

Name - Manav Pahilwani

Roll No - 37

Class - D11AD

Experiment no. 7

Aim: To study and implement Identity and Access Management (IAM) practices on AWS/Azure cloud.

Theory:

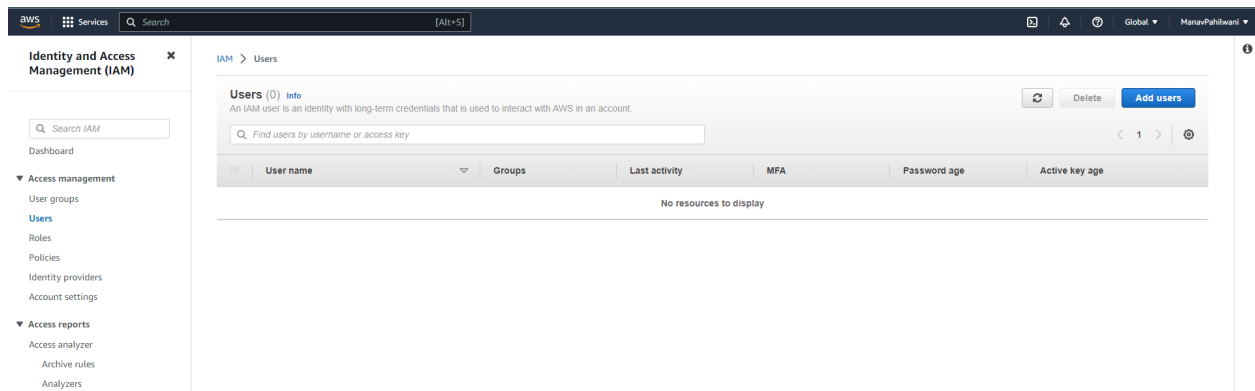
AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. The service is targeted at organizations with multiple users or systems that use AWS products such as Amazon EC2, Amazon RDS, and the AWS Management Console. With IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access.

During this lab experience, you will learn how to create IAM users and groups with specific policies.

Implementation:

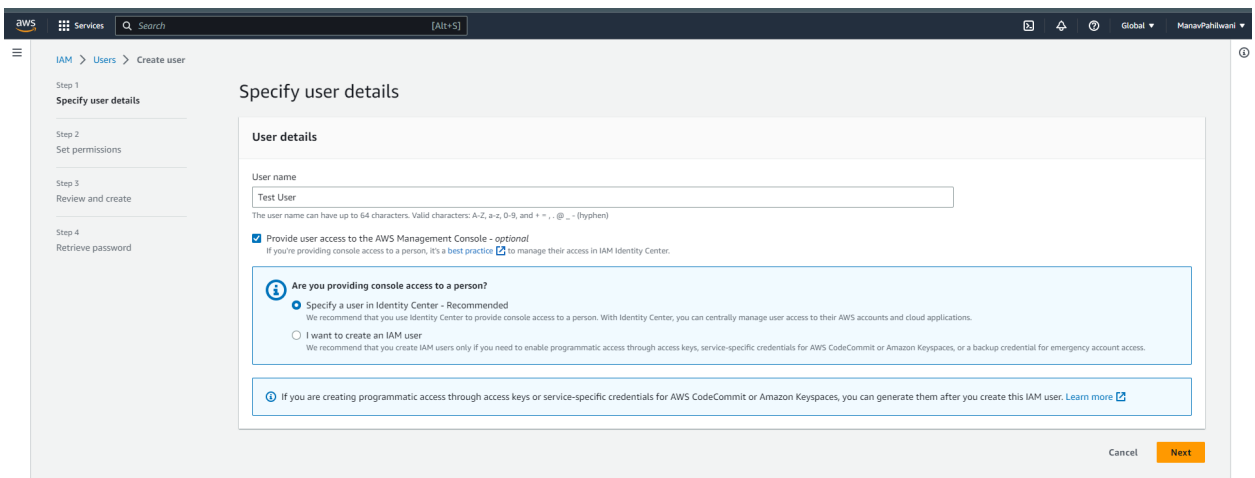
Create IAM user:

Step1: Click on Add user and add name of the user. Click on Next.



