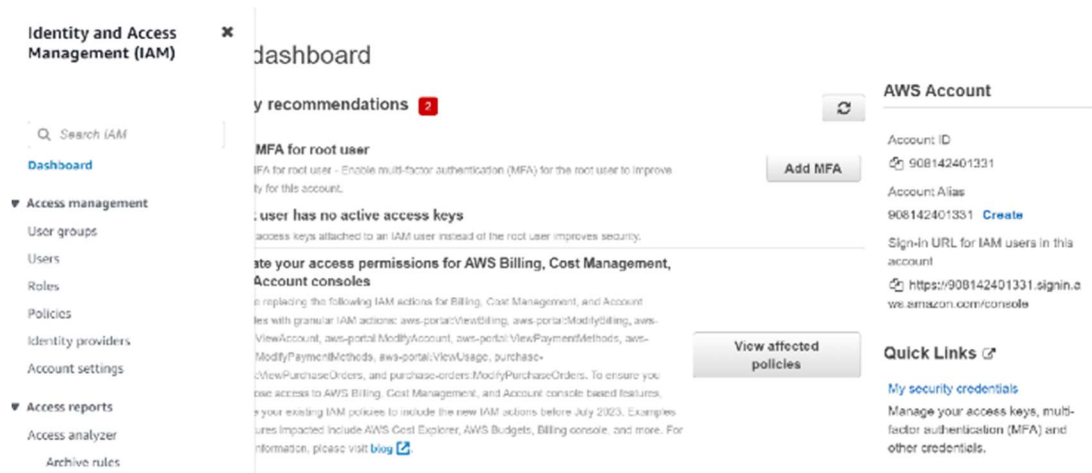


PRACTICAL 6

Aim: Study Cloud Security management

STEPS:

1. Go to AWS and login as Root user and you will get the following page.

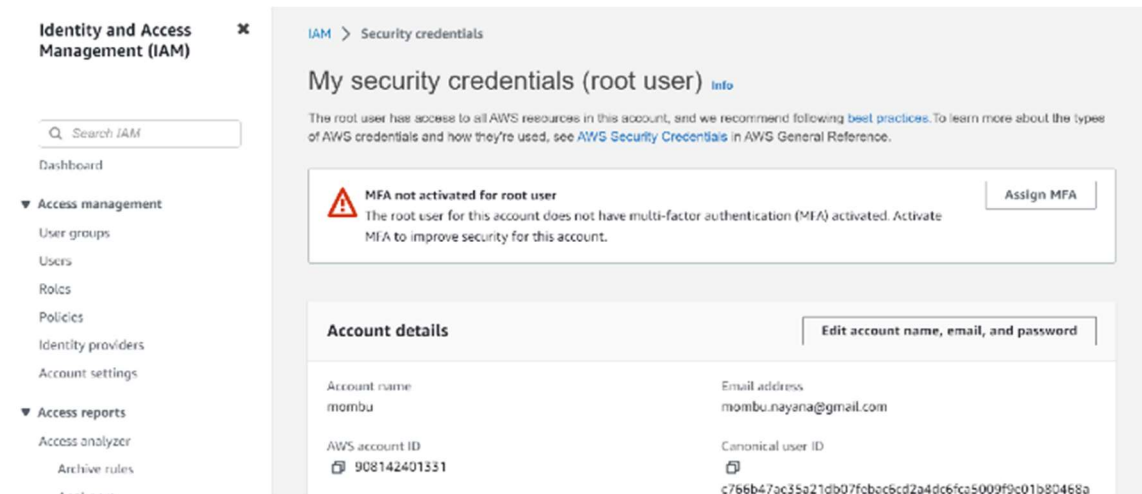


The screenshot shows the AWS IAM dashboard for the root user. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and a search bar. The main content area displays the dashboard with several recommendations:

- MFA for root user:** A recommendation to enable multi-factor authentication (MFA) for the root user to improve security. It includes an "Add MFA" button.
- user has no active access keys:** A message stating that no access keys are attached to the root user, which improves security. It includes a "View affected policies" button.
- Update your access permissions for AWS Billing, Cost Management, and Account consoles:** A message explaining that the root user's permissions are being updated to include granular IAM actions for Billing, Cost Management, and Account consoles. It includes a "View affected policies" button.

On the right side, the **AWS Account** section displays the Account ID (908142401331), Account Alias (908142401331), and a link to the Sign-in URL for IAM users. Below this, the **Quick Links** section provides a link to "My security credentials" and a brief description of what it manages.

2. Click on security credentials.



The screenshot shows the "My security credentials (root user)" page in the AWS IAM console. The page displays the following information:

- Account details:** A table showing the Account name (mombu), Email address (mombu.nayana@gmail.com), AWS account ID (908142401331), and Canonical user ID (c766b47ac35a21db07fcbac6cd2a4dc6ca5009f9c01b80468a).
- MFA not activated for root user:** A warning message stating that the root user does not have multi-factor authentication (MFA) activated. It includes an "Assign MFA" button.

