50 IAM Concepts that every Cloud Engineer should know

1. **Access Advisor:**

   Access Advisor shows the service permissions granted to a user, group, or role and when those services were last accessed.

2. **IAM Identities (Federation):**

   IAM federation allows you to grant external identities (federated users) permissions to use resources in your AWS account.

3. **Identity Providers (IdP):**

   IAM supports identity federation by using open standard SAML 2.0, which includes a range of identity providers such as Microsoft Active Directory Federation Services or any other SAML-compliant provider.

4. **Permission Boundaries:**

   You can set the maximum permissions that an identity-based policy can grant to an IAM entity.

5. **IAM Access Analyzer:**

   It helps you identify the resources in your organization and accounts, such as Amazon S3 buckets or IAM roles, that are shared with an external entity.

6. IAM Users:

Each IAM user is an identity with specific permissions. You can create users in IAM, assign them individual security credentials, or request temporary security credentials to provide users access to AWS services and resources.

7. IAM Groups:

An IAM group is a collection of IAM users. You can use groups to specify permissions for a collection of users, which can make those permissions easier to manage for those users.

8. IAM Roles:

IAM roles are a secure way to grant permissions to entities that you trust. Examples of entities include EC2 instances, or AWS services like AWS Lambda.

9. IAM Policies:

A policy is an object in AWS that, when associated with an identity or resource, defines their permissions.

10. Password Policies:

You can manage the password policy for your organization to enforce a strong password practice.

11. Multi-Factor Authentication (MFA):

MFA adds an extra layer of protection on top of a username and password.

12. AWS STS:

The AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-privilege credentials for IAM users or for users that you authenticate (federated users).

13. Service Control Policies (SCPs):

SCPs are a type of organization policy that you can use to manage permissions in your organization.

14. Policy Versions:

IAM stores up to five versions of your managed policies. This allows you to roll back to a previous version of a policy if you need to.

15. Tagging IAM Identities:

You can add metadata to IAM users, groups, roles, and policies in the form of tags.

16. AWS Managed Policies:

These are standalone policies that you can attach to multiple users, groups, and roles in your AWS account.

17. AWS Organizations:

This is a service for grouping and centrally managing the AWS accounts of your organization.

18. Cross-account Access:

Let users from other AWS accounts access your AWS resources without having to create IAM users in your own AWS account.

19. IAM Roles for Service-Linked Role:

This role is linked directly to a service. Service-linked roles are predefined by the service and include all the permissions that the service requires to call other AWS services on your behalf.

20. Integrated AWS Services:

Many AWS services integrate with IAM for managing permissions to their resources.

21. AWS CLI and SDKs Integration:

AWS Command Line Interface (CLI) and various Software Development Kits (SDKs) support IAM for managing and applying IAM permissions.

22. Event Logging with AWS CloudTrail:

IAM is integrated with CloudTrail, which captures all IAM and AWS Management Console sign-in events. It helps to track changes to resources and troubleshoot issues.

23. EC2 Instance Profiles:

These are IAM roles that you can use to delegate permissions to EC2 instances, enabling applications running on the instance to make API requests.

24. IAM Instance Profiles for Amazon EC2:

Provide AWS credentials to your EC2 instances automatically.

25. Delegated administration:

You can delegate the management of identities and permissions in your AWS accounts without granting full access.

26. IAM Access Report:

This feature helps you identify who in your organization did what action in which context, and when the action occurred.

27. Attribute-Based Access Control (ABAC):

ABAC is an authorization strategy that defines permissions based on attributes.

28. AWS Directory Service Integration:

IAM works seamlessly with AWS Directory Service for Microsoft Active Directory, enabling you to manage access to your AWS services.

29. SAML 2.0 Integration:

IAM supports federation with identity providers that are compatible with SAML 2.0 (Security Assertion Markup Language 2.0).

30. Access Levels for AWS IAM Permissions:

AWS provides a set of access levels for each AWS service to help you decide which permissions to grant to your IAM entities.

31. Resource-Based Policies:

These are inline policies that you can attach to a resource, such as an S3 bucket or a Glacier vault.

32. Principal Tags in IAM Policies:

When granting permissions using IAM policies, you can use principal tags to specify the principal that is allowed or denied access to a resource.

33. Request Context in IAM Policies:

When granting permissions, you can use request context conditions to specify when a policy is in effect.

34. AWS Sign-in Endpoint:

IAM offers a unique sign-in URL for your AWS account's console login page, which includes your account ID.

35. Global Service:

Unlike many AWS services, IAM is a global service and not region-specific.

36. JSON Policy Document:

IAM uses JSON (JavaScript Object Notation) policy documents to define permissions.

37. Resource-Level Permissions:

For certain services, you can define permissions for specific resources.

38. IAM Policy Simulator:

The IAM Policy Simulator is a tool that helps you understand, test, and validate the effects of your access control policies.

39. Policy Evaluation Logic:

Understand how AWS determines whether a request should be allowed or denied.

40. Last Used Access Information:

IAM provides information about when IAM users and roles last used AWS services.

41. Fine-Grained Access Control:

With IAM, you can specify granular permissions down to the action level for each AWS service that supports IAM.

42. Security Token Service (STS):

IAM integrates with AWS STS for trusted access to AWS services with temporary, limited-privilege credentials.

43. Support for AWS Organizations:

IAM supports AWS Organizations for managing access to your AWS accounts centrally.

44. Controlled Access to AWS Billing:

IAM enables you to control who in your organization has permission to access AWS billing information.

45. IAM for Compliance:

Use IAM to set up a governance model, manage permissions, and help maintain regulatory and compliance standards.

46. IAM Policy Validation:

The IAM console includes a JSON policy validator that checks the syntax of your JSON policy documents.

47. Amazon Cognito User Pools Integration:

Amazon Cognito user pools are user directories that provide sign-up and sign-in options for your app users with AWS managed user data security and user profiles.

48. Identity Federation for Mobile Apps:

IAM roles enable identity federation for mobile applications by providing temporary security credentials to access AWS services.

49. Permission Boundaries for IAM Entities:

A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity.

50. Public and Private Policy Elements:

Public policies govern access to the public APIs of services, while private policies govern access to the service's internal APIs.