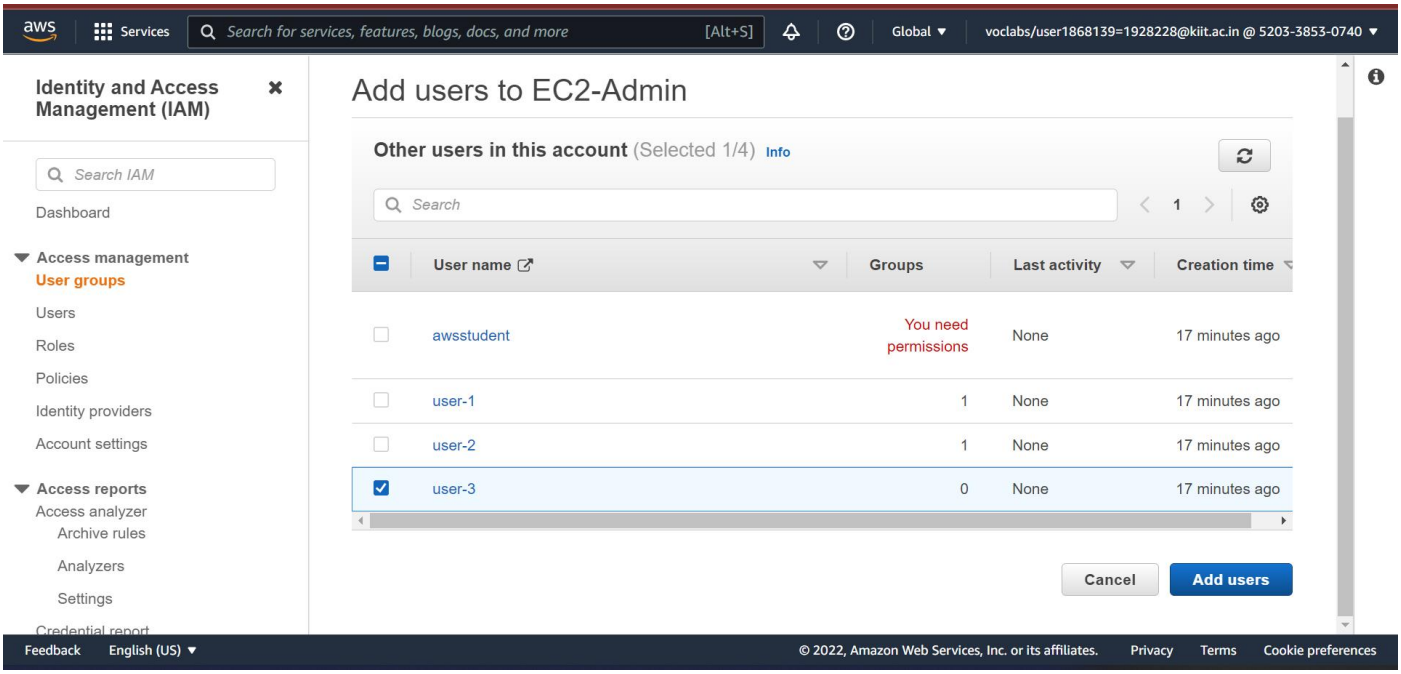


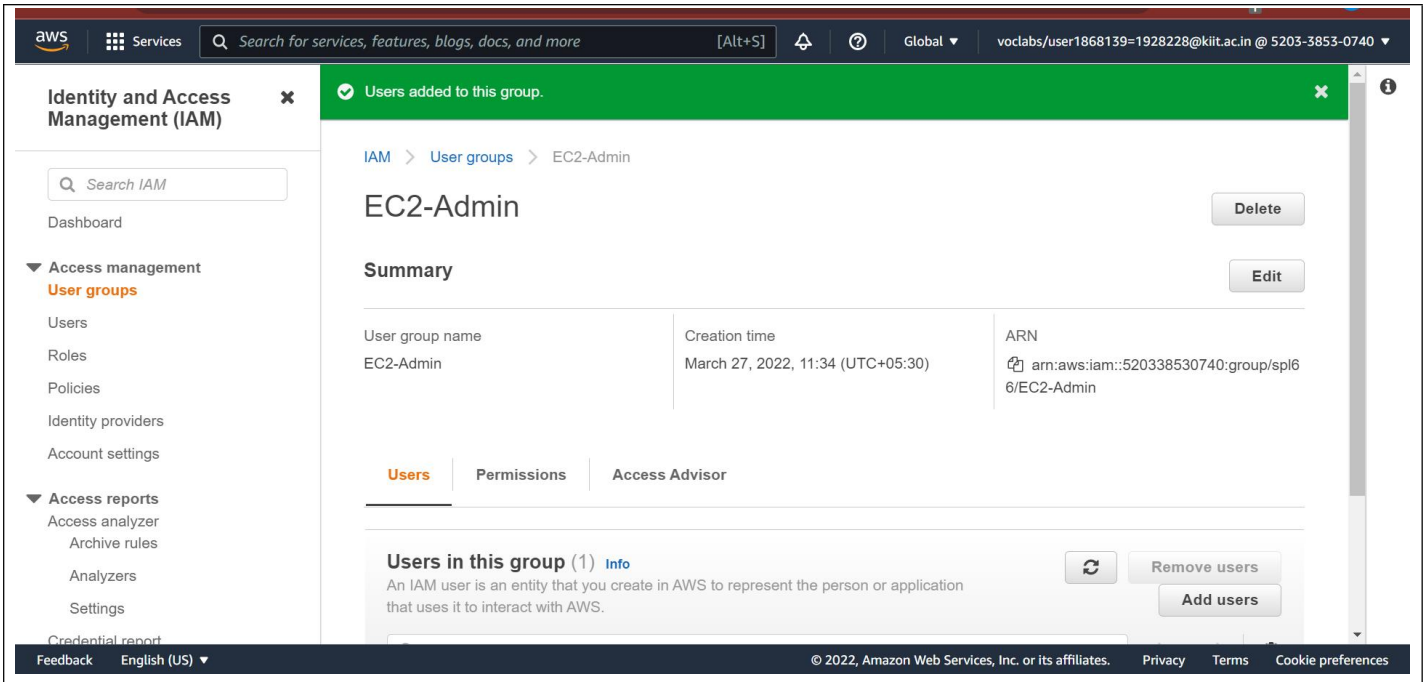
Add user-3 to the EC2-Admin group

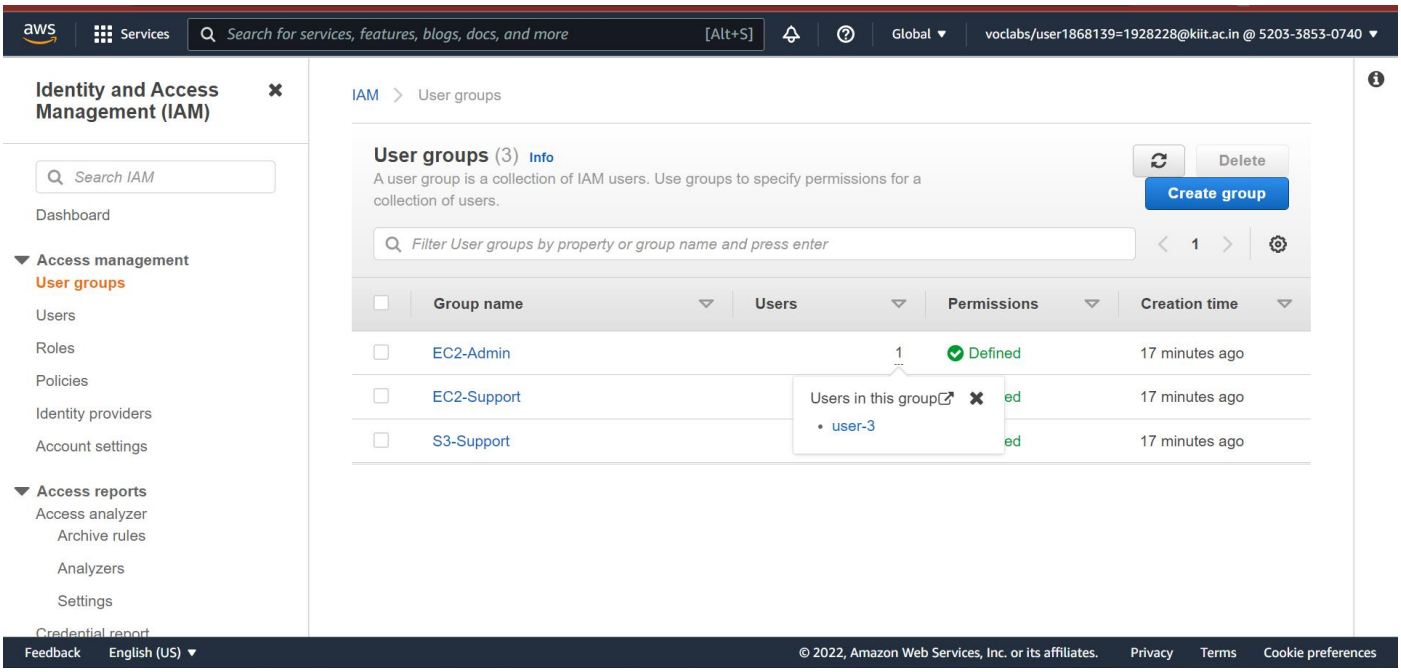
53. You have hired user-3 as your Amazon EC2 administrator to manage your EC2 instances. You will add them to the EC2-Admin group so that they inherit the necessary permissions via the attached EC2-Admin-Policy.
54. Use what you learned from the previous steps to add user-3 to the EC2-Admin group.



55. user-3 should now be part of the EC2-Admin group.
56.In the navigation pane on the left, choose User groups.
57. Each group should have a 1 in the Users column. This indicates the number of users in each group.





