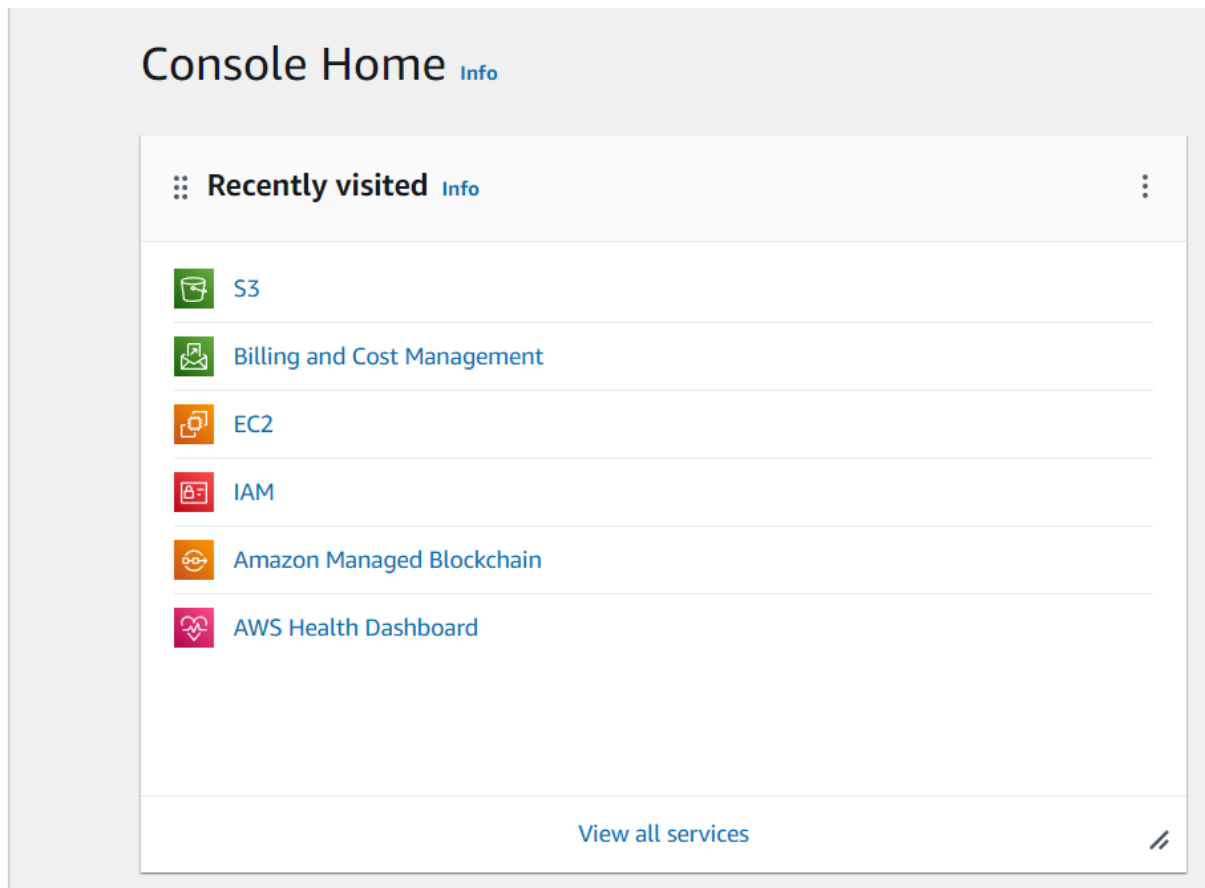


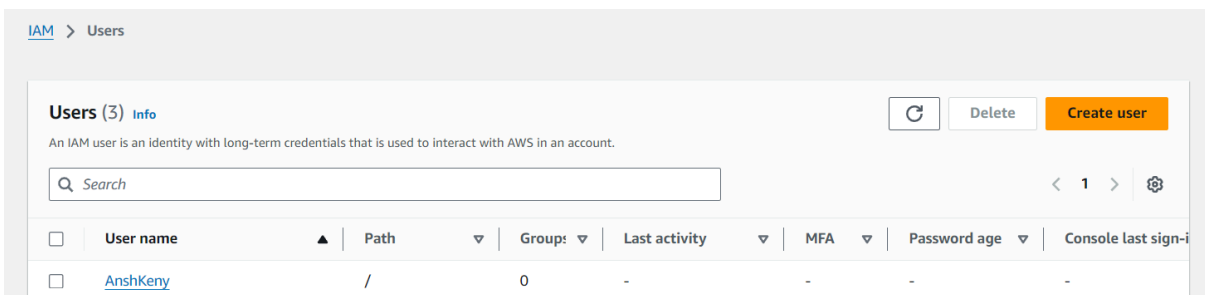
Practical No: - 07

Implementation of Identity Management

Login to your AWS Account, click on IAM



Click on create users



Enter the username of your own and select “I want to create an IAM user”

Specify user details


User details

User name

vinayakgupta

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.

