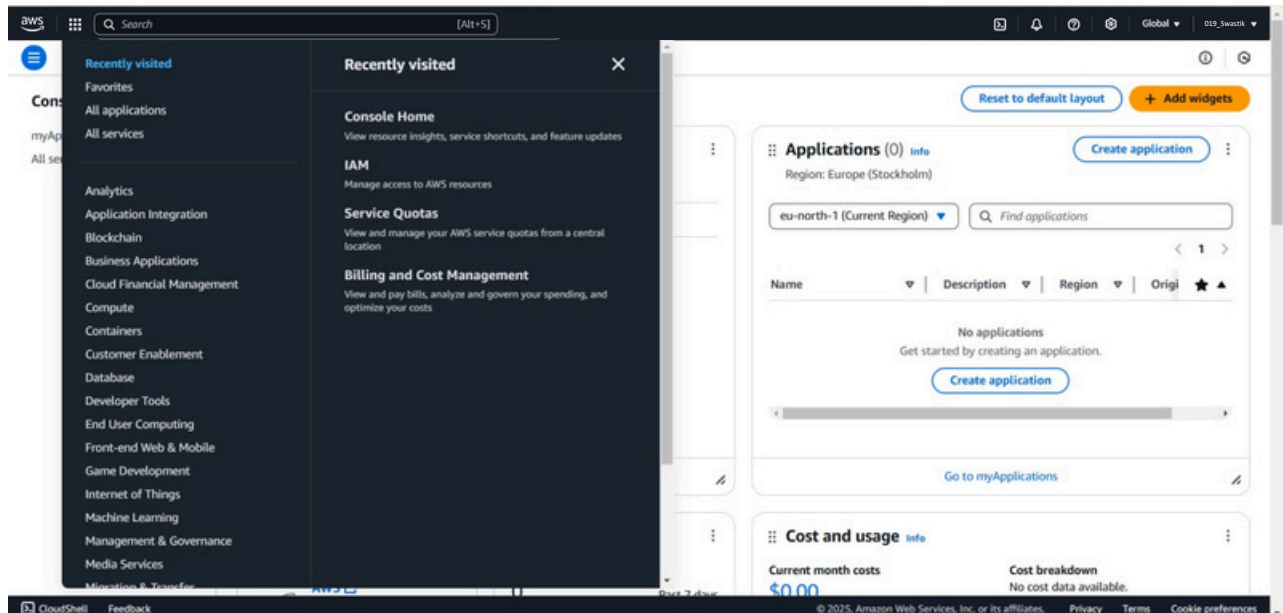


Assignment No:03

Title: Create IAM User and give full access to S3.

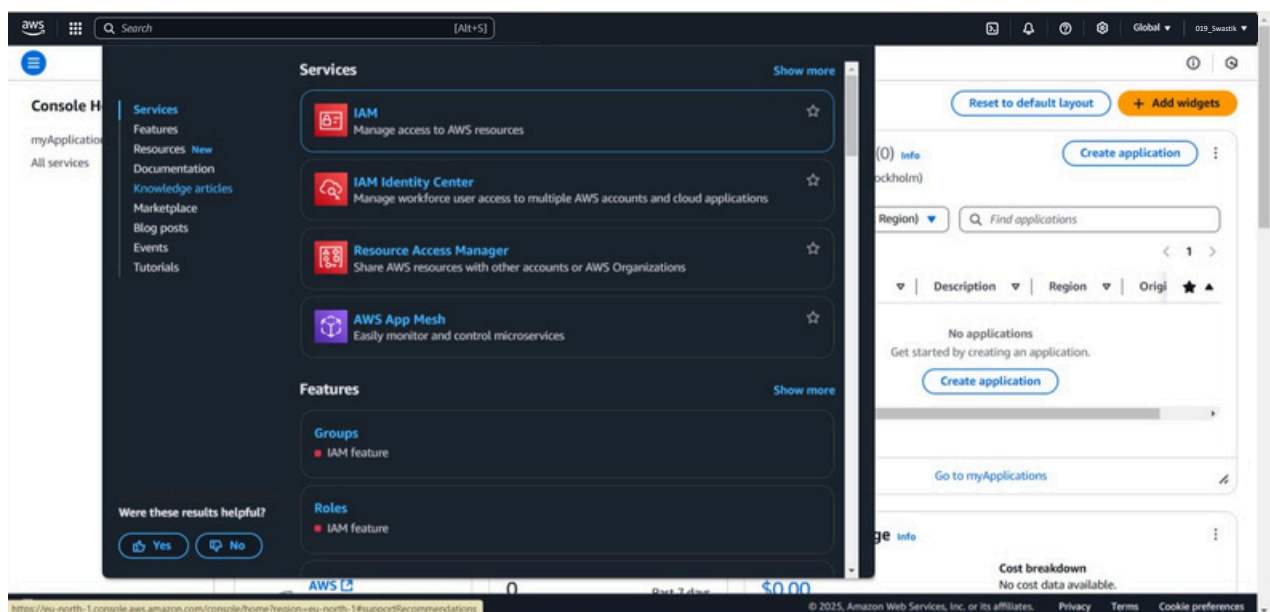
Step-1:

