

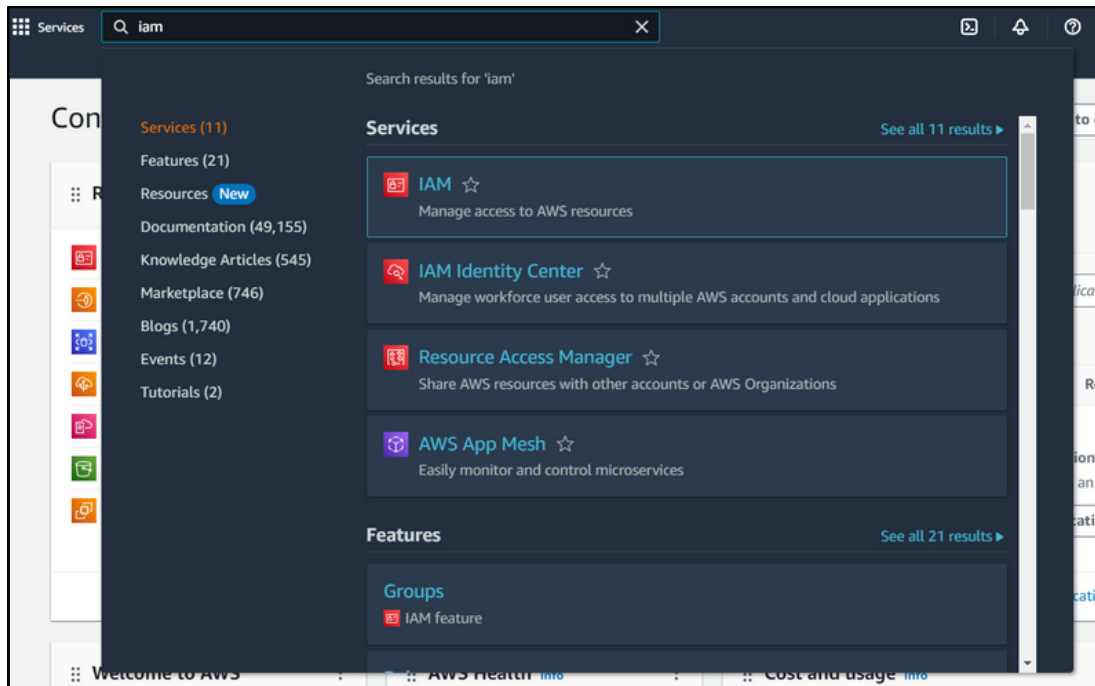
Assignment 3

Problem Statement: Create an IAM user and assign full S3 access

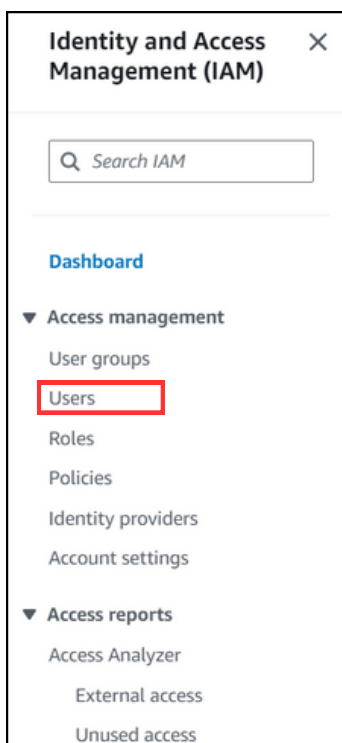
Solution:

1. Create an IAM user

Step 1.1: Log into your AWS console and search IAM on the search bar, click on it



Step 1.2: Click on Users and then Create user



A screenshot of the AWS IAM console 'Users' page. The page title is 'Users (2) Info'. Below the title, there is a search bar and a table of users. The table has columns for 'User name', 'Path', 'Group', 'Last activity', 'MFA', 'Password age', and 'Console last sign-in'. There are two users listed: 'mainak_admin' and 'mainak_mckv'. The 'mainak_admin' user has a password age of 32 days and a console last sign-in of February 04, 2024, 22:00. The 'mainak_mckv' user has a password age of 12 days and a console last sign-in of January 31, 2024, 11:00.

