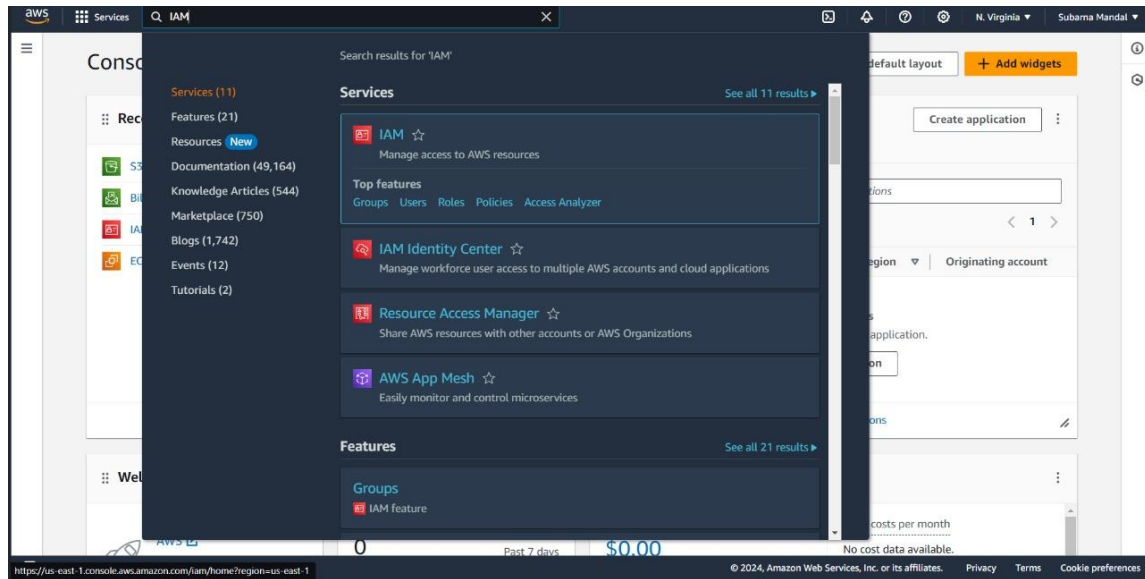


Assignment : 3

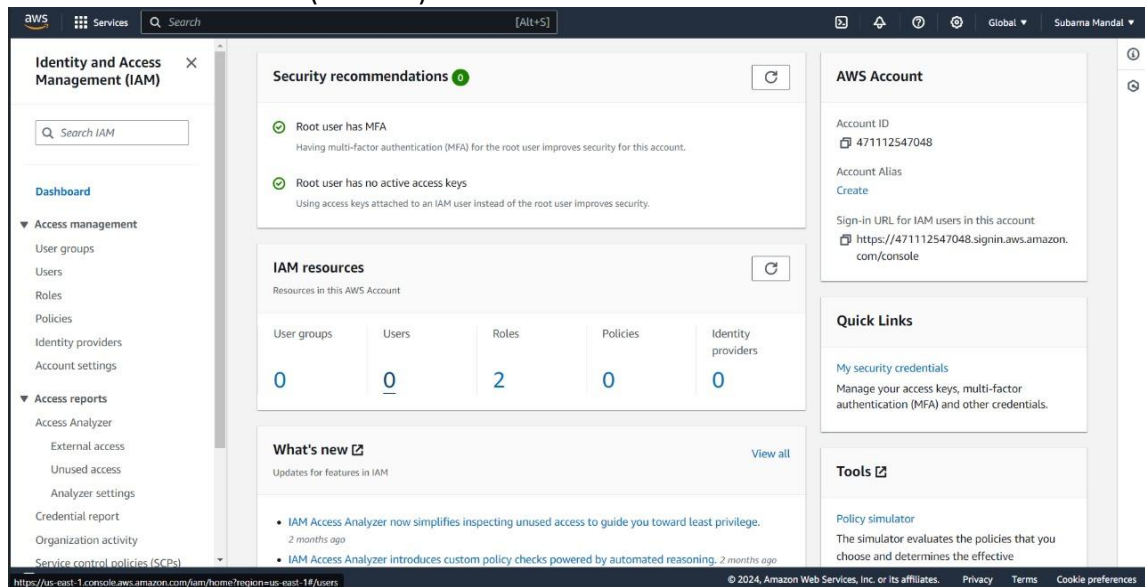
Statement : Create IAM user and give full access to S3.