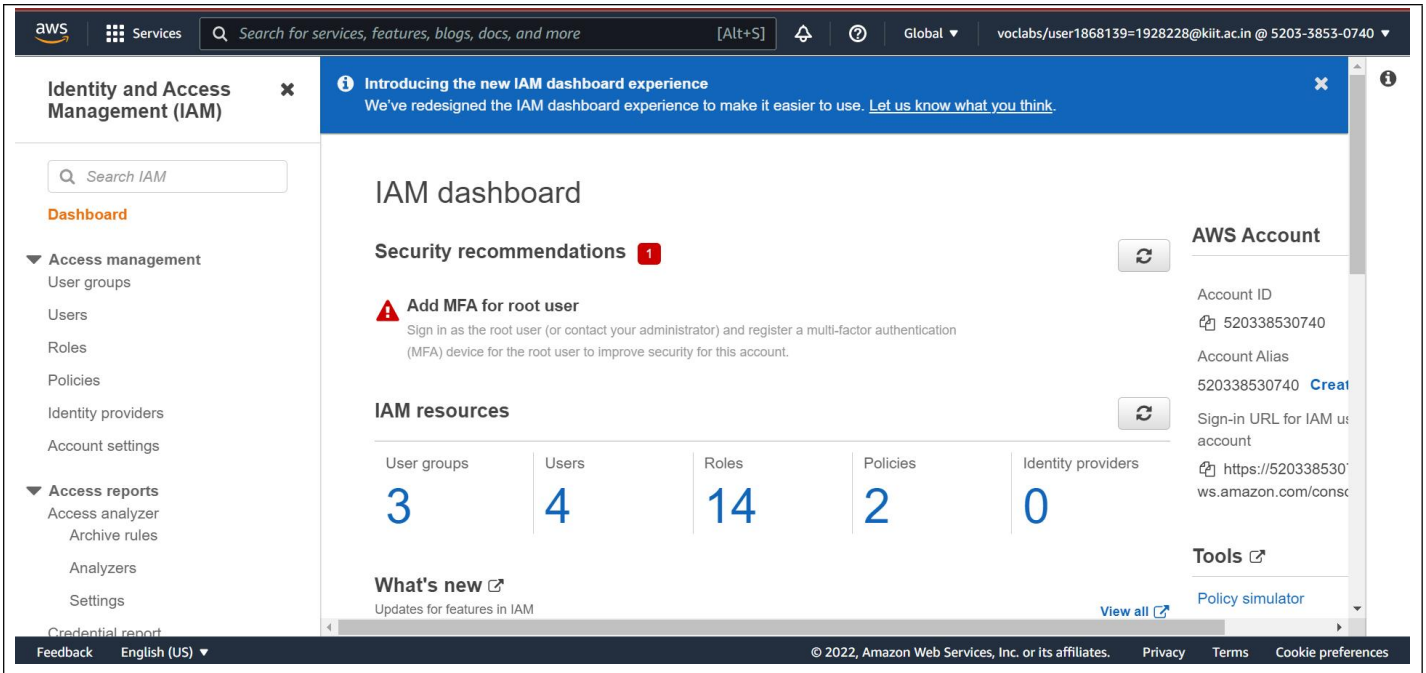


58. If you do not have a 1 for the Users column for a group, revisit the previous steps to ensure that each user is assigned to a group, as shown in the table in the Business scenario section.

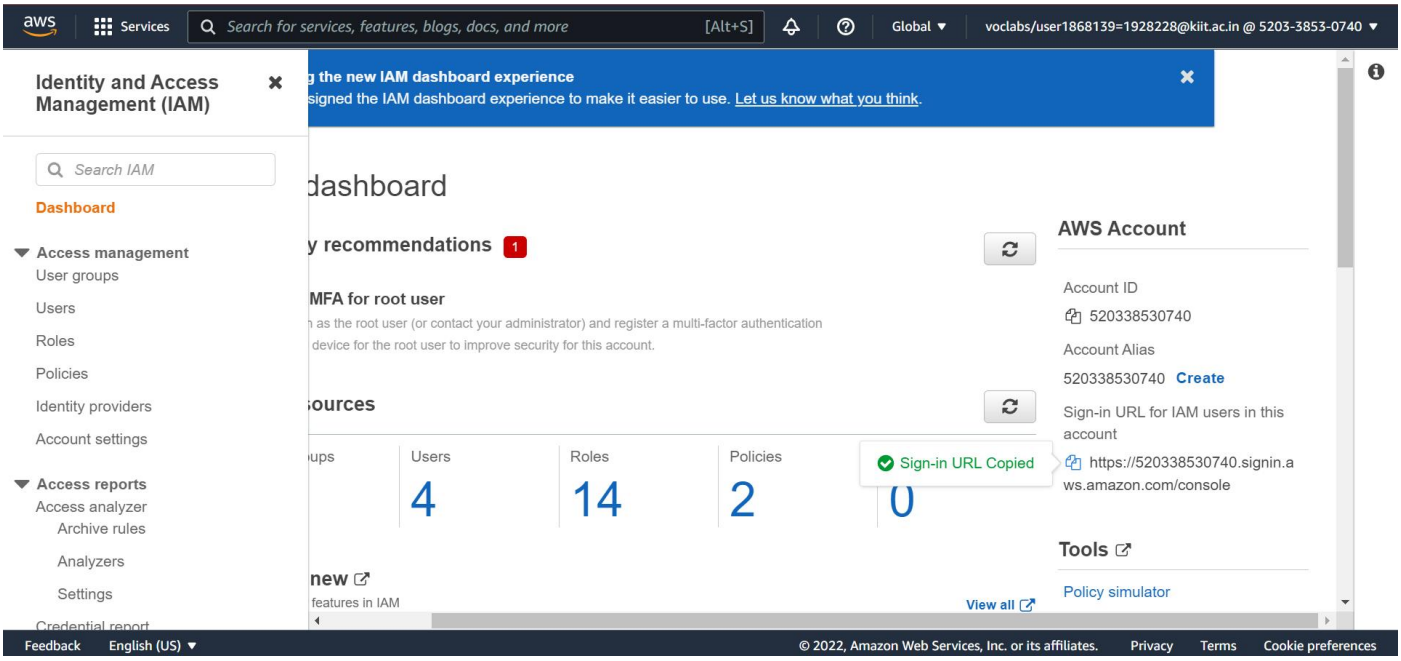
Sign in and test users

In this task, you will test the permissions of each IAM user in the console.

59. Get the console sign-in URL
60. In the navigation pane on the left, choose Dashboard.



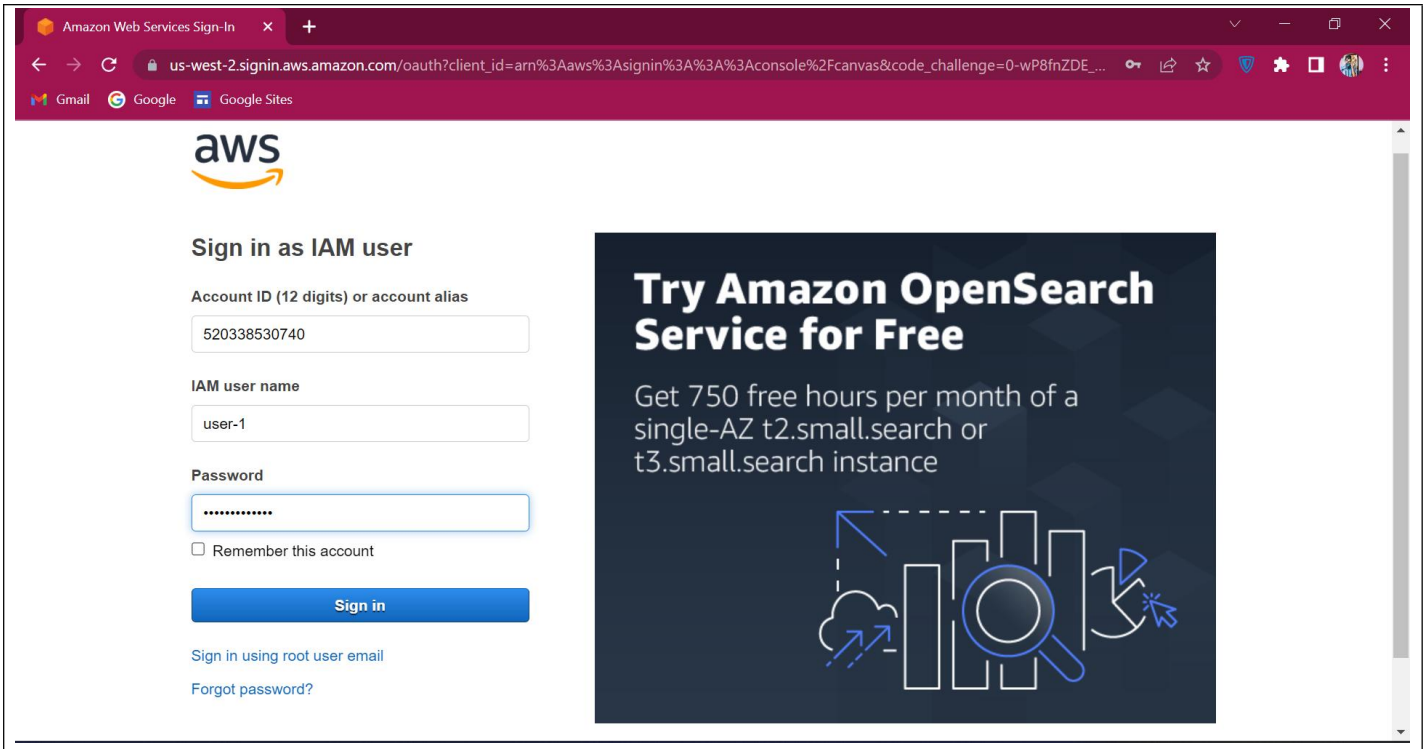
61. Notice the Sign-in URL for IAM users in this account section at the top of the page. The sign-in URL looks similar to the following: https://123456789012.signin.aws.amazon.com/console