<input type="checkbox"/>	User name	Path	Group	Last activity	MFA	Password age	Console last sign-in
<input type="checkbox"/>	mainak_admin	/	2		-	32 days	February 04, 2024, 22:00
<input type="checkbox"/>	mainak_mckv	/	1		Virtual	12 days	January 31, 2024, 11:00

Step 1.3: Specify the user details, tick on **Provide user access to AWS Management console** to give the user access to the AWS Console and choose **I want to create an IAM user**

Specify user details

User details

User name
demo-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?

User type

☐ 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.

Step 1.4: Specify the password, you can give a **Custom password** or let AWS **generate a password** for the user. Optionally, you may tick **User must create a new password at next sign-in**, so that, the user can be able to change the password at the next sign-in. Click on **Next**.

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](#)

Cancel Next

Step 1.5: To **set permissions** to the user, create a group by clicking on **Create group**

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

☒ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

☐ Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

User groups (2)

Search

<input type="checkbox"/>	Group name	Users	Attached policies	Created
<input type="checkbox"/>	admin_iam_practice	2	AdministratorAccess	2024-01-03 (4 weeks ago)
<input type="checkbox"/>	developer_iam_practice	1	AlexaForBusinessReadOnlyAcce...	2024-01-03 (4 weeks ago)

Create group

Step 2: Create group and attach AmazonS3FullAccess policy

Step 2.1: Set a **group-name** and search **AmazonS3FullAccess** policy. Select it and click on **Create user group**.

The screenshot shows the 'Create user group' dialog box. At the top, it says 'Create a user group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)'. Below this, there's a section for 'User group name' with a text input field containing 'demo-s3-access' and a note: 'Maximum 128 characters. Use alphanumeric and '+=, @, -, _' characters.' The main section is 'Permissions policies (1/914)' with a search bar containing 's3' and a dropdown for 'Filter by Type' set to 'All types', showing '9 matches'. A table lists several AWS managed policies. The 'AmazonS3FullAccess' policy is selected with a blue checkmark. At the bottom right, there are 'Cancel' and 'Create user group' buttons.

	Policy name	Type	Use...	Description
<input type="checkbox"/>	AmazonDMSRedsh...	AWS managed	None	Provides access to manage S3 setti
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS managed	None	Provides full access to all buckets v
<input type="checkbox"/>	AmazonS3ObjectL...	AWS managed	None	Provides AWS Lambda functions pe
<input type="checkbox"/>	AmazonS3Outpost...	AWS managed	None	Provides full access to Amazon S3 c
<input type="checkbox"/>	AmazonS3Outpost...	AWS managed	None	Provides read only access to Amazc

Step 2.2: Select the group you just created, for me, it is **demo-s3-access**. Click Next.

The screenshot shows the 'demo-s3-access user group created' confirmation screen. It has a green header bar. On the left, there's a sidebar with 'Step 3: Review and create' and 'Step 4: Retrieve password'. The main area has three radio button options: 'Add user to group' (selected), 'Copy permissions', and 'Attach policies directly'. Below these is a table titled 'User groups (1/3)' with columns: Group name, Users, Attached policies, and Created. The 'demo-s3-access' group is highlighted with a blue checkmark.

Group name	Users	Attached policies	Created
admin_iam_practice	2	AdministratorAccess	2024-01-03 (4 weeks ago)
demo-s3-access	0	AmazonS3FullAccess	2024-02-04 (Now)
developer_iam_practice	1	AlexaForBusinessReadOnlyAcce...	2024-01-03 (4 weeks ago)

Step 2.3: Click on **Create user** to finalize the creation of **IAM user**. Now you can check the created user on the **Users** tab.

Permissions summary

< 1 >

Name	Type	Used as
demo-s3-access	Group	Permissions group
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

IAM > Users

Users (1/3) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Q Search

< 1 > ⌕

	User name	Path	Group	Last activity	MFA	Password age	Console last sign-in
<input checked="" type="checkbox"/>	demo-user	/	0		-	Now	-
<input type="checkbox"/>	mainak_admin	/	2		-	32 days	February 04, 2024, 22
<input type="checkbox"/>	mainak_mckv	/	1		Virtual	12 days	January 31, 2024, 11:

Definitions

- **IAM** stands for **Identity and Access Management**. IAM is an AWS service that helps to create and manage resources such as **Users**, **Groups**, **Policies** and **IAM Roles**.
- An AWS Identity and Access Management (IAM) user is an entity that you create in AWS. The IAM user represents the human user or workload who uses the IAM user to interact with AWS. A user in AWS consists of a name and credentials.