

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 stands for identity and access management and it is a very useful and powerful service of AWS with the help of which we can assign only the services required to perform task to specific or different users as it is not feasible to provide root credentials to all the users

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

- One should initially always provide least privileges in IAM policy.

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

- Creating own IAM policies can be useful in many cases such as one can create custom IAM policy where in the administrator wants to deactivate or revoke all services provided to users if there is no user activity in certain duration (months) or we can say like for only certain given duration services will be accessible after that it would not allow to user to

access the services.

4. Why do we prefer not using root account?

- We do not prefer because Root has all the privileges and can access all the services and data including billing details and if when working root credentials are shared or get exploited then it may be cause to a bigger problem .




5. How to revoke policy for an IAM user?

- Policy can be revoked by going to the User profile in permissions section. In permissions section, assigned policies to user can be seen and from here you can revoke policy by clicking cancel (cross sign)

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

- Yes, single IAM user can be part of multiple policy via group and root.
- One can add IAM user to more than one group and assign more than one policy to user.

[Alt+S]



Global

Sheet

IAM > Users > ironman

ironman

Delete

Summary

ARN
am:aws:iam::677212140661:user/ironman

Console access
Disabled

Access key 1
Not enabled

Created
February 02, 2023, 00:19 (UTC+05:30)

Last console sign-in
-

Access key 2
Not enabled

Permissions

Groups (2)

Tags

Security credentials

Access Advisor

Permissions policies (3)

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

Find policies

< 1 >

<input type="checkbox"/>	Policy name	Type	Attached via
<input type="checkbox"/>	AdministratorAccess	AWS managed - job function	Group NO.1
<input type="checkbox"/>	AmazonRDSFullAccess	AWS managed	Group Developer
<input type="checkbox"/>	IAMFullAccess	Customer managed	Group Developer

IAM > Users > ironman

ironman

Delete

Summary

ARN
am:aws:iam::677212140661:user/ironman

Console access
Disabled

Access key 1
Not enabled

Created
February 02, 2023, 00:19 (UTC+05:30)

Last console sign-in
-

Access key 2
Not enabled

Permissions

Groups (2)

Tags

Security credentials

Access Advisor

User groups membership (2)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users. A user can be a member of up to 10 groups at a time.

Group name

Attached policies

Developer	IAMFullAccess and AmazonRDSFullAccess
NO.1	AdministratorAccess