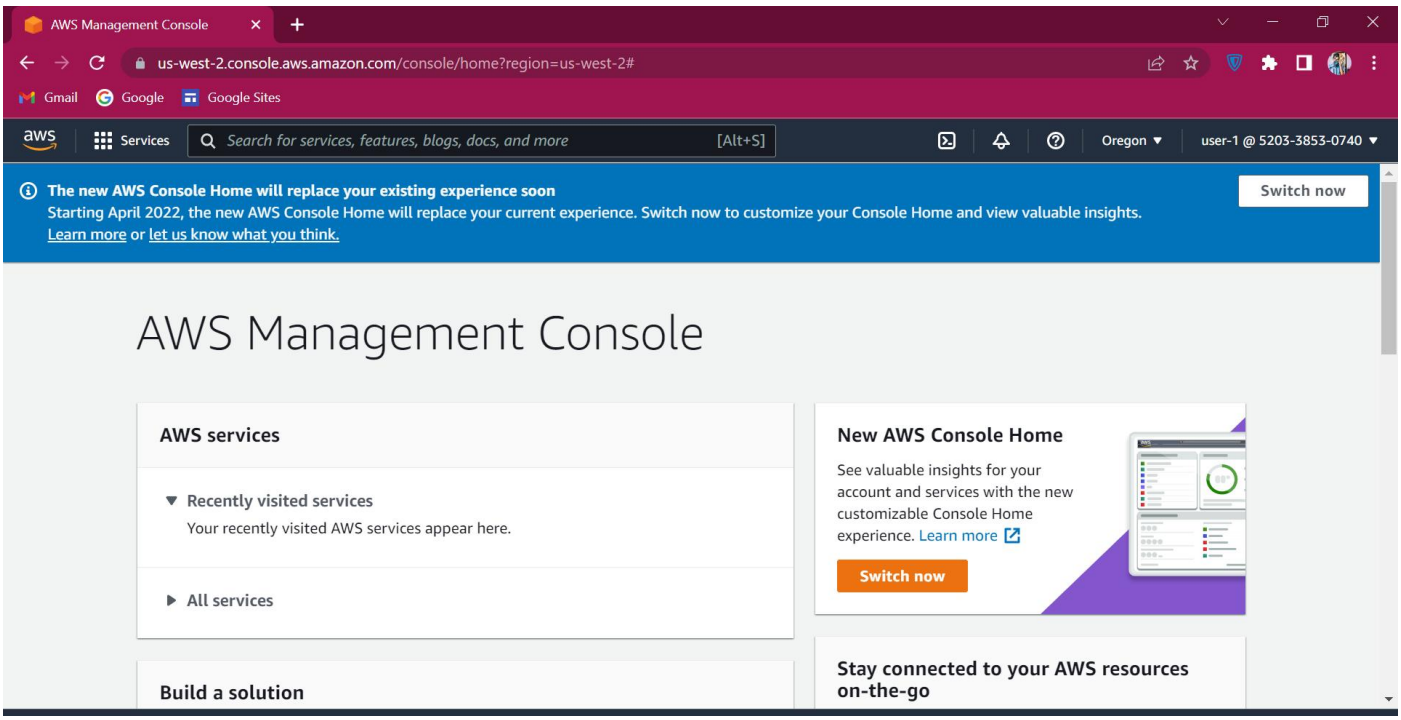


62. This link can be used to sign in to the AWS account that you are currently using.
63. Copy the sign-in link to a text editor.
    https://520338530740.signin.aws.amazon.com/console

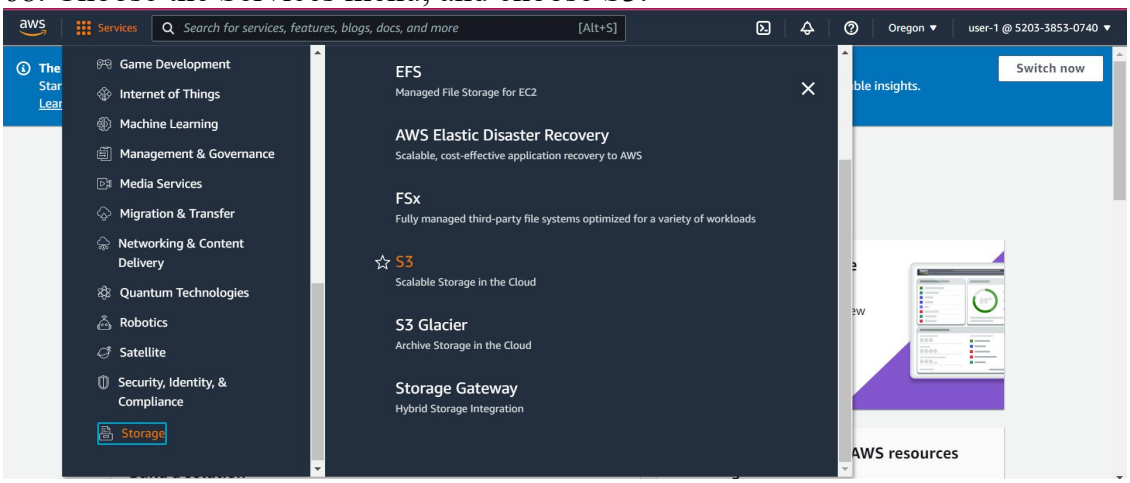
Test user-1 permissions

64. Open a private or incognito window in your browser.
65. Paste the sign-in link into the private browser, and press ENTER.
66. You will now sign-in as user-1, who has been hired as your Amazon S3 storage support staff.
67. Sign in with the following credentials:
    a) IAM user name: user-1
    b) Password: Lab-Password1

