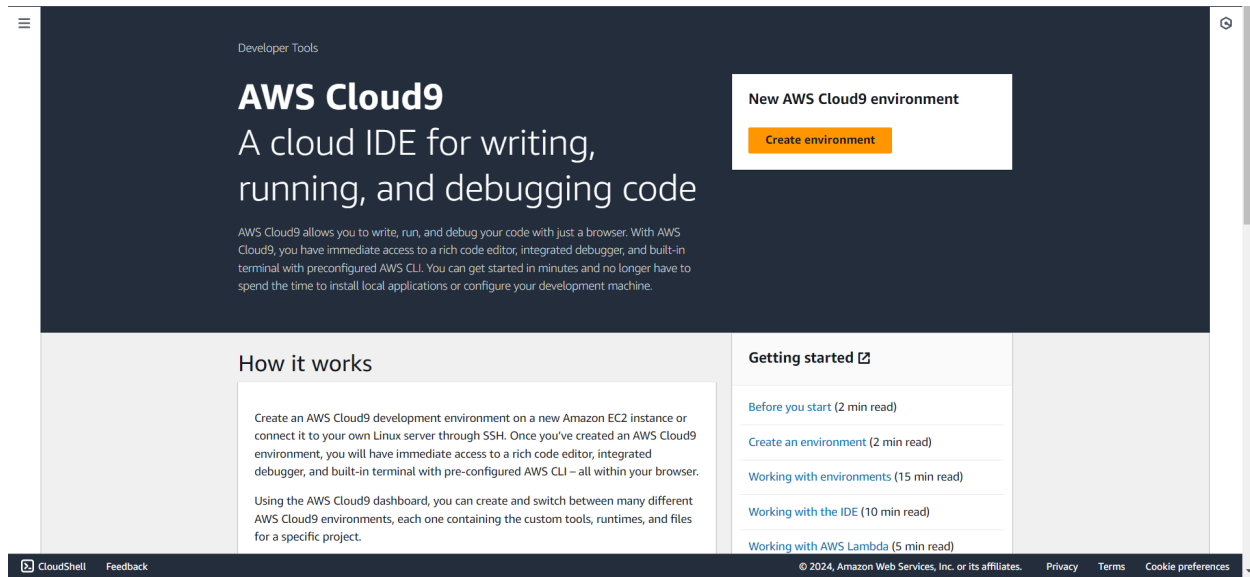
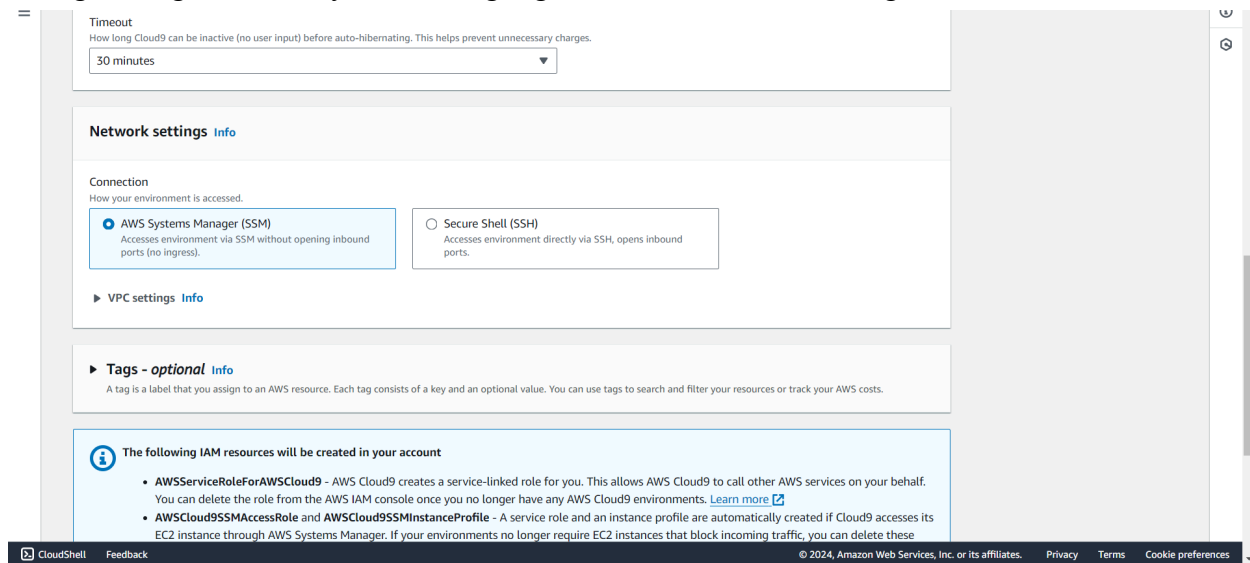


