IAM Session

Created	@2023년 1월 11일 오후 7:25
Class	AWS
Type	Lecture
Materials	
Reviewed	☐
Number	1

TOPIC

(PPT - p.21 ~ p.37)

- AWS - IAM Session
  - Types
  - Policy
  - How can users access AWS?
  - IAM Roles for Services
  - IAM Security Tools
  - **IAM Guidelines & Best Practices**

IAM Service

IAM Service is a service give a permission to someone.

We can manage Identity and Access by using it.

And it’s an Global Service(It means that this service has no relationship with Regions)

1. Types
    a. Root Account : It’s created by default, shouldn’t be used or shared.
    b. Users : It’s person within my organization, and can be grouped
    c. Groups : It can contains only users, not other groups.
        - Some people can have more than 2 groups which have different permission polices.

2. Policy
    a. Structure
        i. Consists of
            1. version : policy language version (default, always include “2012-10-17”)
            2. id : an identifier for the policy (optional)
            3. statement : one or more individual statements (required)
                a. Sid : an identifier for the statement (optional)
                b. Effect : whether the statement allows or denies access (Allow, Deny)
                c. Principal : account/user/role to which this policy applied to
                d. Action : list of actions this policy allows or denies
                e. Condition : conditions for when this policy is in effect (optional)
    b. Password Policy
        i. Strong Password
            - In AWS, you can setup a password policy
                - Minimum password length
                - Require Specific character types
                - Allow all IAM users to change their own passwords

        - Require Users to change their password after some time (password expiration)
        - Prevent password re-use
    ii. MFA (Multi Factor Authentication)
        - Virtual MFA device
        - Universal 2nd Factor(U2F) Security Key
        - Hardware Key

3. How can users access AWS?
    a. AWS Management Console
    b. AWS Command Line Interface (CLI)
    c. AWS Software Developer Kit (SDK)

4. IAM Roles for Services
    - Some AWS service need a permissions to use. we will assign permissions to AWS services with IAM Roles
    - Common Roles
        1. EC2 Instance Roles
        2. Lambda Function Roles
        3. Roles for CloudFormation

5. IAM Security Tools
    a. IAM Credentials Report (account-level)
        - A report that **lists all your account's** users and the status of their various credentials
    b. IAM Access Advisor (user-level)
        - It shows the service permissions granted to a user and when those services were last accessed.

6. **IAM Guidelines & Best Practices ****
    a. Don’t use the root account **except for AWS account setup**
    b. One physical user = One AWS user (don’t share a account)
    c. Assign users to groups and assign permissions to groups
    d. Create a strong password policy
    e. Use and enforce the use of MFA
    f. Create and use Roles for giving permissions to AWS services
    g. Use access keys for programmatic access(CLI / SDK)
    h. Audit permissions of your account with the IAM Credential Report
    i. Never Share IAM users & Access keys