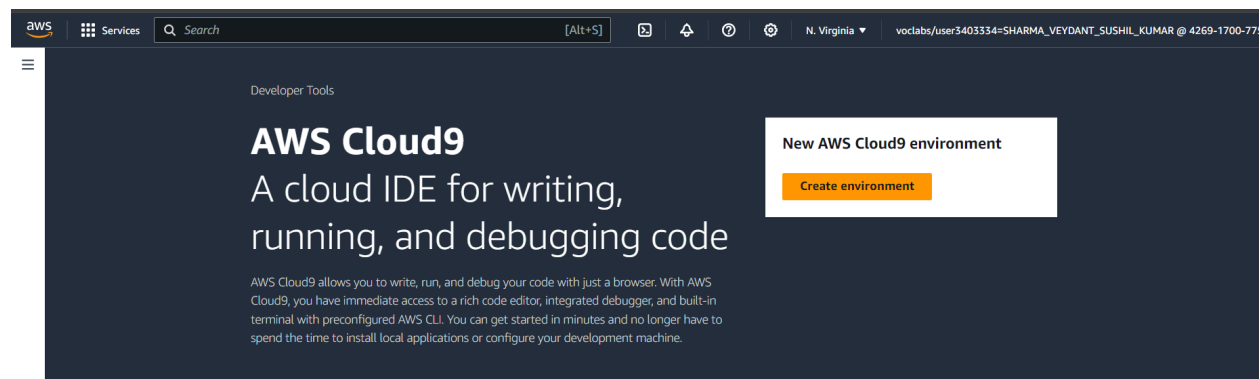
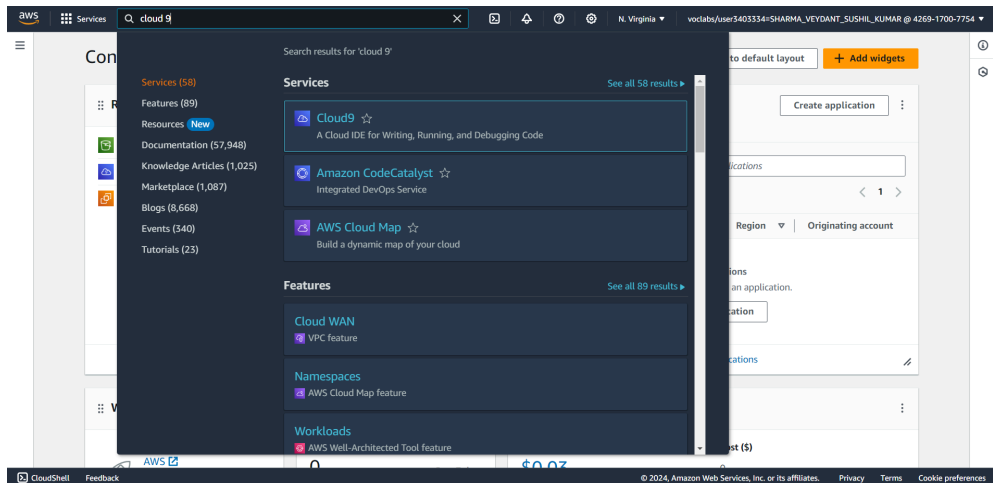


## Aim: To understand the benefits of Cloud Infrastructure and Setup AWS Cloud9 IDE, Launch AWS Cloud9 IDE and Perform Collaboration Demonstration.

### Step 1: Navigate to Cloud 9 service



### Step 2: Create Environment

A screenshot of the AWS Cloud9 'Create environment' form. The breadcrumb navigation at the top shows 'AWS Cloud9 > Environments > Create environment'. The main heading is 'Create environment' with an 'Info' link. The form is divided into sections: 'Details', 'Name', 'Description - optional', and 'Environment type'. The 'Name' field contains 'vey-env' with a note 'Limit of 60 characters, alphanumeric, and unique per user.' The 'Description - optional' field is empty with a note 'Limit 200 characters.' The 'Environment type' section has two radio buttons: 'New EC2 instance' (selected) and 'Existing compute'. The 'New EC2 instance' option has a note 'Cloud9 creates an EC2 instance in your account. The configuration of your EC2 instance cannot be changed by Cloud9 after creation.' The 'Existing compute' option has a note 'You have an existing instance or server that you'd like to use.'