1. Open the AWS account and search for Cloud9. Click on create environment.



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



The screenshot shows the AWS Cloud9 console interface. At the top, there's a navigation bar with a hamburger menu, 'VPC settings Info', and user icons. Below this, there's a section for 'Tags - optional Info' with a description of tags. The main content area features a blue box titled 'The following IAM resources will be created in your account' containing two bullet points about AWS roles and instance profiles. Below this box are 'Cancel' and 'Create' buttons. Three red error messages are displayed: 'There was an error creating the IAM resources needed for SSM connection.', 'You don't have the permission required to perform this operation. Ask your administrator to give you permissions.', and a detailed message about the user 'arn:aws:sts::354256622778:assumed-role/voclabs/user3404112=SHARMA_RAKSHIT_KUMAR' not being authorized to perform 'iam:CreateRole' on the resource 'arn:aws:iam::354256622778:role/service-role/AWSCloud9SSMAccessRole'.

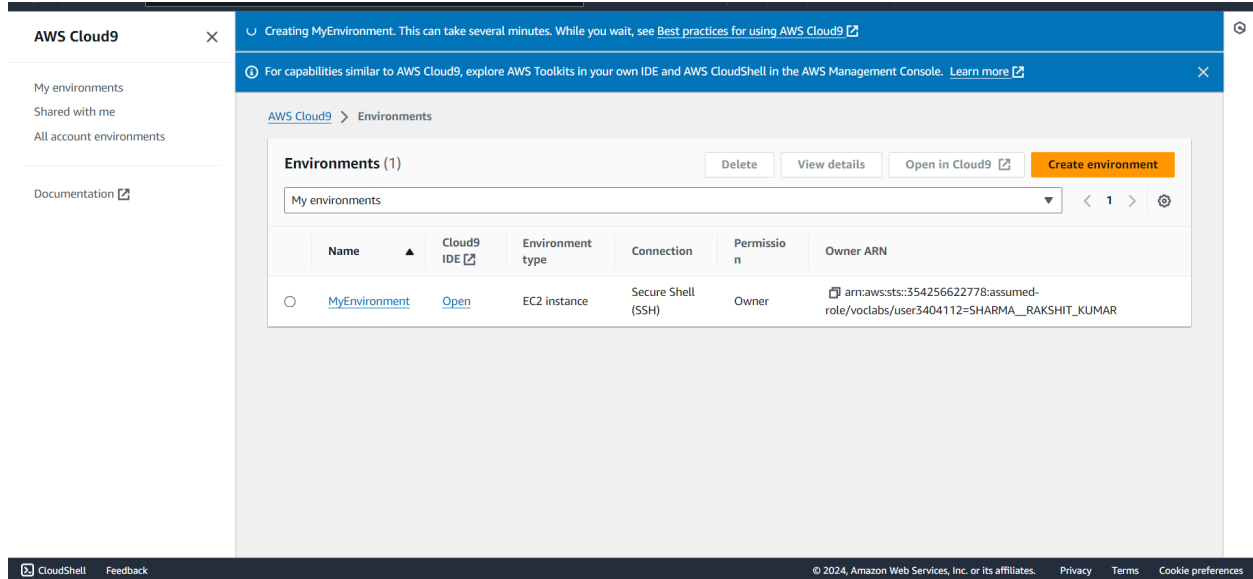
CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

