1. Basics & Concepts

• What is IAM?: Identity and Access Management (IAM) is used to securely control access to AWS services and resources.

• IAM Users vs Roles vs Groups: Users = individual identities. Groups = collections of users for shared permissions. Roles = temporary access with specific permissions.

• Root User Best Practices: Use only for account setup. Enable MFA. Do not use for daily operations.

• IAM Policies: JSON documents defining permissions. Can be AWS-managed, customer-managed, or inline.

2. Security Best Practices

• Enable MFA: Require Multi-Factor Authentication for root and all IAM users.

• Principle of Least Privilege: Grant only the permissions needed to perform tasks.

• Password Policies: Set strong password requirements and rotation periods.

• Access Keys: Avoid long-term access keys. Use IAM roles or temporary credentials via STS.

3. Roles & Permissions

• When to Use IAM Roles: Use for EC2, Lambda, or cross-account access instead of embedding credentials.

• Service-Linked Roles: Automatically created for specific AWS services to access resources on your behalf.

• Cross-Account Access: Use roles with trust policies to allow secure access between AWS accounts.

4. Policies & Management

• Managed vs Inline Policies: Managed = reusable, can be AWS or customer-managed. Inline = attached to a single user/group/role.

• Policy Evaluation Logic: Explicit deny overrides allow. If no allow is found, request is denied.

• Policy Size Limits: JSON policy documents have size limits; use managed policies for reusability.

5. Auditing & Monitoring

• IAM Access Analyzer: Detects resources shared with external entities.

• CloudTrail Integration: Track IAM changes and API calls for auditing.

• Credential Report: Generate CSV with user credentials and last activity for compliance checks.

6. Common Problems

• Access Denied Errors: Check attached policies, evaluate conditions, verify MFA requirements.

• Too Many Permissions: Use IAM Access Advisor to identify unused permissions and remove them.

• User Cannot Assume Role: Ensure trust policy allows principal, and user has sts:AssumeRole permission.

7. Cost & Maintenance

• IAM Cost: IAM itself is free, but resources accessed via IAM may incur costs.

• Policy Maintenance: Regularly review and update policies to match current business needs.

• Orphaned Accounts: Disable or remove IAM users no longer in use.