



IAM:

- IAM → Identity and Access Management
 - Global Service.
- Root Account Never share/reuse.
- Users → created, can be grouped.
- Groups only have users
- Users can be in two groups

Permissions:

- JSON document as policies
- Users has permission
- Least privilege permissions.

Console:

- Create an admin account.
- Create group for admin
- Tags are more info
- Administration access policy.
- Change alias
- Use admin for things.

Policies:

- Group
- Inline → Single
- Shared group

Structure: (JSON)

- Version = 2012-10-17
- Id → optional
- Statement = Required

Statement:

- Sid = optional
- Effect = Allow, Deny
- Principal: account/user/role
- Action: list of actions allows/denies
- Resource: list of resources for which actions can be done

Policies Handons:

- create own policy
- Groups permission will be inherited to users

Password Policy:

- Strong Password strength
- Change passwords
- Password expiration
- Reuse password.

MFA:

- Multi-factor Auth
- Authy
- Physical key.

Access AWS:

- Management Console
- CLI
- SDK

Access key = Passwords for CLI + SDK.

CLI:

- Command line interface
- Free, open source

SDK:

- Lang. Specific
- Embedded in app
- APIs to AWS
- AWS Cli is built on AWS SDK for python

AWS Cli:

- Same as management console
- Permissions everything works the same.

AWS Cloudshell:

- Browser Cli
- Persist storage
- only few regions.

IAM Roles

→ IAM Roles

↳ AWS Services require roles
for working in AWS

→ EC2 will need a role to
run.

Common:

→ EC2

→ Lambda

Security Tools:

→ Credentials Report (account-level)

→ IAM Access Advisor (user-level)

→ Remove least used permission.

Best Practices:

→ Don't use Root account

→ One physical user - one AWS user

→ Groups is better & must

→ Strong

→ Enforce MFA

→ Roles

→ Access keys for CLI & SDK

→ Audit with security report &
Advisor

→ Never share

Summary:

→ Users = physical user → has password

→ Groups = User only

→ Policies = JSON doc for permissions

→ Roles = AWS Service permissions

→ Security = MFA + Password Policy

→ Access key: CLI & SDK

→ Audit: IAM Cred Report & Advisor
account level + User-level.