3. Use the Secure Shell option in Network settings.

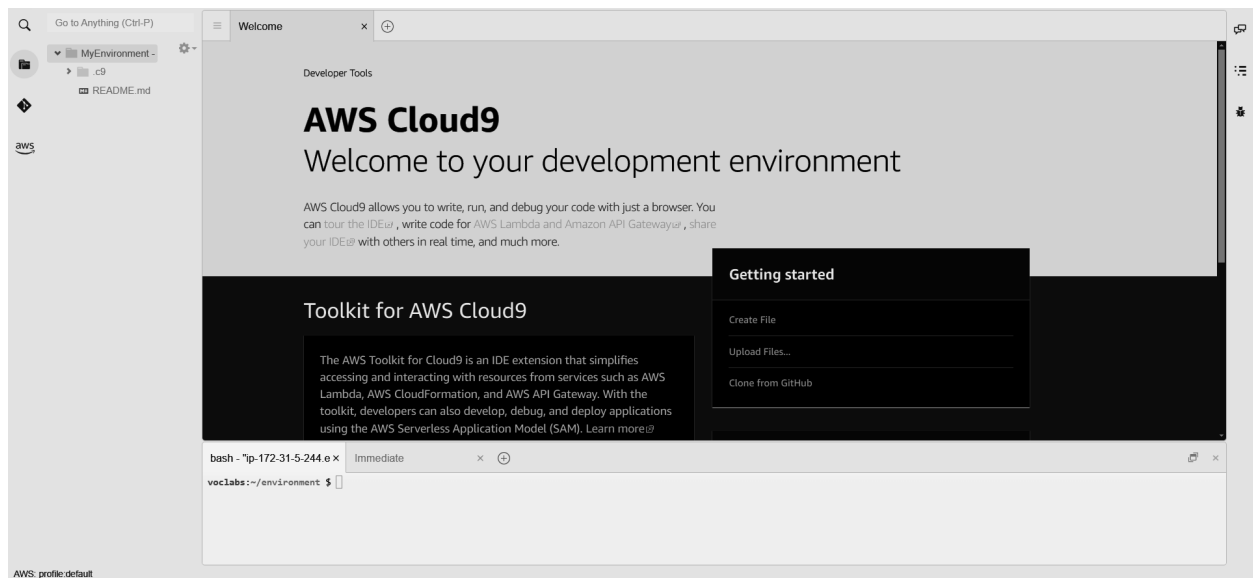
The screenshot shows the AWS Cloud9 console interface. At the top, there's a navigation bar with a hamburger menu, 'Timeout' (set to 30 minutes), and user icons. Below this, there's a section for 'Network settings Info'. Under the 'Connection' heading, the 'Secure Shell (SSH)' option is selected, with a description 'Accesses environment directly via SSH, opens inbound ports.' Below this, there's a section for 'Tags - optional Info' with a description of tags. The main content area features a blue box titled 'The following IAM resources will be created in your account' containing two bullet points about AWS roles and instance profiles. Below this box are 'Cancel' and 'Create' buttons. Three red error messages are displayed: 'There was an error creating the IAM resources needed for SSM connection.', 'You don't have the permission required to perform this operation. Ask your administrator to give you permissions.', and a detailed message about the user 'arn:aws:sts::354256622778:assumed-role/voclabs/user3404112=SHARMA_RAKSHIT_KUMAR' not being authorized to perform 'iam:CreateRole' on the resource 'arn:aws:iam::354256622778:role/service-role/AWSCloud9SSMAccessRole'.