Open the AWS Management Console and click on services on the top left corner.



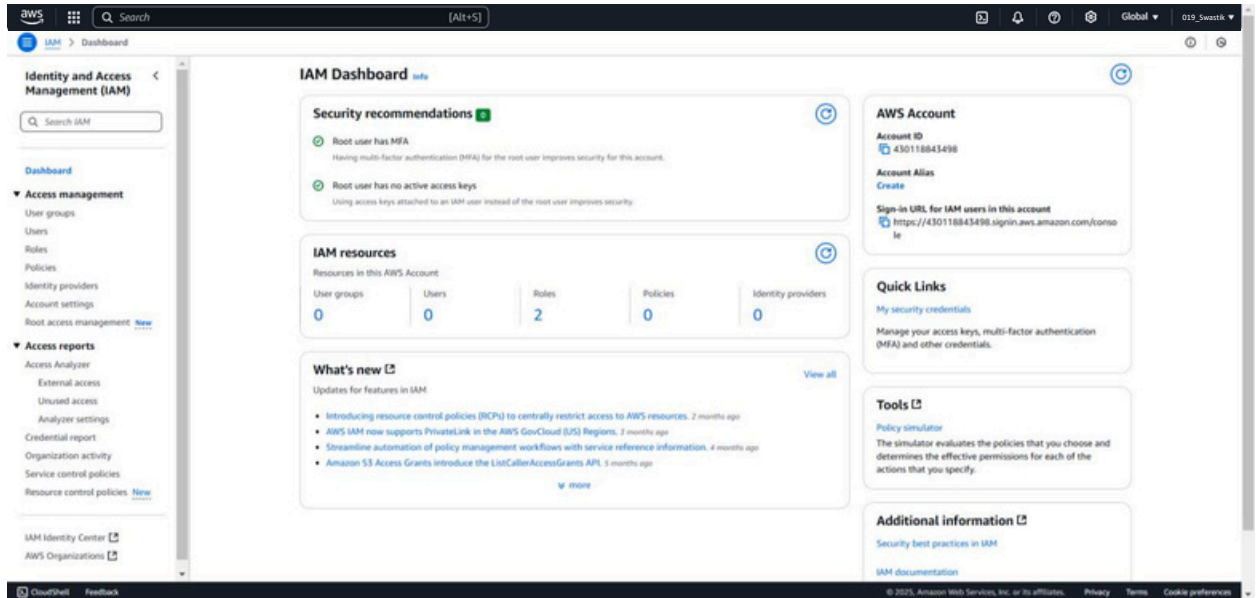
Step-2:

Click on all services and open the IAM.



