EX:9 IMPLEMENT IDENTITY MANAGEMENT IN CLOUD ENVIROINMENT

AIM:  
 To implement identity management in cloud enviroinment.

DISCRIPTION:

AWS identity management: Users

You can give access to your AWS account to specific users and provide them specific permissions to access resources in your AWS account. You can use both IAM and AWS IAM Identity Center to create new users or federate existing users into AWS. The main difference between the two is that IAM users are granted long-term credentials to your AWS resources while users in IAM Identity Center have temporary credentials that are established each time the user signs-in to AWS. As a best practice, require human users to use federation with an identity provider to access AWS using temporary credentials instead of as an IAM user. A primary use for IAM users is to give workloads that cannot use IAM roles the ability to make programmatic requests to AWS services using the API or CLI.

PROCEDURE:

Topics involved in identity management are,

1.First-time access only: Your root user credentials

2.IAM users and users in IAM Identity Center

3.Federating existing users

1.First-time access only: Your root user credentials

When you create an AWS account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account root user and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you don't use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list of tasks that require you to sign in as the root user, see Tasks that require root user credentials in the IAM User Guide. Only service control policies (SCPs) in organizations can restrict the permissions that are granted to the root user.

2.IAM users and users in IAM Identity Center

IAM users are not separate accounts; they are users within your account. Each user can have its own password for access to the AWS Management Console. You can also create an individual access key for each user so that the user can make programmatic requests to work with resources in your account.

IAM users are granted long-term credentials to your AWS resources. As a best practice, do not create IAM users with long-term credentials for your human users. Instead, require your human users to use temporary credentials when accessing AWS.

In contrast, users in AWS IAM Identity Center are granted short-term credentials to your AWS resources. For centralized access management, we recommend that you use AWS IAM Identity Center (IAM Identity Center) to manage access to your accounts and permissions within those accounts. IAM Identity Center is automatically configured with an Identity Center directory as your default identity source where you can create users and groups, and assign their level of access to your AWS resources.

3.Federating existing users

If the users in your organization already have a way to be authenticated, such as by signing in to your corporate network, you don't have to create separate IAM users or users in IAM Identity Center for them. Instead, you can federate those user identities into AWS using either IAM or AWS IAM Identity Center.

Your users already exist in a corporate directory.

If your corporate directory is compatible with Security Assertion Markup Language 2.0 (SAML 2.0), you can configure your corporate directory to provide single-sign on (SSO) access to the AWS Management Console for your users.

Your users already have Internet identities.

If you are creating a mobile app or web-based app that can let users identify themselves through an Internet identity provider like Login with Amazon, Facebook, Google, or any OpenID Connect (OIDC) compatible identity provider, the app can use federation to access AWS

Result:

To implement identity management in cloud enviroinment is done successfully.

Diagram:

