

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.

The screenshot shows the AWS Academy Lab 7 interface. On the left is a sidebar with icons for Account, Dashboard, Courses, Calendar, Inbox, History, and Help. The main area has a header 'AICv1Sem1EN-15376 : Modules > Module 4 - Virtual Serv... > Lab 4.1 - EC2'. Below the header is a navigation bar with 'Home', 'Modules', 'Discussions', and 'Grades'. The central part of the screen shows a terminal window with the command 'ddid_v1_w_b4_110594@runweb58771:~\$'. To the right of the terminal is a 'Help' panel titled 'EN-US'. It contains instructions: '1. To start the lab session, choose Start Lab in the upper-right corner of the page.' It also includes a tip: 'Tip: To refresh the session length at any time, choose Start Lab again before the timer reaches 0:00.' At the bottom are 'Previous' and 'Next' buttons.

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

The screenshot shows two pages side-by-side. On the left is the 'Sign in' page for AWS. It has a 'Root user' radio button selected, with a tooltip 'Account owner that performs tasks requiring unrestricted access. Learn more'. Below it is an 'IAM user' radio button with a tooltip 'User within an account that performs daily tasks. Learn more'. There is a 'Root user email address' field containing '1928228@kiit.ac.in' and a 'Next' button. At the bottom are links for 'By continuing, you agree to the AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.' and 'New to AWS?'. On the right is the 'Amazon Lightsail' landing page. It features a large orange and yellow background image with the text 'Amazon Lightsail' and 'Lightsail is the easiest way to get started on AWS'. It includes a 'Learn more »' button and a cartoon robot icon giving a thumbs up.

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.

The screenshot shows the AWS Management Console with the Services menu open. The 'IAM' service is highlighted in the navigation pane. A banner at the top informs users about the transition to the new AWS Console Home.

AWS Management Console

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

The screenshot shows the AWS Management Console with the Services menu open. The 'IAM' service is selected and highlighted. The main content area displays various AWS security services.

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

The screenshot shows the IAM dashboard. The left sidebar is titled 'Identity and Access Management (IAM)' and includes sections for Dashboard, Access management, Users, Policies, Identity providers, Account settings, Access reports, and Credential report. The main content area shows 'Security recommendations' with a red notification badge '1' for 'Add MFA for root user'. It also features 'IAM resources' with counts: User groups (3), Users (4), Roles (14), Policies (2), and Identity providers (0). A 'What's new' section indicates updates for features in IAM. On the right, there are sections for 'AWS Account' (Account ID: 520338530740, Account Alias: 520338530740) and 'Tools' (Policy simulator).

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.

The screenshot shows the AWS IAM console. The left sidebar is titled 'Identity and Access Management (IAM)' and includes options like Dashboard, Access management (with 'Users' selected), Roles, Policies, Identity providers, Account settings, and Access reports. The main content area has tabs for Permissions, Groups, Tags (1), Security credentials, and Access Advisor. Under 'Permissions policies', there's a box for 'Get started with permissions' and a button to 'Add permissions'. Below it, under 'Permissions boundary (not set)', there's a box with a red 'X' icon stating 'You need permissions' and listing a specific permission denial for the user.

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.

The screenshot shows the AWS IAM Groups page for user-1. The left sidebar is the same as the previous screenshot. The main content area shows the 'Summary' section for user-1, which includes details like User ARN, Path, and Creation time. Below this, the 'Groups' tab is selected, showing a table with columns for Group name and Attached permissions. The table is currently empty, indicating no groups are assigned to the user.

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

The screenshot shows the AWS Identity and Access Management (IAM) console. The left sidebar is titled "Identity and Access Management (IAM)" and includes sections for "User groups", "Users", "Roles", "Policies", "Identity providers", and "Account settings". The main content area is titled "User groups (3) Info" and displays a table of user groups. The table has columns for "Group name", "Users", "Permissions", and "Creation time". The groups listed are EC2-Admin, EC2-Support, and S3-Support, all of which were created 8 minutes ago and have "Defined" permissions.

Group name	Users	Permissions	Creation time
EC2-Admin	0	Defined	8 minutes ago
EC2-Support	0	Defined	8 minutes ago
S3-Support	0	Defined	8 minutes ago

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

The screenshot shows the "EC2-Support" summary page within the AWS IAM console. The left sidebar is identical to the previous screenshot. The main content area is titled "EC2-Support" and includes a "Summary" section with details like the user group name (EC2-Support), creation time (March 27, 2022, 11:34 (UTC+05:30)), and ARN (arn:aws:iam::520338530740:group/spl66/EC2-Support). Below the summary are tabs for "Users", "Permissions", and "Access Advisor", with "Users" currently selected. The "Users" tab shows "0" users in the group and includes buttons for "Add users" and "Remove users".

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.

The screenshot shows the AWS IAM Policies page for the policy 'AmazonEC2ReadOnlyAccess'. The left sidebar navigation includes 'Identity and Access Management (IAM)' and various other services like 'Dashboard', 'Access management', 'User groups', 'Users', 'Roles', and 'Policies'. The main content area displays the 'Summary' tab for the policy. It shows the Policy ARN as 'arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess' and a description stating 'Provides read only access to Amazon EC2 via the AWS Management Console.' Below this, there are tabs for 'Permissions', 'Policy usage', 'Policy versions', and 'Access Advisor'. The 'Permissions' tab is selected, showing a table with four columns: Service, Access level, Resource, and Request condition. The table lists several services with their respective access levels and resource scopes. A 'Policy summary' button and a 'JSON' button are also present. At the bottom, there are links for 'Feedback', 'English (US)', and copyright information.

22. Choose the {} JSON tab.

The screenshot shows the AWS IAM Policies page for the policy 'AmazonS3ReadOnlyAccess'. The left sidebar navigation is identical to the previous screenshot. The main content area displays the 'Summary' tab for the policy. It shows the Policy ARN as 'arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess' and a description stating 'Provides read only access to all buckets via the AWS Management Console.' Below this, there are tabs for 'Permissions', 'Policy usage', 'Policy versions', and 'Access Advisor'. The 'Permissions' tab is selected, showing a table with four columns: Service, Access level, Resource, and Request condition. A 'Policy summary' button and a 'JSON' button are also present. The 'JSON' button is highlighted. Below the table, the JSON code for the policy is displayed, showing the structure of the policy document. At the bottom, there are links for 'Feedback', 'English (US)', and copyright information.

