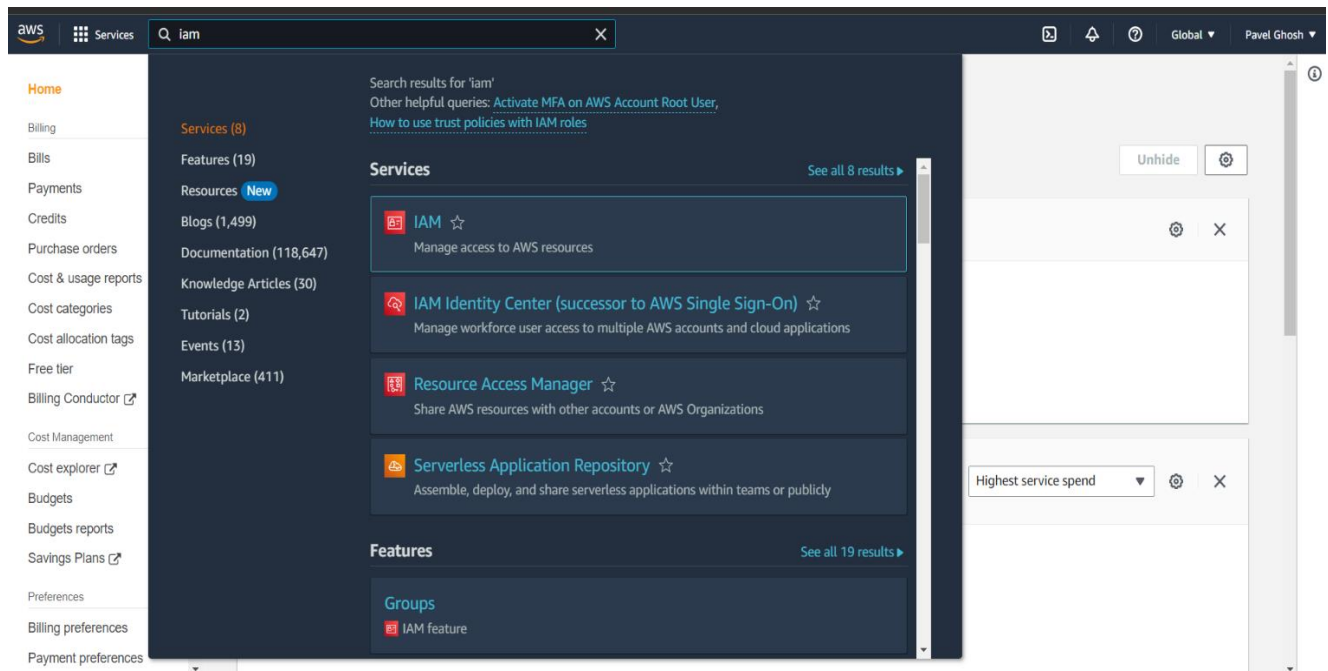


Assignment 3

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

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analizers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Related consoles

IAM Identity Center [New](#)

Set permissions

Step 3
Review and create

Step 4
Retrieve password

User name

PavelIAM

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](#)

Cancel Next

7. Now under **Permissions Options**, select **Add user to Group** option.

8. Under **User Groups** click on **Create Group** button.

Test user group created.

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.

User groups (1)

[Search groups](#)

[Create group](#)

<input type="checkbox"/>	Group name ↗	Users	Attached policies ↗	Created
<input type="checkbox"/>	Test	0	AmazonDMSRedshiftS3Role and AmazonS3Full...	2023-02-20 (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

9. A pop-up will appear where you have to specify the new group name and edit the policies/permissions associated with it.

a. Enter the **User Group Name**

b. Next in the find policies search bar type **S3** as we have to give permission only for S3.

c. Select the **first two** options

d. Then click on **Create User Group**

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**.

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

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.

The screenshot shows the AWS IAM console interface. At the top, there's a navigation bar with the AWS logo, 'Services', a search bar, and a user profile 'Pavel Ghosh'. Below this, a green banner says 'Test user group created.' The main content area is titled 'Set permissions' and includes a sub-header '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](#)'. There are three radio button options under 'Permissions options': 'Add user to group' (selected), 'Copy permissions', and 'Attach policies directly'. Below these is a section for 'User groups (1/1)' with a search bar and a table. The table has columns for 'Group name', 'Users', 'Attached policies', and 'Created'. One group named 'Test' is listed with 0 users and two policies. At the bottom, there's a 'Permissions boundary - optional' section and 'Cancel', 'Previous', and 'Next' buttons.

Group name	Users	Attached policies	Created
Test	0	AmazonDMSRedshiftS3Role and AmazonS3Full...	2023-02-20 (Now)

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!