Step 2:

Select I want to create an IAM user. Enter custom password and click on next



Step 3

Review and create

Step 4

Retrieve password

User name

Test User

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and +, -, @, _ - (hyphen)

☒ Provide user access to the AWS Management Console - optional

If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

Are you providing console access to a person?

☐ Specify a user in Identity Center - Recommended

We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

☒ I want to create an IAM user

We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

☐ Autogenerated password

You can view the password after you create the user.

☒ Custom password

Enter a custom password for the user.

Must be at least 8 characters long

Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols (! @ # \$ % ^ & * () _ + - (hyphen) = [] { })

☐ Show password

☒ Users must create a new password at next sign-in (recommended).

Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Step3: Finally click on create user.

us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/users/create

Google Classroom

College Id

Personal Id

College Drive

CoinDCX - Crypto E...

Imv-Coincident

The Official Home...

Imv-Coincident

2021 Complete Pyt...

Services

Search

[Alt+S]

Step 1

Specify user details

Step 2

Set permissions

Step 3

Review and create

Step 4

Retrieve password

Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name	Console password type	Require password reset
TestUser	Custom password	Yes

Permissions summary

Name

Type

Used as

IAMUserChangePassword	AWS managed	Permissions policy
-----------------------	-------------	--------------------

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel

Previous

Create user

After creating a user you can download a .csv file which contains the password.

Services

Search

[Alt+S]

User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

View user

IAM > Users > Create user

Step 1

Specify user details

Step 2

Set permissions

Step 3

Review and create

Step 4

Retrieve password

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

Email sign-in instructions

Console sign-in URL

https://343561994611.signin.aws.amazon.com/console

User name

TestUser

Console password

***** Show

Download .csv file

Return to users list

Create IAM groups:

Step1:

In user group, click on Create group.

The screenshot shows the AWS IAM console interface. On the left is a navigation sidebar with sections like 'Access management' and 'Access reports'. The main content area is titled 'Create user group' and includes a 'Name the group' section with a text input field containing 'TestGroup'. Below this is a section 'Add users to the group - Optional' with a table listing users. The table has columns for 'User name', 'Groups', 'Last activity', and 'Creation time'. One user, 'TestUser', is listed with 0 groups and a creation time of '2 minutes ago'. At the bottom, there is a section 'Attach permissions policies - Optional' with a 'Create policy' button.

Create user group

User group name
Enter a meaningful name to identify this group.
TestGroup
Maximum 128 characters. Use alphanumeric and '+', '@', '_' characters.

Add users to the group - Optional (Selected 1/1) [Info](#)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user can belong to up to 10 groups.

User name	Groups	Last activity	Creation time
TestUser	0	None	2 minutes ago

Attach permissions policies - Optional (828) [Info](#)

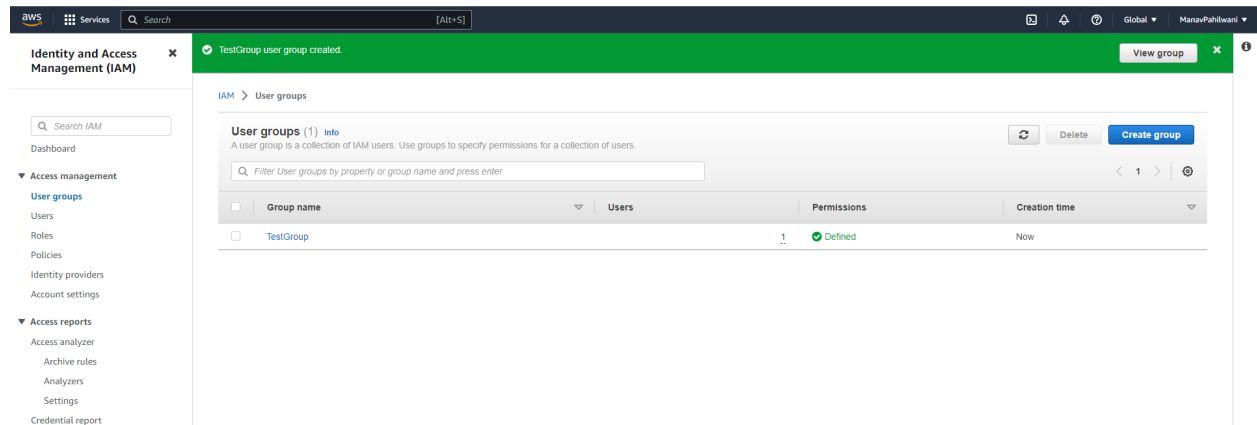
You can attach up to 10 policies to this user group. All the users in this group will have