Steps :

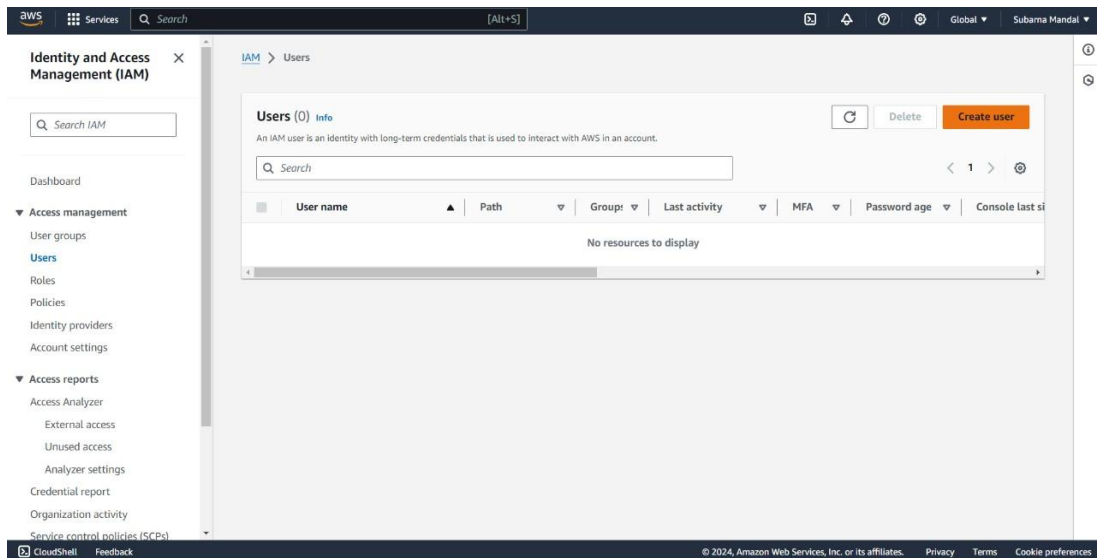
1) First Search 'IAM' on the search bar and click over 'IAM'.



2) Then click below 'users' (here '0')



3) click on 'Create User'.



4) provide 'User details'(name and password) and fill the check boxes given below.

Specify user details

User details

User name

user1

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.

user1@aws

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

5) Under 'Permission option' click 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.

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

Set permissions boundary - optional

Cancel Previous Next

6) For 'Create user group' first provide 'user name' then on 'permissions policies' search S3 and choose 'AmazonS3Fullaccess' for the group and 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.

s3fullgroup

Maximum 128 characters. Use alphanumeric and "+", "@", "_" characters.

Permissions policies (1/912)