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

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

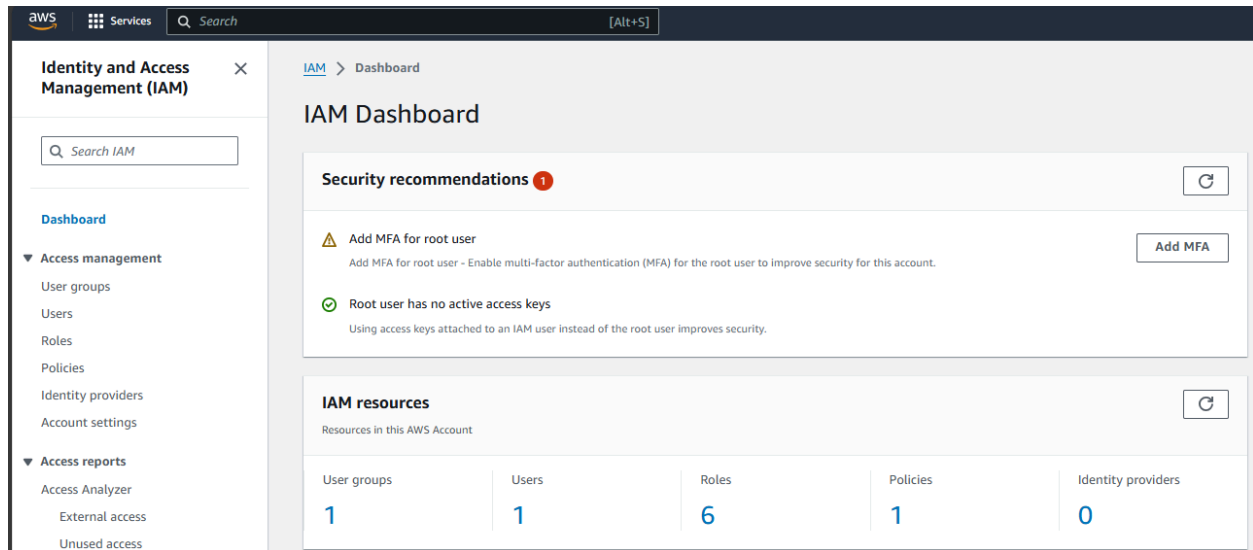


5. Cloud9 Environment is opened when u click on the environment name



IAM user creation steps

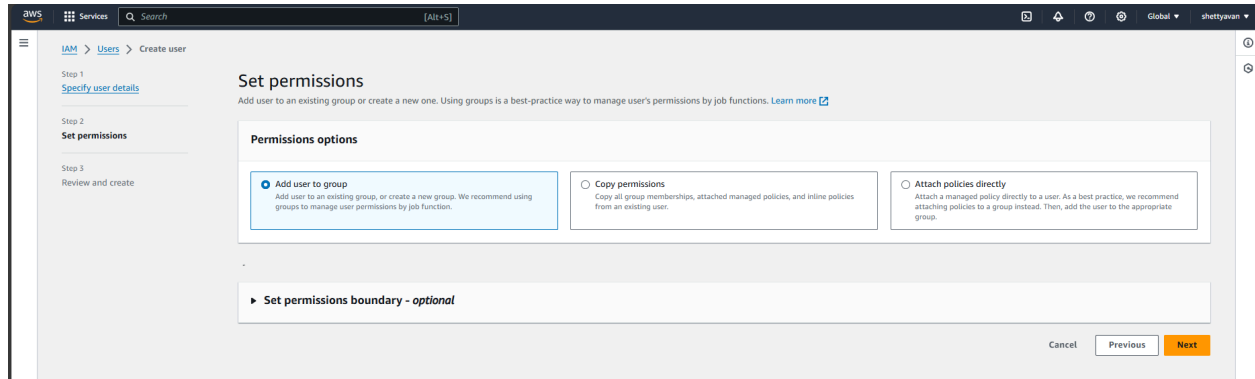
1. Open the aws account and search for IAM service.



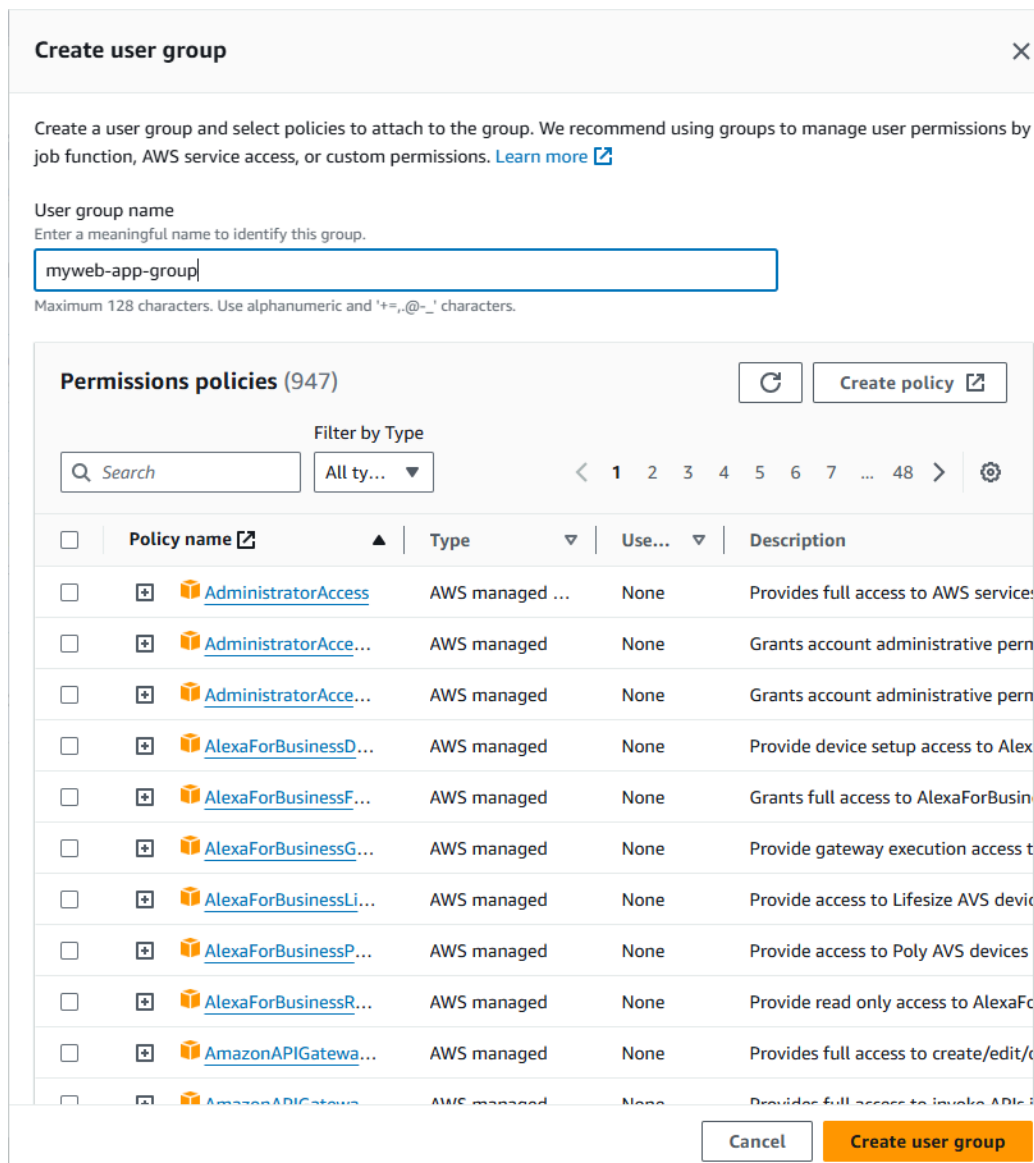
2. Select the users option from the left panel and click on create user button. Give the user name, select the “provide user access” checkbox. Also select the option “I want to create an IAM user”. Otherwise we will have to enable the Identity center and specify a user there. Add your custom password

