

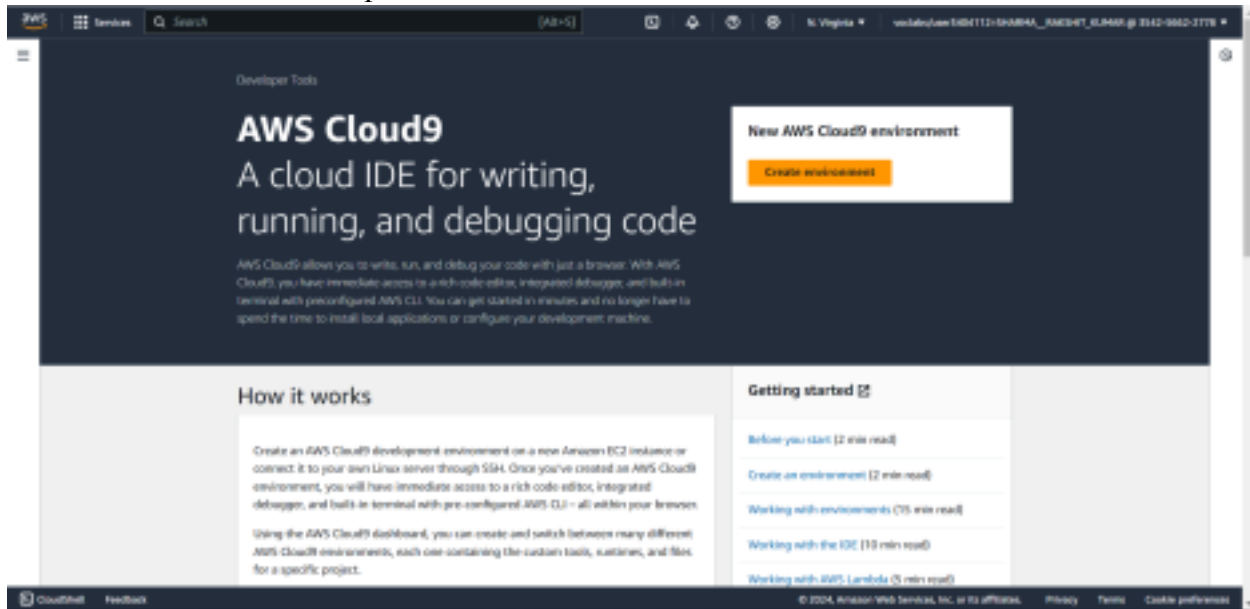
**Name: Ishan Hemwani**

**Div: D15C**

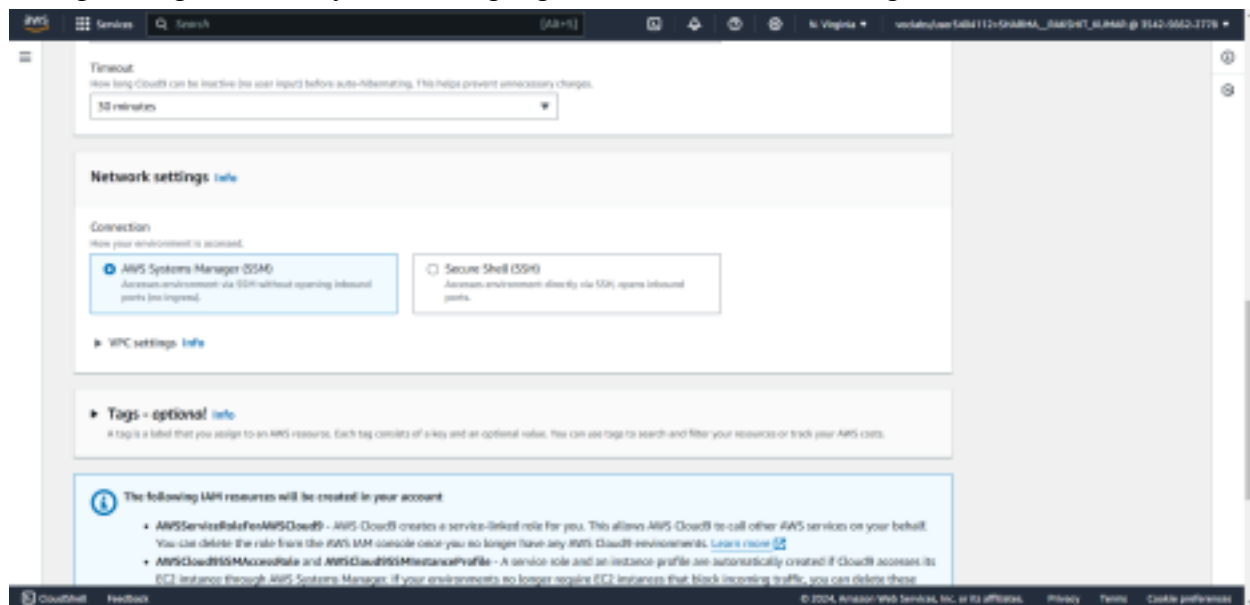
**Roll No: 16**

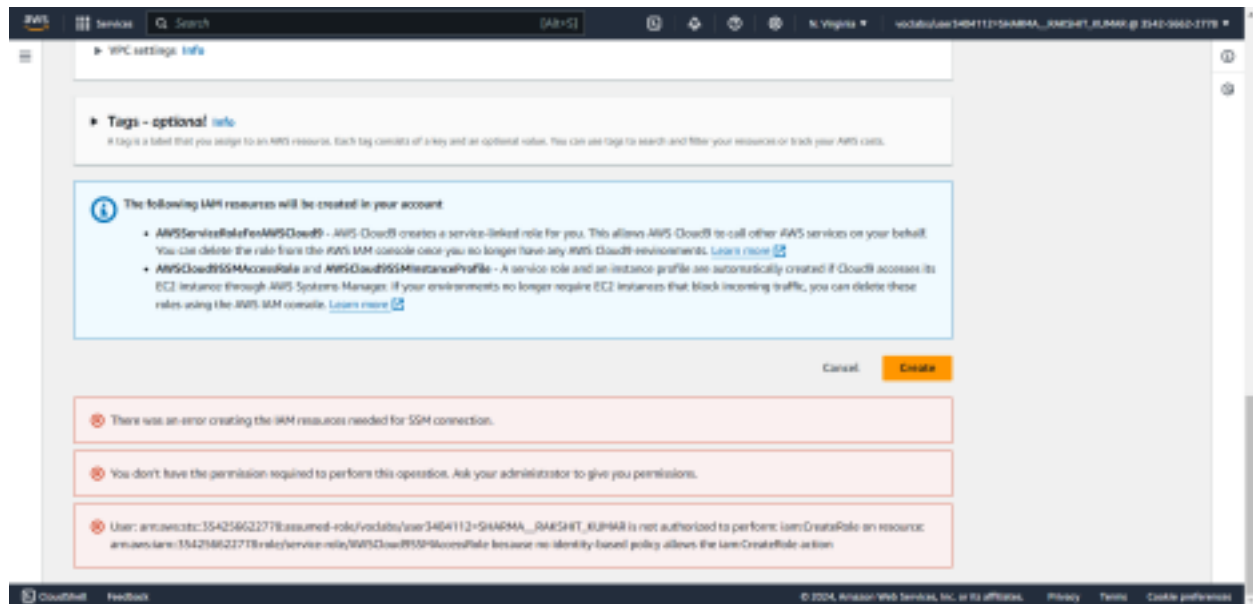