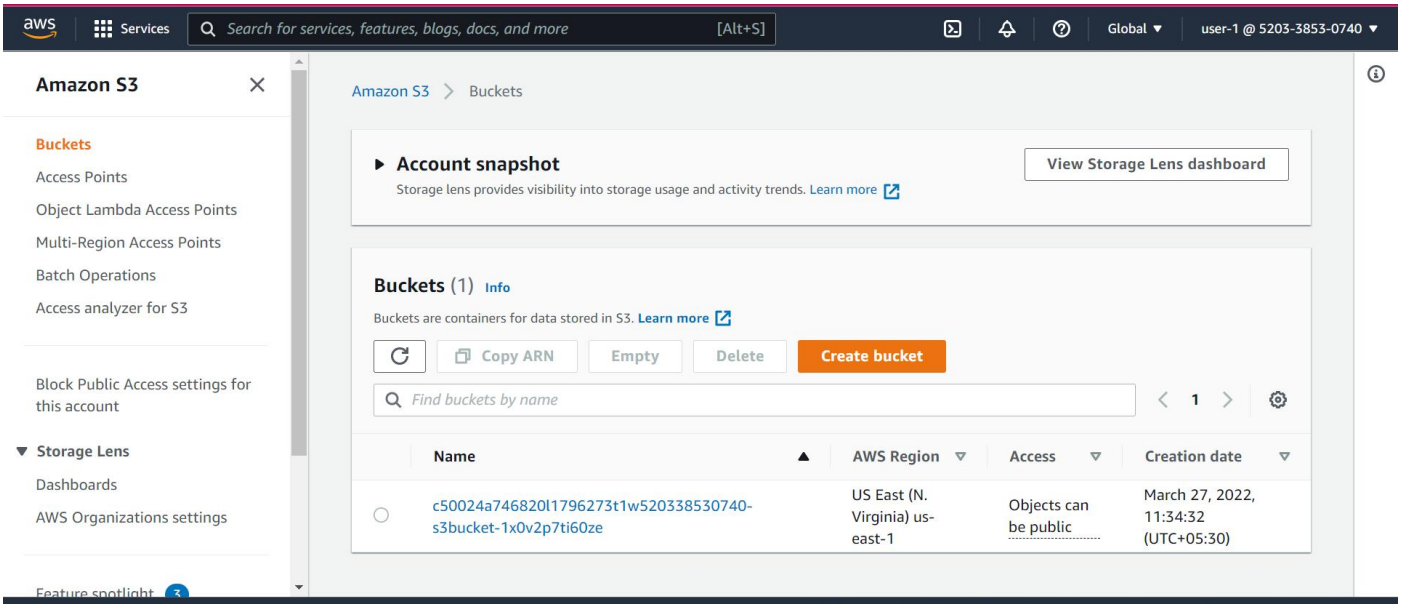


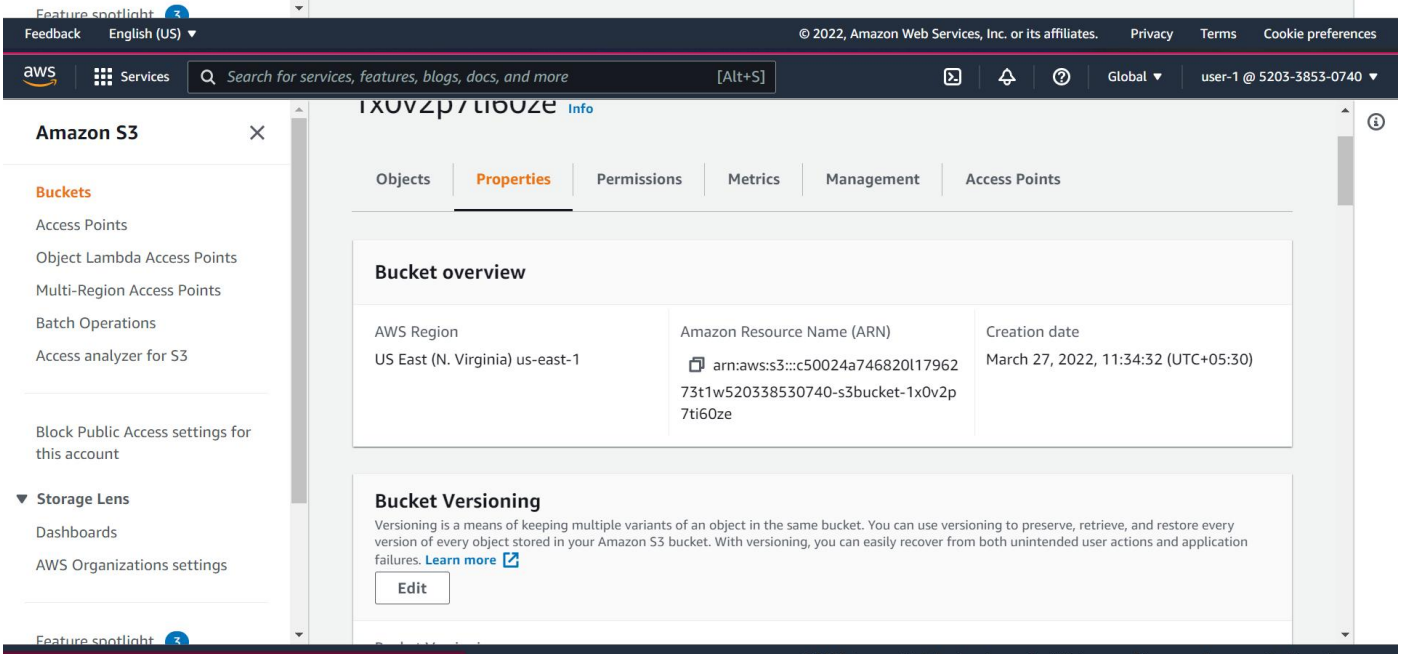


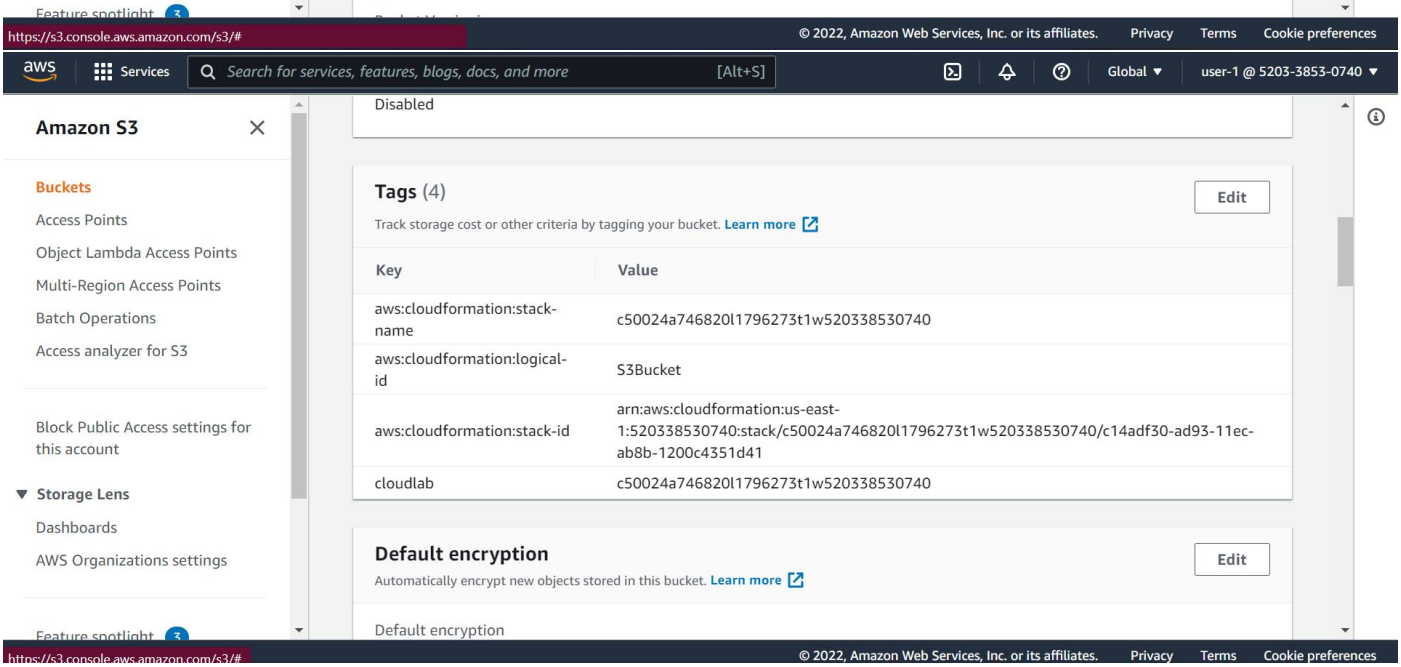
68. Choose the Services menu, and choose S3.



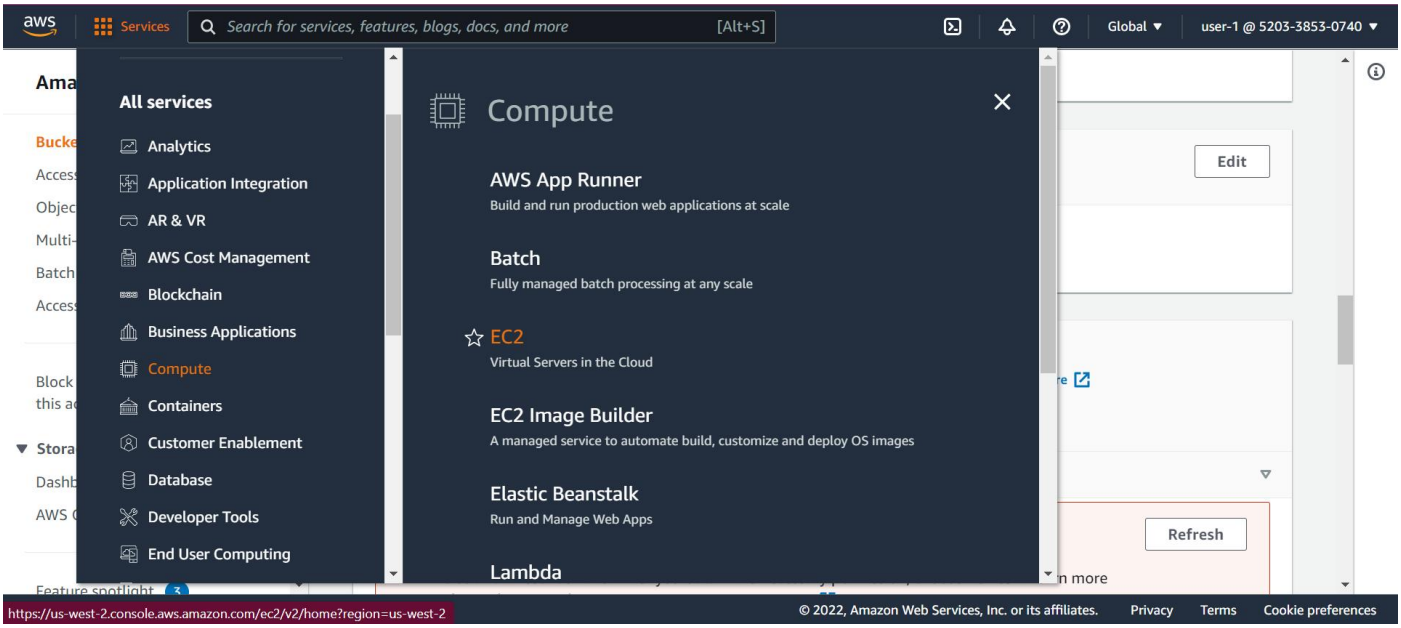
69. Choose the name of one of your buckets, and browse the contents.
70. Because this user is part of the S3-Support group in IAM, they have permissions to view a list of Amazon S3 buckets and their contents.



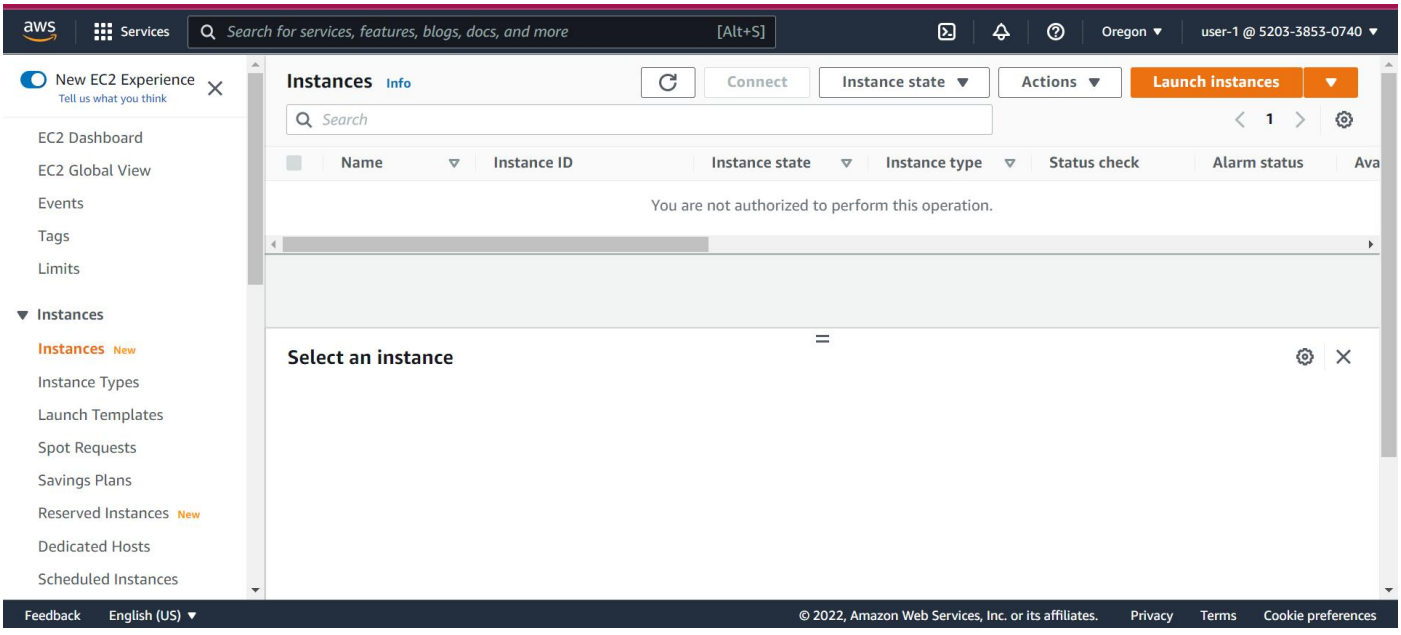




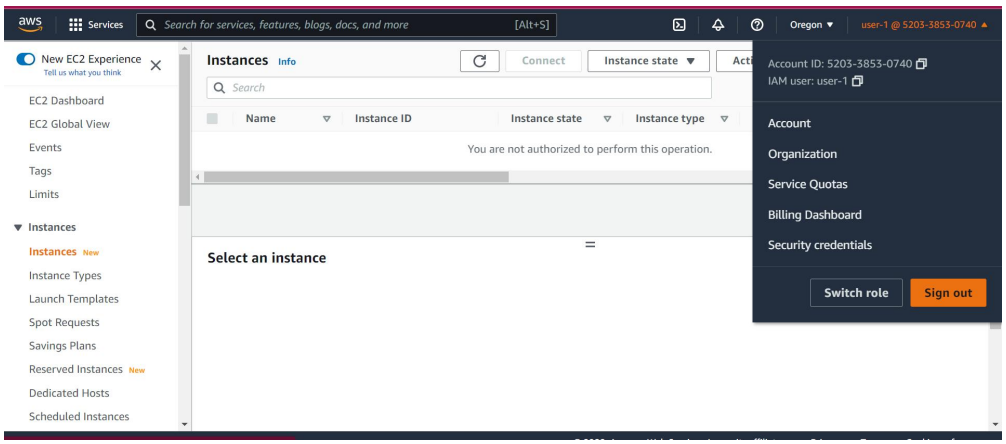
71. Now, test whether the user has access to Amazon EC2.
72. Choose the Services menu, and choose EC2.



73. In the left navigation pane, choose Instances
74. You cannot see any instances. Instead, an error message says you are not authorized to perform this operation. This user has not been assigned any permissions to use Amazon EC2.