The screenshot shows the 'Specify user details' form in the AWS IAM console. The form is titled 'User details'. It has a 'User name' field with the value 'avan-shetty'. Below it, there's a checkbox labeled 'Provide user access to the AWS Management Console - optional' which is checked. A note below the checkbox says 'If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.' Below this is a section titled 'Are you providing console access to a person?' with two options: 'Specify a user in Identity Center - Recommended' (unselected) and 'I want to create an IAM user' (selected). Below this is a 'Console password' section with two options: 'Autogenerated password' (unselected) and 'Custom password' (selected). Below the 'Custom password' option is a password field with a masked password '*****'. Below the password field are two bullet points: 'Must be at least 8 characters long' and '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) = [] { } | ' '. Below the password field is a checkbox labeled 'Show password' which is unchecked. At the bottom, there's a checkbox labeled 'Users must create a new password at next sign-in - Recommended' which is checked. A note below the checkbox says 'Users automatically get the IAMUserChangePassword policy to allow them to change their own password.'

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



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
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) Create group

Search

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

► **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

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 avan-shetty	Console password type Custom password	Require password reset Yes
--------------------------	--	-------------------------------

Permissions summary < 1 >

Name ↗	Type	Used as
IAMUserChangePassword	AWS managed	Permissions policy

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.

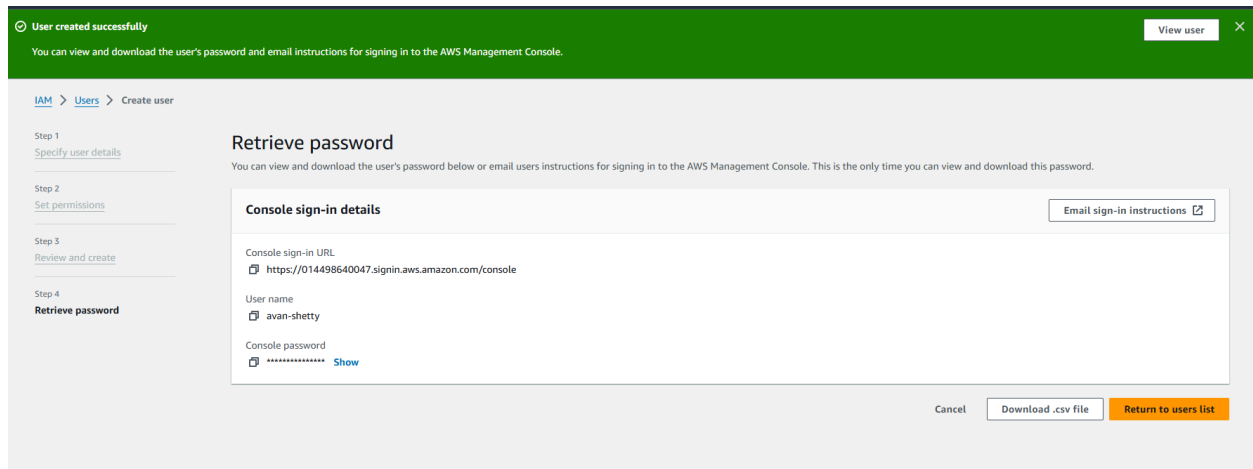
No tags associated with the resource.