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.

The screenshot shows the AWS Identity and Access Management (IAM) console. On the left, the navigation pane is open with 'Access management' expanded, showing 'User groups'. The main content area displays 'User groups (3)'. A table lists three user groups: 'EC2-Admin', 'EC2-Support', and 'S3-Support'. Each group has 0 users and is defined. They were created 11 minutes ago. The table includes columns for Group name, Users, Permissions, and Creation time.

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.

The screenshot shows the 'Summary' page for the 'S3-Support' user group. It displays basic information: User group name (S3-Support), Creation time (March 27, 2022, 11:34 (UTC+05:30)), and ARN (arn:aws:iam::520338530740:group/spl6/S3-Support). The 'Permissions' tab is selected, showing one attached policy: 'AmazonS3ReadOnlyAccess'. This policy is described as 'Provides read only access to all buckets via the AWS Management Console.' The policy ARN is listed as arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess.

33. Choose the {} JSON tab.

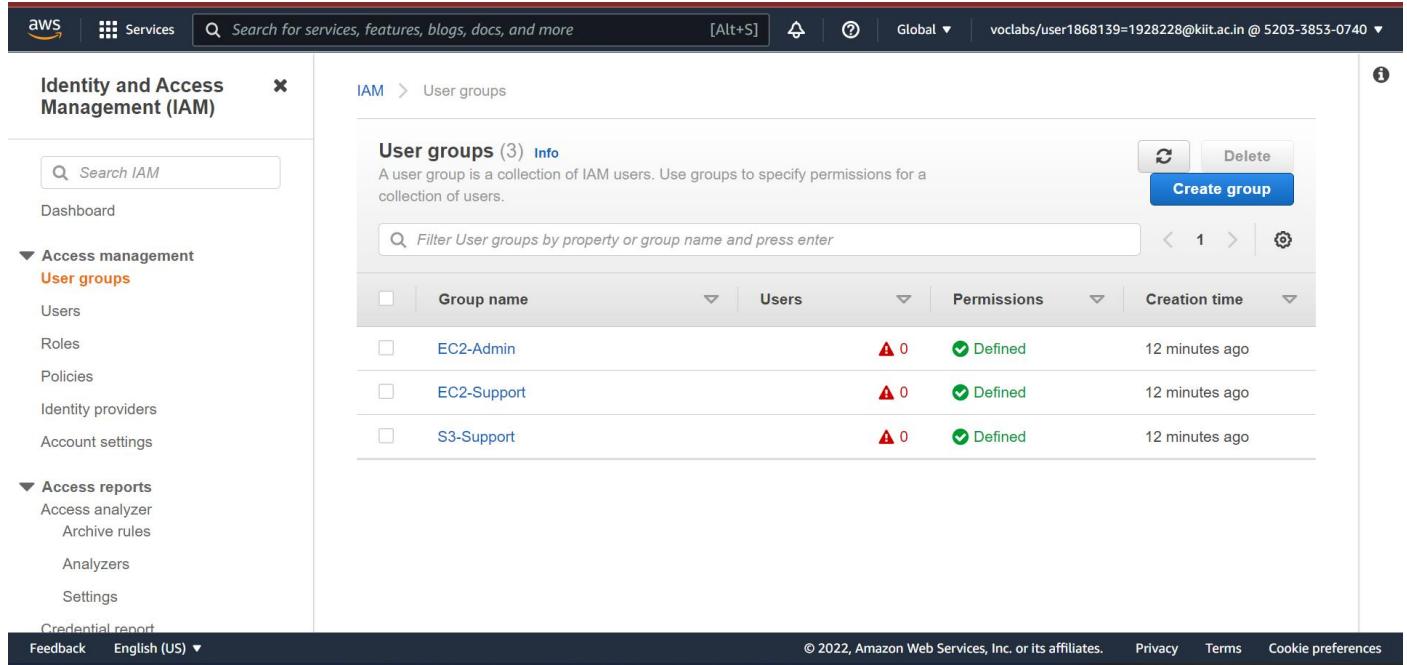
The screenshot shows the 'Summary' page for the 'AmazonS3ReadOnlyAccess' policy. It provides a brief description: 'Provides read only access to all buckets via the AWS Management Console.' Below this, there are tabs for 'Permissions', 'Policy usage', 'Policy versions', and 'Access Advisor'. The 'Permissions' tab is selected, showing the policy's JSON structure. The JSON code is as follows:

```

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    }
13  ]
14}

