Name :- Rushikesh Anil Mashidkar

Email Id :- rishikeshmashidkar@gmail.com

Note :- The answer is in bullets (➔)

Assignment Interview question IAM 30th Oct'22

1. What is the need of IAM?
   ➔ To secure AWS root account we create a IAM user or groups. We cannot give root account to the team so. And When we have project or something to do but you are not able to do that work and you want the work can done by someone then you can simply create IAM user and only for that work you can give access/permission to your AWS account for that user. And by creating IAM user your work has to done by user you pemitted and also your account will be safely secure.

2. If i am a non tech person, how will you define policies in IAM.
   ➔ IAM policies Securely control individual and group access to your AWS account.

3. Please define a scenerio in which you would like to create your on own IAM policy.
   ➔ I have assignment from ineuron to create an 3 IAM user and put them in one group And I complete that so I wanted to check that assignment directly through my AWS account so for that I created a IAM policy to see ineuron my IAM users and groups and policies.

4. Why do we prefer not using root account?
   ➔ Because root can do whatever he want. Root has full access to your machine/AWS account. He can delet server , important file so we try to keep root access private so we measurly prefer to not use root account safe.

5. How to revoke policy for an IAM user?
   ⇨ For that you can Sign in as an administrator/root account, and open the IAM console. Choose the name of the user with the policy that you want to delete. Choose Delet , If you are deleting a single inline policy in User , type the name of the policy and choose Delete.

6. 6. Can a single IAM user be a part of multiple policy via groupand root? how?
   ⇨ According to google search You can assign IAM users to up to 10 groups. You can also attach up to 10 managed policies to each group, for a maximum of **120 policies** (20 managed policies attached to the IAM user, 10 IAM groups, with 10 policies each). For that you can Sign in as an administrator/root account, and open the IAM console. Choose User groups, and then choose Developers. Choose the Permissions tab, choose Add permissions, and then choose Create inline policy.