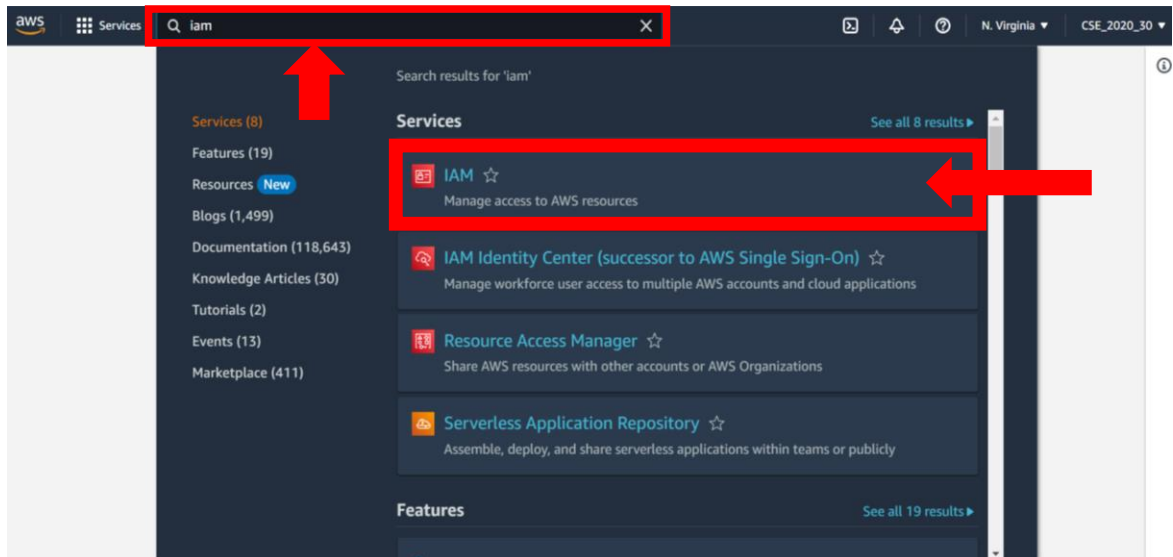


ASSIGNMENT 3

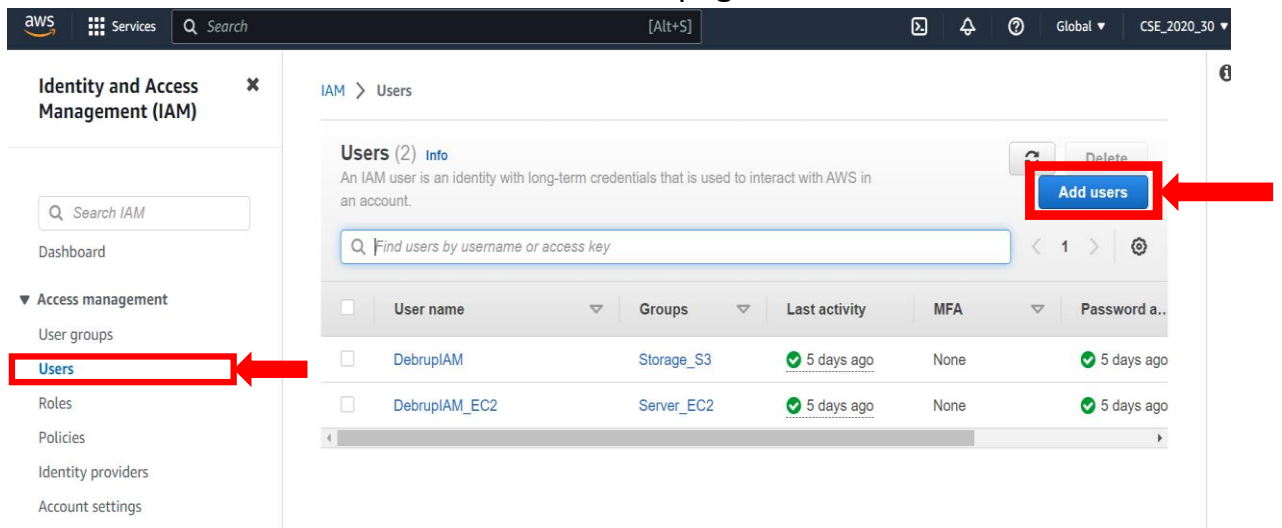
Problem Statement: Create IAM resource giving full access of S3(storage).

Procedure:

1. Sign in to your console (as root user).
2. On the top side of the page go to the **Search bar** and type “IAM”.
3. Click on the first result showing “IAM”.