```

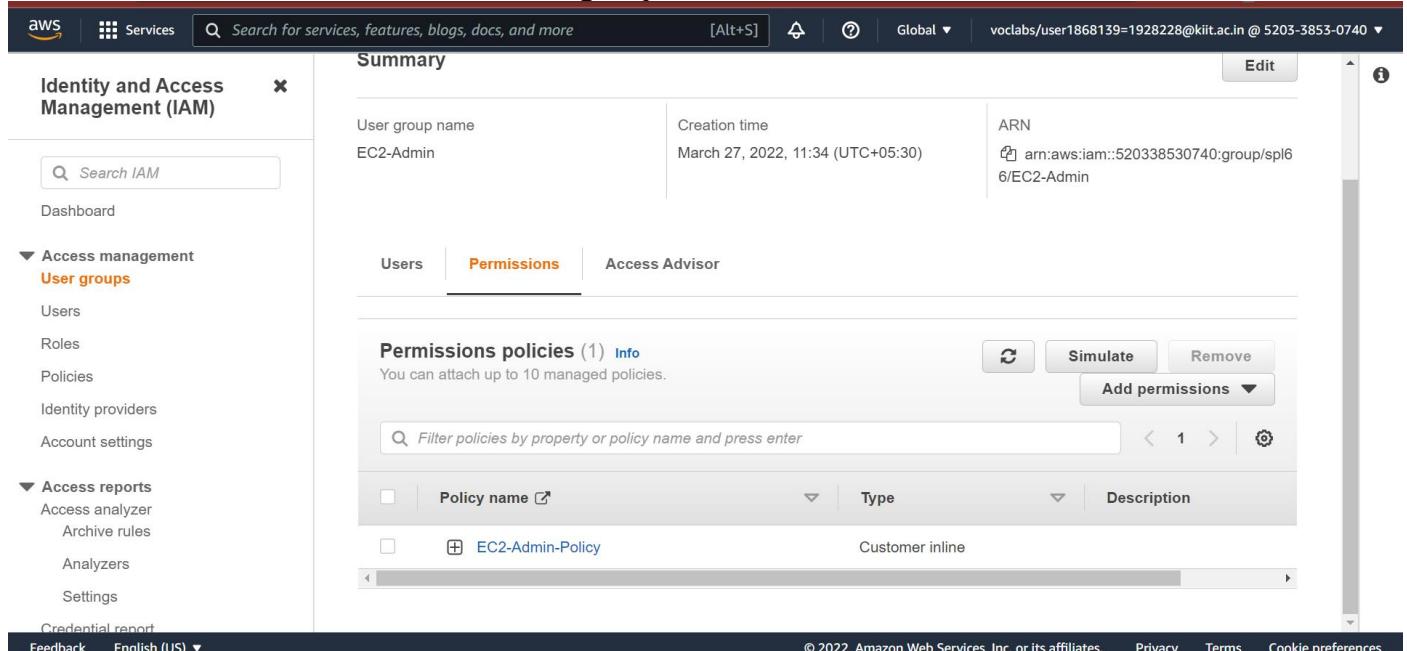
34. This policy has permissions to Get and List for all resources in Amazon S3.
 35. In the navigation pane on the left, choose User groups.



The screenshot shows the AWS IAM User groups page. The left sidebar shows 'User groups' selected under 'Access management'. The main area displays a table of user groups:

Group name	Users	Permissions	Creation time
EC2-Admin	0	Defined	12 minutes ago
EC2-Support	0	Defined	12 minutes ago
S3-Support	0	Defined	12 minutes ago

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



The screenshot shows the AWS IAM User group details page for 'EC2-Admin'. The left sidebar shows 'User groups' selected under 'Access management'. The main area shows the group summary and its permissions:

Summary

User group name EC2-Admin	Creation time March 27, 2022, 11:34 (UTC+05:30)	ARN arn:aws:iam::520338530740:group/spl66/EC2-Admin
------------------------------	--	--

Permissions

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

Policy name	Type	Description
EC2-Admin-Policy	Customer inline	

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.

A screenshot of the AWS IAM Policy Editor interface. At the top, there's a navigation bar with the AWS logo, 'Services', a search bar ('Search for services, features, blogs, docs, and more'), and account information ('voclabs/user1868139=1928228@kiit.ac.in @ 5203-3853-0740'). Below the header, the title 'Edit EC2-Admin-Policy' is displayed. The main area shows a JSON editor with the following policy code:

```
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    }  
14  ]  
15}
```

Below the JSON code, there are status indicators: Security: 0, Errors: 0, Warnings: 0, and Suggestions: 0. A message box at the bottom left says 'You need permissions' with a note: 'You do not have the permission required to perform this operation. Ask your administrator to add permissions.' At the bottom of the screen, there are links for 'Feedback', 'English (US)', '© 2022, Amazon Web Services, Inc. or its affiliates.', 'Privacy', 'Terms', and 'Cookie preferences'.

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

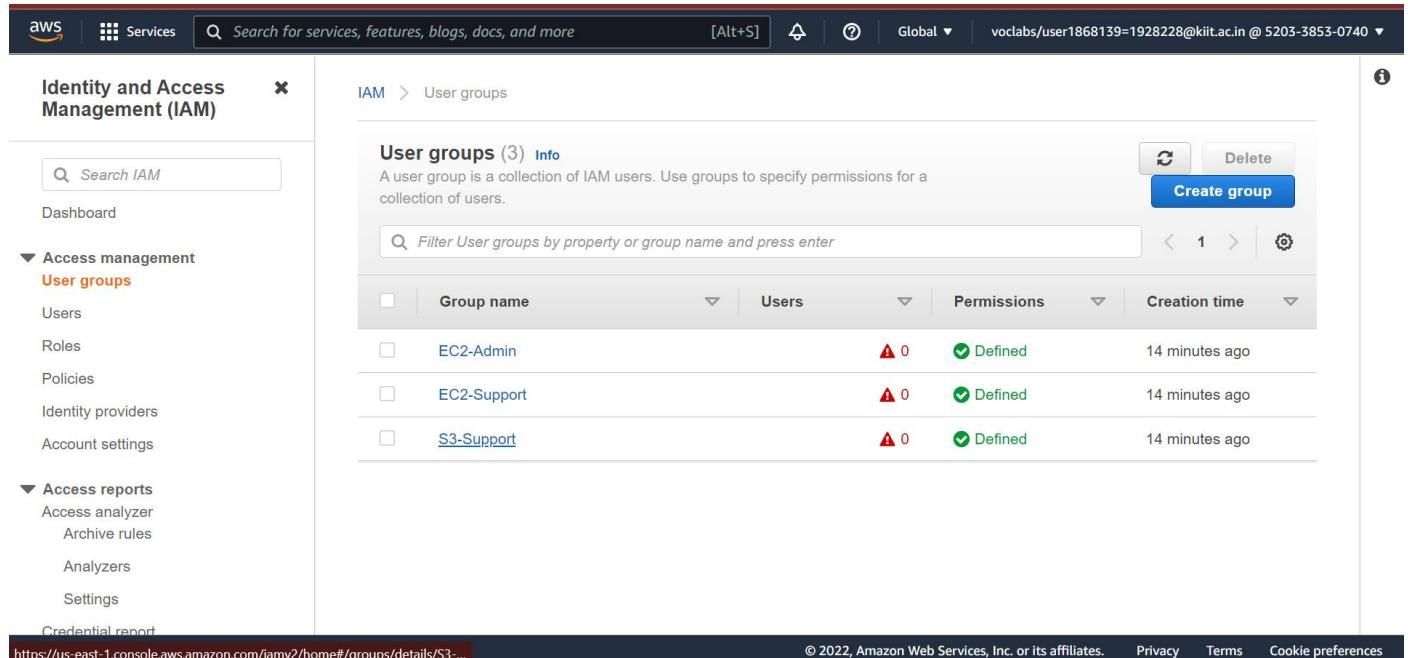
Add users to groups

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.

