

# Assignment Interview question

**Note :- Please prepare the answer of these questions in brief :- (in your own words)**

## 1. What is the need of IAM?

IAM is very powerful service in AWS. With IAM we can manage users and groups of users. From the organization perspective we can't give root credential to all the developers. So it is best practice to create IAM user for other users working in the organization or create a IAM group to manage those user. Using IAM organization can have complete control over AWS services like which service IAM user can access and what operation that user can perform on particular service and which not by using IAM policy.

## 2. If I am a non tech person, how will you define policies in IAM.

It is always best practice to provide least privileges in IAM policy. So, for non tech person I will only provide the access which is needed and restrict all other services.

## 3. Please define a scenario in which you would like to create your own IAM policy.

it is best practice to create own policy instead of using AWS pre-defined policy. Because it is easy to understand our own created IAM policy from scratch. We can have more control over user by creating own IAM policy.

## 4. Why do we prefer not using root account?

After creation of AWS account, we can access the service by logging into root user credential to use the services. Root user has all the privileges like it can access all the AWS services, can see billing dashboard and changing the password as well. So, while working in team If you share your root credential or if it gets exploit then it might be a big problem. So, it is good practice not to use root account.

## 4. How to revoke policy for an IAM user?

On user profile, in the permission section you can check the policies assigned to that user and you can revoke the policy by clicking on cancel button.

Users > Rahul

Summary Delete user ?

User ARN: am:aws:iam::563684797122:user/Rahul

Path: /

Creation time: 2022-04-20 11:24 UTC+0530

Permissions Groups (2) Tags (1) Security credentials Access Advisor

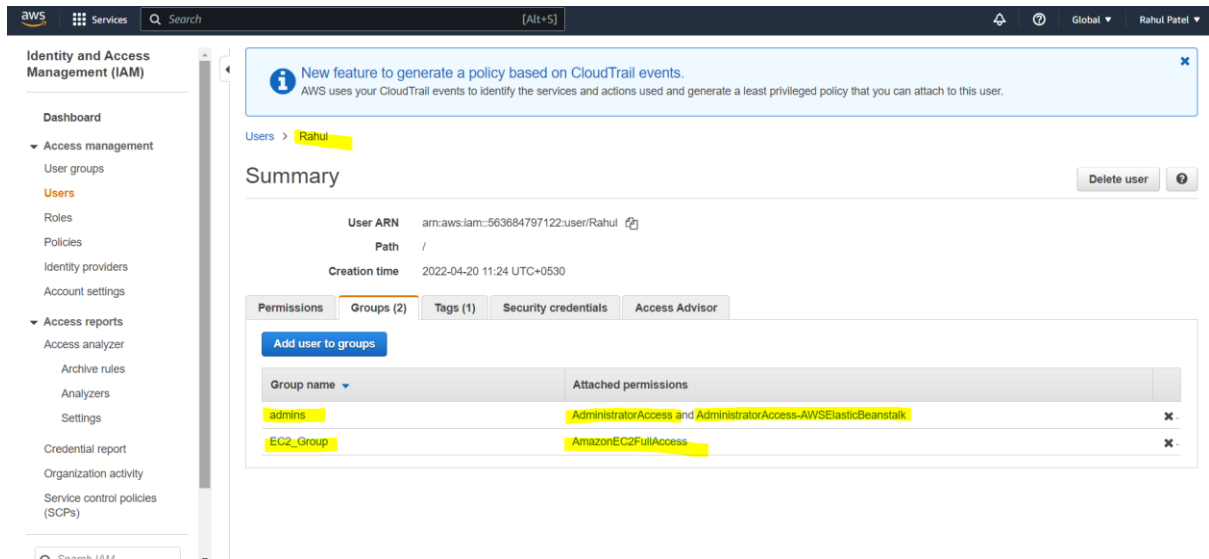
▼ Permissions policies (3 policies applied)

[Add permissions](#) [Add inline policy](#)

Policy name ▼	Policy type ▼
Attached from group	
AdministratorAccess	AWS managed policy from group admins
AdministratorAccess-AWSElasticBeanstalk	AWS managed policy from group admins
<a href="#">Show 1 more</a>	
▶ Permissions boundary (not set)	

## 6. Can a single IAM user be a part of multiple policy via group and root? how?

Yes, single IAM user can be a part of multiple policy via group. You can add single IAM user to Multiple groups by just adding that user in particular group.



The screenshot shows the AWS IAM console interface. On the left is a navigation menu with options like Dashboard, Access management, Users, Roles, Policies, Identity providers, Account settings, Access reports, Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, and Service control policies (SCPs). The main content area displays the 'Summary' page for a user named 'Rahul'. At the top, there's a notification about a new feature to generate a policy based on CloudTrail events. Below the notification, the user's details are shown: User ARN (arn:aws:iam::563684797122:user/Rahul), Path (/), and Creation time (2022-04-20 11:24 UTC+0530). There are buttons for 'Delete user' and a help icon. Below the summary, there are tabs for 'Permissions', 'Groups (2)', 'Tags (1)', 'Security credentials', and 'Access Advisor'. The 'Groups (2)' tab is selected, showing a table with two groups: 'admins' and 'EC2\_Group'. The 'admins' group has two attached permissions: 'AdministratorAccess' and 'AdministratorAccess-AWSElasticBeanstalk'. The 'EC2\_Group' has one attached permission: 'AmazonEC2FullAccess'. Each group entry has a delete icon (X) on the right.

**Identity and Access Management (IAM)**

**Dashboard**

- Access management
  - User groups
  - Users**
  - Roles
  - Policies
  - Identity providers
  - Account settings
- Access reports
  - Access analyzer
  - Archive rules
  - Analyzers
  - Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

**Summary** Delete user ?

**User ARN** arn:aws:iam::563684797122:user/Rahul ?

**Path** /

**Creation time** 2022-04-20 11:24 UTC+0530

**Permissions** **Groups (2)** **Tags (1)** **Security credentials** **Access Advisor**

**Add user to groups**

Group name	Attached permissions	
admins	AdministratorAccess and AdministratorAccess-AWSElasticBeanstalk	X
EC2_Group	AmazonEC2FullAccess	X