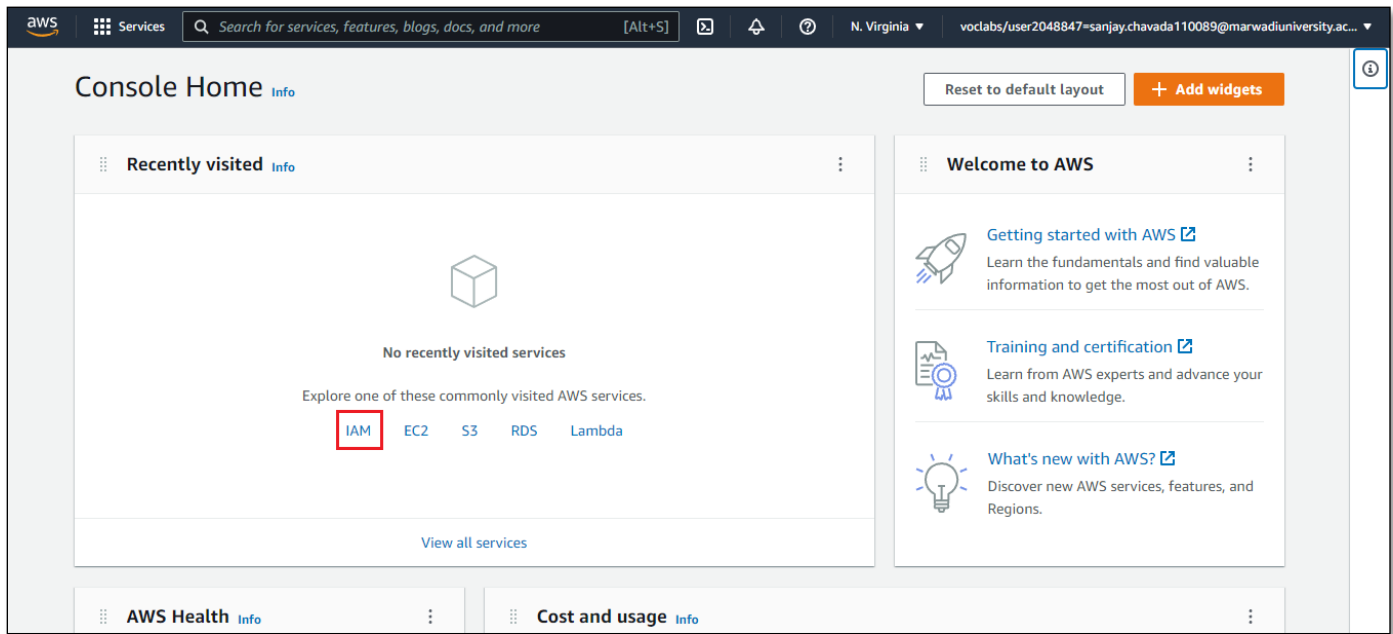


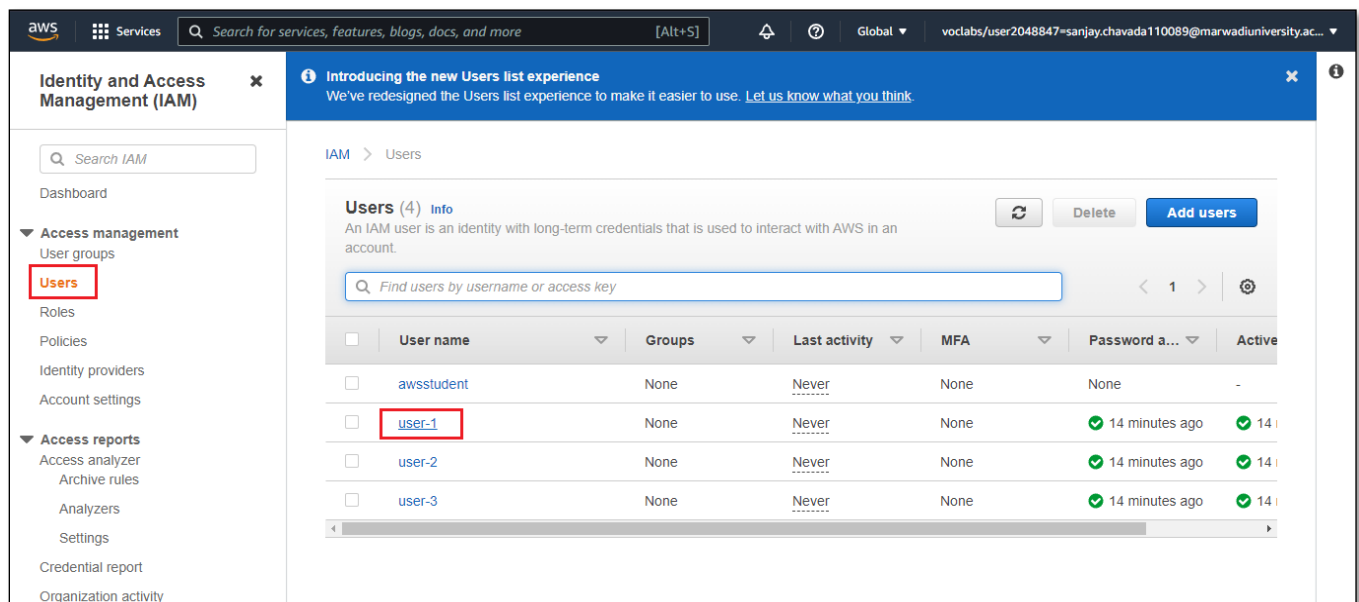
Practical 6 : Introduction to AWS Identity and Access Management(IAM)

Task 1: Explore the Users and Groups

1. In the **AWS Management Console**, on the **Services** menu, select **IAM**.



2. In the navigation pane on the left, choose **Users**.
3. Choose **user-1**.



4. Choose the **Groups** tab.
5. Choose the **Security credentials** tab.

user-1 is assigned a **Console password**

Users > user-1

Summary

User ARN am:aws:iam::372835209530:user/spl66/user-1

Path /spl66/

Creation time 2022-08-30 08:06 UTC+0530

Permissions Groups Tags (1) Security credentials Access Advisor

Add user to groups

Group name	Attached permissions
No results	

Users > user-1

Summary

User ARN am:aws:iam::372835209530:user/spl66/user-1

Path /spl66/

Creation time 2022-08-30 08:06 UTC+0530

Permissions Groups Tags (1) Security credentials Access Advisor

Sign-in credentials

Summary • Console sign-in link: <https://372835209530.signin.aws.amazon.com/console>

Console password	Enabled (never signed in) Manage
Assigned MFA device	Not assigned Manage
Signing certificates	None

Task 2: Add Users to Groups

Add user-1 to the S3-Support Group

6. In the left navigation pane, choose **User groups**.
7. Choose the **S3-Support** group.
8. Choose the **Users** tab.
9. In the **Users** tab, choose **Add users**.
10. In the **Add Users to S3-Support** window, configure the following:
 - Select **user-1**.
 - At the bottom of the screen, choose **Add Users**.

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Service control policies (SCPs)

Filter: User groups by property or group name and press enter

<input type="checkbox"/>	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	EC2-Admin	↕ Loading	↕ Loading	4 minutes ago
<input type="checkbox"/>	EC2-Support	↕ Loading	↕ Loading	4 minutes ago
<input type="checkbox"/>	S3-Support	↕ Loading	↕ Loading	4 minutes ago

Users

Permissions

Access Advisor

Users in this group (0) 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

Search

1

<input type="checkbox"/>	awsstudent	You need permissions	None	36 minutes ago
<input checked="" type="checkbox"/>	user-1	0	None	37 minutes ago
<input type="checkbox"/>	user-2	0	None	37 minutes ago
<input type="checkbox"/>	user-3	0	None	37 minutes ago

Cancel

Add users

Add user-2 to the EC2-Support Group

You have hired **user-2** into a role where they will provide support for Amazon EC2.