## Experiment 1B: IAM and cloud9

1. Open the AWS account and search for Cloud9.

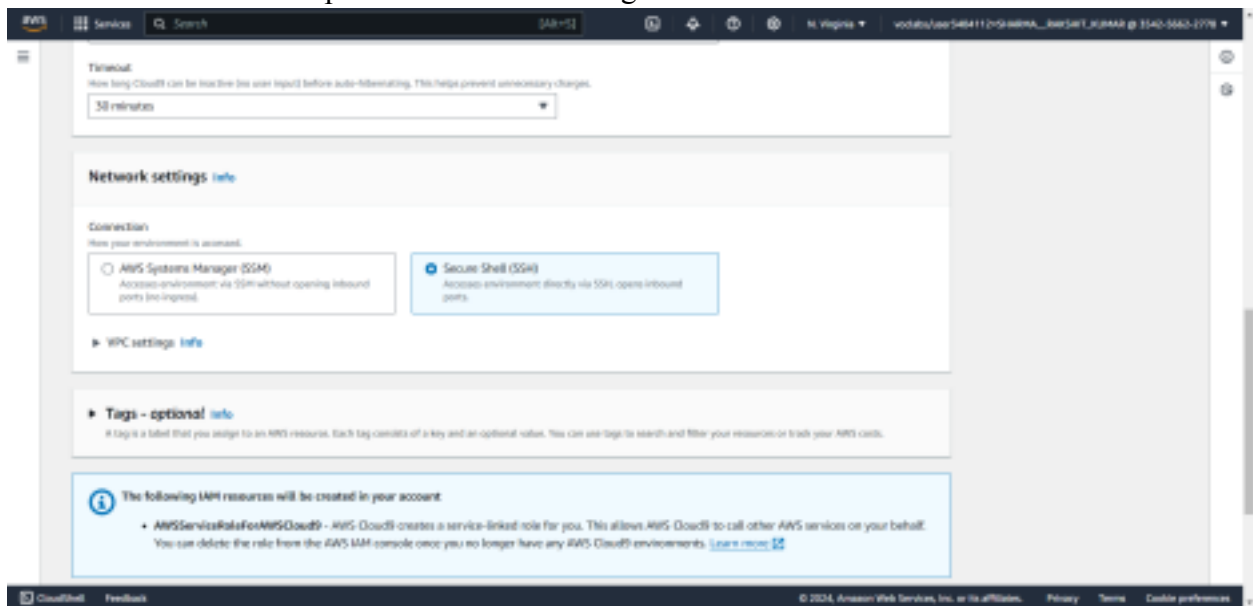


2. Enter the name and other required configuration for creating an environment. In network settings, using the AWS system manager gives an error while creating the environment