Filter by Type

s3

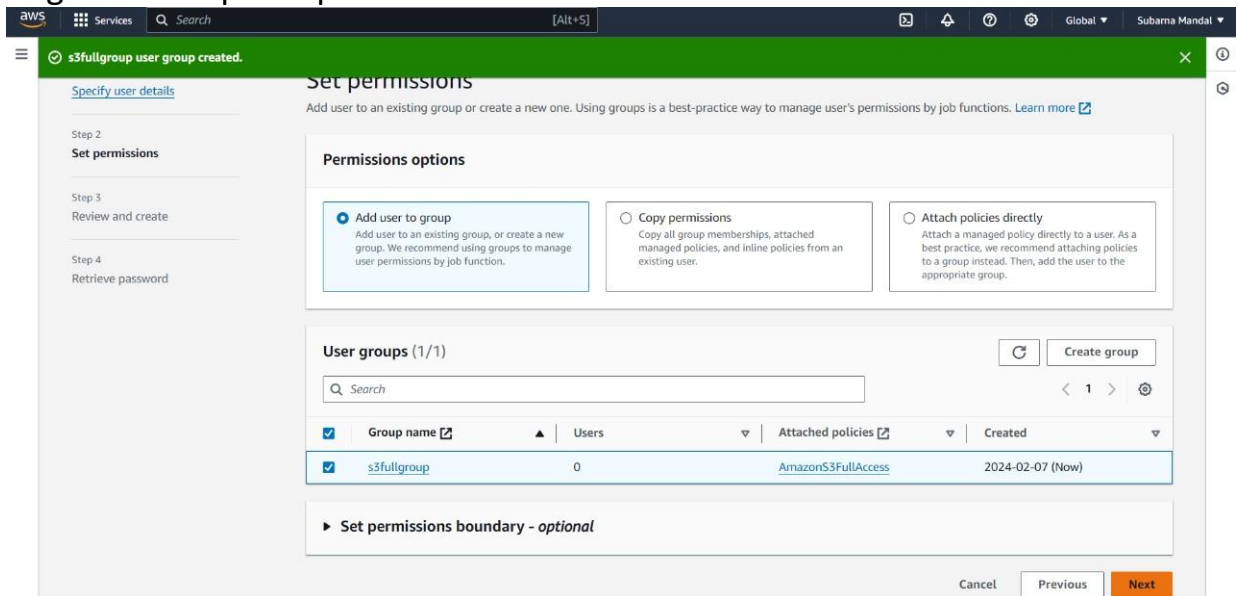
All types

9 matches

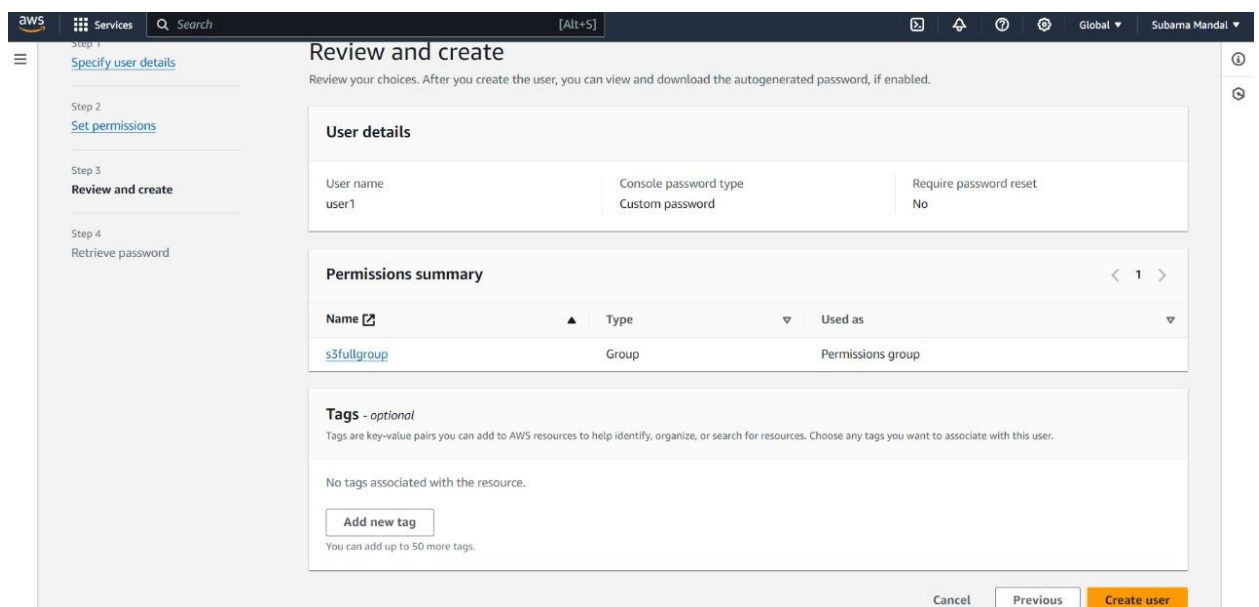
	Policy name	Type	Use...	Description
<input type="checkbox"/>	AmazonDMSRedsh...	AWS managed	None	Provides access to manage S3 setti
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS managed	None	Provides full access to all buckets v
<input type="checkbox"/>	AmazonS3ObjectL...	AWS managed	None	Provides AWS Lambda functions pe
<input type="checkbox"/>	AmazonS3Outpost...	AWS managed	None	Provides full access to Amazon S3
<input type="checkbox"/>	AmazonS3Outpost...	AWS managed	None	Provides read only access to Amaz
<input type="checkbox"/>	AmazonS3ReadOn...	AWS managed	None	Provides read only access to all buc
<input type="checkbox"/>	AWSBackupService...	AWS managed	None	Policy containing permissions nece