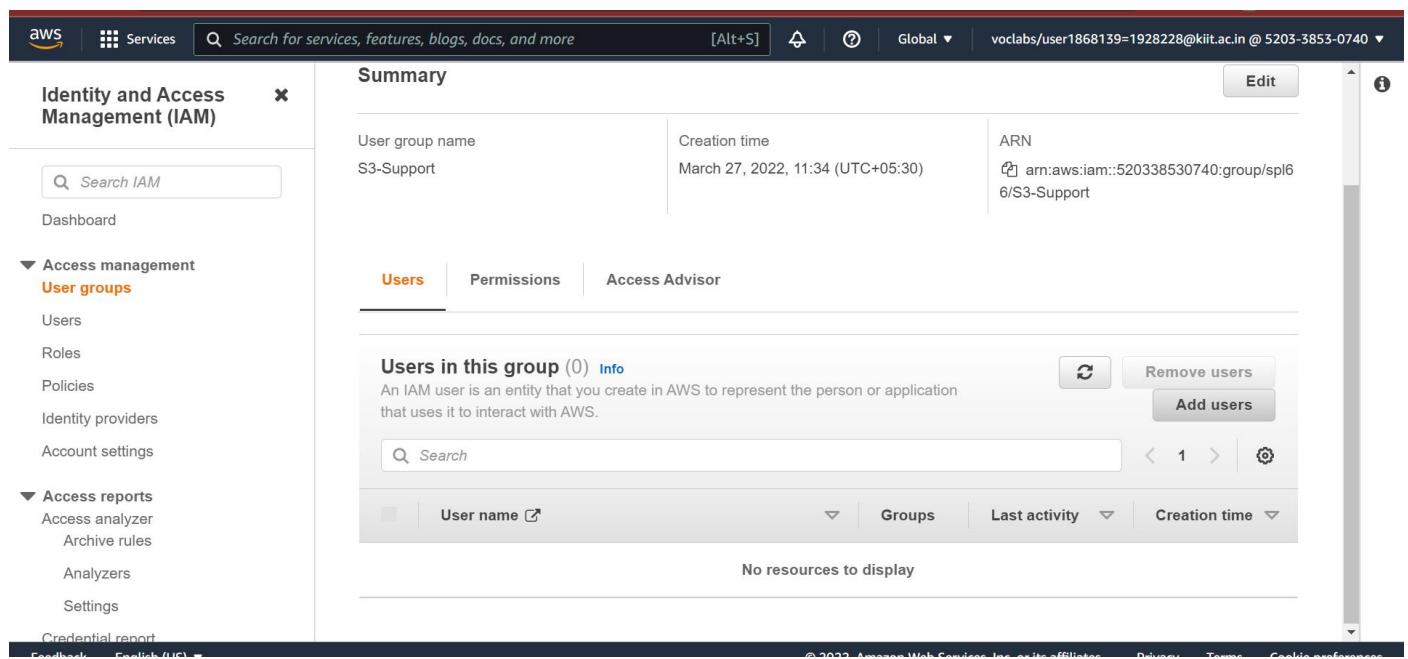


The screenshot shows the AWS IAM User groups page. The left sidebar has 'Identity and Access Management (IAM)' selected under 'Access management'. The main area shows 'User groups (3)'. A table lists the groups:

Group name	Users	Permissions	Creation time
EC2-Admin	0	Defined	14 minutes ago
EC2-Support	0	Defined	14 minutes ago
<u>S3-Support</u>	0	Defined	14 minutes ago

47. On the Users tab, choose Add users.

48. Select user-1, and choose Add users.



The screenshot shows the AWS IAM User group summary page for 'S3-Support'. The left sidebar has 'Identity and Access Management (IAM)' selected under 'Access management'. The main area shows the 'Summary' tab. Under 'Users in this group (0)', there is a table with one row:

User name	Groups	Last activity	Creation time
No resources to display			

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

Add users to S3-Support

Other users in this account (Selected 1/4) [Info](#)

User name	Groups	Last activity	Creation time
awsstudent	You need permissions	None	15 minutes ago
<input checked="" type="checkbox"/> user-1	0	None	15 minutes ago
<input type="checkbox"/> user-2	0	None	15 minutes ago
<input type="checkbox"/> user-3	0	None	15 minutes ago

[Cancel](#) [Add users](#)

S3-Support

Summary

User group name S3-Support	Creation time March 27, 2022, 11:34 (UTC+05:30)	ARN arn:aws:iam::520338530740:group/spl6/S3-Support
-------------------------------	--	--

[Edit](#)

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](#)

User groups (3) [Info](#)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

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

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.

The screenshots illustrate the steps to add user-2 to the EC2-Support group:

- Screenshot 1: Add users to EC2-Support**

This screen shows a list of users in the account. The user "user-2" is selected, indicated by a checked checkbox. Other users listed are awsstudent, user-1, and user-3. The "Add users" button is visible at the bottom right.
- Screenshot 2: Confirmation dialog - Users added to this group**

A confirmation dialog box is displayed, stating "Users added to this group." It lists the user "user-2" and provides options to "Delete," "Edit," or "Add users".
- Screenshot 3: User groups list**

This screen shows the "User groups" list. The "EC2-Support" group is selected. A modal window displays the group details: "User group name: EC2-Support", "Creation time: March 27, 2022, 11:34 (UTC+05:30)", and "ARN: arn:aws:iam::520338530740:group/spl6/EC2-Support". The "Users" tab is selected, showing "Users in this group (1)". The user "user-2" is listed with a "Remove users" button next to it.

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.

The screenshot shows the AWS Identity and Access Management (IAM) service. In the left navigation pane, under 'Access management', 'User groups' is selected. The main content area displays the 'Summary' for the 'EC2-Admin' group. It shows the group name, creation time (March 27, 2022, 11:34 (UTC+05:30)), and ARN (arn:aws:iam::520338530740:group/spl66/EC2-Admin). Below this, the 'Users' tab is selected, showing a table with one row: 'User name' (user-3), 'Groups' (empty), 'Last activity' (None), and 'Creation time' (17 minutes ago). A button labeled 'Add users' is visible at the top right of the user list.