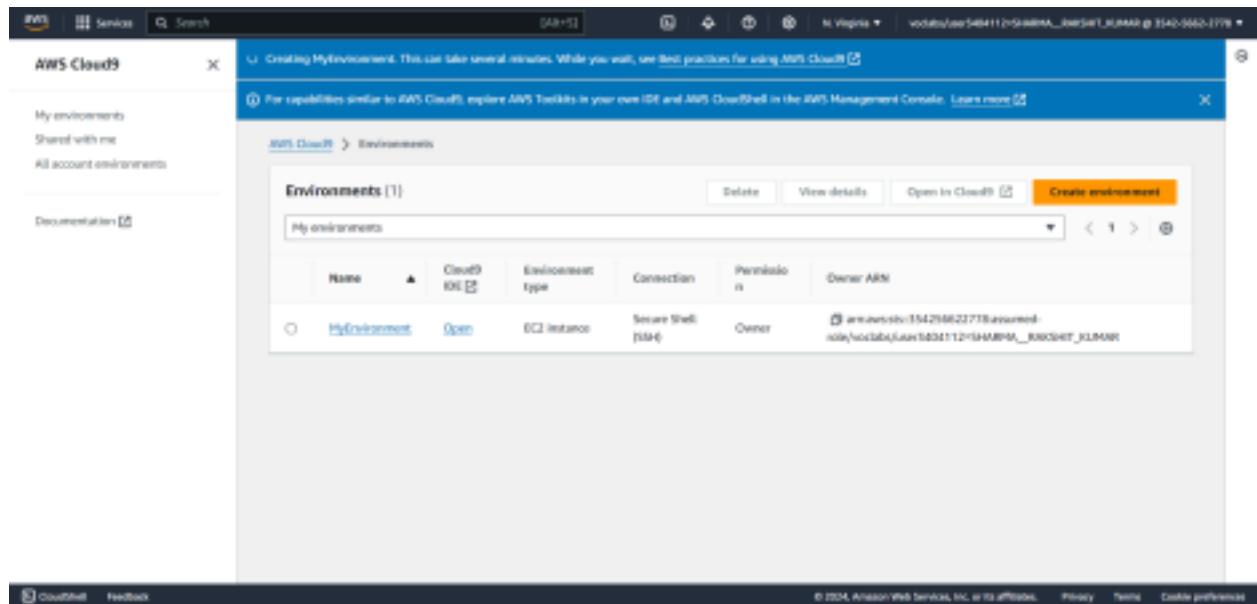




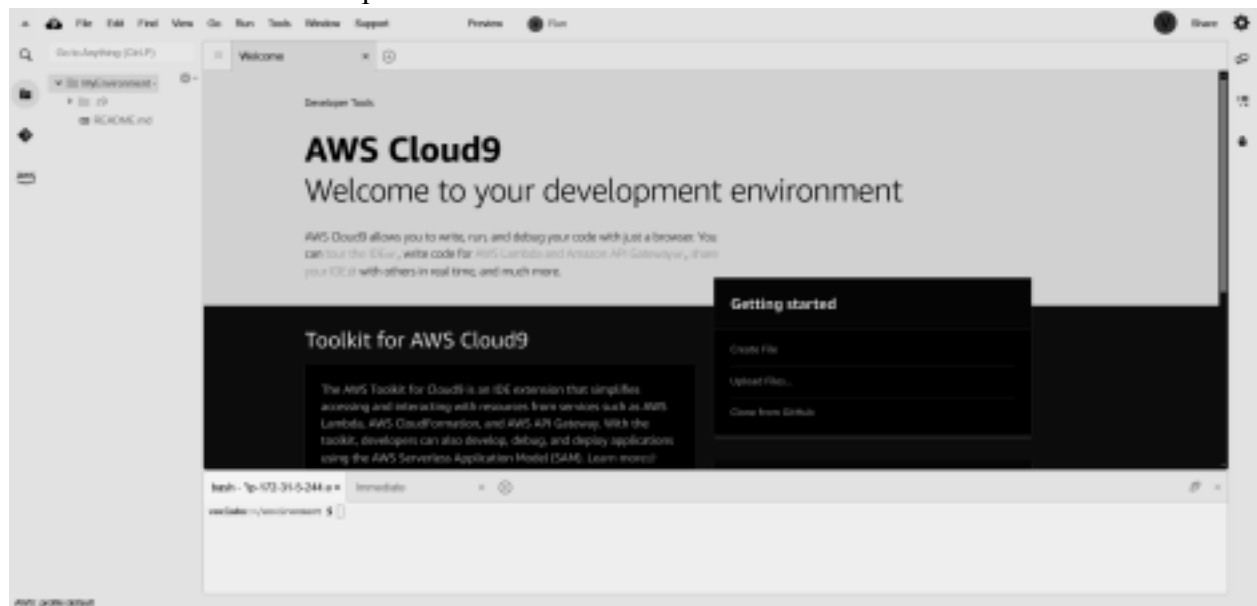
3. Use the Secure Shell option in Network settings.