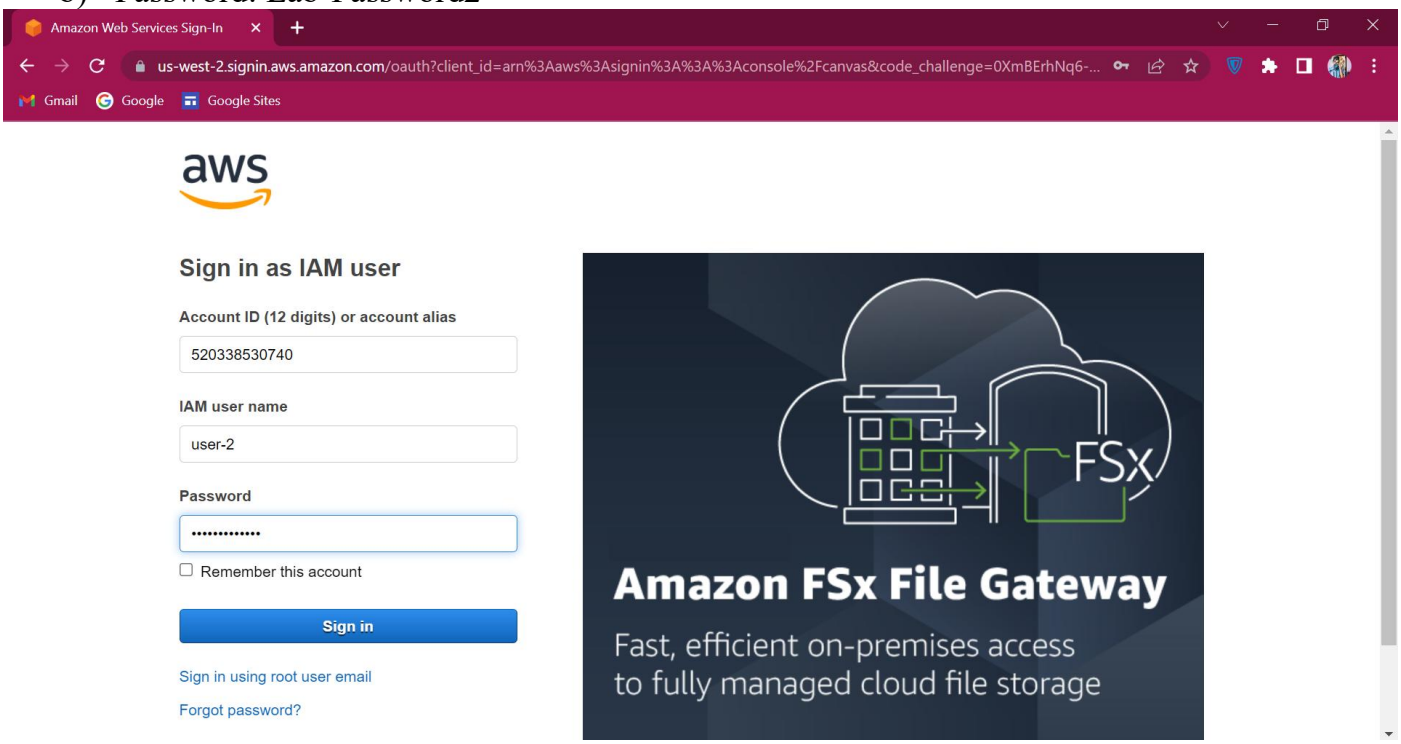


75. You will now sign in as user-2, who has been hired as your Amazon EC2 support person.
76. First, sign out user-1 from the console:
77. In the upper-right corner of the page, choose user-1.
78. Choose Sign Out.

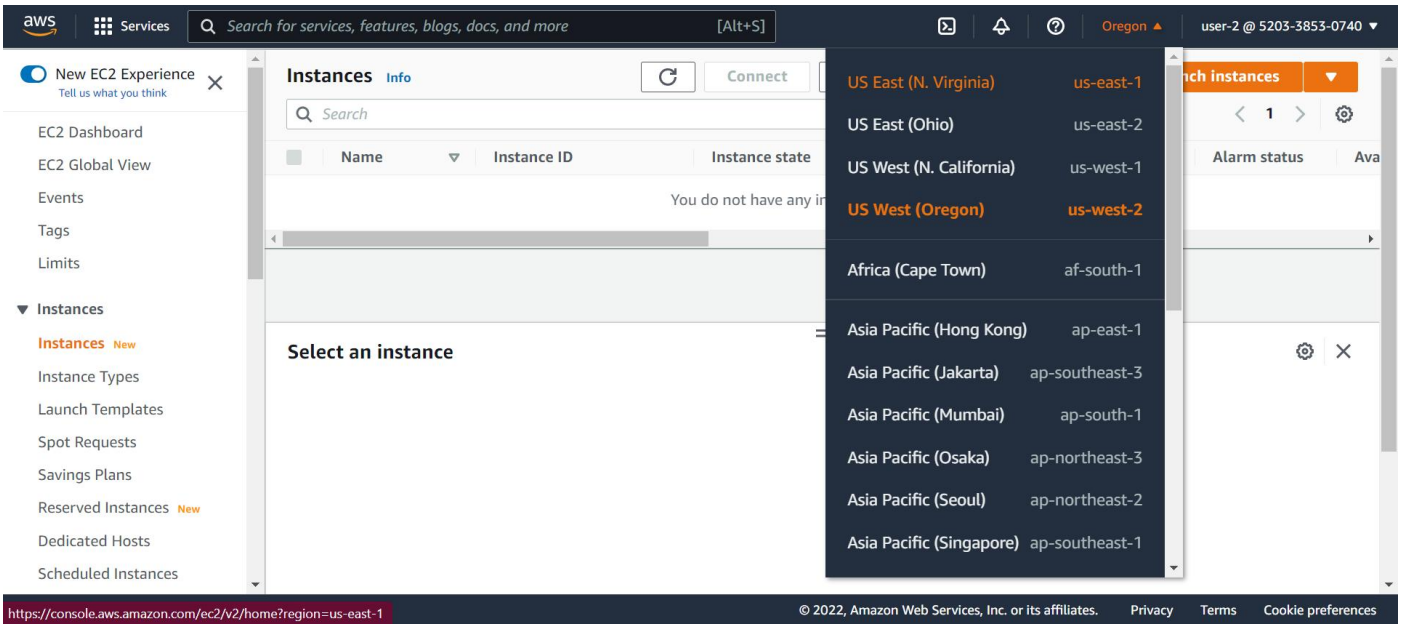


Test user-2 permissions

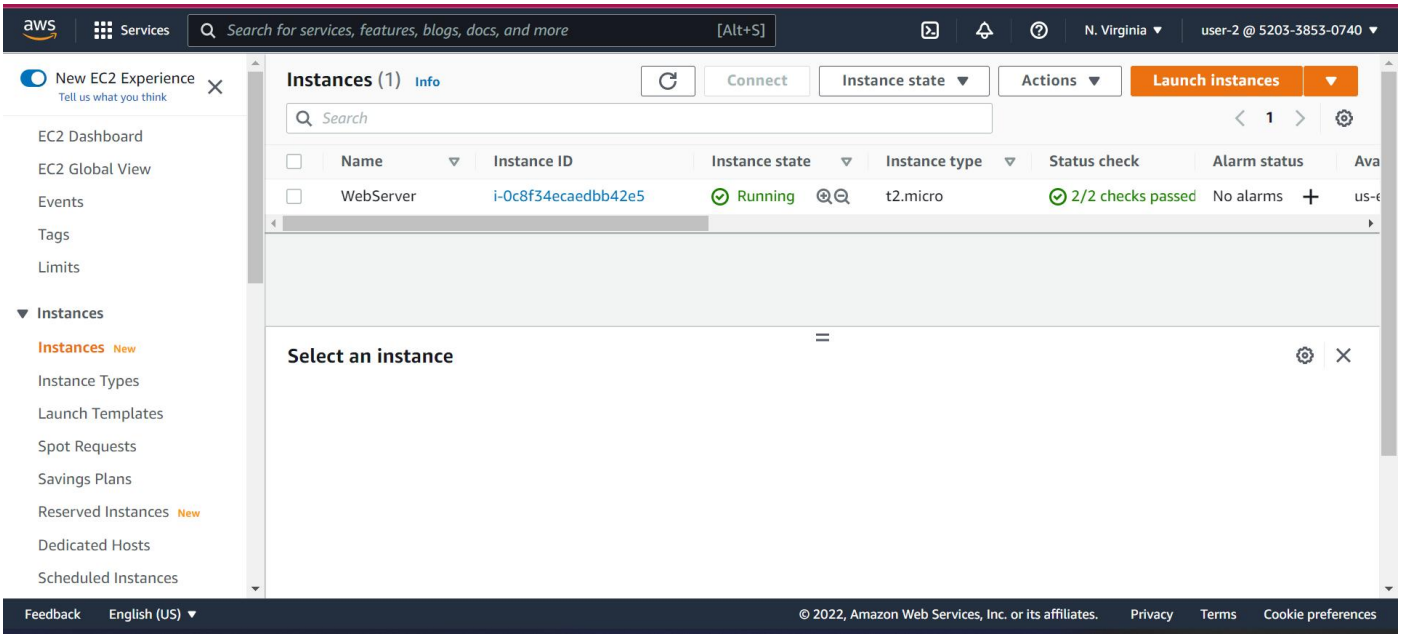
79. Paste the sign-in link into the private browser again, and press ENTER.
80. Sign in with the following credentials:
    a) IAM user name: user-2
    b) Password: Lab-Password2



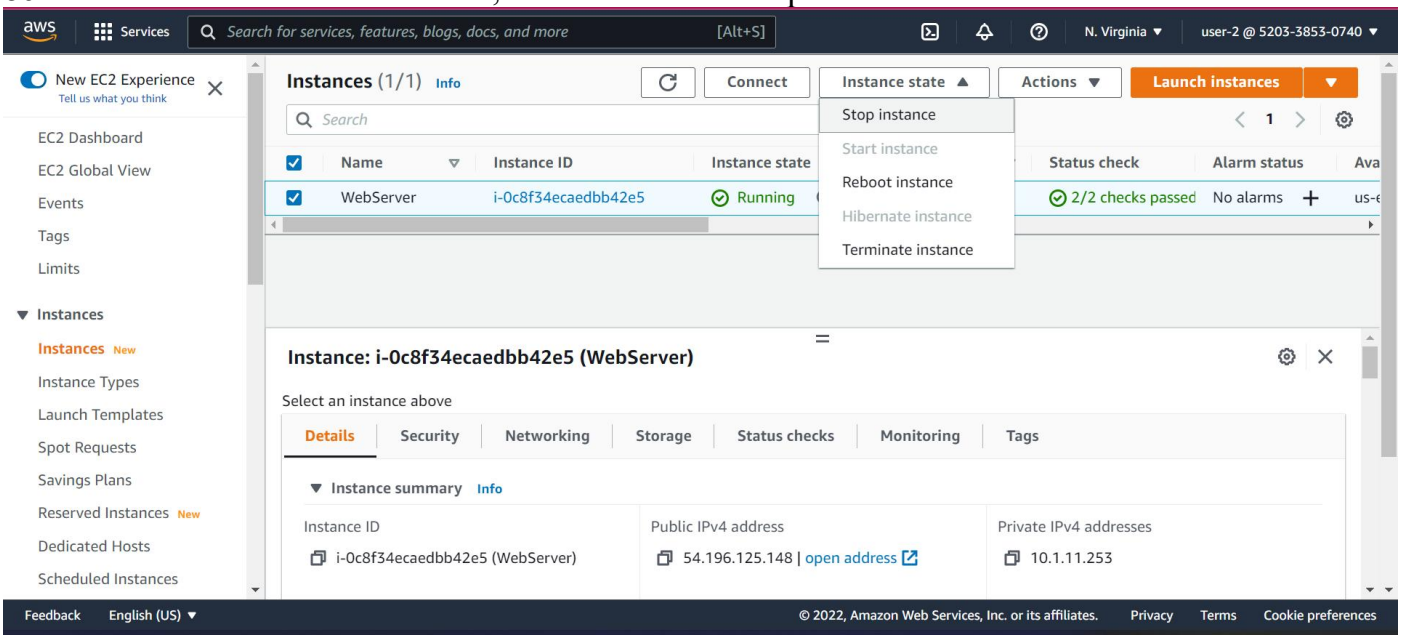
81. Choose the Services menu, and choose EC2.
82. In the navigation pane on the left, choose Instances.
83. You are now able to see an EC2 instance. However, you cannot make any changes to Amazon EC2 resources because you have read-only permissions.
84. If you cannot see an EC2 instance, then your Region might be incorrect. In the upper-right corner of the page, choose the Region name, and then choose the Region that you were in at the beginning of the lab (for example, N. Virginia).