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.

The screenshot shows the 'Add users to EC2-Admin' dialog. Under 'Other users in this account', the user 'user-3' is selected, indicated by a checked checkbox. Other users listed are 'awsstudent', 'user-1', and 'user-2'. At the bottom right of the dialog are 'Cancel' and 'Add users' buttons.

The screenshot shows the AWS Identity and Access Management (IAM) console. In the left navigation pane, under 'Access management', 'User groups' is selected. The main content area displays the 'EC2-Admin' user group. The 'Summary' tab is active, showing details like the user group name (EC2-Admin), creation time (March 27, 2022, 11:34 (UTC+05:30)), and ARN (arn:aws:iam::520338530740:group/spl6/EC2-Admin). Below the summary, there are tabs for 'Users', 'Permissions', and 'Access Advisor'. Under the 'Users' tab, it says 'Users in this group (1)' with a link to 'Info'. A note explains that an IAM user is an entity created in AWS to represent a person or application. There are buttons for 'Remove users' and 'Add users'. At the bottom of the page, there are links for 'Feedback', 'English (US)', and copyright information.

The screenshot shows the AWS IAM User Groups page. The left navigation pane is identical to the previous screenshot. The main content area shows a list of user groups: EC2-Admin, EC2-Support, and S3-Support. Each group has a status indicator (green checkmark for 'Defined'), the number of users in the group (1 for EC2-Admin, 2 for EC2-Support, 0 for S3-Support), and the creation time (all 17 minutes ago). A modal window is open over the table, showing the 'user-3' user assigned to the EC2-Support group. The modal includes a 'Remove' button and a 'Cancel' button. The bottom of the page includes standard footer links.

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.

The screenshot shows the AWS Identity and Access Management (IAM) dashboard. At the top, there is a blue banner with the text "Introducing the new IAM dashboard experience" and a link to "Let us know what you think". Below the banner, the title "IAM dashboard" is displayed. On the left sidebar, there are several navigation items under "Access management" and "Access reports". The main content area includes a "Security recommendations" section with a red notification for "Add MFA for root user" and a "IAM resources" summary table.

User groups	Users	Roles	Policies	Identity providers
3	4	14	2	0

Below the table, there is a "What's new" section with a link to "View all". On the right side, there are sections for "AWS Account" (Account ID: 520338530740, Account Alias: 520338530740, Sign-in URL: https://520338530740.signin.aws.amazon.com/console) and "Tools" (Policy simulator).

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>

This screenshot is identical to the one above, but it includes a green checkmark icon and the text "Sign-in URL Copied" next to the sign-in URL in the "AWS Account" section, indicating that the URL has been copied to the clipboard.

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:

- IAM user name: user-1
- Password: Lab-Password1

Amazon Web Services Sign-In

Sign in as IAM user

Account ID (12 digits) or account alias
520338530740

IAM user name
user-1

Password
.....

Remember this account

Sign in

Sign in using root user email

Forgot password?

Try Amazon OpenSearch Service for Free

Get 750 free hours per month of a single-AZ t2.small.search or t3.small.search instance



AWS Management Console

The new AWS Console Home will replace your existing experience soon

Starting April 2022, the new AWS Console Home will replace your current experience. Switch now to customize your Console Home and view valuable insights.

[Learn more](#) or [let us know what you think.](#)

Switch now

AWS Management Console

AWS services

▼ Recently visited services

Your recently visited AWS services appear here.

► All services

Build a solution

New AWS Console Home

See valuable insights for your account and services with the new customizable Console Home experience. [Learn more](#)



Stay connected to your AWS resources on-the-go

68. Choose the Services menu, and choose S3.

The Star Learner

Game Development

Internet of Things

Machine Learning

Management & Governance

Media Services

Migration & Transfer

Networking & Content Delivery

Quantum Technologies

Robotics

Satellite

Security, Identity, & Compliance

Storage

EFS

Managed File Storage for EC2

AWS Elastic Disaster Recovery

Scalable, cost-effective application recovery to AWS

FSx

Fully managed third-party file systems optimized for a variety of workloads

S3

Scalable Storage in the Cloud

S3 Glacier

Archive Storage in the Cloud

Storage Gateway

Hybrid Storage Integration

Switch now

AWS resources

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.

The screenshot shows the AWS S3 Buckets page. On the left, there's a sidebar with 'Buckets' selected. The main area has a heading 'Account snapshot' with a link to 'View Storage Lens dashboard'. Below it, there's a section for 'Buckets (1) Info' with a note that 'Buckets are containers for data stored in S3.' A 'Create bucket' button is visible. A table lists the single bucket: Name is 'c50024a746820l1796273t1w520338530740-s3bucket-1x0v2p7ti6oze', AWS Region is 'US East (N. Virginia) us-east-1', Access is 'Objects can be public', and Creation date is 'March 27, 2022, 11:34:32 (UTC+05:30)'.

The screenshot shows the AWS S3 Bucket Properties page for the same bucket. The sidebar is identical. The main area has tabs for 'Objects', 'Properties' (which is selected), 'Permissions', 'Metrics', 'Management', and 'Access Points'. Under 'Properties', there's a 'Bucket overview' section with details: AWS Region is 'US East (N. Virginia) us-east-1', ARN is 'arn:aws:s3:::c50024a746820l1796273t1w520338530740-s3bucket-1x0v2p7ti6oze', and Creation date is 'March 27, 2022, 11:34:32 (UTC+05:30)'. Below it is a 'Bucket Versioning' section with a 'Edit' button.

The screenshot shows the AWS S3 Bucket Tags page for the same bucket. The sidebar is identical. The main area has a table for 'Tags (4)'. The tags listed are: Key 'aws:cloudformation:stack-name' with Value 'c50024a746820l1796273t1w520338530740'; Key 'aws:cloudformation:logical-id' with Value 'S3Bucket'; Key 'aws:cloudformation:stack-id' with Value 'arn:aws:cloudformation:us-east-1:520338530740:stack/c50024a746820l1796273t1w520338530740/c14adf30-ad93-11ec-ab8b-1200c4351d41'; and Key 'cloudbucket' with Value 'c50024a746820l1796273t1w520338530740'. Below the tags is a 'Default encryption' section with an 'Edit' button.

