Assignment Interview question

Note :-

Please prepare the answer of these questions in brief :- (in

your own words)

1.What is the need of IAM?

- **The demand for secure access has skyrocketed in recent years and on that aspect IAM is must for company for remote workers**
- **slight mismanagement of the user credentials may lead to unprecedented security threats,whether it is password or email addresses,user become a complex issue to track without a proper control system**
- **with large amount of data to be stored,processed etc need modification on daily basis for which they require permissions**
- **and for such scenarios identify and access management (IAM) comes into plays**

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

IAM.

- **To manage access on AWS we generate IAM policies that define levels of permissions and attach them to IAM identities(users, groups, roles) or AWS resources.**
- **there different types of policies that exist in AWS identity-based policies, Inline policies, Resource-based policies , IAM permissions boundaries,Access control lists(ACLs), Organizations Service Control Policies(SCPs) , Session policies**
- **IAM Policies are built using a combination of the below elements:**

- **Version: Defines the version of the policy language. Always use the latest version.**
- **Statement: This argument is used as a parent element for the different statements in the policy.**
- **Sid: This is an optional element that allows us to define a statement ID.**
- **Effect: This element can have the values `Allow` or `Deny`.**
- **Action: The list of actions related to the policy.**
- **Resource: Defines the list of resources to which the policy is applied. For resource-based policies, this is optional since the policy applies to the resource that has it attached.**
- **Principal: Defines the identities that are allowed or denied access to resource-based policies.**

- **Condition: Defines some conditions under which the policy applies. This element is practical when we need to achieve custom rules for fine-grained access.**

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

It is a particular kind of planning which helps businesses to deal with future difficulties. Proper planning is done considering the upcoming scenarios, and businesses lay plans accordingly. All future investment by the company depends on scenario planning. Extreme scenarios are hard to predict; some assumptions can be used to save from the impact.

4. Why do we prefer not using root account?

- **Security:** All the hackers know that there is a root account and they would target the root account to breach in.
- **Applications' Vulnerability:** When an application is served using the root account, in case of vulnerability, hacker can execute code remotely and gain access. Also your application can erase important files or directories mistakenly.
- **Mistakes:** Just like you and me, everyone else can make mistake. While rushing, one can run a command and find himself like "Holy Root! What have I done!". However, typing in "sudo ..." and password would give someone enough time to think twice.
- **Accountability and Responsibility:** To have a clear accountability and responsibility map, users should always use different user accounts based on their roles. This way, we would know who did what and who is responsible for what.

5. How to revoke policy for an IAM user?

- **In the navigation panel choose roles and then choose the name only not the checkbox of the role whose permission you want to revoke and on the summary pages for the selected role choose the revoke sessions tab and on the revoke sessions tab choose the revoke active sessions**

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

- You can not use an IAM policy to restrict access of a root user. The only way to restrict permission to root user is by having Service Control Policy attached to your account You should not use your root user for your everyday task (even administrative ones).