# AWS IAM Interview Questions and Answers

---

**1. What is IAM in AWS?**

**Answer:**
IAM (Identity and Access Management) is a service that helps manage access to AWS resources securely by creating users, groups, roles, and policies.

---

**2. What are IAM users, groups, and roles?**

**Answer:**

- **User**: Represents an individual with access to AWS.
- **Group**: A collection of users with the same permissions.
- **Role**: Grants temporary access to AWS services, typically used by applications or external accounts.

---

**3. What is an IAM policy?**

**Answer:**
An IAM policy is a JSON document that defines permissions to allow or deny actions on AWS resources.

---

**4. What are managed policies and inline policies?**

**Answer:**

- **Managed Policies**: Predefined and reusable policies created by AWS or the user.
- **Inline Policies**: Policies directly attached to a single IAM user, group, or role.

---

**5. What is the difference between IAM roles and IAM users?**

**Answer:**

- **IAM User**: Represents an individual and has permanent access credentials.
- **IAM Role**: Grants temporary access to AWS resources and is used by applications or other AWS services.

---

**6. How can you secure access to IAM users?**

**Answer:**

- Enable **Multi-Factor Authentication (MFA)**.
- Use strong passwords with a password policy.
- Grant least privilege by assigning only necessary permissions.

---

**7. What is an IAM policy simulator?**

**Answer:**
It's a tool to test and troubleshoot IAM policies to ensure they work as expected before applying them.

---

**8. How do you implement Multi-Factor Authentication (MFA)?**

**Answer:**

- Go to the IAM console, select the user, and click **Security credentials**.
- Enable MFA and follow the steps to pair an MFA device like a mobile authenticator app.

---

**9. What are permission boundaries in IAM?**

**Answer:**
Permission boundaries are limits that control the maximum permissions an IAM entity (user or role) can have, regardless of the policies attached.

---

**10. What is AWS STS (Security Token Service)?**

**Answer:**
AWS STS provides temporary security credentials for users or applications to access AWS resources securely.

---

**11. What are resource-based policies and identity-based policies?**

**Answer:**

- **Resource-Based Policy**: Attached to a resource (e.g., S3 bucket policy).
- **Identity-Based Policy**: Attached to an IAM user, group, or role.

---

**12. How do you troubleshoot an "Access Denied" error in AWS?**

**Answer:**

- Check if the IAM policy allows the required action.
- Verify the resource-based policy (if applicable).
- Use the IAM **Policy Simulator** to test the permissions.

---

**13. How can you delegate access using IAM roles across AWS accounts?**

**Answer:**

- Create a role in the target account.
- Configure a trust relationship to allow access from the source account.
- Attach necessary policies to the role.

---

**14. What are service-linked roles?**

**Answer:**
Service-linked roles are predefined roles that allow AWS services to access other AWS resources on your behalf.

---

**15. What is the difference between AWS Organizations SCPs and IAM policies?**

**Answer:**

- **SCP (Service Control Policy)**: Applies at the organizational level to set limits on permissions.
- **IAM Policy**: Applies to individual users, groups, or roles.

---

**16. How would you enforce MFA for all IAM users?**

**Answer:**

- Create an IAM policy that denies all actions unless MFA is enabled.
- Attach the policy to all users or groups.

---

**17. How would you give read-only access to an external partner for specific resources?**

**Answer:**

- Create a role with read-only permissions.
- Set a trust relationship for the partner's AWS account.
- Share the role's ARN with the partner.

**18. How do you audit and monitor IAM activity?**

**Answer:**
Use **AWS CloudTrail** to log and monitor IAM activities like logins and API calls.

---

**19. What is a least-privilege policy?**

**Answer:**
It's a policy that grants only the permissions needed to perform a task, minimizing the risk of unauthorized actions.

---

**20. How do you connect a Lambda function securely to an RDS instance?**

**Answer:**

- Create an IAM role with permissions to access RDS.
- Attach the role to the Lambda function.
- Use VPC settings if required for network access.

**21.How do you restrict API calls from specific IP addresses in IAM?**

**Answer:**

Use a condition in the IAM policy with the aws:SourceIp key to allow or deny actions based on specific IP ranges