Cancel Create user group

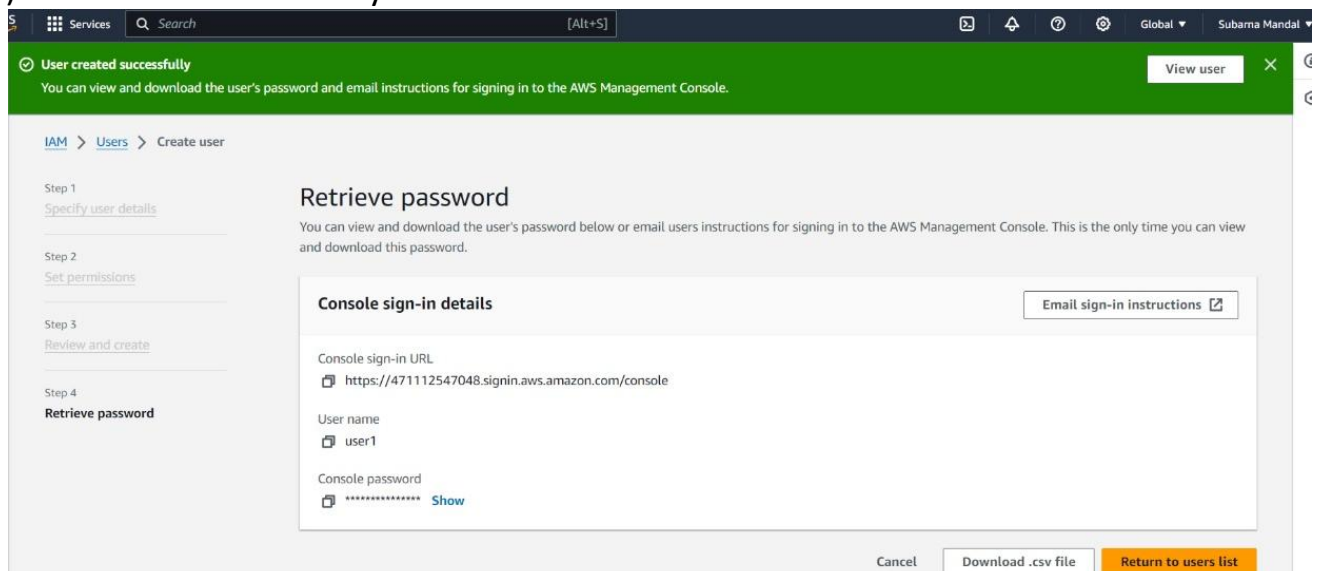
7) 's3fullgroup' is created now tick the checkbox of required group so that the user can gets the required permissions. Then click 'next'.