4. Once the configuration is complete, click on create environment to create a Cloud9 environment.

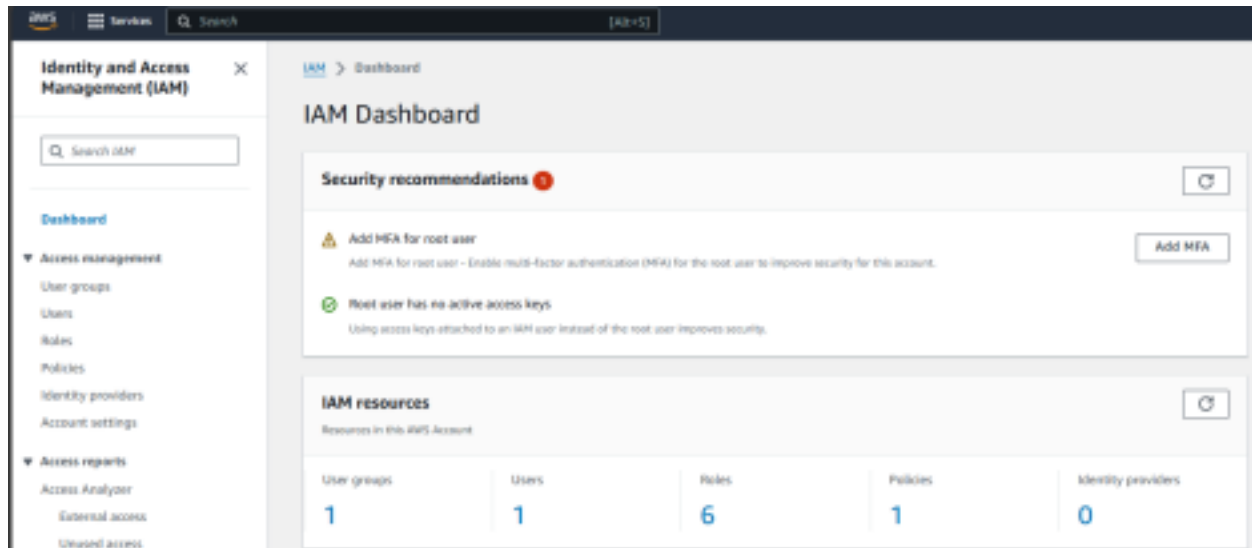


5. Cloud9 Environment is opened when u click on the environment name



IAM user creation steps

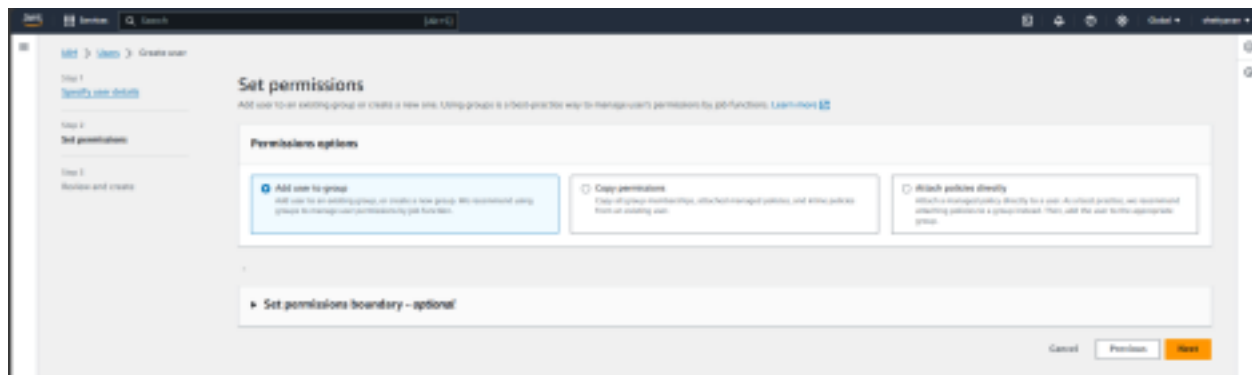
1. Open the aws account and search for IAM in service.



2. Select the users option from the left panel and click on create user button. Give the user name,



3. Click the add user option if you don't have an existing user group



4. Give a name to your user group and check the policies if required any

IAM > User groups > Create user group

## Create user group

**Name the group**

User group name

Enter a meaningful name to identify this group.

Maximum 128 characters. Use alphanumeric and '-', '@', '\_' characters.

**Add users to the group - Optional (1/1)** [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.

< 1 > ⓘ

<input type="checkbox"/>	User name ⓘ	Groups	Last activity
<input checked="" type="checkbox"/>	sample	0	None

**Attach permissions policies - Optional (9/45)** [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

< 1 2 3 4 5 6 7 ... 48 > ⓘ

<input type="checkbox"/>	Policy name	Type	Used as	Description
<input type="checkbox"/>	AdministratorAccess	AWS managed - job function	None	Provides full access to all AWS services and resources.
<input type="checkbox"/>	AdministratorAccess-Ampify	AWS managed	None	Grants account access to the Amazon Music service.
<input type="checkbox"/>	AdministratorAccess-AWSIoTDeviceSetup	AWS managed	None	Grants account access to the Amazon IoT service.
<input type="checkbox"/>	AmazonForBusinessDeviceSetup	AWS managed	None	Provide device access to the Amazon For Business service.

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

5. Once the user group is created select the name and click next to create your user

myweb-app-group user group created.