## Network settings [Info](#)

**Connection**  
How your environment is accessed.

☐ **AWS Systems Manager (SSM)**  
Accesses environment via SSM without opening inbound ports (no ingress).

☒ **Secure Shell (SSH)**  
Accesses environment directly via SSH, opens inbound ports.

► [VPC settings](#) [Info](#)

Click on “Create”

Step 3: Environment Will be created.

The screenshot shows the AWS Cloud9 console. A green notification banner at the top states: "Successfully created vey-env. To get the most out of your environment, see [Best practices for using AWS Cloud9](#)". Below this, a blue banner says: "For capabilities similar to AWS Cloud9, explore AWS Toolkits in your own IDE and AWS CloudShell in the AWS Management Console. [Learn more](#)".

The main content area is titled "AWS Cloud9 > Environments". It shows a table with one environment:

Name	Cloud9 IDE	Environment type	Connection	Permission	Owner ARN
vey-env	<a href="#">Open</a>	EC2 instance	Secure Shell (SSH)	Owner	arn:aws:sts::426917007754:assumed-role/voclabs/user3403334=SHARMA_VEYDANT_SUSHIL_KUMAR

Buttons at the top of the table include "Delete", "View details", "Open in Cloud9", and "Create environment".

Step 4: Navigate to IAM service in AWS.

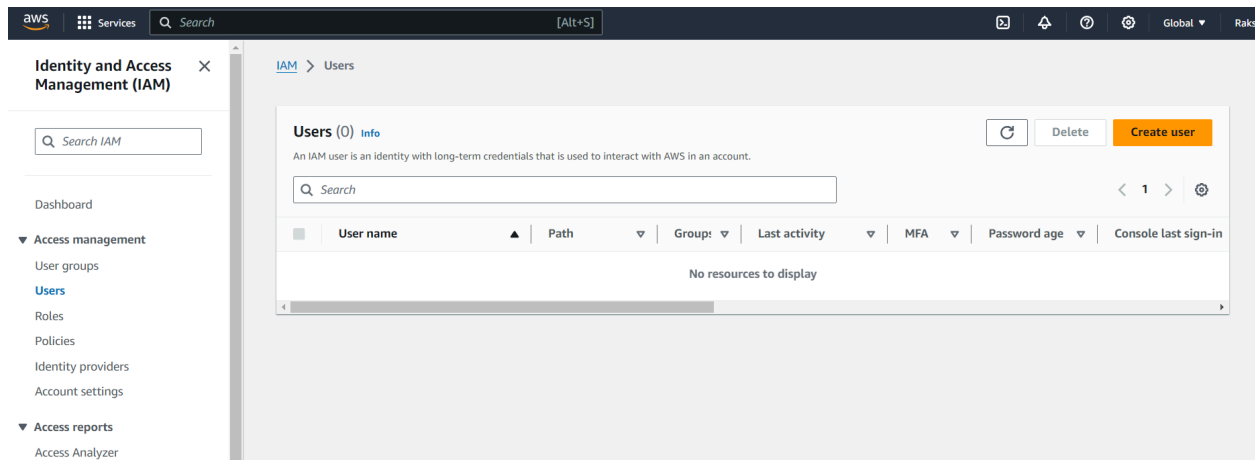
The screenshot shows the AWS IAM service page. The search bar at the top contains "IAM". The left sidebar lists various categories: Services (11), Features (24), Resources (New), Documentation (59,384), Knowledge Articles (471), Marketplace (857), Blogs (1,838), Events (12), and Tutorials (1).