[Create policy](#)

You can attach permission policies if needed. And click on the create group button.

The screenshot shows the AWS IAM console interface, specifically the 'Policy name' list. The table lists various AWS managed policies with columns for 'Policy name', 'Type', and 'Description'. The policies include AWSDirectConnectReadOnlyAccess, AmazonGlacierReadOnlyAccess, AWSMarketplaceFullAccess, AWSSSODirectoryAdministrator, AWSIoTClickReadOnlyAccess, AutoScalingConsoleReadOnlyAccess, AmazonDMSRedshiftS3Role, AWSQuickSightListIAM, AWSHealthFullAccess, AlexaForBusinessGatewayExecution, AmazonElasticTranscoder_ReadOnlyAcc..., AmazonRDSFullAccess, SupportUser, AmazonEC2FullAccess, SecretsManagerReadWrite, AWSIoTThingsRegistration, and AmazonDocDBReadOnlyAccess.

Policy name	Type	Description
AWSDirectConnectReadOnlyAccess	AWS managed	Provides read only access to AWS Direct Connect via the AWS Management Co...
AmazonGlacierReadOnlyAccess	AWS managed	Provides read only access to Amazon Glacier via the AWS Management Console.
AWSMarketplaceFullAccess	AWS managed	Provides the ability to subscribe and unsubscribe to AWS Marketplace software, ...
AWSSSODirectoryAdministrator	AWS managed	Administrator access for SSO Directory
AWSIoTClickReadOnlyAccess	AWS managed	Provides read only access to AWS IoT 1-Click.
AutoScalingConsoleReadOnlyAccess	AWS managed	Provides read-only access to Auto Scaling via the AWS Management Console.
AmazonDMSRedshiftS3Role	AWS managed	Provides access to manage S3 settings for Redshift endpoints for DMS.
AWSQuickSightListIAM	AWS managed	Allow QuickSight to list IAM entities
AWSHealthFullAccess	AWS managed	Allows full access to the AWS Health APIs and Notifications and the Personal He...
AlexaForBusinessGatewayExecution	AWS managed	Provide gateway execution access to AlexaForBusiness services
AmazonElasticTranscoder_ReadOnlyAcc...	AWS managed	Grants users read-only access to Elastic Transcoder and list access to related s...
AmazonRDSFullAccess	AWS managed	Provides full access to Amazon RDS via the AWS Management Console.
SupportUser	AWS managed - job function	This policy grants permissions to troubleshoot and resolve issues in an AWS acc...
AmazonEC2FullAccess	AWS managed	Provides full access to Amazon EC2 via the AWS Management Console.
SecretsManagerReadWrite	AWS managed	Provides read/write access to AWS Secrets Manager via the AWS Management ...
AWSIoTThingsRegistration	AWS managed	This policy allows users to register things at bulk using AWS IoT StartThingRegis...
AmazonDocDBReadOnlyAccess	AWS managed	Provides read-only access to Amazon DocumentDB with MongoDB compatibility...



IAM User Group is created successfully with the user you just created.

Conclusion - Identity and Access Management (IAM) is a critical component of any cloud infrastructure. IAM provides a framework for controlling access to resources in the cloud, ensuring that only authorized users have access to sensitive data and applications.