11. Using similar steps to the ones above, add **user-2** to the **EC2-Support** group.

user-2 should now be part of the **EC2-Support** group.

aws

Services

Search for services, features, blogs, docs, and more

[Alt+S]

Global

voclabs/user2048847-sanjay.chavada110089@marwadiuniversity

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

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.

Filter User groups by property or group name and press enter

1

<input type="checkbox"/>	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	EC2-Admin	0	Defined	23 minutes ago
<input checked="" type="checkbox"/>	EC2-Support	0	Defined	23 minutes ago
<input type="checkbox"/>	S3-Support	0	Defined	23 minutes ago

	User name	Groups	Last activity	Creation time
<input type="checkbox"/>	awsstudent	You need permissions	None	48 minutes ago
<input type="checkbox"/>	user-1	1	None	49 minutes ago
<input checked="" type="checkbox"/>	user-2	0	None	49 minutes ago
<input type="checkbox"/>	user-3	0	None	49 minutes ago

Cancel
Add users

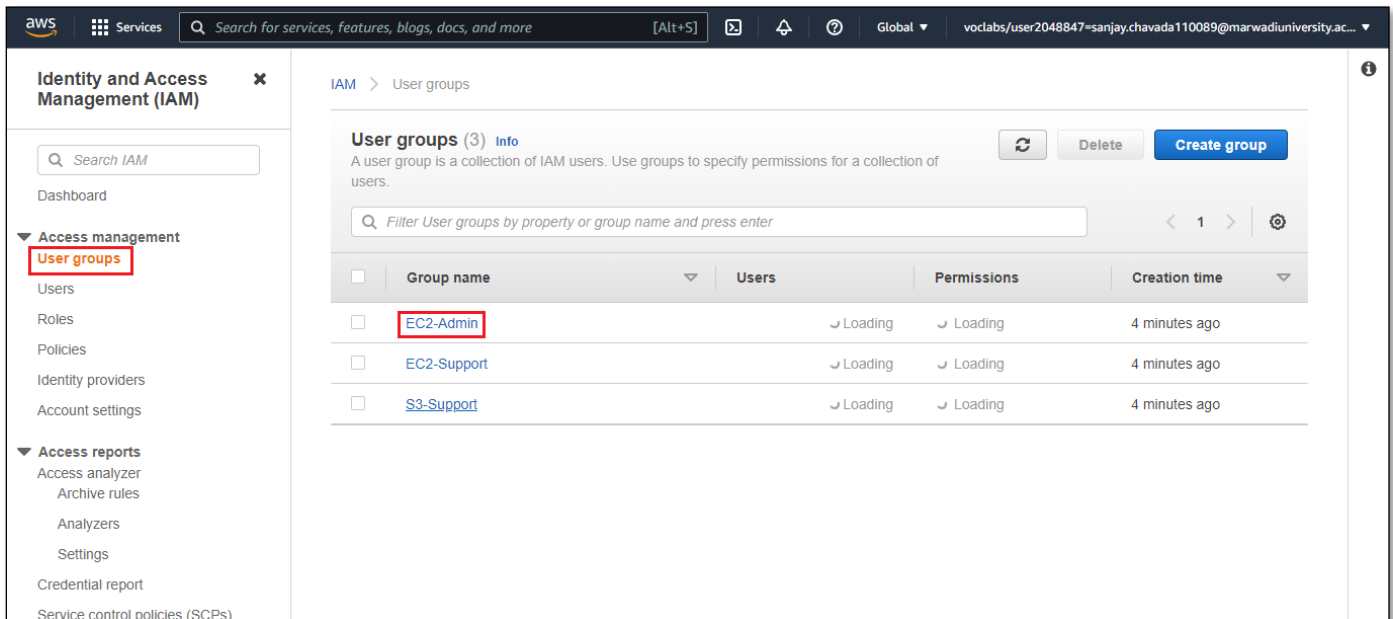
Add user-3 to the EC2-Admin Group

You have hired **user-3** as your Amazon EC2 administrator, who manage your EC2 instances.

