Chapter 8
IAM Best Practices

Episode 8.01
User Accounts

IAM Best Practices

- User Accounts
- Password Policies
- Credential Rotation
- Enable MFA
- Use Lease Privilege Guidelines
- Use IAM Roles
- Implement Policy Conditions
- Enable CloudTrail

DEMO

- Creating user accounts

Episode 8.02
Password Policies

Default Password Policy

- Min 8 characters
- Max 128 characters
- At least 3 of these 4 character types:
  - Uppercase
  - Lowercase
  - Numbers
  - Special characters
- Can’t be the same as the account name or email

Password Best Practices

- Change password periodically
- Use a unique password for AWS
- Avoid easily guessed passwords

DEMO

- Setting IAM User Password Policies
- https://docs.amazonaws.cn/en_us/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

Episode 8.03
Credential Rotation

Credential Rotation

- Reduces vulnerabilities
  - Limits the time for an attack
  - Reminds users of security focus
  - Helps reduce reuse of passwords across systems

DEMO

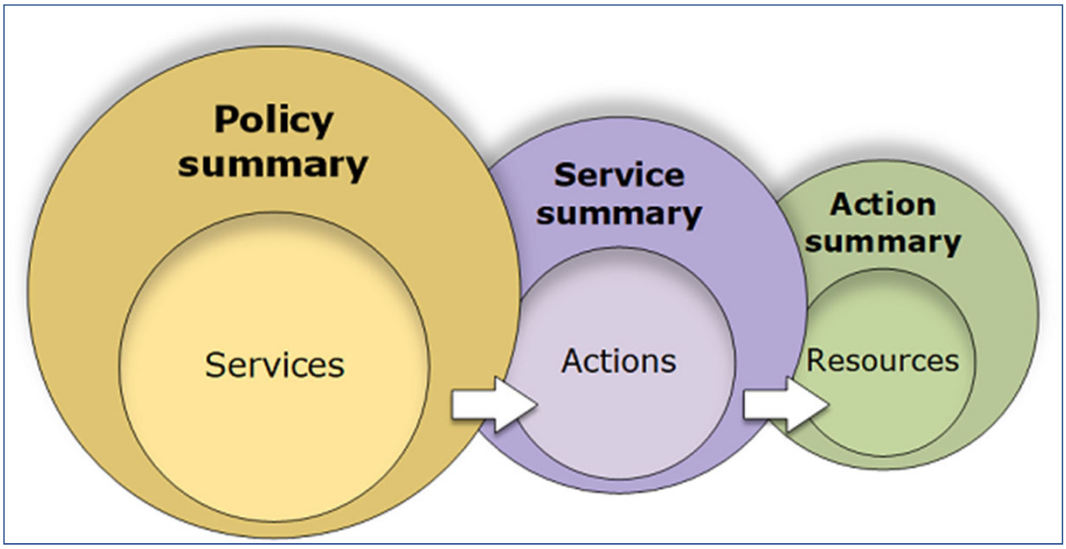
- Password Rotation Policies

Episode 8.04
Principle of Least Privilege

Least Privilege Principle

- Principals need the access they need
- Grant only that level of access
- Granting more access may be easier
  - Opens the door to mistakes
  - Opens the door for attackers
    - Internal
    - External

Review Permissions



DEMO

- Viewing Policy Summaries

Episode 8.05
IAM Roles

DEMO

- Creating Roles
- Configuring Roles

Episode 8.06
Policy Conditions

DEMO

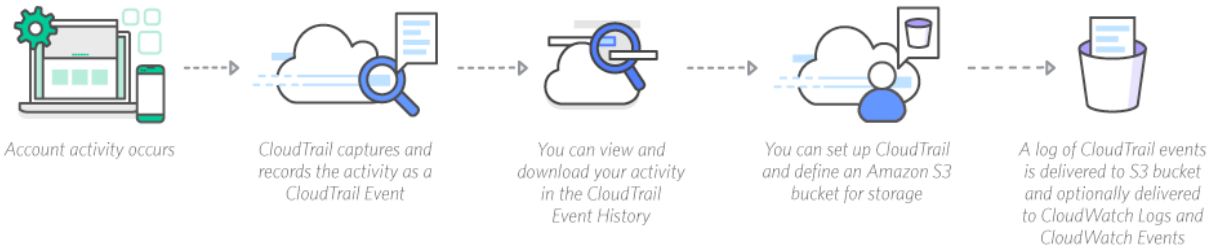
- Creating an IAM policy
- Defining policy conditions
- Additional Best Practices
  - https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

Episode 8.07
CloudTrail

CloudTrail

- Logging services
  - Governance
  - Compliance
  - Auditing
- Provides event histories
  - Management Console actions
  - AWS SDK actions
  - Command line actions
  - Additional AWS services

CloudTrail


Account activity occurs
CloudTrail captures and records the activity as a CloudTrail Event
You can view and download your activity in the CloudTrail Event History
You can set up CloudTrail and define an Amazon S3 bucket for storage
A log of CloudTrail events is delivered to S3 bucket and optionally delivered to CloudWatch Logs and CloudWatch Events

DEMO

- Enabling CloudTrail