AWS IAM Important Questions and Answers

1. What is AWS Identity and Access Management (IAM)?

IAM is Identity and Access Management Service, provided by AWS. It helps you securely control access to AWS resources

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 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. What is the IAM policy "Effect" field, and what are the possible values?

Answer: The "Effect" field in an IAM policy can have two values: — "Allow": Grants permissions to perform specified actions. — "Deny": Explicitly denies permissions, even if they are allowed in other policies. Deny statements should be used sparingly.

14. What are the different types of AWS IAM policies? Which are most important and why?

There are 5 types of AWS IAM policies:

1. Service Control
2. Identity
3. Permission Boundary
4. Session
5. Resource

The three most important policy types are:

Service Control: A policy attached to an AWS account or organizational unit that establishes guardrails for what services and operations can be used within an account. A service control policy can only deny or limit allowed access; it cannot allow a principal to perform an operation on its own.

Identity: A policy attached to an IAM principal used by people and applications that allows, or sometimes denies, them to use AWS services and resources. The most common policy.

Resource: A policy attached to a data resource that allows or denies access to a specific data resource such as an S3 bucket. Often used to enable cross-account access to a data resource.