12. Using similar steps to the ones above, add **user-3** to the **EC2-Admin** group.

user-3 should now be part of the **EC2-Admin** group.

13. In the navigation pane on the left, choose **User groups**.



The screenshot shows the AWS IAM console interface. On the left, the 'Identity and Access Management (IAM)' navigation pane is visible, with 'User groups' highlighted under the 'Access management' section. The main content area displays 'User groups (3)' with a table listing the groups. The 'EC2-Admin' group is highlighted with a red box.

Group name	Users	Permissions	Creation time
EC2-Admin	↕ Loading	↕ Loading	4 minutes ago
EC2-Support	↕ Loading	↕ Loading	4 minutes ago
S3-Support	↕ Loading	↕ Loading	4 minutes ago

	User name	Groups	Last activity	Creation time
<input type="checkbox"/>	awsstudent	You need permissions	None	49 minutes ago
<input type="checkbox"/>	user-1	1	None	50 minutes ago
<input type="checkbox"/>	user-2	1	None	50 minutes ago
<input checked="" type="checkbox"/>	user-3	0	None	50 minutes ago

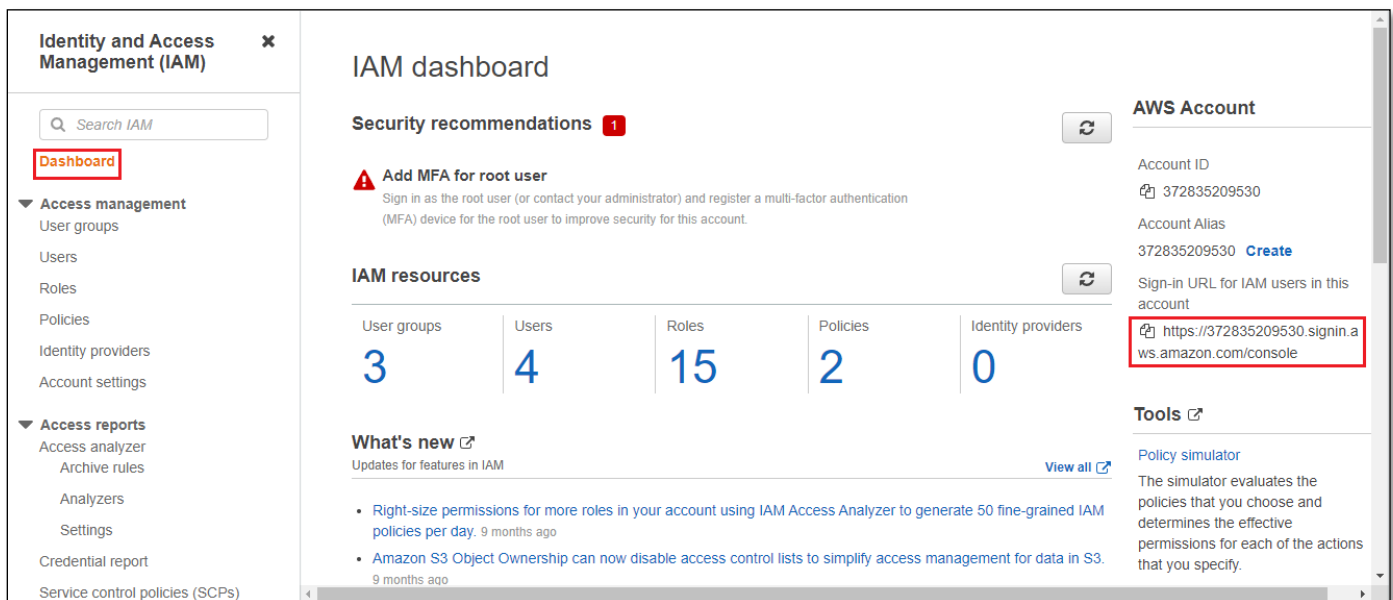
Cancel
Add users

Task 3: Sign-In and Test Users

In this task, you will test the permissions of each IAM User.