4. We are then redirected to the Identity and Access Management (IAM) dashboard. We then have to select the **user** option in the left side panel under **Access Management**.
5. Next click on **Add Users** button in the **Users** page.



6. After that you have to create a user and specify the details.
 - a. Specify the name of the user
 - b. **Check** the “Provide user access to the AWS Management Console” box
 - c. **Select** the option “I want to create an IAM user”.
 - d. Select custom password and enter it.
 - e. **Uncheck** the “Users must create a new password at next sign-in” box.
 - f. Then click on next

User details

User name

Test

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.

.....

☐ 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

- Now under **Permissions Options**, select **Add user to Group** option.
- Under **User Groups** click on **Create Group** button.

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 groups

< 1 >

<input type="checkbox"/>	Group name	Users	Attached policies ...	Created
<input type="checkbox"/>	Server_EC2	1	AmazonEC2FullAcce...	2023-02-13 (5 days ...)
<input type="checkbox"/>	Storage_S3	1	AmazonDMSRedshift...	2023-02-13 (5 days ...)

Create group

- A pop-up will appear where you have to specify the new group name and edit the policies/permissions associated with it
 - Enter the **User Group Name**
 - Next in the find policies search bar type **S3** as we have to give permission only for S3.
 - Select the **first two** options
 - Then click on **Create User Group**

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.
Test
Maximum 128 characters. Use alphanumeric and '+', '@', '-' characters.

Permissions policies (2/816)

Search: S3 9 matches

Policy name	Type	Used as	D...
<input checked="" type="checkbox"/> AmazonDMSRedshiftS3Role	AWS managed	Permissio...	Pr...
<input checked="" type="checkbox"/> AmazonS3FullAccess	AWS managed	Permissio...	Pr...
<input type="checkbox"/> AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	None	Pr...
<input type="checkbox"/> AmazonS3OutpostsFullAccess	AWS managed	None	Pr...
<input type="checkbox"/> AmazonS3OutpostsReadOnlyAccess	AWS managed	None	Pr...

10. Now the pop-up closes and under the **User Groups** section our newly created group is visible in a table format. Select the group.

11. Then click on **Next**.

User groups (1/3)

Search groups

Group name	Users	Attached policies ...	Created
<input type="checkbox"/> Server_EC2	1	AmazonEC2FullAcce...	2023-02-13 (5 days ...)
<input type="checkbox"/> Storage_S3	1	AmazonDMSRedshift...	2023-02-13 (5 days ...)
<input checked="" type="checkbox"/> Test	0	AmazonDMSRedshift...	2023-02-18 (1 minut...

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**

12. We arrive at the **Review and Create** page. After reviewing click on the **Create User** button.

Permissions summary

Name	Type	Used as
Test	Group	Permissions group
IAMUserChangePassword	AWS managed	Permissions policy

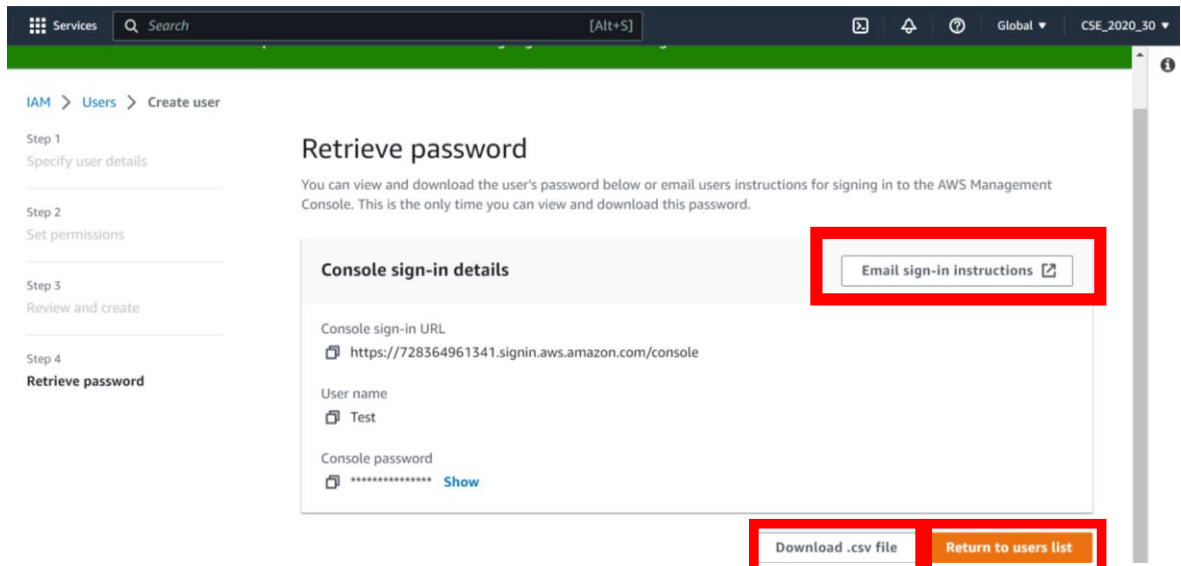
Tags - optional
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