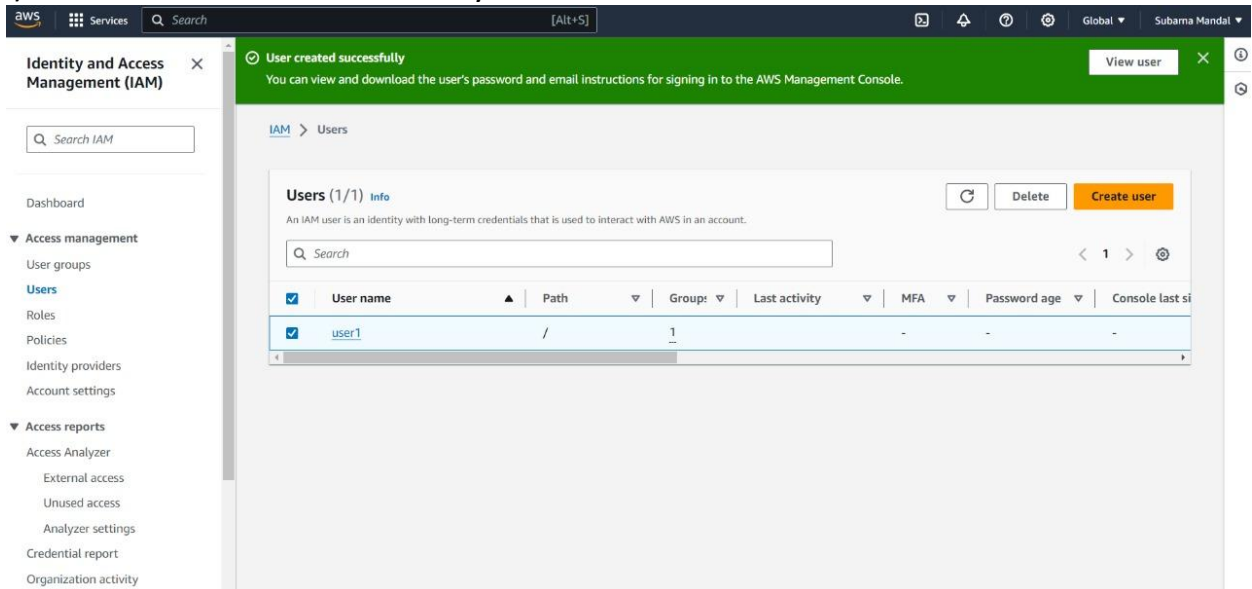
8) Under 'review and create' click on 'Create user' to create the user.



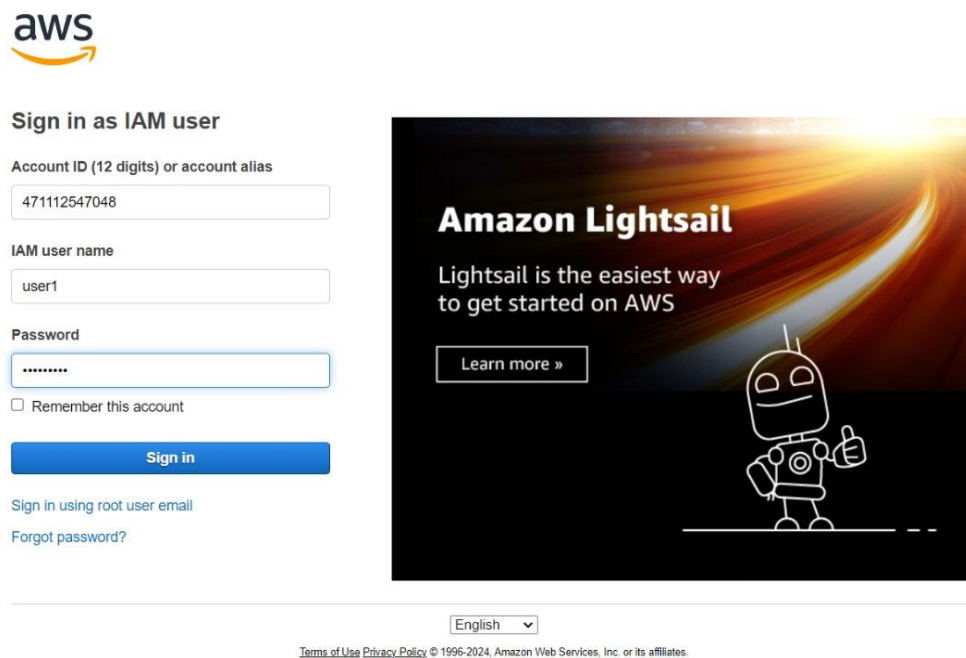
9) IAM user is Successfully created now click on 'Return on user list'.