14. In the navigation pane on the left, choose **Dashboard**.

15. Copy the **Sign-in URL for IAM users in this account** to a text editor.



The screenshot shows the AWS IAM dashboard. On the left, the navigation pane has 'Dashboard' highlighted. The main content area shows the IAM dashboard with a security recommendation to add MFA for the root user. Below this, the IAM resources summary shows 3 user groups, 4 users, 15 roles, 2 policies, and 0 identity providers. The 'What's new' section lists updates for IAM features. On the right, the 'AWS Account' section displays the account ID, alias, and the sign-in URL for IAM users, which is highlighted with a red box: <https://372835209530.signin.aws.amazon.com/console>.

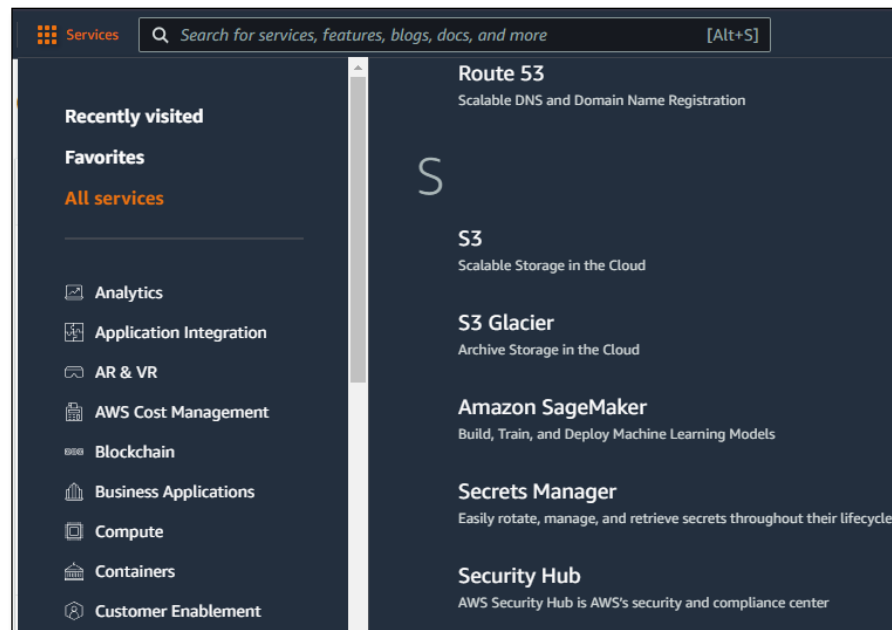
16. Open a private (Incognito) window.

17. Paste the **IAM users sign-in** link into the address bar of your private browser session and press **Enter**.

18. Sign-in with:

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

19. In the **Services** menu, choose **S3**.



20. Choose the name of the bucket that exists in the account and browse the contents.

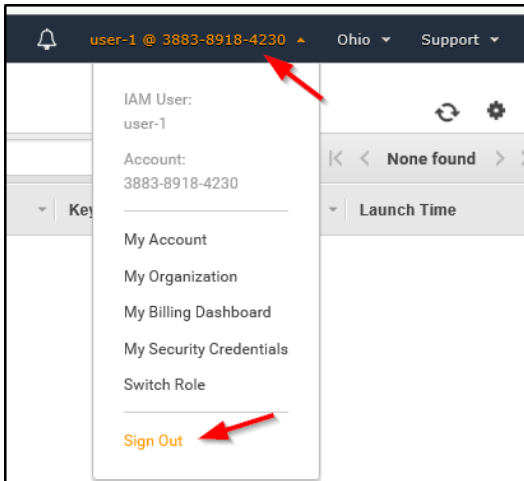
Since your user is part of the **S3-Support** Group in IAM, they have permission to view a list of Amazon S3 buckets and the contents.