71. Now, test whether the user has access to Amazon EC2.

72. Choose the Services menu, and choose EC2.

The screenshot shows the AWS Management Console interface. The top navigation bar includes the AWS logo, a 'Services' button, a search bar, and account information ('user-1 @ 5203-3853-0740'). A sidebar on the left lists various AWS services under categories like Compute, Storage, and Database. The 'Compute' section is expanded, showing options like AWS App Runner, Batch, EC2 (selected), EC2 Image Builder, Elastic Beanstalk, and Lambda. The main content area displays a brief description of EC2: 'Virtual Servers in the Cloud'. A right-hand panel shows a list of resources, with an 'Edit' button visible. At the bottom, there's a 'Refresh' button and a link to 'https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2'.

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.

The screenshot shows the EC2 Instances page. The left sidebar is identical to the previous screenshot. The main content area features a table header with columns: Name, Instance ID, Instance state, Instance type, Status check, and Alarm status. Below the header, a message reads 'You are not authorized to perform this operation.' A modal window titled 'Select an instance' is open at the bottom. The bottom navigation bar includes links for Feedback, English (US), and links to other AWS services like S3, Lambda, and CloudWatch.

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.

This screenshot is identical to the one above, showing the EC2 Instances page with the 'You are not authorized to perform this operation.' message. However, the top right corner of the screen shows the user profile 'user-1 @ 5203-3853-0740'. A dropdown menu next to the profile shows 'Account ID: 5203-3853-0740' and 'IAM user: user-1'. Other options in the menu include 'Account', 'Organization', 'Service Quotas', 'Billing Dashboard', and 'Security credentials'. Buttons for 'Switch role' and 'Sign out' are also present.

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:

- IAM user name: user-2
- Password: Lab-Password2

The screenshot shows a browser window with the AWS sign-in URL: us-west-2.signin.aws.amazon.com. The sign-in form includes fields for Account ID (520338530740), IAM user name (user-2), and Password. Below the form is a checkbox for Remember this account and a blue Sign in button. To the right of the sign-in form is an advertisement for Amazon FSx File Gateway, featuring a diagram of a cloud storage system and the text: "Amazon FSx File Gateway" and "Fast, efficient on-premises access to fully managed cloud file storage".

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).

The screenshot shows the AWS EC2 Instances page. The left sidebar is expanded to show the 'Instances' section. The main area displays a table with columns for Name, Instance ID, and Instance state, stating "You do not have any instances". A modal dialog titled "Select an instance" is open. In the top right corner of the page, there is a dropdown menu for the Region, currently set to "Oregon". A dropdown menu for "Search instances" is also visible. The bottom of the screen shows the browser's address bar with the URL "https://console.aws.amazon.com/ec2/v2/home?region=us-east-1" and a footer with copyright information and links to Privacy, Terms, and Cookie preferences.

85. Select the EC2 instance.

The screenshot shows the AWS EC2 Instances page. On the left sidebar, under the 'Instances' section, 'Instances' is selected. In the main content area, there is a table titled 'Instances (1)'. It shows one instance: 'WebServer' with Instance ID 'i-0c8f34ecaedb42e5', which is 'Running' on 't2.micro' type. The status check shows '2/2 checks passed' and no alarms. At the top right of the table, there is a 'Launch instances' button. Below the table, a modal window titled 'Select an instance' is open.

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

The screenshot shows the AWS EC2 Instances page. The 'Actions' dropdown menu is open, and the 'Stop instance' option is highlighted. The main content area shows the same instance 'WebServer' as in the previous screenshot, but now with a 'Stop' icon next to its name. The 'Details' tab is selected in the instance summary panel.

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

The screenshot shows the AWS EC2 Instances page with a confirmation dialog box titled 'Stop instance?'. The dialog lists the instance ID 'i-0c8f34ecaedb42e5 (WebServer)' and contains the message 'To confirm that you want to stop the instance, choose the Stop button below.' There are 'Cancel' and 'Stop' buttons at the bottom of the dialog. The main content area shows the instance 'WebServer' with a 'Stop' icon next to its name, and the 'Details' tab is selected in the instance summary panel.

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.

The screenshot shows the AWS EC2 Instances page. A modal window is open with the title "Failed to stop the instance i-0c8f34ecaedb42e5". The message states: "You are not authorized to perform this operation. Encoded authorization failure message: 9zihGbMGbq_2gqJelKV182ky0lwhfcM82qmBhgyW4gZaMj6WMXeSfarHezNlZ5R9OQpwZ3BMGae8-gW2SeqknhN2B-QkzLSzSGZylH3JkIrgAWUTDfc99oeTalHzbDvSosSBx5Sh1zCb0s_wpNV_4avghpHOi7RlBo66nfpmKurspy1n4tIA3B5MZOUBoOu0yskD6l8WnYY4QclkxAoL067dRo-E0zjPifchU7o16VFL4DqMcLaPmQWZ0OsSwRIEPie4lh9_tJkIk3SgouQxRPYQwGR0MrDi_Vo9qmtcPqJASCLsgpp_VL7kaSHbrgLnaPseY4f5Ok7K1mLQCqjIMMPvOoPbvB9lp_yo22DVoZx8oy7gCLOANQU3C9LwU_SdaFnCfYRIPZuQ315Zd1MxyM3pVWEHDsgMtHTk_ZhilFcUjamD5qJhisYVSO2DthlqWYXg3HtanYqIUHtnqeSwjLuYX8obAK73PSNK7TbUH_4OaqQhHt4r9qii2X76XCOGnXcxSNmsTL_kzv7xJmlnEzyIBDLf9RTVYkeydrRWkqd5P0ChWHTISZUAcwqdBKUq1gSDmhR0XbmCtDXIu7E-Wd9UGGeSKS6JHRGPMMJ980f1o7BU1Xj3Y0jA8XII7xATHtUq2D9LCoNqKcsOSSPvPVXzkGNuNoeeXkwsxrhrzzq3xLoOGXEH4JVq_Y4AuLSJzPR6gYB25DOPh4toDzmMKFwVNA3uMg3nyFnDzzbApuyJnT31ooa8FR7FQzb4BeRA_ohE-PeGbwBQ_KG23BIL4LfM66PttxDUnVQmN2jyhFOPfUP4nvfOY6tdZ0opw0FleYz0YdA". Below the modal, the main EC2 Instances table shows one instance (1/1) with the status "Running".

