AWS Lab 26

IAM (Identify and Access Management)

Overview of the lab

In this lab you will learn to how to enable MFA for root user / how to create users, group and map permissions policy

IAM

It is used to manage who can use aws resources (authentication) and what resources can be used in what ways (authorization)

Authentication

It is a process verifying the credentials (email & password / access key and secret access key)

Authorization

Allowing access to services based on permission

Users

root user - will have unrestricted permission
IAM user - can be created with required permissions

Group

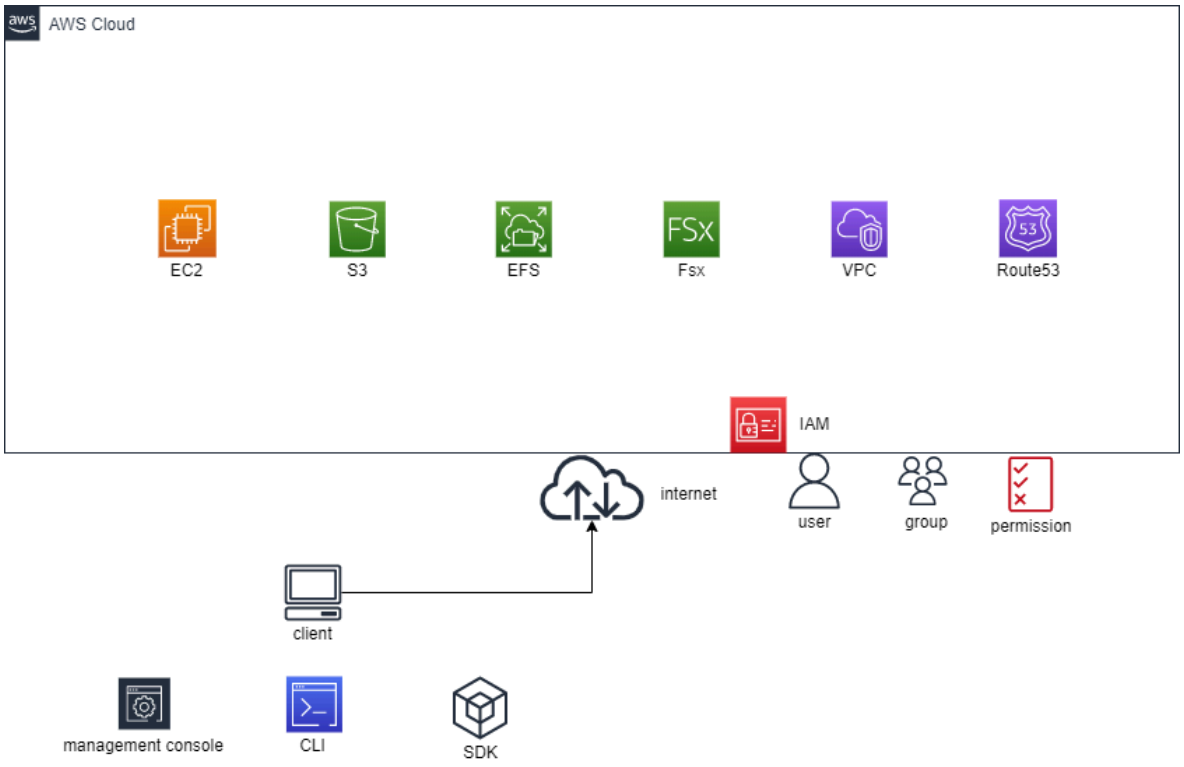
Multiple users can be grouped to easily manage permissions

IAM Policy or Permissions

It is a JSON file which has permission/restriction to services

- aws managed
- customer managed

Architecture



Step by Step Lab

Enable MFA for root user (can be enabled for IAM users)

1. Download and install authenticator app in mobile phone(MS authenticator, Google authenticator or any)
2. Login to aws account, in right top click on username and click on Security credentials
3. Click on Assign MFA device
    a. Device name - myphone - click next
    b. Click on Show QR code
    c. Scan from authenticator app
    d. Enter MFA code1 and MFA code2 and click on Add MFA

4. Now logout from aws account and logging in will additional prompt for MFA code

IAM User

5. In IAM management console - Click on Users
6. Click on Create user
    a. User name - operator1
    b. Select - provide user access to the AWS Management console
    c. Select - I want to create an IAM user
    d. Select Custom password and set a password
    e. Uncheck user must create a new password at next sign-in
    f. Click on Next
7. Select Attach policies directly
    a. Search for AmazonEC2ReadOnlyAccess and select
    b. Search for AmazonS3ReadOnlyAccess and select
8. Click on Next
9. Click on Create user

(use the Console sign-in URL, User name and Console password from a different browser to login to check the permissions)

IAM Group

10. In IAM management console - Click on User groups
11. Click on Create group
    a. User group name - developers
    b. Attach permissions policies - AmazonS3ReadOnlyAccess
12. Click on Create group

IAM User(s) to group

13. In IAM management console - Click on Users
14. Click on Create user
    a. User name - developer1
    b. Select - provide user access to the AWS Management console
    c. Select - I want to create an IAM user
    d. Select Custom password and set a password
    e. Uncheck user must create a new password at next sign-in
    f. Click on Next
15. Select Add user to group
16. User groups Select - developers
17. Click on Next
18. Click on Create user

(use the Console sign-in URL, User name and Console password from a different browser to login to check the permissions)