The page also includes a search bar and navigation links for Identity and Access Management (IAM), Access management, Access reports, and a search bar.

3. Click on user groups > Click on create group

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

Name the group

User group name
Enter a meaningful name to identify this group.

Maximum 128 characters. Use alphanumeric and "-", "@", "." characters.

Add users to the group - Optional (2) [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. A user can belong to up to 10 groups.

Search

<input type="checkbox"/>	User name ?	Groups	Last activity	Creation time
<input type="checkbox"/>	rehan	0	None	34 minutes ago
<input type="checkbox"/>	shweta	0	22 minutes ago	25 minutes ago

4. Enter group name, and select the users to be added to group. Then click on create group.

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

User groups (1) [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

[Create group](#)

<input type="checkbox"/>	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	ruparel	2	Loading	Now

5. Click on users and then click on a particular user.

Identity and Access Management (IAM)

Created: February 09, 2023, 09:40 (UTC+05:30) | Last console sign-in: - | Access key 2: Not enabled

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Permissions | Groups (1) | Tags | Security credentials | Access Advisor

Permissions policies (0)

Permissions are defined by policies attached to the user directly or through groups.

Find policies

Policy name | Type | Attached via

No policies

6. Then add permissions.

☐ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ Copy permissions
Copy all group memberships, attached managed policies, inline policies, and any existing permissions boundaries from an existing user.

☒ Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1038)

Find policies

1 2 3 4 5 6 7 ... 52

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	AccessAnalyzerService...	AWS managed	0
<input type="checkbox"/>	AdministratorAccess	AWS managed - job function	1
<input type="checkbox"/>	AdministratorAccess-A...	AWS managed	0
<input type="checkbox"/>	AdministratorAccess-A...	AWS managed	0

7. Click on attach policies directly and select administrator access. Click on next.

Step 1
[Add permissions](#)

Step 2
Review

Review

The following policies will be attached to this user. [Learn more](#)

User details

User name
rohan

Permissions summary (1)

Name	Type	Used as
AdministratorAccess	AWS managed - job function	Permissions policy

[Cancel](#)
[Previous](#)
[Add permissions](#)

8. Click Add permissions

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

Analysers

1 policy added

Created: February 09, 2023, 09:40 (UTC+05:30)

Last console sign-in: -

Access key 2: Not enabled

Permissions | Groups (1) | Tags | Security credentials | Access Advisor

Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

Find policies

Policy name	Type	Attached via
AdministratorAccess	AWS managed - job function	Directly

Permissions boundary (not set)

Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. [Learn more](#)

9. Go to the tab security credentials. Click on Assign MFA device.

The screenshot shows the AWS IAM console interface. On the left is a navigation sidebar with links like 'Dashboard', 'Access management', 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings', 'Access reports', 'Access analyzer', and 'Archive rules'. The main content area is titled 'Multi-factor authentication (MFA) (0)' and includes a description: 'Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)'. Below this are three buttons: 'Remove', 'Resync', and 'Assign MFA device'. A table below the buttons has headers 'Device type', 'Identifier', and 'Created on'. At the bottom, a message states 'No MFA devices. Assign an MFA device to improve the security of your AWS environment' with an 'Assign MFA device' button.

10. Enter device name, select MFA device as authenticator app and click on next.

The screenshot shows the 'Assign MFA device' wizard. The first step is 'Device name', with the instruction 'Enter a meaningful name to identify this device.' and a text input field containing 'device123@'. Below the field is a note: 'Maximum 128 characters. Use alphanumeric and '+', '-', '@', and '_' characters.' The second step is 'Select MFA device', with the instruction 'Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.' and an 'Info' link. There are two options: 'Authenticator app' (selected with a blue radio button) and 'Security Key' (unselected with a white radio button). The 'Authenticator app' option includes an icon of a smartphone and the description: 'Authenticate using a code generated by an app installed on your mobile device or computer.' The 'Security Key' option includes an icon of a USB key and the description: 'Authenticate using a code generated by a USB key or a Windows Hello facial scanner.'

11. Click show QR code. Open the google authenticator app on mobile and enter the MFA codes 1 and 2, click **ADD MFA**.

1 Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer. [See a list of compatible applications](#)

2 [Show QR code](#)

Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key. [Show secret key](#)

Fill in two consecutive codes from your MFA device.

MFA code 1

MFA code 2

12. Then add copy the console sign in link and enter the username and password. Enter the MFA code. The user will be given access to the console.

Identity and Access Management (IAM)

Created: February 09, 2023, 09:40 (UTC+05:30) | Last console sign-in: - | Access key 2: Not enabled

Permissions | Groups (1) | Tags | **Security credentials** | Access Advisor

Console sign-in [Enable console access](#)

Console sign-in link: <https://908142401331.signin.aws.amazon.com/console> | Console password: Not enabled

Multi-factor authentication (MFA) (1)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

[Remove](#) [Resync](#) [Assign MFA device](#)

Device type	Identifier	Created on
-------------	------------	------------