The main content area is titled "Search results for 'IAM'". It lists several services:

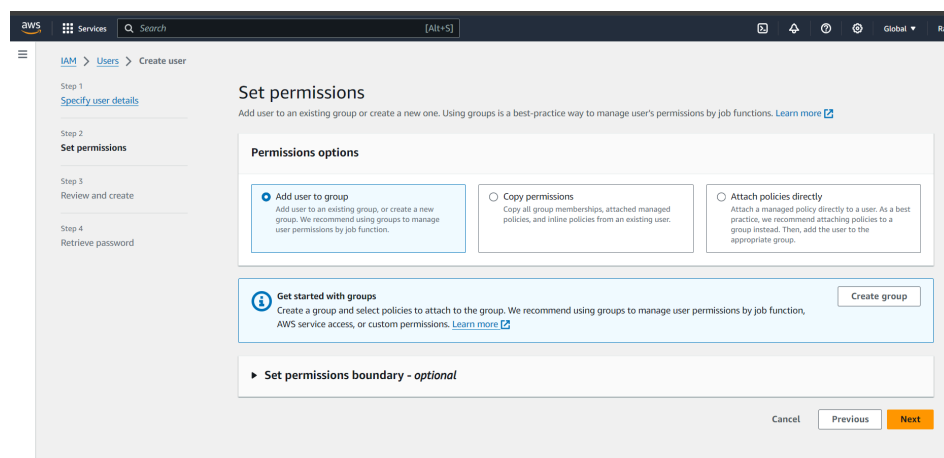
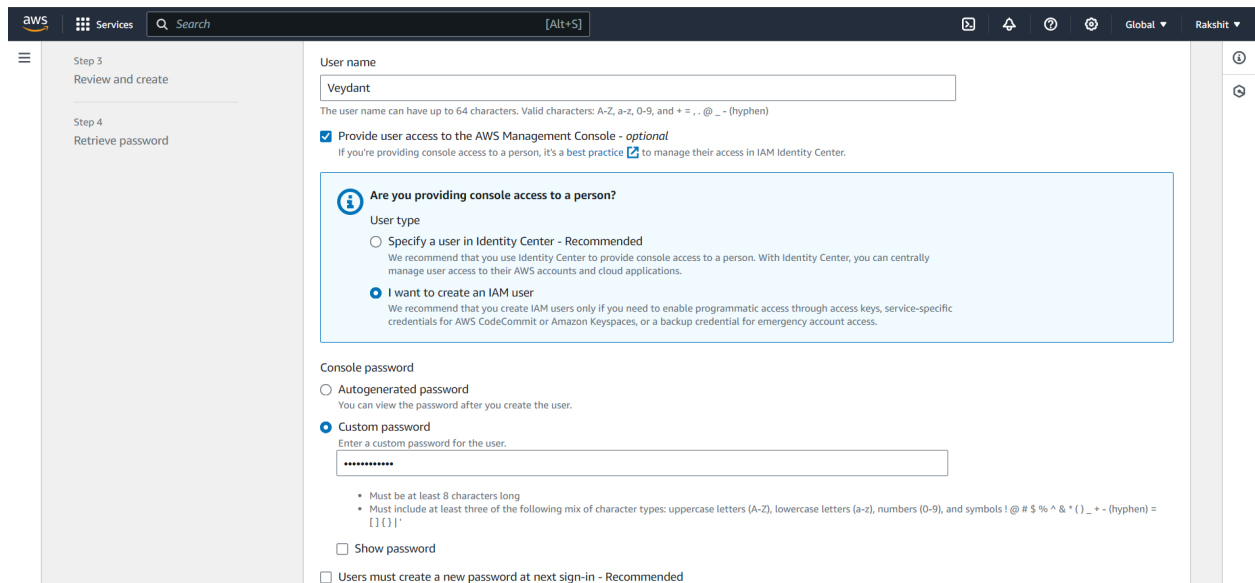
- IAM**: Manage access to AWS resources. Top features: Groups, Users, Roles, Policies, Access Analyzer.
- IAM Identity Center**: Manage workforce user access to multiple AWS accounts and cloud applications.
- Resource Access Manager**: Share AWS resources with other accounts or AWS Organizations.
- AWS App Mesh**: Easily monitor and control microservices.

Below the services list, there is a section for "Features" with a link to "See all 24 results". The first feature listed is "Groups" under the "IAM feature" category.



## Step 5: Navigate to users tab and Create new User.



Add name, custom password. Keep the “Users create new password at next sign in” button checked



Select default settings for the rest.

