ACF Lab 1: Introduction to IAM

Student name: Do DuyHung Student ID: 104182779

Tutorial session: Monday 1PM

1. INTRODUCTION

Identity and Access Management (IAM) in Amazon Web Services (AWS) is a fundamental component that empowers users to securely control access to AWS resources. IAM provides a comprehensive and flexible framework for managing identities, such as users, groups, and roles, and their respective permissions within an AWS environment. By defining granular policies, administrators can precisely tailor access rights, ensuring that users have the appropriate level of permissions needed to perform their tasks while maintaining a strong security posture. IAM plays a pivotal role in safeguarding sensitive data, regulating resource usage, and facilitating a scalable and organized approach to managing user access across the vast array of AWS services. With IAM, AWS users can establish a robust security foundation, enforcing the principle of least privilege and promoting a secure and efficient cloud computing environment.

1. IAM

**Task 1: Explore the Users and Groups**

4, Search IAM and open the console in Services’ menu

A screenshot of a computer

Description automatically generated

*Figure 1 IAM Searching*

5, See some users in IAM users. There are 3 default users for you

A screenshot of a computer

Description automatically generated

*Figure 2 IAM console*.

A screenshot of a computer

Description automatically generated

*Figure 3 3 default users*

6, User-1 link does not have any permissions.

A screenshot of a computer

Description automatically generated

*Figure 4 user-1 permissions*

8, User-1 also is not a member of any groups

A screenshot of a computer

Description automatically generated

*Figure 5 user-1 groups*

9, User-1 is assigned a Console password in Security credentials tab

A screenshot of a computer

Description automatically generated

*Figure 6 user-1 Security credentials*

10, Choose User Groups in the left navigation pane, there are 3 groups have already been created. Click on the EC2-Support group link.

A screenshot of a computer

Description automatically generated

*Figure 7 EC2-Support security group*

12, Choose the Permissions tab

A screenshot of a computer

Description automatically generated

*Figure 8 EC2-Support permissions*

13, Choose the icon + next to the AmazonEC2ReadOnlyAccess policy. It is granting permission to List and Describe information about EC2, Elastic Load Balancing, CloudWatch and Auto Scaling. The basic structure of the statements in an IAM policy is: Effect, Action and Resource

A screenshot of a computer

Description automatically generated

*Figure 9 AmazonEC2ReadOnlyAccess*

15, Choose the Permisssions tab in S3-Support. And it has the AmazonS3ReadOnlyAccess policy attached

*A screenshot of a computer

Description automatically generated*

*Figure 10 S3-Support Security Groups*

17, Choose the + icon to view the policy details.

A screenshot of a computer

Description automatically generated

*Figure 11 AmazonS3ReadOnlyAccess*

20, Choose the Permissions tab in the EC2-Admin, it has an Inline Policy, which is a policy assigned to just one User or Group.

A screenshot of a computer

Description automatically generated

*Figure 12 EC2-Admin-Policy*

**Task 2: Add Users to Groups**

23, Choose User Groups to see all default groups. After that, select S3-Support group link

A screenshot of a computer

Description automatically generated

*Figure 13 S3-Support*

27, Choose Add users in the Users tab, and select user-1 group to S3-Support.

A screenshot of a computer

Description automatically generated

*Figure 13 Add users to S3-Support*

28, Similar to the steps above, add user-2 to the EC2-Support group

A screenshot of a computer

Description automatically generated

*Figure 14 Successful added users to EC2-Support*

29, Add user-3 to the EC2-Admin group

A computer screen with a message

Description automatically generated

*Figure 15 Successful added users to EC2-Admin*

Choose against User Groups. Currently, Each Group have a 1 in the Users colum

**Task 3: Sign-in and Test Users**

31, Choose Dashboard to see overview of IAM console

A screenshot of a computer

Description automatically generated

*Figure 16 IAM Dashboard*

32, Copy the Sign-in URL for IAM users in the account to a text editor, and open to a private window. Use suername user 1 to open the IAM user.

A screenshot of a computer

Description automatically generated

*Figure 17 Sign-in IAM users*

1. CREATETHUMBNAIL LAMBDA FUNCTION

36, Choose S3 to open console

A screenshot of a computer

Description automatically generated

*Figure 18 S3 Searching*

40, Search and open the EC2 console, and then choose Instance.

A screenshot of a computer

Description automatically generated

*Figure 19 EC2 searching*

40, Sign out the user-1 and sign in by the user 2

A screenshot of a computer

Description automatically generated

*Figure 20 user 1 sign out*

A computer screen shot of a computer

Description automatically generated

*Figure 21 User 2 sign in*

A screenshot of a computer

Description automatically generated

*Figure 22 User 2 console*

44, Choose Instances in the left navigation pane, change the region to N.Virginia and select LabHost’s instance

A screenshot of a computer

Description automatically generated

*Figure 23 EC2 Instance*

46, In the Instance State menu above, select Stop instance

A screenshot of a computer

Description automatically generated

*Figure 24 Stop LabHost instance*

47, But you will receive an error message because the policy only allows you to view informations, without edit or change anything.

A screenshot of a computer

Description automatically generated

*Figure 25 Failed notification about stop instance*

48, Search S3 and open S3 console, but you can’t see anything related to S3

A screenshot of a computer

Description automatically generated

*Figure 26 S3 console*

49, Sign out user-2 and sign in user 3

A screenshot of a computer

Description automatically generated

*Figure 27 User 3 sign in user*

A screenshot of a computer

Description automatically generated

*Figure 28 User 3 console*

49, Choose EC2 from the Services and choose Instances

A screenshot of a computer

Description automatically generated

*Figure 27 EC2 Instance*

49, Select the instance named LabHost and stop that, now we can see the stopping state and shutdown successfully

A screenshot of a computer

Description automatically generated

*Figure 27 Successfully stopped instance*