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, the main purpose of IAM is to grant access as per user requirement. For example, if we have a management user then there is no need to provide him the full access of AWS instead, he should be provided with billing access or if we have a user whose work is to upload and download files to S3 bucket then he should only get access of S3 bucket so that he does not messes with other costly services like EC2 and increase the bill of cloud account.

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

For a non tech person we need to define policies with the service the person is going to perform like if the work of non tech person is to download files from S3 bucket then he should be given only that access in policy even we should define expiry of policy. We can even define custom policy with least privilege. It is not recommended to provide full access to a non-tech person.

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

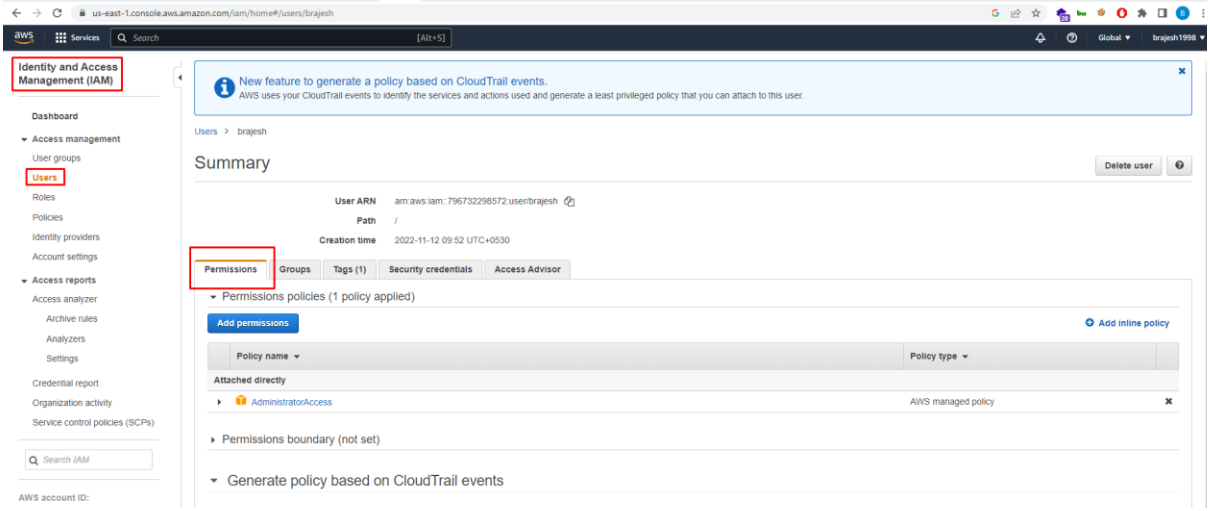
Suppose AWS account which is used by organization needs to be audited by a 3rd Party. So, in that case it is not required to provide them administrative access of AWS account instead we can provide read access of the services used in the organization as auditor does not needs to perform any application specific tasks like creating EC2 instance or adding files to S3 bucket so in that case read permission is sufficient for auditing person to perform his task.

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

Root user is the person who is having all the access and rights in an AWS account. So, if we are doing our work using root user account and if anyhow root user gets compromised by a hacker, then he can do anything with all the resources and there is no way to stop the attacker in a short span, but on the other side if we have an IAM user and his account gets compromised then in that case root user can delete the IAM user whose account has been compromised. In case of IAM user action can be taken quickly just by logging into root user and closing account. So, it is recommended to never use root user for performing any task, root user should be used only to create user, group and for manging bills.

5. **How to revoke policy for an IAM user?**

For revoking policy for an IAM user root user has to login into his account and go to IAM then he needs to choose the IAM user whose policy needs to be revoked and choose permissions and can add or revoke different available policies. Root user can even add custom policies as per requirement.



New feature to generate a policy based on CloudTrail events.
AWS uses your CloudTrail events to identify the services and actions used and generate a least privileged policy that you can attach to this user.

Summary

User ARN: arn:aws:iam::796732298572:user/brajesh
Path: /
Creation time: 2022-11-12 09:52 UTC+0530

Permissions policies (1 policy applied)

Policy name	Policy type
Attached directly	
AdministratorAccess	AWS managed policy

Permissions boundary (not set)

Generate policy based on CloudTrail events

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

Yes, a single IAM user can be a part of multiple policy as an IAM user can be part of multiple groups and in each group, he can have different policy permissions like in one group he might be having access to EC2 in another he might be having access to S3 and so on also that particular user can have different policy permission by root user like having access to CloudFront. So in this way single user can have multiple policy attached.