  **User created successfully** View user ×

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

[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://975050293750.signin.aws.amazon.com/console>

User name  
 Veydant




Console password  
 \*\*\*\*\* [Show](#)

Cancel

Download .csv file

Return to users list

Step 6: Navigate to User groups tab.


   Search [Alt+S]

**Identity and Access Management (IAM)** ×

[Dashboard](#)  
**Access management**  
[User groups](#)  
[Users](#)  
[Roles](#)  
[Policies](#)  
[Identity providers](#)  
[Account settings](#)  
**Access reports**  
[Access Analyzer](#)  
[External access](#)  
[Unused access](#)  
[Analyzer settings](#)  
[Credential report](#)  
[Organization activity](#)

[IAM](#) > User groups

**User groups (0)** [Info](#)

 [Delete](#) [Create group](#)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.


Group name




Users

Permissions

Creation time

No resources to display

 CloudShell [Feedback](#) © 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

   Search [Alt+S]


**Identity and Access Management (IAM)** ×

[Dashboard](#)  
**Access management**  
[User groups](#)  
[Users](#)  
[Roles](#)  
[Policies](#)  
[Identity providers](#)  
[Account settings](#)  
**Access reports**  
[Access Analyzer](#)  
[External access](#)  
[Unused access](#)  
[Analyzer settings](#)  
[Credential report](#)  
[Organization activity](#)

User group name  
Enter a meaningful name to identify this group.  
  
Maximum 128 characters. Use alphanumeric and "+,=,@,\_" characters.

**Add users to the group - Optional (1)** [Info](#)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

☐ User name 

Groups

Last activity

Creation time

☐ Veydant 0 None 1 minute ago

**Attach permissions policies - Optional (945)** [Info](#)

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter by Type 


All types


☐ Policy name


Type


Used as

Description

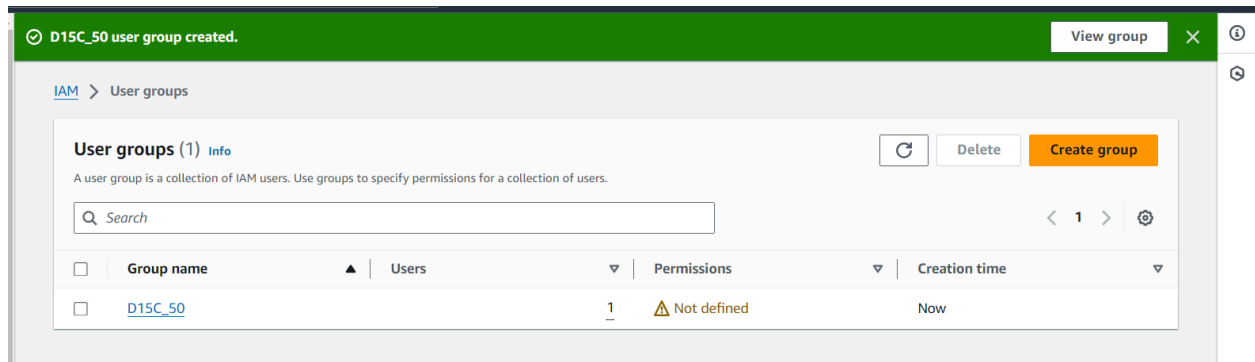
☐  [AdministratorAccess](#) AWS managed - job function None Provides full access to AWS services an...

☐  [AdministratorAccess-...](#) AWS managed None Grants account administrative permissi...