21. In the **Services** menu, choose **EC2**.

22. In the left navigation pane, choose **Instances**.

23. Sign user-1 out of the **AWS Management Console** by completing the following actions:

- At the top of the screen, choose **user-1**
- Choose **Sign Out**



24. Paste the **IAM users sign-in** link into your private browser tab's address bar and press **Enter**.

25. Sign-in with:

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

26. In the **Services** menu, choose **EC2**.

27. In the navigation pane on the left, choose **Instances**.

28. In the **Instance state** menu above, select **Stop instance**.

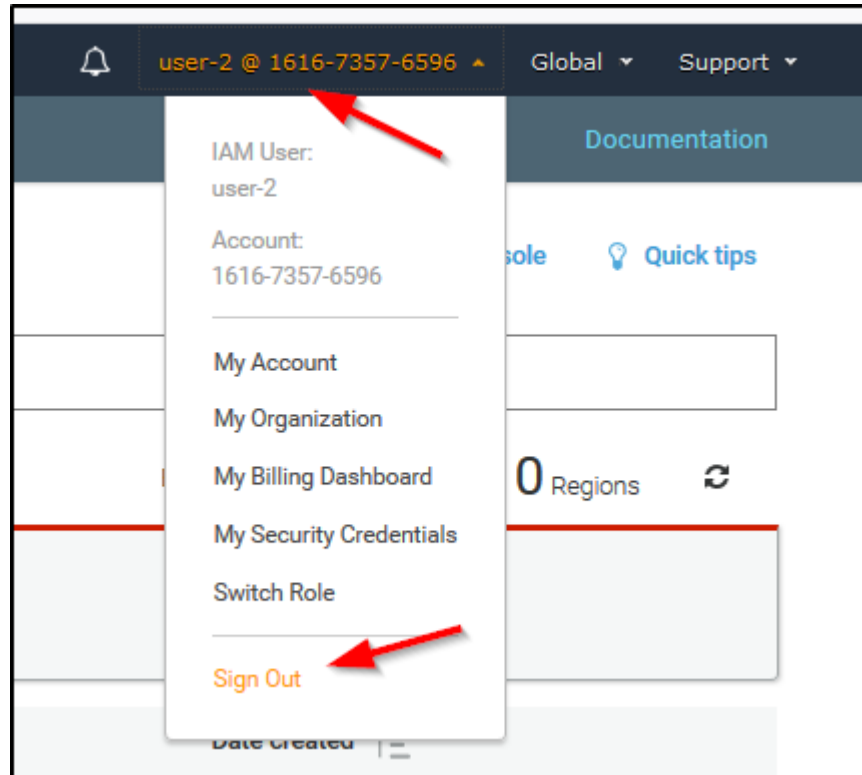
29. In the **Stop Instance** window, select **Stop**.

30. Choose the X to close the *Failed to stop the instance* message.

31. In the **Services**, choose **S3**.

32. Sign user-2 out of the **AWS Management Console** by completing the following actions:

- At the top of the screen, choose **user-2**
- Choose **Sign Out**



33. Paste the **IAM users sign-in** link into your private window and press **Enter**.

34. Paste the sign-in link into the address bar of your private web browser tab again. If it is not in your clipboard, retrieve it from the text editor where you stored it earlier.

35. Sign-in with:

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

36. In the **Services** menu, choose **EC2**.

37. In the navigation pane on the left, choose **Instances**.

38. In the **Instance state** menu, choose **Stop instance**.

39. In the **Stop instance** window, choose **Stop**.

40. Close your private browser window.