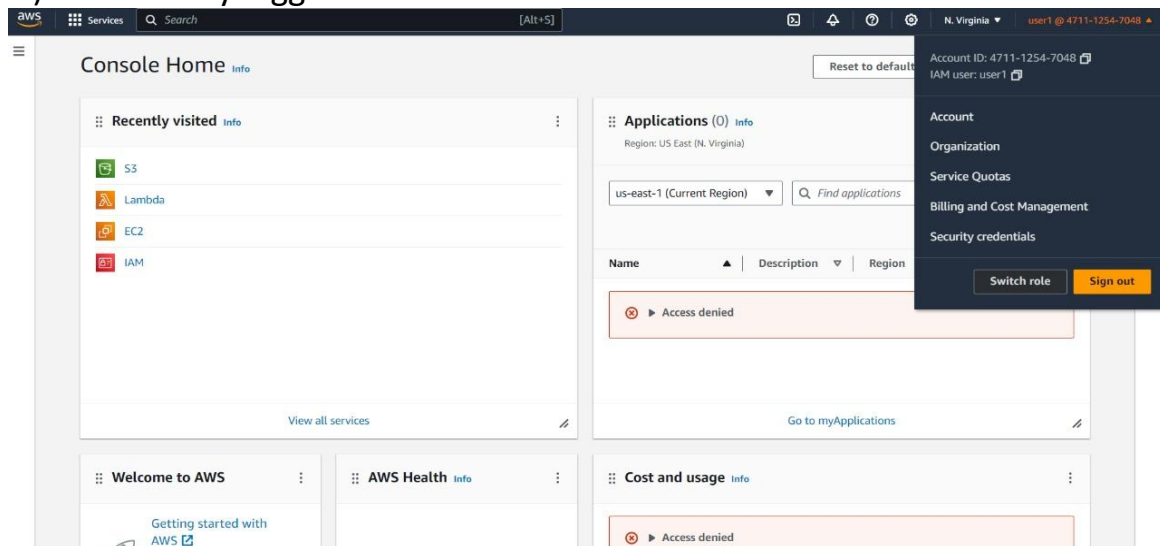
10) 'user1' is created successfully and it is shown in 'Users'.



