- 1
  - Introduction
    - 1 Defines who is allowed to do what with which AWS resources
    - 2 Controls access to AWS services and resources.
    - 3 A set of rules in a JSON Format
    - 4 Helps keep your AWS environment secure
    - 5 Can be attached to three types of entities
      - 1 Users
      - 2 Groups
      - 3 Roles
    - 6 In AWS IAM there are essentially three types of policies
      - 1 AWS Managed Policies
      - 2 Customer Managed Policies
      - 3 Inline Policies
- IAM Policies
- 2
  - AWS Managed Policies
    - 1 Created and managed by AWS
    - 2 Designed for common use cases across a wide range of AWS services
    - 3 Ready to attach to multiple IAM users, groups, or roles within an AWS account.
    - 4 Automatically updated by AWS to grant access to new services or actions without requiring manual policy updates.
    - 5 Provide a way to quickly assign necessary permissions based on job function or application need.
    - 6 Divided into two types
      - 1 AWS managed policies (general use)
      - 2 Service-linked policies (specific to AWS services).
    - 7 Example
      - 1 Objective: Enable the EC2MasterMind user to fully manage EC2 instances.
      - 2 Policy Used: AmazonEC2FullAccess
      - 3 Entity: IAM user named EC2MasterMind
      - 4 Permissions Included
        - 1 Launch EC2 instances with chosen
          - 1 AMIs
          - 2 Instance types
          - 3 Configurations.
        - 2 Perform operations like
          - 1 Start
          - 2 Stop
          - 3 Reboot
          - 4 Terminate
        - 3 Handle instance storage options like
          - 1 Volumes
          - 2 Snapshots
        - 4 Configure network settings and security groups for instances
        - 5 Create and manage SSH key pairs for secure login to instances
        - 6 Utilize AWS CloudWatch for monitoring instances and setting up alerts
    - 8 Benefits & Limitations
      - 1
        - Benefits
          - 1 Simplicity
          - 2 Predefined by AWS
          - 3 Automatic Updates
          - 4 Reusable
          - 5 Best Practices
      - 2
        - Limitations
          - 1 Resource-Specific Access Control 1
          - 2 No Customization 1
          - 3 Broad Permissions 1
          - 4 Dependence on AWS 1
          - 5 Understanding Complexity 1
- 3 52
- 4 37