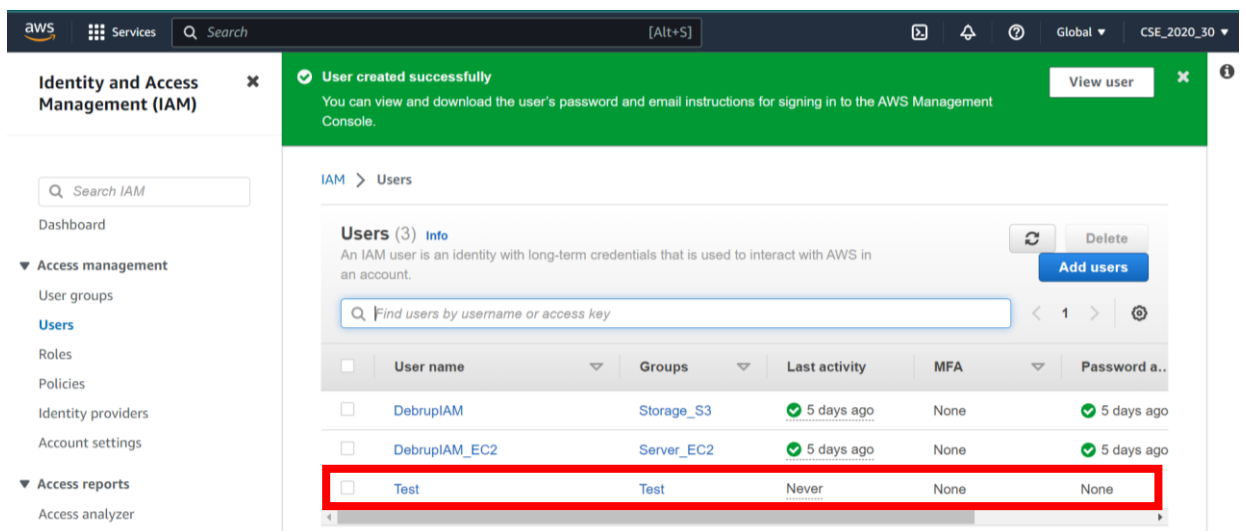
Add new tag
You can add up to 50 more tags.

Cancel Previous **Create user**

13. Next, we arrive at the **Retrieve Password** page where we can download a **.csv file** or **email the sign-in details of the newly created IAM user**.



14. After that we can return to users list and see that our new user has been added to the users' table.



15. Now we logout of our console.

16. Next, we again try to login to the console. But now we select **IAM user login**.

17. Here we have to enter **Account ID** of the root user. We can get that in the drop-down menu after logging in our root user account.