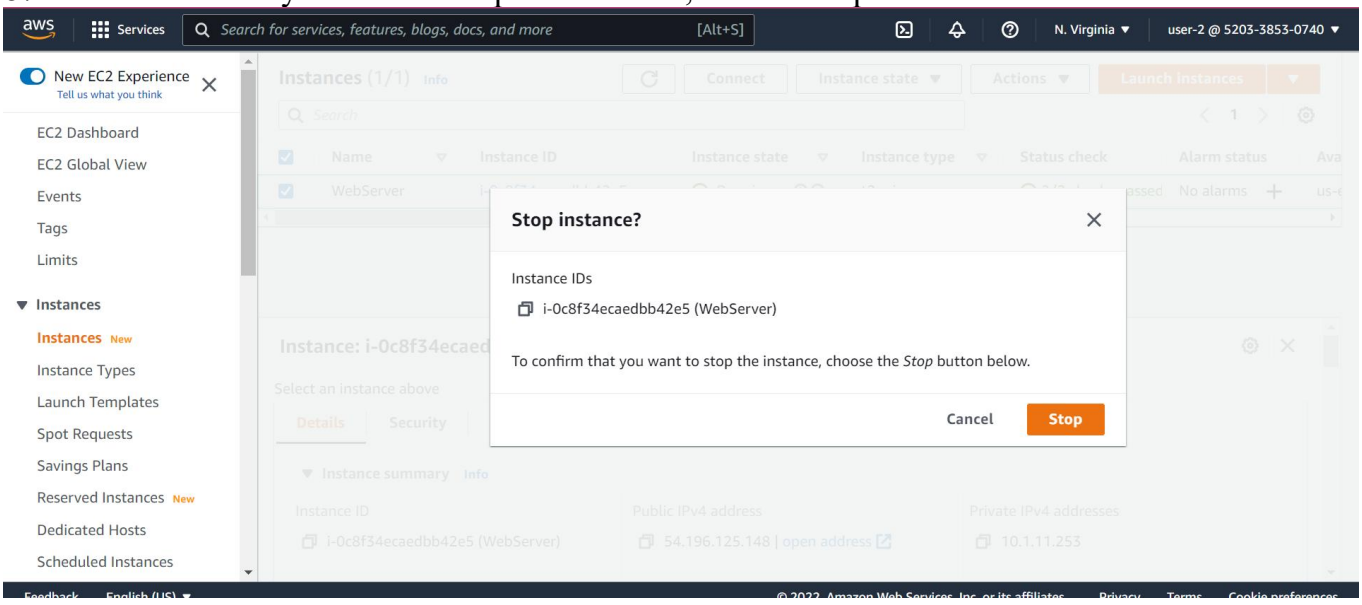
85. Select the EC2 instance.



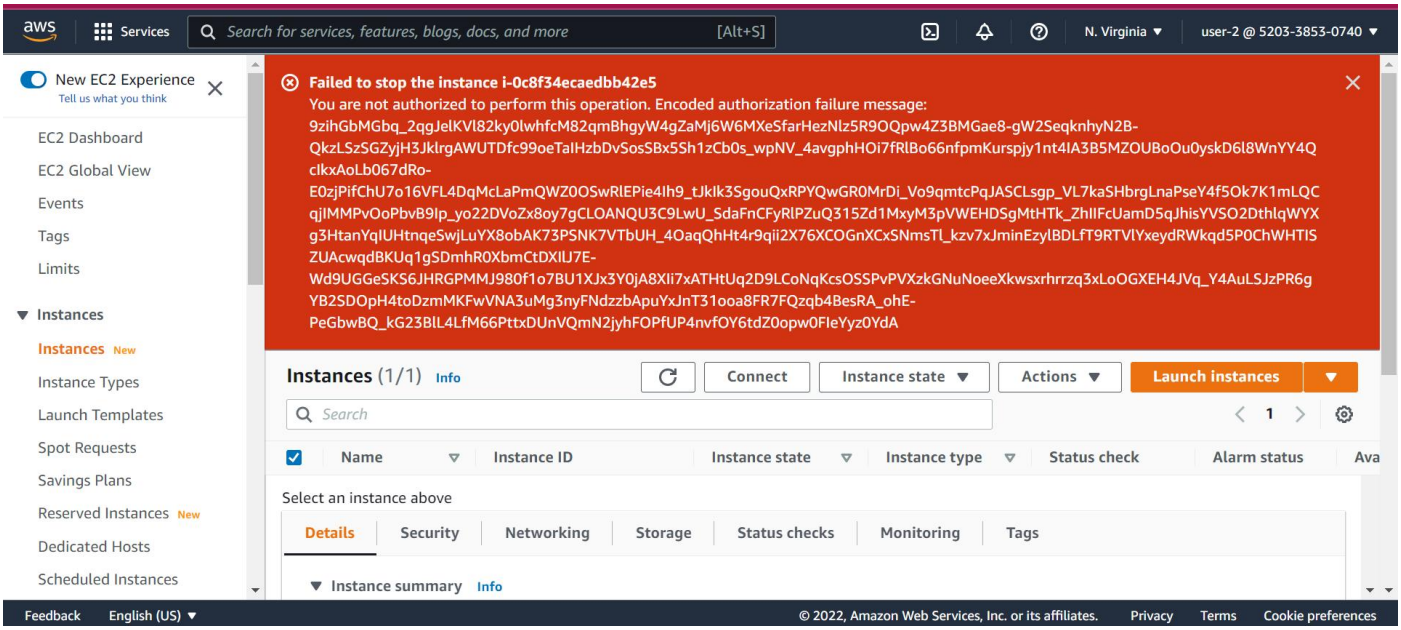
86. Choose the Instance state menu, and then choose Stop instance.



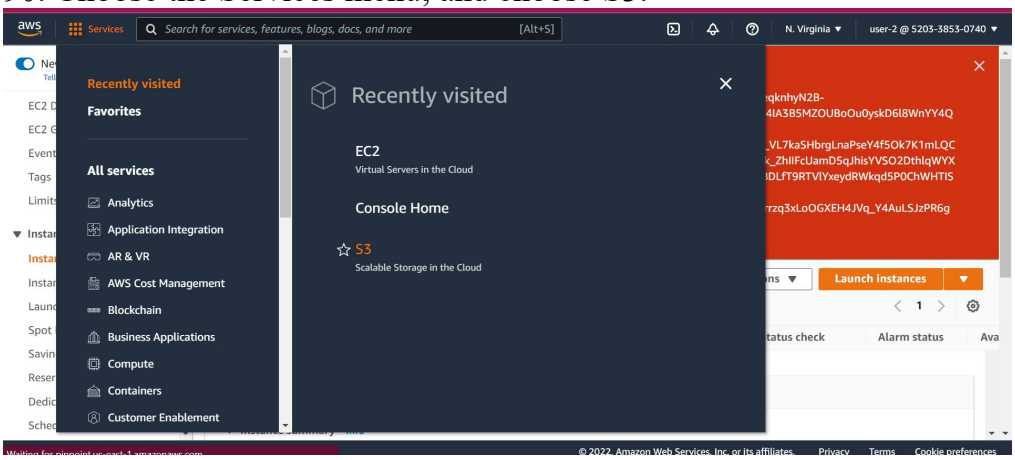
87. To confirm that you want to stop the instance, choose Stop.



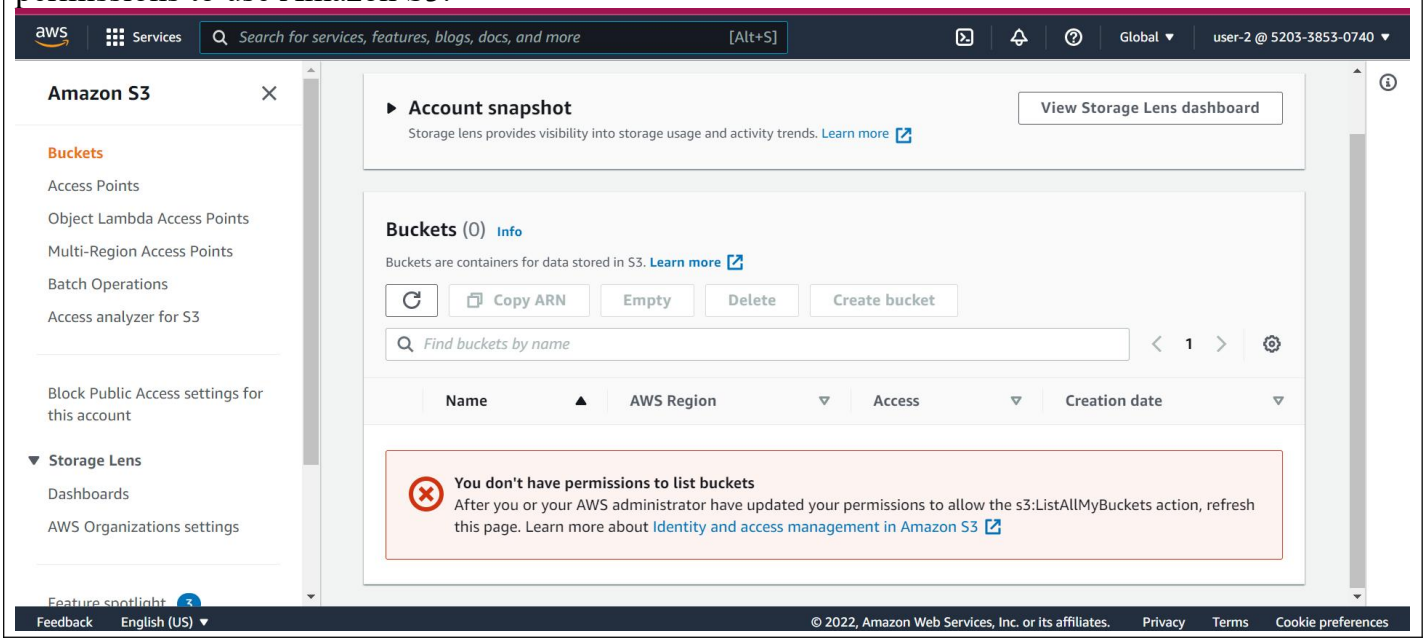
88. An error message appears and says that You are not authorized to perform this operation. This demonstrates that the policy only allows you to view information without making changes.



