Ex:8 IMPLEMENT SECURE USER MANAGEMENT IN CLOUD

AIM:

To Implement secure user management in cloud.

DISCRIPTION:

Managing IAM users

Amazon Web Services offers multiple tools for managing the IAM users in your AWS account. You can list the IAM users in your account or in a user group, or list all user groups that a user is a member of. You can rename or change the path of an IAM user. If you are moving to using federated identities instead of IAM users, you can delete an IAM user from your AWS account, or deactivate the user.

For information about managing inline policies for IAM users, see Adding and removing IAM identity permissions, Editing IAM policies, and Deleting IAM policies. As a best practice, use managed policies instead of inline policies. AWS managed policies grant permissions for many common use cases. Keep in mind that AWS managed policies might not grant least-privilege permissions for your specific use cases because they are available for use by all AWS customers. As a result, we recommend that you reduce permissions further by defining customer managed policies that are specific to your use cases. For more information, see AWS managed policies.

ALGORITHM:

Managing passwords for IAM users

IAM users who use the AWS Management Console to work with AWS resources must have a password in order to sign in. You can create, change, or delete a password for an IAM user in your AWS account.

After you have assigned a password to a user, the user can sign in to the AWS Management Console using the sign-in URL for your account, which looks like this:

https://12-digit-AWS-account-ID or alias.signin.aws.amazon.com/console

Topics involved managing users in aws are,

1.View user access

2.Listing IAM users

3.Renaming an IAM user

4.Deleting an IAM user

5.Deactivating an IAM user

1.View user access :

Before you delete a user, you should review its recent service-level activity. This is important because you don't want to remove access from a principal (person or application) who is using it. For more information about viewing last accessed information, see Refining permissions in AWS using last accessed information.

2.Listing IAM users:

To list all the users in the account

AWS Management Console: In the navigation pane, choose Users. The console displays the users in your AWS account.

2.1.AWS CLI: aws iam list-users

2.2.AWS API: ListUsers

2.3.To list the users in a specific user group

AWS Management Console: In the navigation pane, choose User groups, choose the name of the user group, and then choose the Users tab.

2.4.AWS CLI: aws iam get-group

2.5.AWS API: GetGroup

2.6.To list all the user groups that a user is in

AWS Management Console: In the navigation pane, choose Users, choose the user name, and then choose the Groups tab.

2.7.AWS CLI: aws iam list-groups-for-user

2.8.AWS API: ListGroupsForUser

3.Renaming an IAM users:

To change a user's name or path, you must use the AWS CLI, Tools for Windows PowerShell, or AWS API. There is no option in the console to rename a user. For information about the permissions that you need in order to rename a user, see Permissions required to access IAM resources.

When you change a user's name or path, the following happens:

* Any policies attached to the user stay with the user under the new name.
* The user stays in the same user groups under the new name.
* The unique ID for the user remains the same. For more information about unique IDs, see Unique identifiers

For example,

user Richard has a policy attached to him that lets him manage his security credentials. If an administrator renames Richard to Rich, the administrator also needs to update that policy to change the resource from this:

arn:aws:iam::111122223333:user/division\_abc/subdivision\_xyz/Rich

This is true also if an administrator changes the path; the administrator needs to update the policy to reflect the new path for the user.

To rename a user:

3. 1.AWS CLI: aws iam update-user

3.2.AWS API: UpdateUser

4.Deleting an IAM users:

When you use the AWS Management Console to delete an IAM user, IAM automatically deletes the following information for you:

The user

Any user group memberships—that is, the user is removed from any IAM user groups that the user was a member of

Any password associated with the user

Any access keys belonging to the user

To delete an IAM user (console)

4.1.Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.

4.2.In the navigation pane, choose Users, and then select the check box next to the user name that you want to delete.

4.3.At the top of the page, choose Delete.

In the confirmation dialog box, enter the username in the text input field to confirm the deletion of the user. Choose Delete.

5.Deactivating an IAM users:

You might need to deactivate an IAM user while they are temporarily away from your company. You can leave their IAM user credentials in place and still block their AWS access.

To deactivate a user, create and attach a policy to deny the user access to AWS. You can restore the user's access later.

Here are two examples of deny policies that you can attach to a user to deny their access.

The following policy does not include a time limit. You must remove the policy to restore the user's access.

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Deny",

"Action": "\*",

"Resource": "\*"

}

]

}

The following policy includes a condition that starts the policy on December 24, 2024 at 11:59 PM (UTC) and ends it on February 28, 2025 at 11:59 PM (UTC).

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Deny",

"Action": "\*",

"Resource": "\*",

"Condition": {

"DateGreaterThan": {"aws:CurrentTime": "2024-12-24T23:59:59Z"},

"DateLessThan": {"aws:CurrentTime": "2025-02-28T23:59:59Z"}

}

}

]

}

Result:

To Implement secure user management in cloud is done successfully.

Diagram:


        Users who are already authenticated elsewhere can be federated into AWS and assume
          an IAM role that gives them permissions to access specific resources.For more
          information about roles, see Roles terms and concepts.
      