89. Next, check if user-2 can access Amazon S3.

90. Choose the Services menu, and choose S3.

The screenshot shows the AWS Services menu. The "Recently visited" section includes EC2, EC2 Global View, Events, Tags, Limits, and Instances. The "Favorites" section includes Analytics, Application Integration, AR & VR, AWS Cost Management, Blockchain, Business Applications, Compute, Containers, and Customer Enablement. The "All services" section has S3 selected, which is highlighted with a star icon. Other services listed include EC2, Virtual Servers in the Cloud, and Console Home.

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

The screenshot shows the Amazon S3 Account snapshot page. The left sidebar lists Buckets, Storage Lens, and Feature spotlight. The main area shows an "Account snapshot" with a "Storage lens provides visibility into storage usage and activity trends. Learn more" link. Below it is a "Buckets (0) Info" section with a table header: Name, AWS Region, Access, Creation date. A red error box at the bottom states: "You don't have permissions to list buckets. After you or your AWS administrator have updated your permissions to allow the s3>ListAllMyBuckets action, refresh this page. Learn more about Identity and access management in 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.

The screenshot shows the AWS S3 console. The left sidebar includes 'Buckets', 'Access Points', 'Object Lambda Access Points', 'Multi-Region Access Points', 'Batch Operations', 'Access analyzer for S3', and 'Block Public Access settings for this account'. Under 'Storage Lens', there are 'Dashboards' and 'AWS Organizations settings'. The main area displays an 'Account snapshot' with 'Storage lens provides visibility into storage usage and activity trends. Learn more'. Below it, 'Buckets (0) Info' is shown with a note: 'Buckets are containers for data stored in S3. Learn more'. A toolbar with 'Copy ARN', 'Empty', 'Delete', and 'Create bucket' buttons is present. A search bar 'Find buckets by name' is also visible. A prominent error message in a red-bordered box states: 'You don't have permissions to list buckets. After you or your AWS administrator have updated your permissions to allow the s3>ListAllMyBuckets action, refresh this page. Learn more about Identity and access management in Amazon S3'. The top right shows 'Account ID: 5203-3853-0740', 'IAM user: user-2', and 'Sign out' buttons. The bottom navigation bar includes links for 'Feature spotlight', 'https://s3.console.aws.amazon.com/s3/logout/doLogout', '© 2022, Amazon Web Services, Inc. or its affiliates.', 'Privacy', 'Terms', and 'Cookie preferences'.

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:

- IAM user name: user-3
- Password: Lab-Password3

The screenshot shows a private browser window with the title 'Amazon Web Services Sign-In'. The address bar shows 'us-west-2.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3Aconsole%2Fcanvas&code_challenge=OybK5YGVu...'. The page features the AWS logo and a 'Sign in as IAM user' form. The form includes fields for 'Account ID (12 digits) or account alias' (520338530740), 'IAM user name' (user-3), 'Password' (redacted), and a 'Remember this account' checkbox. Below the form is a 'Sign in' button. To the right of the form is an advertisement for 'Try Amazon OpenSearch Service for Free', which offers 750 free hours per month of a single-AZ t2.small.search or t3.small.search instance. It features a magnifying glass icon over a cloud and search interface.

98. Choose the Services menu, and choose EC2.

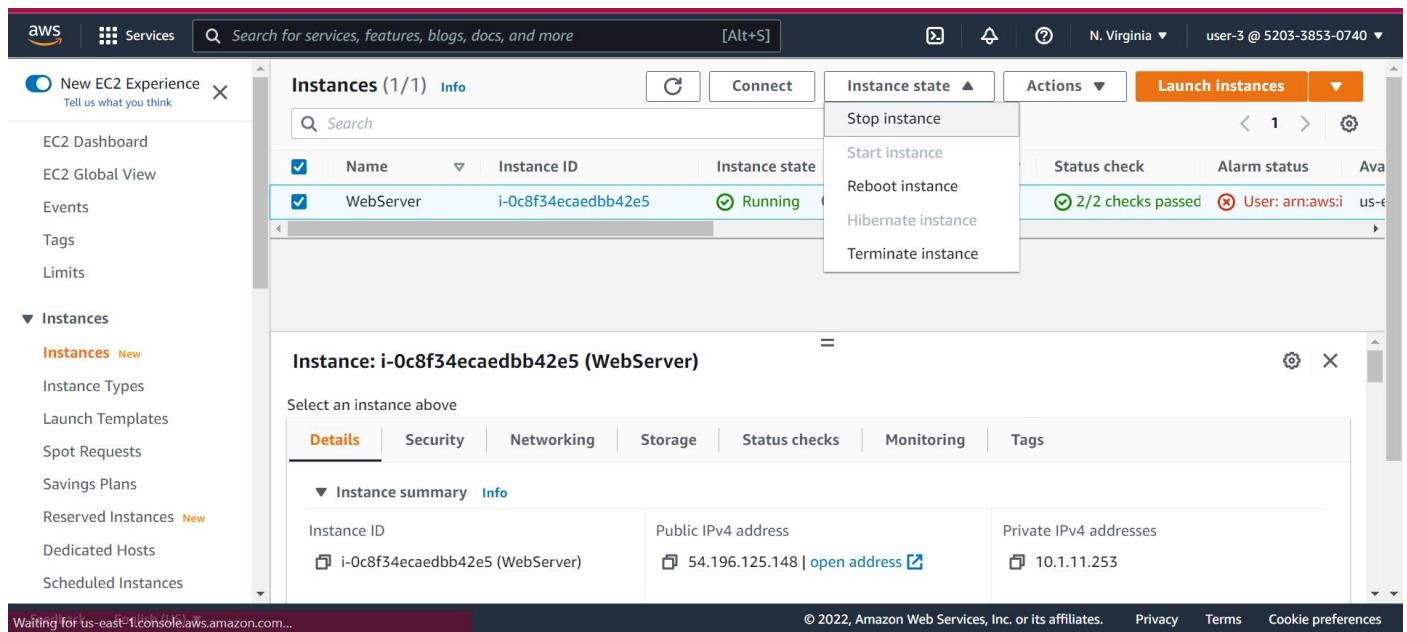
99. In the navigation pane on the left, choose Instances.