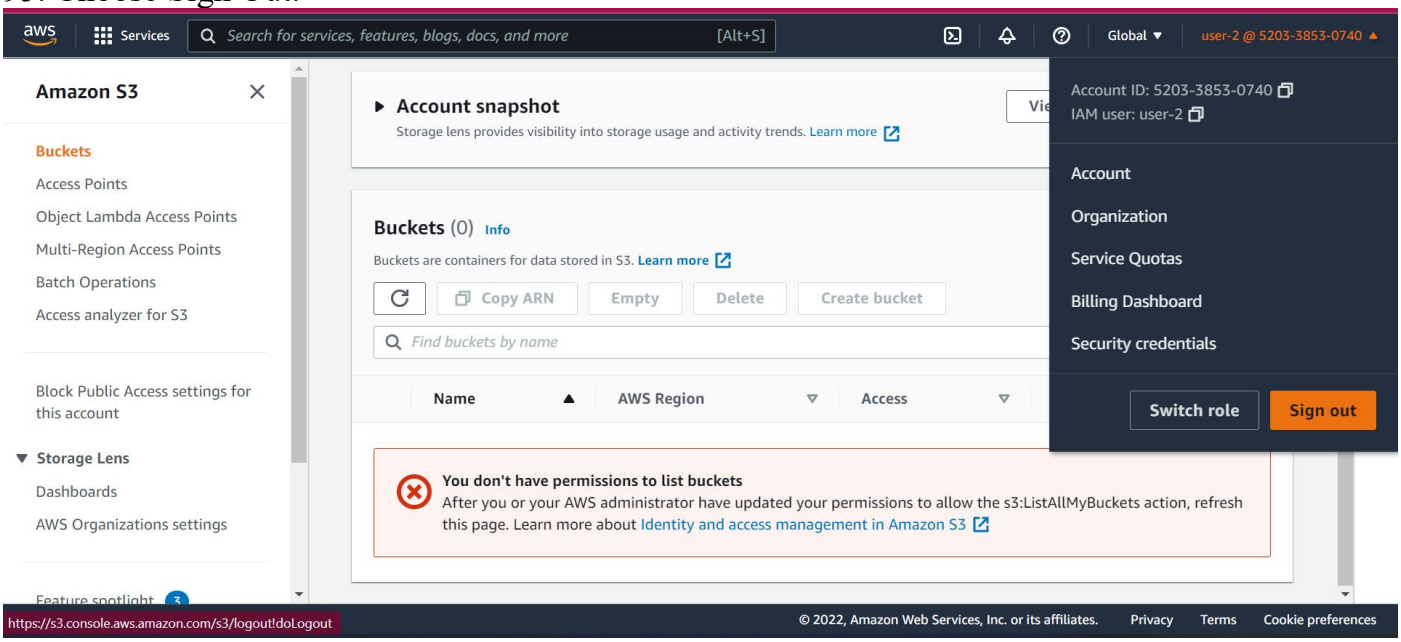
89. Next, check if user-2 can access Amazon S3.
90. Choose the Services menu, and choose S3.



91. An error message says You don't have permissions to list buckets because user-2 does not have permissions to use Amazon S3.

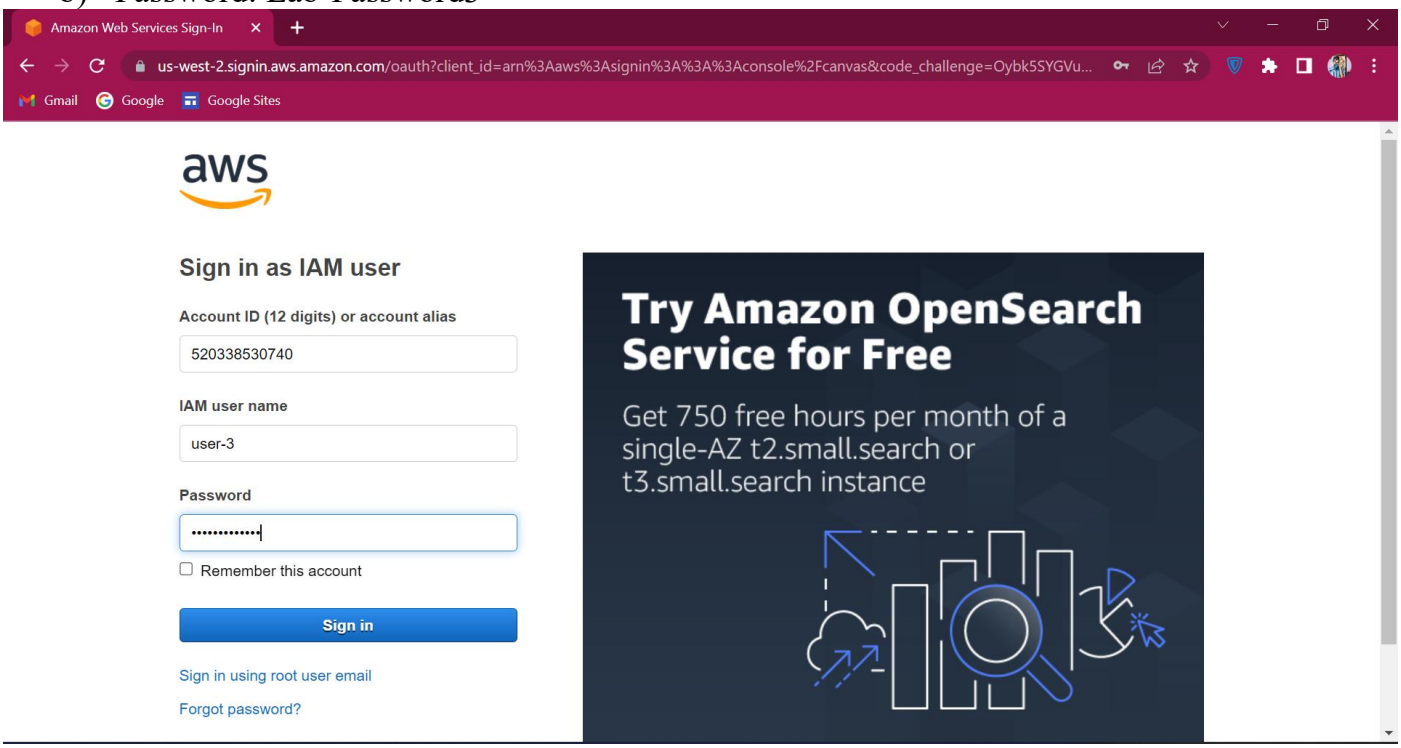


92. You will now sign-in as user-3, who has been hired as your Amazon EC2 administrator.
93. First, sign out user-2 from the console:
94. In the upper-right corner of the page, choose user-2.
95. Choose Sign Out.



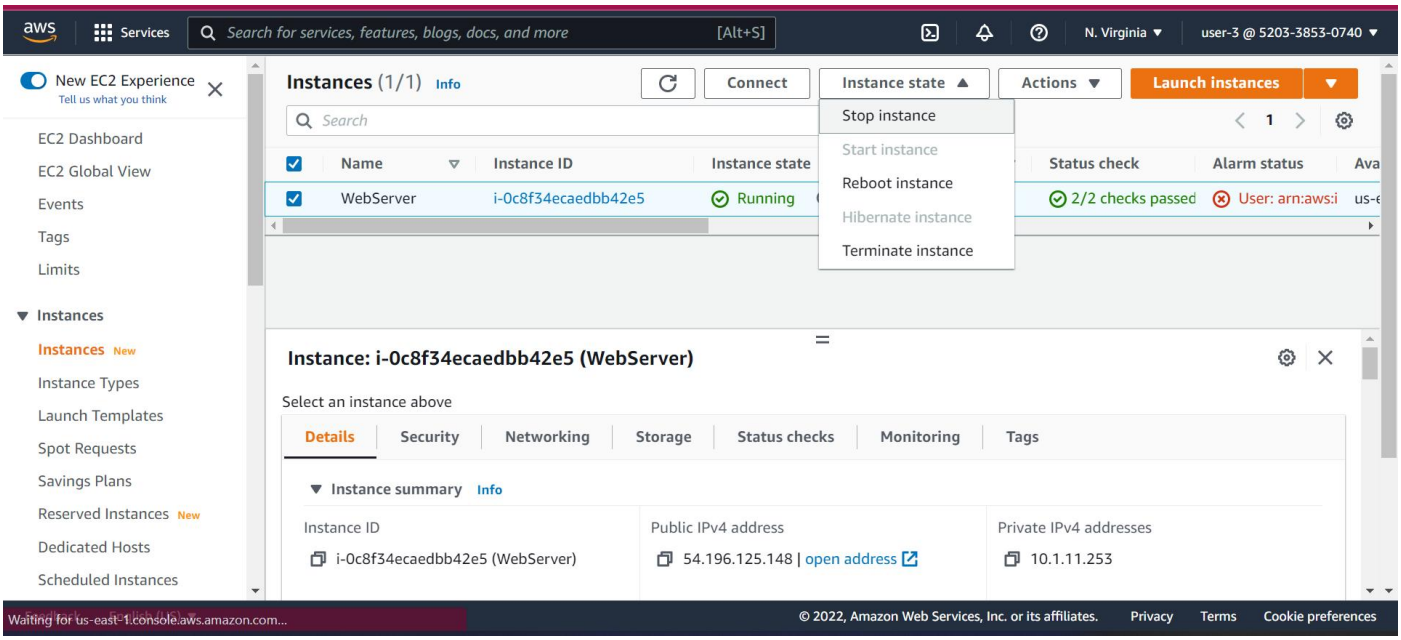
Test user-3 permissions

96. Paste the sign-in link into the private browser again, and press ENTER.
97. Sign in with the following credentials:
    a) IAM user name: user-3
    b) Password: Lab-Password3