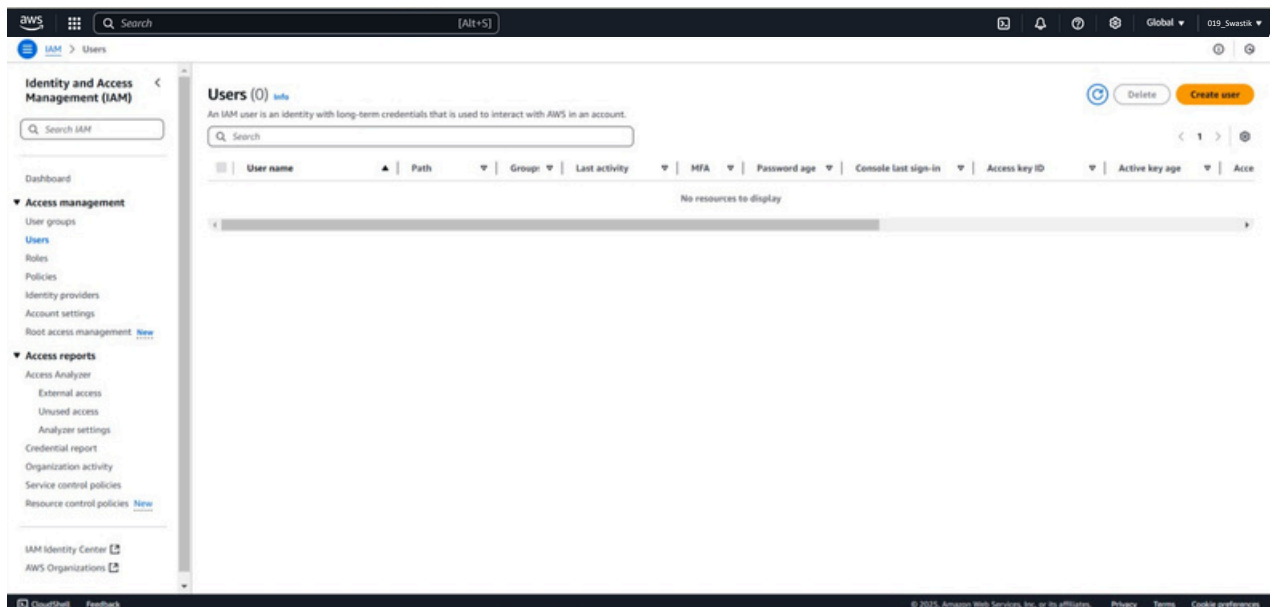
Step-3:

Open the Users in Access management in the left side.



Step-4:

Now click on the Create user.



Step-5:

Now give IAM user a name and check the Provide user access to the AWS management console and select the user type as I want to create an IAM user then choose custom password in the console password section then choose password then click on next.

AB_IAM

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.

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.

[Learn more](#)

Cancel Next

Step-6:

Now select Attach policies directly in the Permissions options. Now check the AmazonS3FullAccess box and click on next.

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.

Permissions policies (1/1319)
Choose one or more policies to attach to your new user.

Filter by Type: All types 16 matches

Policy name	Type	Attached entities
<input type="checkbox"/> AmazonDMSRedshiftS3Role	AWS managed	0
<input checked="" type="checkbox"/> AmazonS3FullAccess	AWS managed	0
<input type="checkbox"/> AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	0
<input type="checkbox"/> AmazonS3OutpostsFullAccess	AWS managed	0
<input type="checkbox"/> AmazonS3OutpostsReadOnlyAccess	AWS managed	0
<input type="checkbox"/> AmazonS3ReadOnlyAccess	AWS managed	0
<input type="checkbox"/> AmazonS3TablesFullAccess	AWS managed	0
<input type="checkbox"/> AmazonS3TablesReadOnlyAccess	AWS managed	0

Next

Step-7:

Now review the account and click on create user.