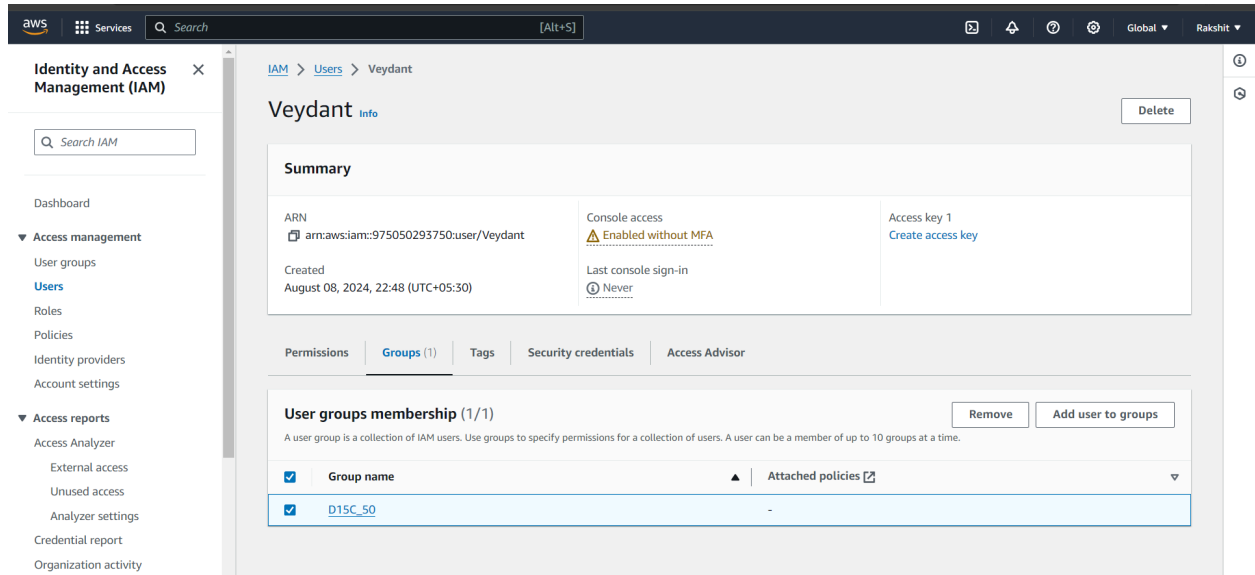
☐  [AdministratorAccess](#) AWS managed None Grants account administrative permissi...

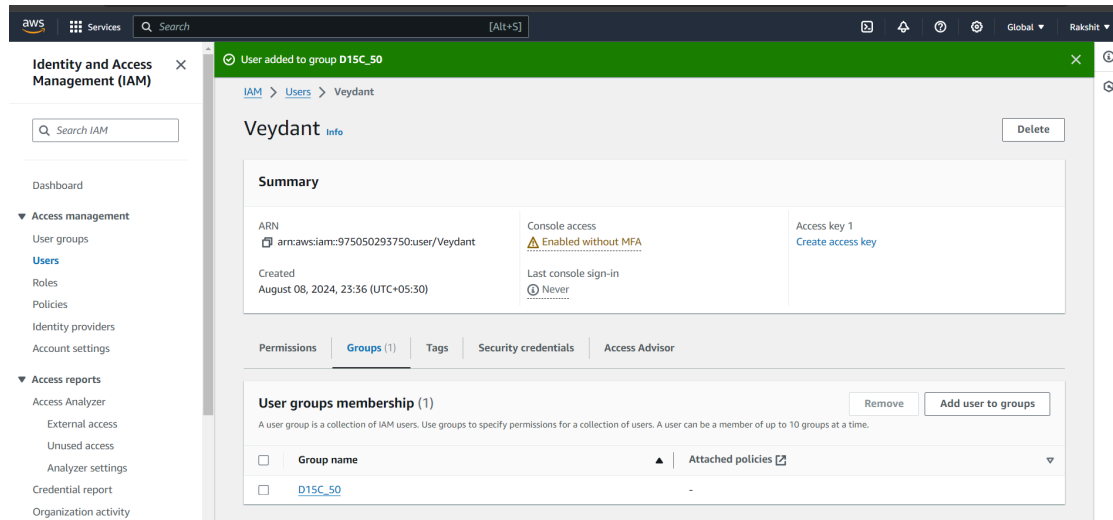
 CloudShell [Feedback](#) © 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Create a new user group.



Step 7: Navigate to Users tab , go to Groups tab and add User to the group.





The user has been added to the the user group.

Step 8 : Navigate to the permissions tab in User group, select “AWSCloud9EnvironmentMember” and add the permissions.