Sign in as IAM user

Account ID (12 digits) or account alias

531939321869

IAM user name

Password

☐ Remember this account

Sign in

[Sign in using root user email](#)

[Forgot password?](#)

Start on Amazon Redshift for Free

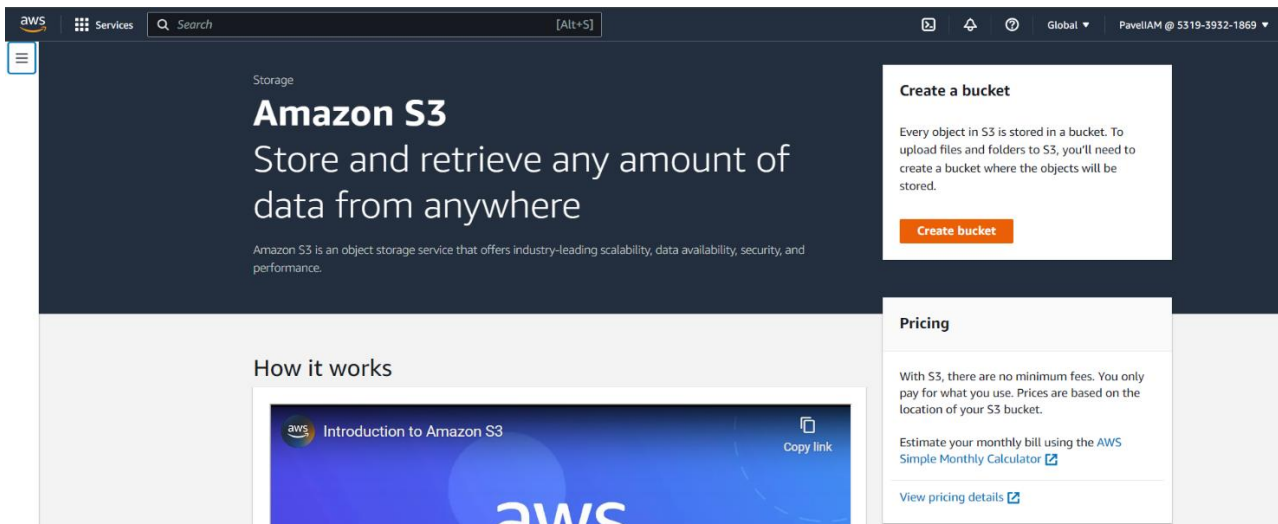
Try a two month free trial of our DC2.Large node with 750 free hours per month



18. Enter the credentials.

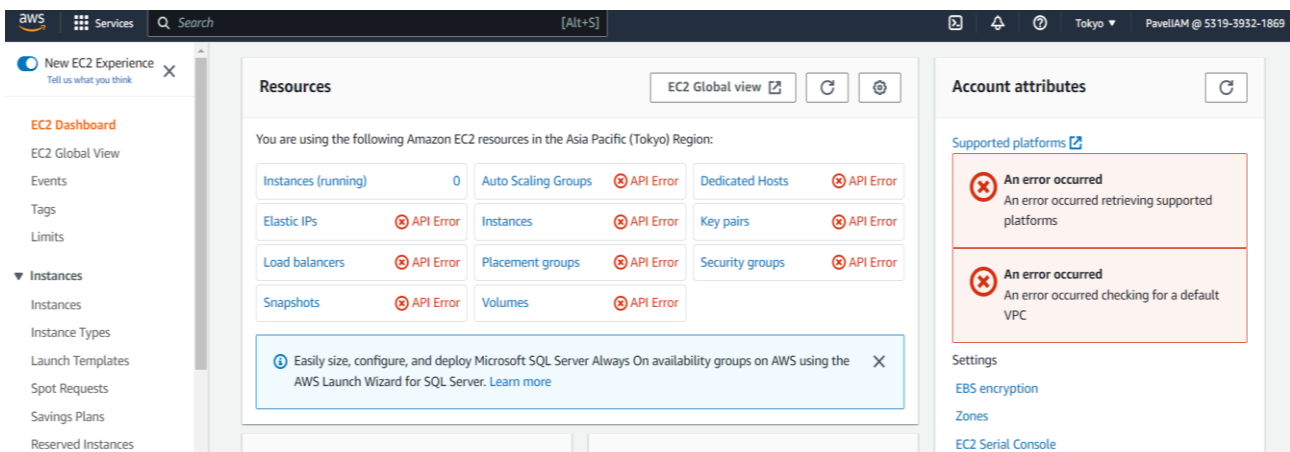
19. Note the username in the top right corner. Also, you cannot access your account page as it is controlled only by your root user.

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.