1. What is AWS Identity and Access Management (IAM)?
AWS IAM is a service that allows you to manage users, groups, and permissions for accessing AWS resources. It provides centralized control over authentication and authorization.

2. What are the key components of AWS IAM?
Key components of AWS IAM include users, groups, roles, policies, permissions, and identity providers.

3. How does AWS IAM work?
AWS IAM allows you to create users and groups, assign policies that define permissions, and use roles to delegate permissions to AWS services and resources.

4. What is the difference between authentication and authorization in AWS IAM?
Authentication is the process of verifying the identity of users or entities, while authorization is the process of granting or denying access to resources based on policies and permissions.

5. How can you secure your AWS account using IAM?
You can secure your AWS account by enforcing the principle of least privilege, creating strong password policies, enabling multi-factor authentication (MFA), and regularly reviewing permissions.

6. How do IAM users differ from IAM roles?
IAM users are individuals or entities that have a fixed set of permissions associated with them. IAM roles are temporary credentials that can be assumed by users or AWS services to access resources.

7. What is an IAM policy?
An IAM policy is a JSON document that defines permissions. It specifies what actions are allowed or denied on which AWS resources for whom (users, groups, or roles).

8. What is the AWS Management Console?
The AWS Management Console is a web-based interface that allows you to interact with and manage AWS resources. IAM users can use the console to access resources based on their permissions.

9. How does IAM manage access keys?
IAM users can have access keys (access key ID and secret access key) associated with their accounts, which are used for programmatic access to AWS resources.

10. What is the purpose of IAM groups?
IAM groups allow you to group users and apply policies to them collectively, simplifying permission management by granting the same set of permissions to multiple users.

11. What is the role of an IAM policy document?
An IAM policy document defines the permissions and actions that are allowed or denied. It is written in JSON format and attached to users, groups, or roles.

12. How can you grant permissions to an IAM user?
You can grant permissions to an IAM user by attaching policies to the user directly or by adding the user to groups with associated policies.

13. How can you delegate permissions to AWS services using IAM roles?
IAM roles allow you to delegate permissions to AWS services like EC2 instances, Lambda functions, and more, without exposing long-term credentials.

14. What is cross-account access in AWS IAM?
Cross-account access allows you to grant permissions to users or entities from one AWS account to access resources in another AWS account.

15. How does IAM support identity federation?

IAM supports identity federation by allowing users to access AWS resources using temporary security credentials obtained from trusted identity providers (e.g., SAML, OpenID Connect).

16. What is the purpose of an IAM access advisor?
IAM access advisors provide insights into the services that users accessed and the actions they performed. This helps in auditing and understanding resource usage.

17. How does IAM enforce the principle of least privilege?
IAM enforces the principle of least privilege by allowing you to define specific permissions for users, groups, or roles, reducing the risk of unauthorized access.

18. What is the difference between IAM policies and resource-based policies?
IAM policies are attached to identities (users, groups, roles), while resource-based policies are attached to AWS resources (e.g., S3 buckets, Lambda functions) to control access from different identities.

19. How can you implement multi-factor authentication (MFA) in IAM?
You can enable MFA for IAM users to require an additional authentication factor (e.g., a code from a virtual MFA device) along with their password when signing in.

20. What is the IAM policy evaluation logic?
IAM uses an explicit deny model, which means that if a user's permissions include an explicit deny statement, it overrides any allow statements in the policy.