Add new tag

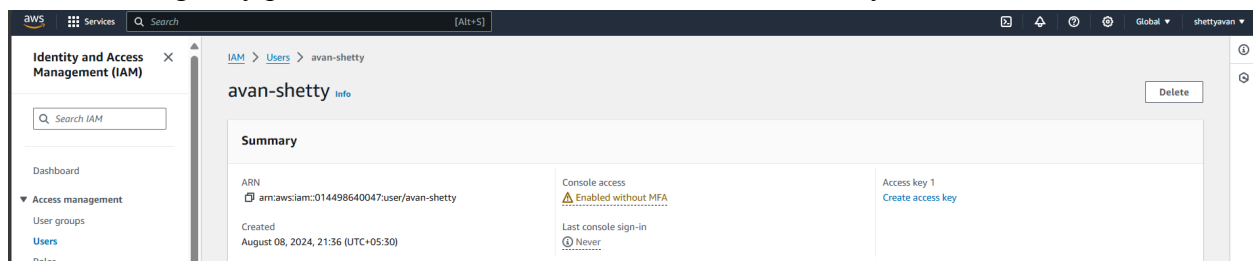
You can add up to 50 more tags.

Cancel Previous **Create user**

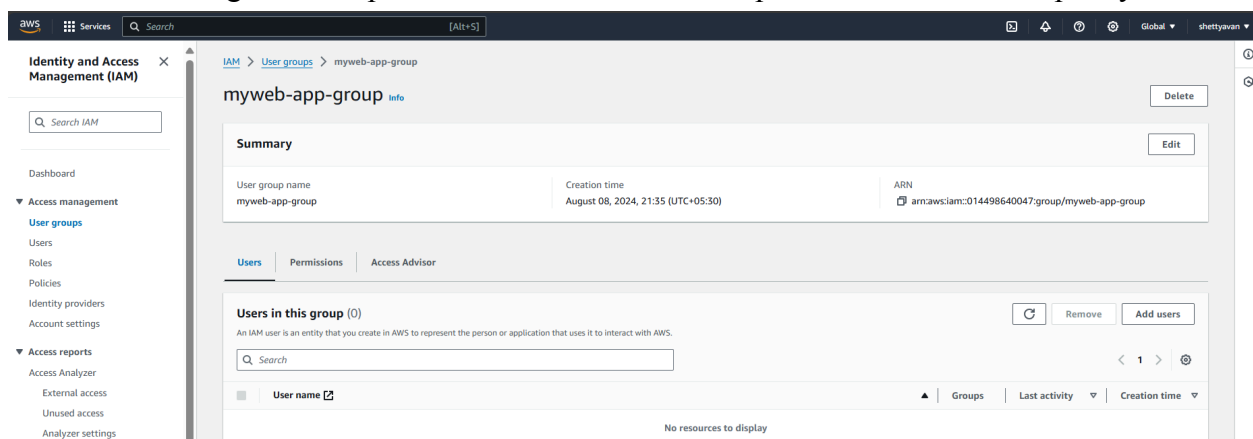
7. You will see the “user created successfully” message and incase you need then store your password by downloading the csv file



8. Click the users tab and you will see the user is created under IAM service. Also this service does not charge any price but this feature is not available in academy lab



9. 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.




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


[IAM](#) > [User groups](#) > [myweb-app-group](#) > Add permissions

Attach permission policies to myweb-app-group

► **Current permissions policies (0)**

Other permission policies (1/945) 


You can attach up to 10 managed policies to this user group. All of the users in this group inherit the attached permissions.




Filter by Type

All types

 1 match

< 1 > 

<input checked="" type="checkbox"/>	Policy name	Type	Used as	Description
<input checked="" type="checkbox"/>	 AWSCloud9EnvironmentMember	AWS managed	None	Provides the ability to be invited into AW...

Cancel

Attach policies