

Assignment – 3

Problem Statement: -

Create IAM user giving full access of S3 in AWS account.

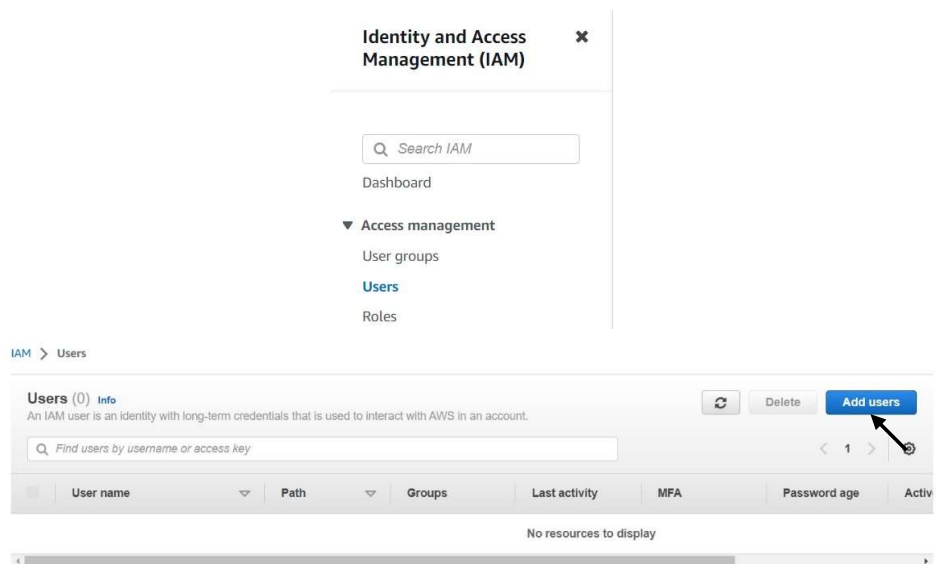
Steps for create IAM user giving full access of S3 in AWS: -

1. Open the **Amazon Web Services** (<https://aws.amazon.com/console/>) home page.
2. Log in your **AWS Management Console** account.
3. Click on your **Username** (*top right corner on home page*).
4. Go **Security credentials**.
5. Go **Users** option (after open *In My security credentials (root user)* info page; click on *Users*).
6. Click on **Add users**.
7. Give a username.
8. Check the box **Provide user access to the AWS Management Console – optional**.
9. Choose **I want to create an IAM user**.
10. Create **Console password** (select **Custom password**).
11. Uncheck (by default check) **Users must create a new password at next sign-in (recommended)** (if you don't want to change password after 1st time login as a IAM user).
12. In **Set permissions**, select **Add user to group** and continue with **Create group**.
13. Open **Create user group** window; give a **User group name** (E.g. **S3fullaccess**) and select which permissions you want to provide to IAM user (for this case **AmazonS3FullAccess**).
14. Now group creation complete. So, select that group and continue with **Next** option.
15. Review and click on **Create user**.
16. Complete IAM user creation with S3 full access. You also download IAM user security credential as .csv file.

Some snapshots of create IAM user giving full access of S3 in AWS: -



Step 1: Go Security credentials



Step 2: Go Users & click on Add Users

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

Specify user details

User details

User name

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](#)

Step 3: Specify user details

Cancel Next

IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

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.

Get started with groups
Create a 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](#)

Create group

Permissions boundary - optional
Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. [Learn more](#)

Step 4: Create group

Cancel Previous Next

Create user group

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](#)

User group name
Enter a meaningful name to identify this group.

Maximum 128 characters. Use alphanumeric and *+=_@_- characters.

Permissions policies (1/816)

1 match < 1 >

<input checked="" type="checkbox"/>	Policy name	Type	Used as
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS managed	Permissi

Step 5: Give permission

Cancel Create user group

- Step 1
Specify user details
- Step 2
Set permissions
- Step 3
Review and create
- Step 4
Retrieve password

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 (2/1)

1

<input checked="" type="checkbox"/>	Group name	Users	Attached policies	Created
<input checked="" type="checkbox"/>	S3fullaccess	0	AmazonS3FullAccess	2023-02-16 (Now)

► **Permissions boundary - optional**

Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. [Learn more](#)

Cancel

Previous

Next

Step 6: Select permissible group

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://189040608428.signin.aws.amazon.com/console>

User name

IAM@ab_17

Console password

***** [Show](#)

Download .csv file

Return to users list

Complete IAM User creation

Users (Selected 1/1) Info

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

1

<input checked="" type="checkbox"/>	User name	Path	Groups	Last activity	MFA	Password a...	Active ke
<input checked="" type="checkbox"/>	IAM@ab_17	/	S3fullaccess	3 minutes ago	None	6 minutes ago	-

After creating IAM User

aws

Services

Search

[Alt+S]

Global

IAM@ab_17 @ 1890-4060-8428

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Amazon S3 > Buckets

Account snapshot

Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

View Storage Lens dashboard

Buckets Info

Copy ARN

Empty

Delete

Create bucket

1

Name	AWS Region	Access	Creation date
No buckets			
No buckets			
<div>Create bucket</div>			

S3 Full Access for IAM User