

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

1. What is the need of IAM?

- Authentication (is it the right user?) and Authorization (do they have the right access?)
- Identities can be AWS users or Federated users (externally authenticated users)
- Provides very granular control Limit a single user: to perform single action on a specific AWS resource from a specific IP address during a specific time window

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

- Two person works in a restaurant, one person has permission to get inside the kitchen but other has only to take orders. 2nd person also has to generate the billing but 1st person does not have. Similarly, in aws using IAM policy we can allow/restrict access to a user/resource.

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

- I'll provide access to terminate, stop and reboot the server, However, using policy I'll restrict the access to terminate the instance.

4. Why do we prefer not using root account?

- Root account is the super user in aws. It has all the privilege to do in aws. For security best practice, we should avoid using root user. Instead create a user and provide admin access to avoid any vulnerability.

5. How to revoke policy for an IAM user?

- Policies can be revokes by deleted it via console, API or CLI.

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

- One user can be part of multiple groups. Two groups can have multiple allow/deny policies.
- For example, one group has ec2FullAccess and another group has s3FullAccess. So, in this case, IAM user can access both the Service, ec2 and s3.

Also, if one group has deny policy and another group has allow policy then deny policy will take precedence over allow.