In Console password, select “Custom Password” and Enter the password(bvimit@123)

Console password

☐ Autogenerated password
You can view the password after you create the user.


☒ Custom password
Enter a custom password for the user.

bvimit@123

- 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

In Permission options, select “Attach policies directly” and search for “Administrator Access”

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 (1/1233)

Choose one or more policies to attach to your new user.



Create policy

Filter by Type			
<input type="text" value="Search"/>	All types	< 1 2 3 4 5 6 7 ... 62 > ⚙	
Policy name	Type	Attached entities	
<input type="checkbox"/> AccessAnalyzerServiceRolePolicy	AWS managed	0	
<input checked="" type="checkbox"/> AdministratorAccess	AWS managed - job function	0	
<input type="checkbox"/> AdministratorAccess	AWS managed	0	

On clicking next, it will the review and permission summary

Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name
vinayakgupta

Console password type
Custom password

Require password reset
Yes

Permissions summary

< 1 >

Name	Type	Used as
AdministratorAccess	AWS managed - job function	Permissions policy
IAMUserChangePassword	AWS managed	Permissions policy

In Tags option, add a new tag, in key give “name” and in value give “Test account user” and click on “Create user”

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.

Key

Value - optional

Remove

Add new tag

You can add up to 49 more tags.

Cancel

Previous

Create user

The IAM user will be created. Now copy the link provided and try logging using the username and password by you

User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

View user

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://564885774690.signin.aws.amazon.com/console

User name
vinayakgupta

Console password
***** Show

Cancel

Download .csv file

Return to users list

Enter the credentials and click on Sign in

Sign in as IAM user

Account ID (12 digits) or account alias

564885774690

IAM user name

vinayakgupta

Password

☐ Remember this account

Sign in

[Sign in using root user email](#)

[Forgot password?](#)

Here in old password, provide “bvimit@123” and in new password and retype new password, provide “vinayak@123”

AWS account 772467074778

IAM user name vinayakgupta

Old password

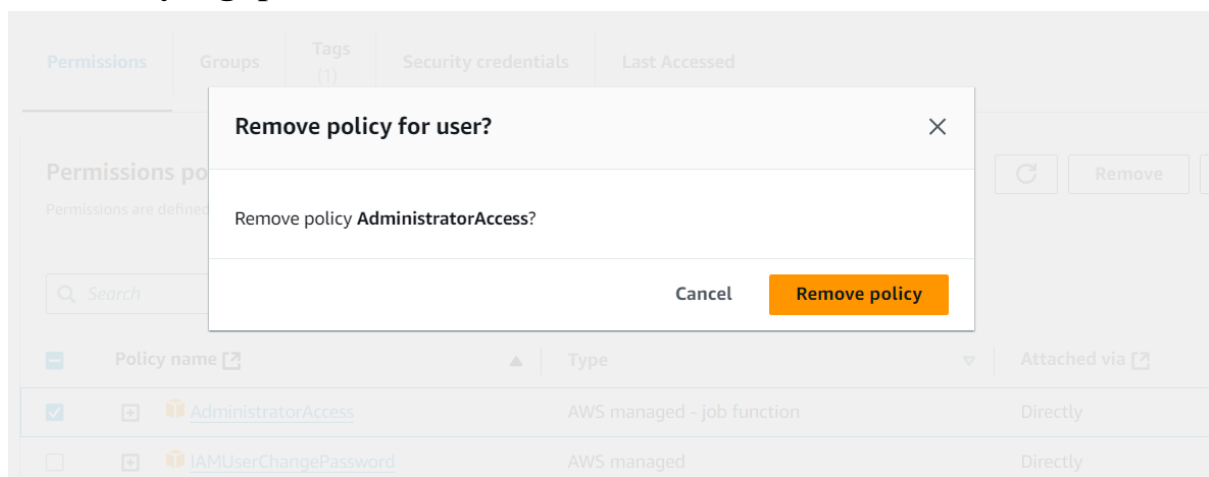
New password

Retype new password

[Confirm password change](#)

[Sign in using root user email](#)


We successfully login with the username and password which we have set before. vinayakgupta is able to add, delete or modify the user as it is having the AdministratorAccess. Now we are removing the AdministratorAccess from vinayakgupta.



Now when the vinayakgupta user tries to add the permissions, the access is denied as the Administrator Access policy was removed from vinayakgupta.



Access denied

You don't have permission to *iam:ListGroup*s. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#) 

User: arn:aws:iam::564885774690:user/vinayakgupta
Action: iam:ListGroup
On resource(s): arn:aws:iam::564885774690:group/
Context: no identity-based policy allows the action

 Copy