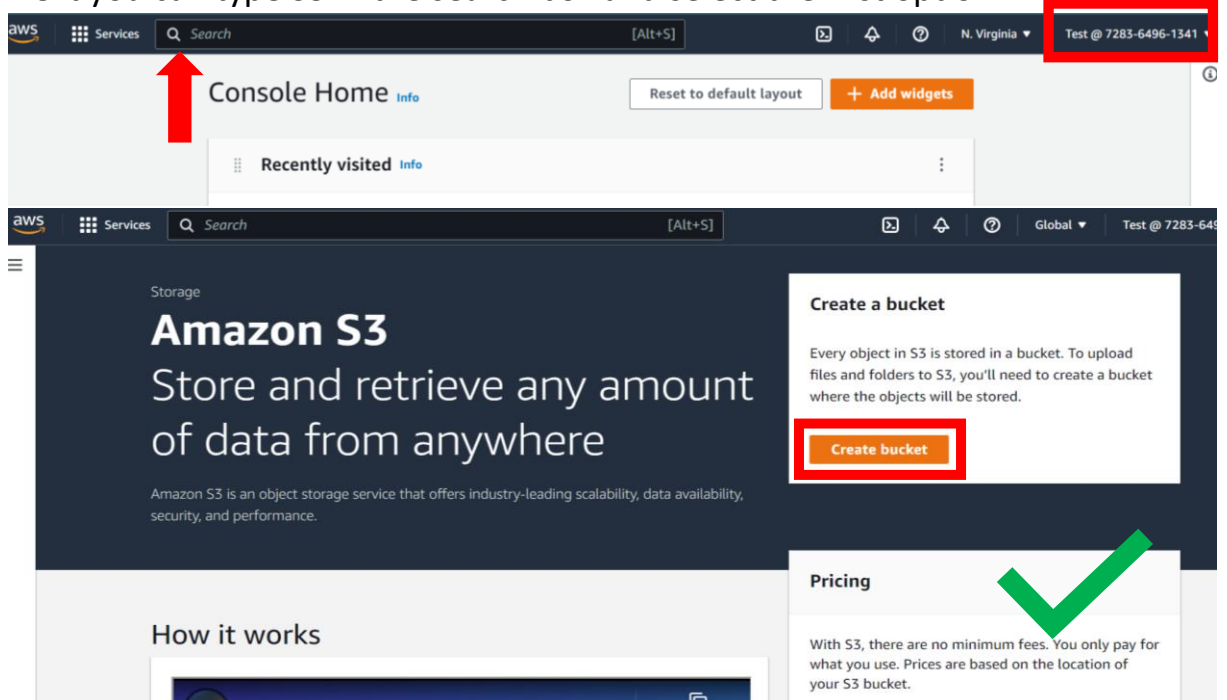
Alternatively, we can use **the link** in our **downloaded .csv file** or our **email** which if used in our **browser** will redirect use to the login page with the Account ID already entered!



18. Enter the credentials.

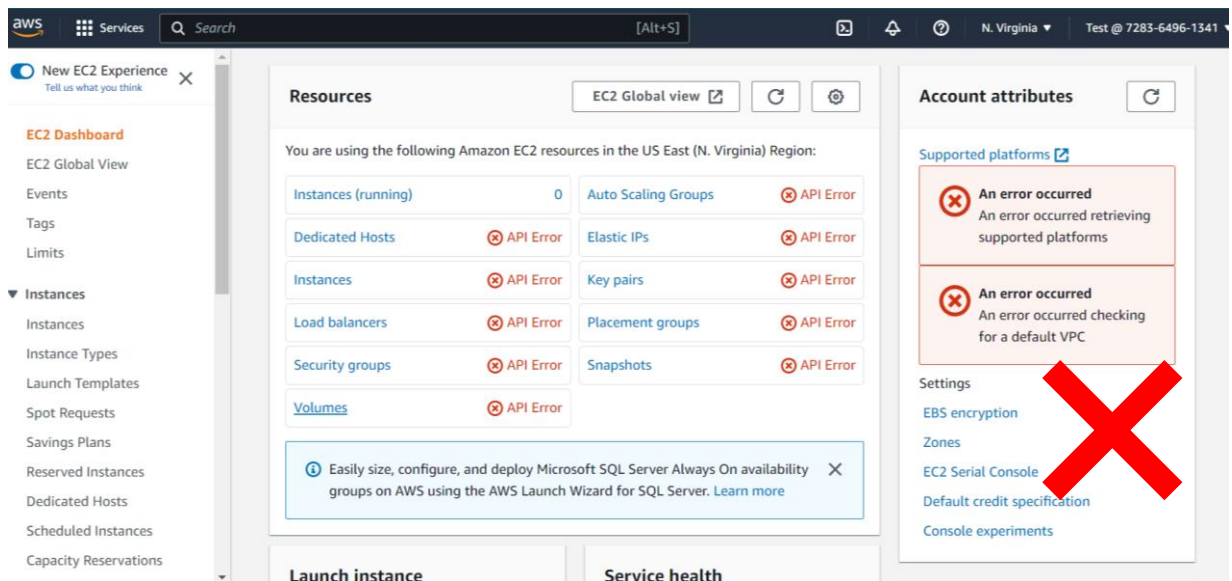
19. Note the username in the top right corner. Also, you cannot access your account page as it is controlled only by your root user.

20. Next you can type S3 in the search box and select the first option.



21. Here we get to Create Bucket. Hence we have full access of S3.

22. Now to check our limits let us search EC2 in search bar. Select the first choice.



23. Here, we encounter API error. This is proof that we do not have access to EC2. Hence, we have successfully restricted access to our IAM user.

24. Thus, we have successfully created an IAM user and given it only S3 access.

25. Now, we can logout.