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).

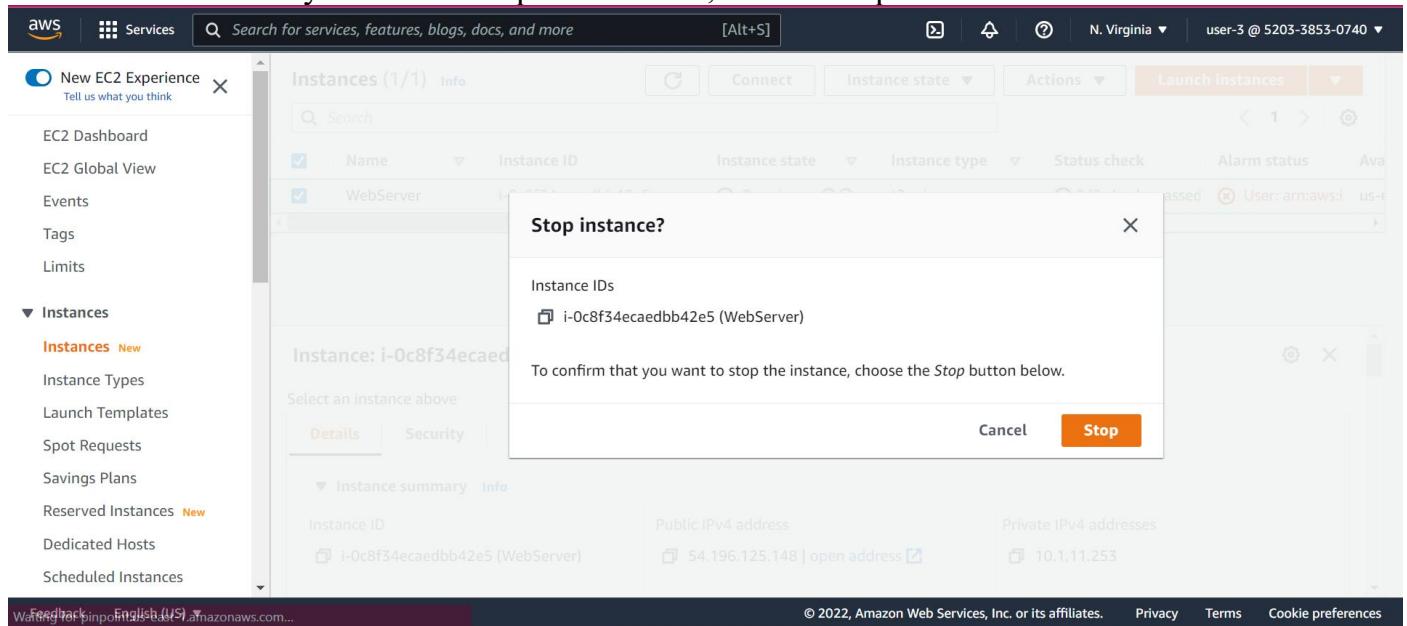
102. Select the EC2 instance.

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



The screenshot shows the AWS EC2 Instances page. A single instance named "WebServer" is listed with the ID "i-0c8f34ecaedb42e5" and a status of "Running". The "Actions" dropdown menu is open, showing options: Stop instance, Start instance, Reboot instance, Hibernate instance, and Terminate instance. The "Stop instance" option is highlighted. The page also includes a search bar, navigation buttons, and a status summary table.

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



The screenshot shows the AWS EC2 Instances page with a confirmation dialog titled "Stop instance?". The dialog lists the instance ID "i-0c8f34ecaedb42e5 (WebServer)". Below the dialog, the main page displays the instance details: Name (WebServer), Instance ID (i-0c8f34ecaedb42e5), Instance state (Running), Instance type (t2.micro), Status check (2/2 checks passed), and Alarm status (User: arn:aws:lambda:us-east-1:...). The "Stop" button in the dialog is highlighted.

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.

The screenshot shows the AWS EC2 Instances page. A success message at the top says "Successfully stopped i-0c8f34ecaedb42e5". The main table lists one instance: "WebServer" (Instance ID: i-0c8f34ecaedb42e5), which is currently "Stopping". It is of type "t2.micro" and has passed 2/2 checks. The "Actions" dropdown menu is open, showing options like "Stop", "Start", "Reboot", "Launch instances", and "Delete". Below the table, a detailed view for the instance "i-0c8f34ecaedb42e5 (WebServer)" is shown, including its details like Instance ID, Public IPv4 address (54.196.125.148), and Private IPv4 addresses (10.1.11.253). The sidebar on the left is expanded to show the "Instances" section.

106. Close your private browser window.

The screenshot shows the AWS IAM Dashboard. At the top, there is a banner about the new IAM dashboard experience. The main area displays the following information:

- Account ID:** 5203-3853-0740
- Federated user:** voclabs/user1868139=1928228@kiit.ac.in
- Dashboard** (highlighted)
- MFA for root user**: A note to enable MFA for the root user.
- Resources** summary:
 - Groups: 4
 - Users: 14
 - Roles: 2
 - Policies: 0
 - Identity providers: 0
- Tools**: Includes links to "Policy simulator" and "Billing Dashboard".

Lab Complete

The screenshot shows the AWS Management Console with the URL "AICv1Sem1EN-15376 > Modules > Module 7 - Security 1 > Lab 7 - IAM". On the left, there is a sidebar with "Account", "Modules", "Discussions", "Grades", "Courses", and "Calendar". The main area shows a confirmation dialog box asking "Are you sure you want to end the lab?". It includes a warning: "If you choose yes, all the resources and data that have been configured in your AWS account will be permanently deleted." Two buttons at the bottom are "Yes" and "No".