ONE PAGE SUMMARY

IT & Software › AWS › IAM

Introduction to IAM

Master IAM for secure AWS resource management!

DEFINITION

> IAM, or Identity and Access Management, is a service that helps you control access to AWS resources. It allows you to manage users, permissions, and security policies effectively.

KEY CONCEPTS

Users

Individuals or applications that need access to AWS resources.

Groups

Collections of users that share the same permissions for easier management.

Roles

Temporary access permissions assigned to users or services to perform specific tasks.

Policies

Documents that define permissions and specify what actions are allowed or denied.

MFA

Multi-Factor Authentication adds an extra layer of security by requiring additional verification.

EXAMPLES

→ Creating a user for a new developer with specific access rights.

→ Assigning a group policy to allow read-only access to S3 buckets.

→ Using a role for an EC2 instance to access DynamoDB securely.

MEMORY TIPS

★ Think 'IAM' as 'I Access Management' to remember its purpose.

★ Use 'UGRP' (Users, Groups, Roles, Policies) to recall key components.

★ Remember 'MFA' as 'More Factors Added' for security.

COMMON MISTAKES

✗ Not using groups for user permissions, leading to management chaos.

✗ Overly permissive policies that grant more access than necessary.

✗ Neglecting to enable MFA for sensitive accounts.

QUICK RECAP

IAM is essential for managing access to AWS resources securely. It involves users, groups, roles, and policies to control permissions effectively. Always remember to implement MFA for enhanced security.