IAM > Users > Create user

Step 1: Specify user details

Step 2: Set permissions

Step 3: Review and create

Step 4: Replace password

## Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user permissions by job function. [Learn more](#)

**Permissions options**

☒ Add user to group  
Add user to an existing group or create a new one. We recommend using groups to manage user permissions by job function.

☐ Copy permissions  
Copy all group membership, attached managed policies, and inline policies from an existing user.

☐ Attach policies directly  
Attach a managed policy directly to a user. Its a more granular way to control access to a group instead. Then, add the user to the appropriate group.

**User groups (1)**

< 1 > ⓘ

<input type="checkbox"/>	Group name ⓘ	Users	Attached policies ⓘ	Created
<input type="checkbox"/>	myweb-app-group	0	-	2024-08-08 (New)

• Set permissions boundary - optional

Cancel Previous **Next**

6. Review the configuration details and check if you have missed any steps and then click on 'Create user' button

IAM > Users > Create user

Step 1  
Specify user details

Step 2  
Set permissions

Step 3  
Review and create

## 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

sample

Console password type

None

Require password reset

No

**Permissions summary**

Name	Type	Used as
No resources		

**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](#)

7. You will see the “user created successfully” message and incase you need then store your password by downloading the csv file

Search [Optional]

**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](#)

Users (1)

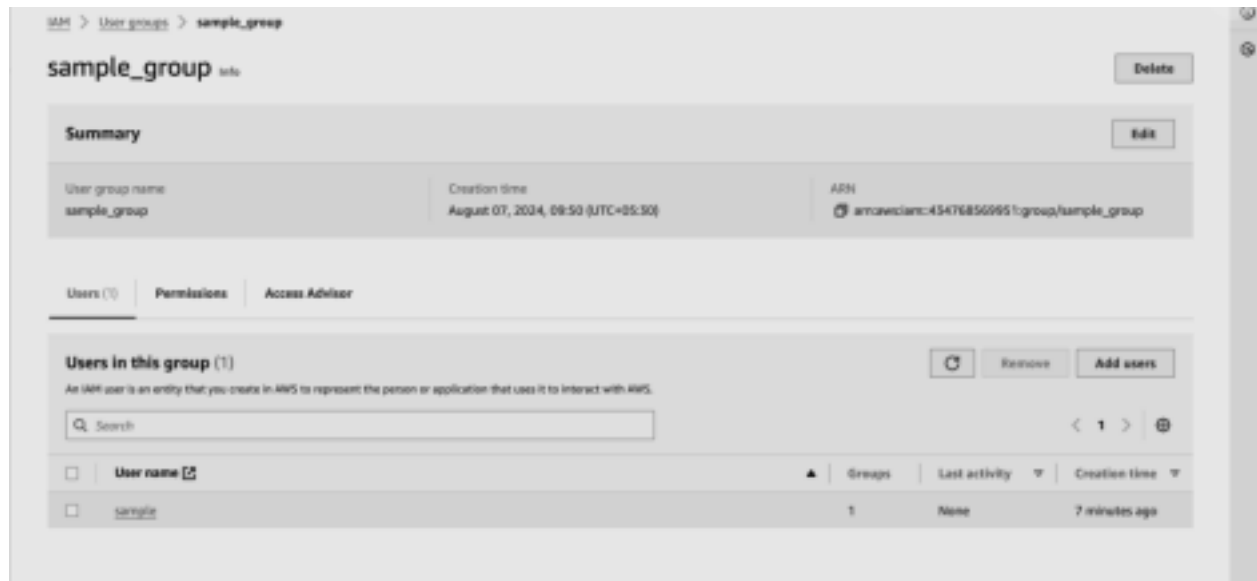
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Search

<input type="checkbox"/>	User name	Path	Group	Last activity	MFA	Password age	Console last sign-in	Access key ID	Action
<input type="checkbox"/>	sample	/	0	-	-	-	-	-	-

[Refresh](#) [Delete](#) [Create user](#)

8. After creation of the user, go to the user groups tab and select the group in which the user has been added. Navigate to the permissions tab. Click on add permissions and attach policy.



9. Search for the “AWSCloud9EnvironmentMember” policy and attach it.