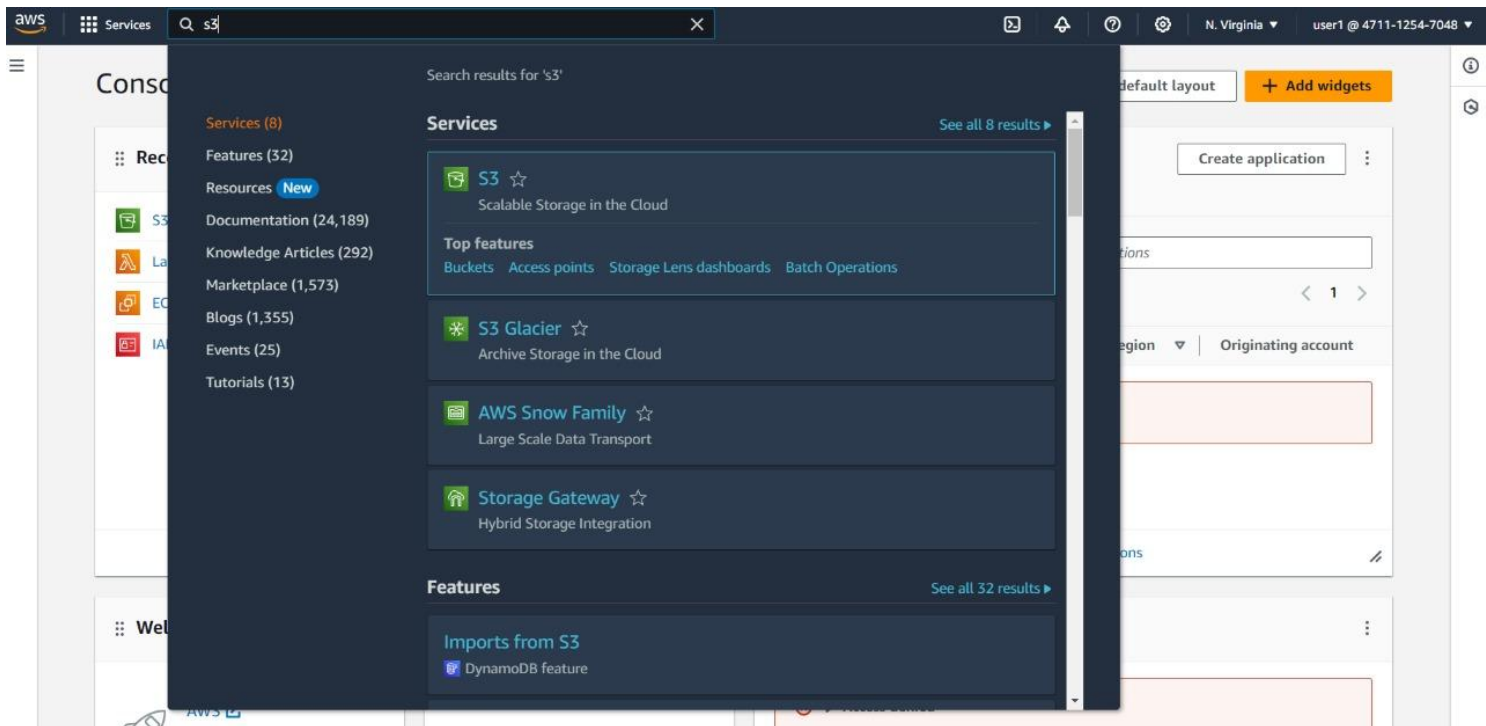
11) Now open another browser or open 'Incognito mode' . login to AWS console as IAM user with the provide Account ID , User name and password.