The screenshot shows the AWS IAM console's 'Create user' wizard at the 'Review and create' step. On the left, a progress bar indicates four steps: 'Specify user details', 'Set permissions', 'Review and create' (the current step), and 'Retrieve password'. The main content area is titled 'Review and create' and includes a sub-header 'Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.' Below this, there are three sections: 'User details' showing 'User name' as 'AB_IAM', 'Console password type' as 'Custom password', and 'Require password reset' as 'Yes'; 'Permissions summary' showing two policies: 'AmazonS3FullAccess' (AWS managed) and 'IAMUserChangePassword' (AWS managed), both used as 'Permissions policy'; and 'Tags - optional' with a note that no tags are currently associated. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Create user'.

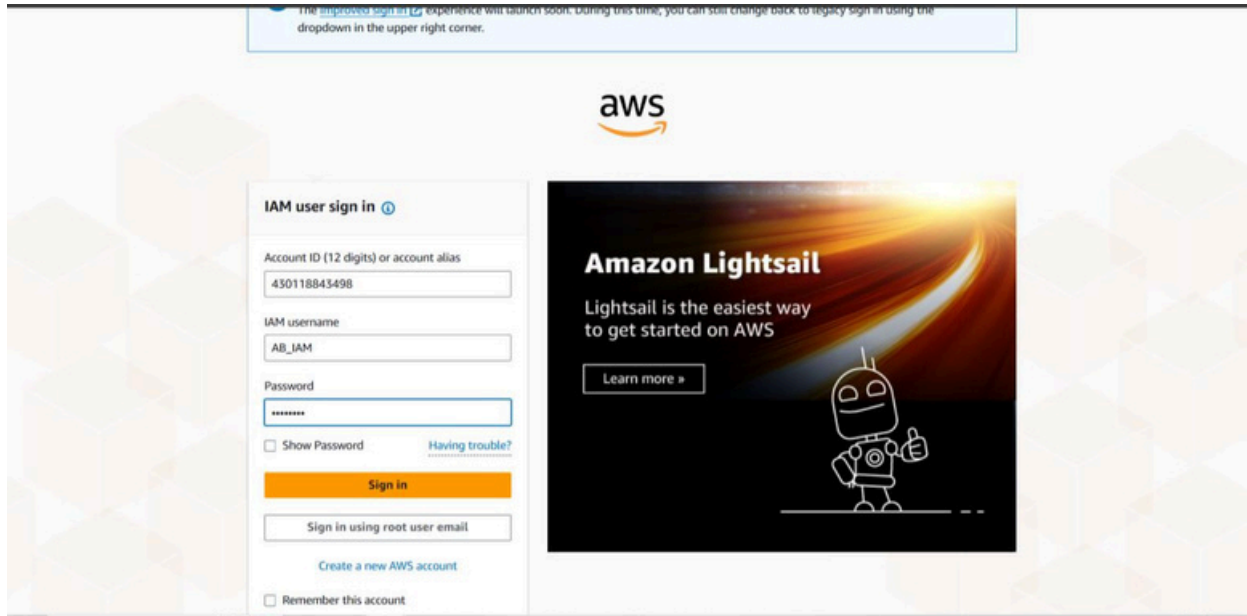
Step-8:

Now download the csv.

The screenshot shows the AWS IAM console's 'Retrieve password' step. A green success banner at the top states 'User created successfully' and provides a 'View user' link. The progress bar on the left now highlights the 'Retrieve password' step. The main content area is titled 'Retrieve password' and includes a sub-header '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.' Below this, there is a 'Console sign-in details' section with a button 'Email sign-in instructions'. It displays the 'Console sign-in URL' as 'https://430118843498.signin.aws.amazon.com/console', the 'User name' as 'AB_IAM', and the 'Console password' as a masked string with a 'Show' button. At the bottom right, there are three buttons: 'Cancel', 'Download .csv file', and 'Return to users list'.

Step-9:

Now login to the IAM user account by giving credentials from the csv file.



Step-10:

Login into the IAM user is successful.