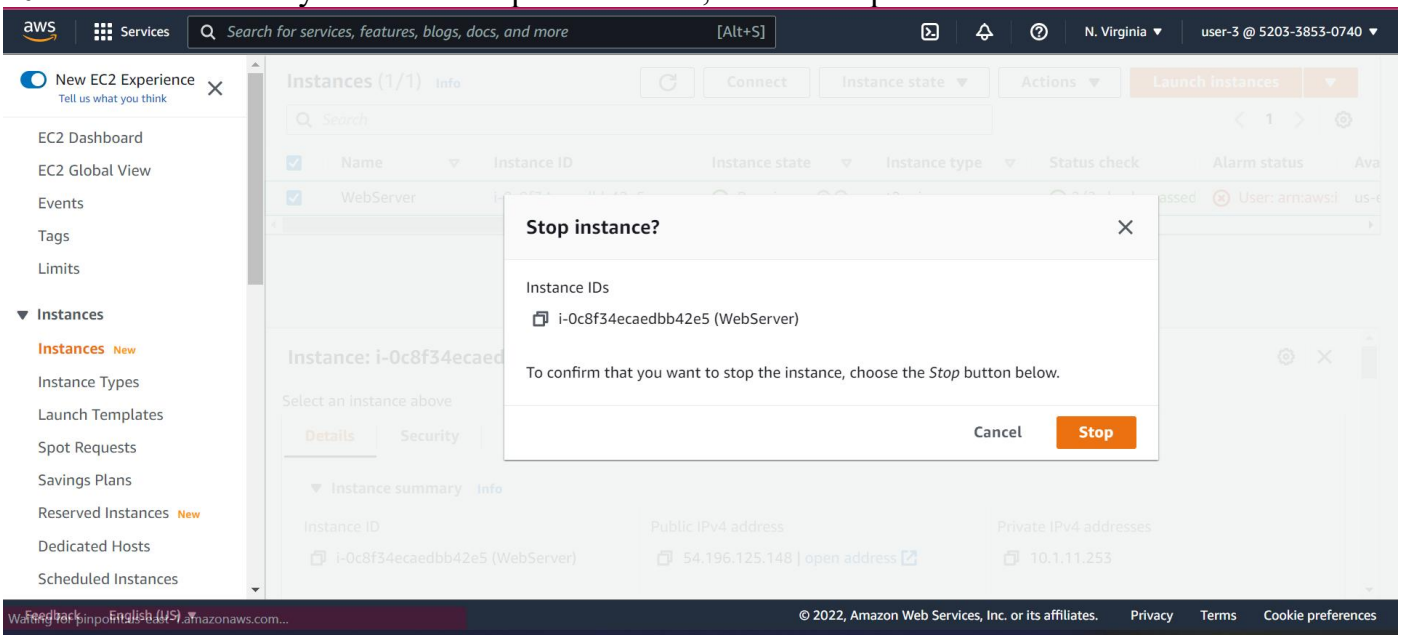


98. Choose the Services menu, and choose EC2.
99. In the navigation pane on the left, choose Instances.
100. An EC2 instance is listed. As an Amazon EC2 Administrator, this user should have permissions to Stop the EC2 instance.

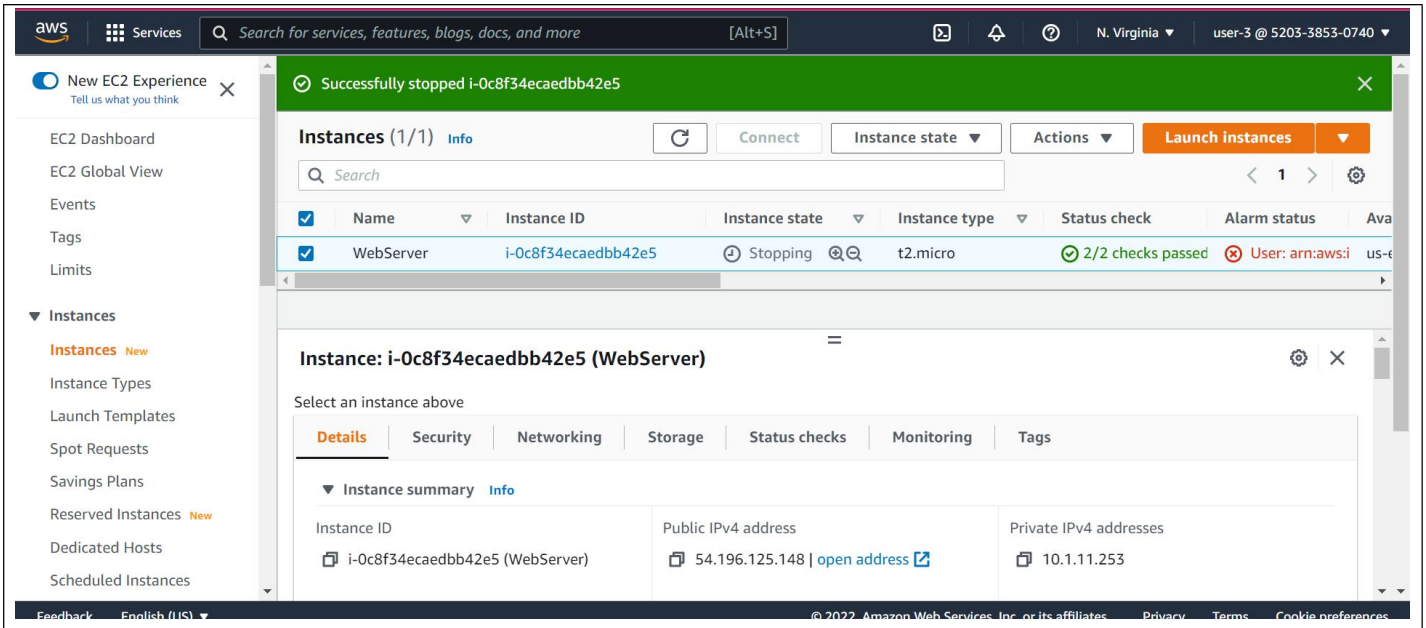
101. If you cannot see an EC2 instance, then your Region might be incorrect. In the upper-right corner of the page, choose the Region name, and then choose the Region that you were in at the beginning of the lab (for example, N. Virginia).
102. Select the EC2 instance.
103. Choose the Instance state menu, and then choose Stop instance.



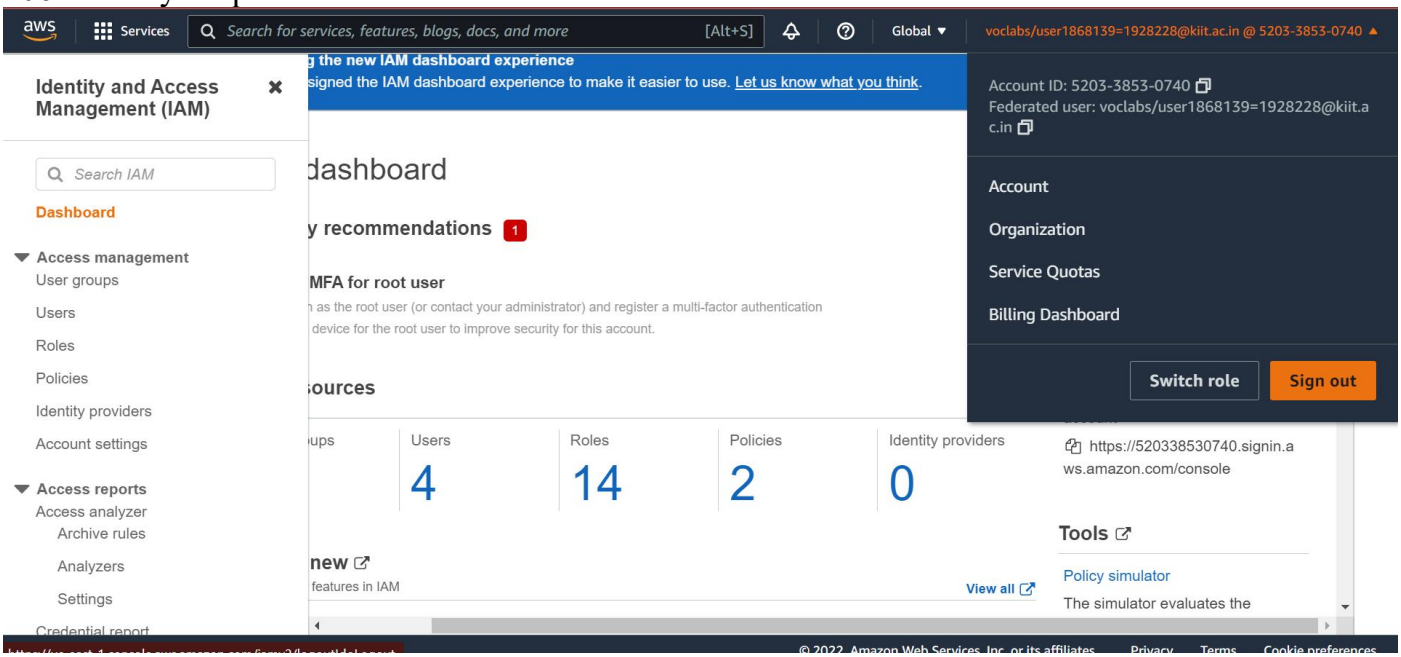
104. To confirm that you want to stop the instance, choose Stop.



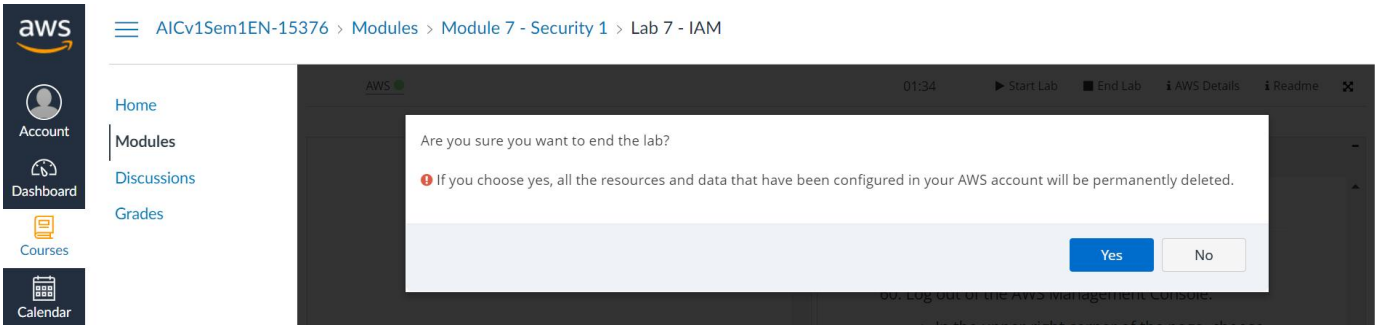
105. This time, the action is successful because user-3 has permissions to stop EC2 instances. The Instance state changes to Stopping and starts to shut down.



106. Close your private browser window.



Lab Complete



==========