**IAM**

1. **Can you briefly describe what AWS IAM does and how you've used it?**
   1. IAM is AWS Identity and Access Management. It allows you to control access to AWS services and resources securely. I've used it to manage user permissions, roles, and policies.
2. **What are the core elements of an AWS IAM policy statement, and what is each element's purpose?**
   1. The core elements are:
      1. **Effect:** Specifies whether the statement allows or denies access.
      2. **Action:** Defines the specific actions allowed or denied.
      3. **Resource:** Specifies the AWS resources affected.
      4. **Condition:** Adds optional constraints.
3. **What identities can you specify in the Principal element?**
   1. You can specify AWS accounts, IAM users, roles, federated users, or assumed-role users.
4. **What happens if you have one IAM statement that allows a principal to perform an operation on a resource and another statement that denies that same operation on the same resource?**
   1. Deny takes precedence over allow. If there's a conflict, the denial will be applied.
5. **What are the basic differences between IAM roles and users? When should you use each?**
   1. Users are long-term identities for people or applications, while roles are temporary and assumed by entities. Use users for individuals and roles for cross-account access or temporary permissions.
6. **What are the different types of AWS IAM policies? Which are most important and why?**
   1. Identity-Based Policies (attached to users, groups, or roles) and Resource-Based Policies (attached to resources). Identity-Based Policies are more common and important for managing access.
7. **When an IAM principal makes an AWS API request, how does IAM evaluate policies in order to decide whether or not to allow access?**
   1. IAM evaluates policies in a top-down order. The first matching policy is applied. If there's an explicit deny, it overrides any allows.
8. **How do you connect or associate people's identities in a corporate directory such as Active Directory to IAM roles?**
   1. This can be done using AWS Directory Service or by establishing federation using Security Assertion Markup Language (SAML).
9. **What are IAM policy conditions, and when are some good times to use them?**
   1. Conditions are used to specify when a policy should take effect. For example, allowing actions only from a specific IP range or during specific times.
10. **How do you implement least privilege with AWS IAM? What's the hardest part of doing that?**
    1. Grant users and roles only the permissions they need to perform their tasks. The hardest part is determining the minimum set of permissions required without over-privileging.
11. **What are some ways to scale permissions management across the Engineering organization?**
    1. Use groups, roles, and policies effectively. Implement a clear organizational structure and adopt naming conventions for policies.
12. **Define AWS users, groups, and roles.**
    1. **Users:** Represent individual AWS accounts.
    2. **Groups:** Collections of users. Policies can be attached to groups.
    3. **Roles:** Used to grant permissions to entities within or outside your AWS account.
13. **What are the best practices you will follow while creating IAM users?**
    1. Follow the principle of least privilege, create individual IAM users, enable MFA, and regularly review and rotate credentials.
14. **Explain AWS IAM Policies.**
    1. IAM policies are documents defining permissions. They consist of statements that grant or deny access to resources, based on conditions.
15. **Explain the IAM Policy Structure.**
    1. IAM policy structure includes the version, statement, effect, action, resource, and condition.
16. **What is MFA in AWS IAM?**
    1. Multi-Factor Authentication (MFA) adds an extra layer of security by requiring users to provide additional verification, usually a temporary code from a hardware token or mobile app, in addition to their password.
17. **What are IAM users' access and secret keys?**
    1. Access keys are used to authenticate API requests, and secret keys are used to sign the requests. They are provided when creating IAM users for programmatic access.
18. **How do you monitor user activity with IAM?**
    1. AWS CloudTrail logs can be used to monitor user activity, providing a record of actions taken by users and roles.
19. **Are root users and IAM users the same?**
    1. No, root users have unrestricted access to all resources, while IAM users have controlled access based on policies.
20. **In the IAM service, can we monitor the IAM user activity?**
    1. Yes, IAM user activity can be monitored using AWS CloudTrail.
21. **How authentication is controlled in the IAM service?**
    1. Authentication is controlled through user credentials (username and password) or through federation with external identity providers.
22. **What is federated user access management?**
    1. Federated user access management allows users to access AWS resources using their existing credentials from an identity provider outside of AWS.
23. **What is Authorization in terms of AWS IAM service?**
    1. Authorization in IAM refers to granting or denying permissions to perform actions on AWS resources.
24. **How to control Authorization in AWS IAM?**
    1. Authorization is controlled through IAM policies attached to users, groups, and roles, specifying the actions allowed or denied.
25. **How AWS IAM allows access?**
    1. IAM allows access by attaching policies to identities (users, groups, or roles) specifying the actions they can perform on resources.
26. **What's the other name of the IAM user?**
    1. IAM users are sometimes referred to as AWS account users.
27. **What is CloudTrail in AWS?**
    1. AWS CloudTrail is a service that logs API requests made on your account. It helps in monitoring and auditing user activity.
28. **What are the 5 top security credentials in AWS IAM?**
    1. Access key ID, Secret access key, Certificate, Key pair, and X.509 certificate.
29. **What are Temporary Security Credentials?**
    1. Temporary Security Credentials are short-term credentials that are generated dynamically and can be used for temporary access to AWS resources.
30. **What are AWS IAM roles?**
    1. IAM roles are AWS identities with permissions policies that determine what the identity can and cannot do in AWS.
31. **What are the top AWS IAM Roles?**
    1. Common roles include Administrator, PowerUser, and ReadOnly. Custom roles can be created based on specific needs.
32. **What is the IAM Hierarchy of Privileges?**
    1. IAM follows a hierarchy where explicit denials take precedence over explicit allows, and policies attached directly to users take precedence over group policies.