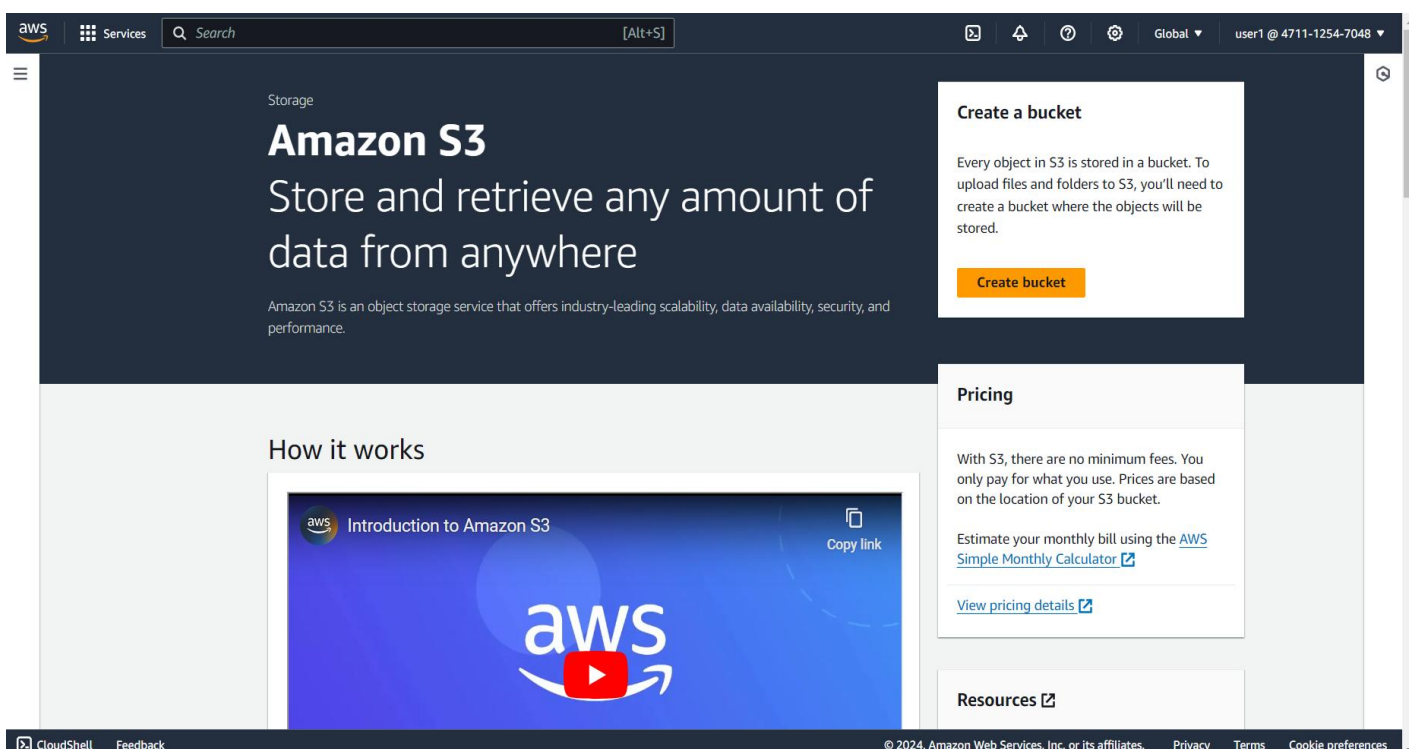
12) Successfully logged into 'user1' account.



13) Now search for 'S3' and click on it.



14) To check 'user1' got the 'S3' access or not click on 'Create Bucket'.



15) Set all as default, just give a 'unique' bucket name and click on 'create bucket'.

The screenshot shows the 'Create bucket' page in the AWS Management Console. The breadcrumb navigation is 'Amazon S3 > Buckets > Create bucket'. The page title is 'Create bucket' with an 'Info' link. Below the title is a note: 'Buckets are containers for data stored in S3. [Learn more](#)'. The 'General configuration' section includes a dropdown for 'AWS Region' set to 'Asia Pacific (Mumbai) ap-south-1', a text input for 'Bucket name' containing '1stbucket', and a 'Choose bucket' button. The 'Object Ownership' section has a note about controlling ownership. The 'Default encryption' section shows 'Encryption type' with three radio buttons: 'Server-side encryption with Amazon S3 managed keys (SSE-S3)' (selected), 'Server-side encryption with AWS Key Management Service keys (SSE-KMS)', and 'Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)'. Below this, 'Bucket Key' is set to 'Enable'. At the bottom, there is a 'Cancel' button and a 'Create bucket' button. A blue information box at the bottom states: 'After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.'

16) Bucket is created. Means 'user1' got the full access of 'S3'.

The screenshot shows the 'Buckets' page in the AWS Management Console. A green success banner at the top reads: 'Successfully created bucket "1stbucket123445"'. Below the banner, there is an 'Account snapshot' section. The 'General purpose buckets' tab is selected, showing a list of buckets. The table has columns: Name, AWS Region, Access, and Creation date. One bucket is listed: '1stbucket123445' in the 'Asia Pacific (Mumbai) ap-south-1' region, with 'Bucket and objects not public' access and a creation date of 'February 7, 2024, 11:44:39 (UTC+05:30)'. Above the table, there are buttons for 'Copy ARN', 'Empty', 'Delete', and 'Create bucket'.

Name	AWS Region	Access	Creation date
1stbucket123445	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	February 7, 2024, 11:44:39 (UTC+05:30)