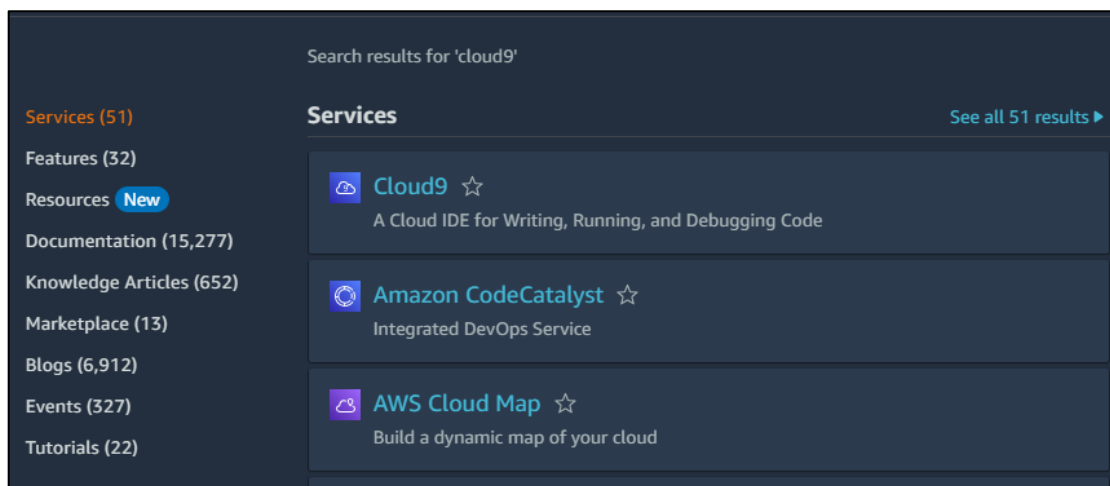


Advance DevOps

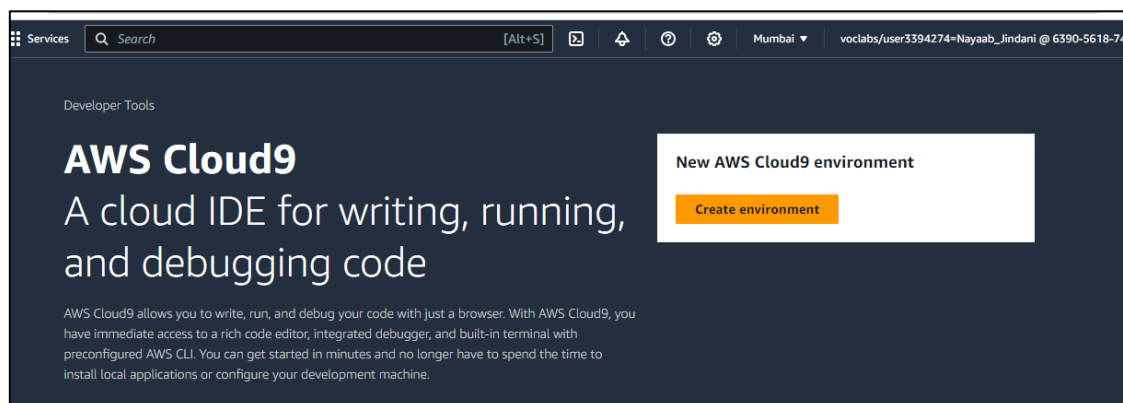
Experiment 1b

Steps to setup AWS Cloud9 IDE, Launch AWS Cloud9 IDE and perform collaboration:

1. Login in your AWS account. Search Cloud9 in services.



2. Select create environment.



3. Provide the name, description (optional).

AWS Cloud9 > Environments > Create environment

Create environment [Info](#)

Details

Name

Limit of 60 characters, alphanumeric, and unique per user.

Description - optional

Limit 200 characters.

Environment type [Info](#)
Determines what the Cloud9 IDE will run on.

☒ **New EC2 instance**
Cloud9 creates an EC2 instance in your account. The configuration of your EC2 instance cannot be changed by Cloud9 after creation.

☐ **Existing compute**
You have an existing instance or server that you'd like to use.

4. Select Secure Shell (SSH) as the connection type and click on create.

Connection
How your environment is accessed.

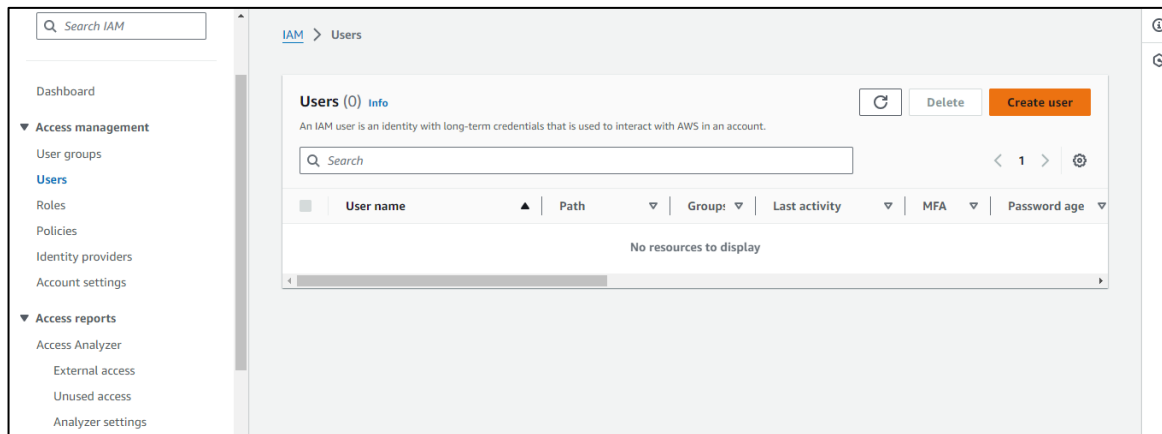
☐ **AWS Systems Manager (SSM)**
Accesses environment via SSM without opening inbound ports (no ingress).

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

5. Your Cloud9 IDE has been created.

Environments (1)						
My environments						
	Name ▲	Cloud9 IDE Info	Environment type	Connection	Permission	Owner ARN
<input type="radio"/>	WebAppIDE	Open	EC2 instance	Secure Shell (SSH)	Owner	arn:aws:sts::639056187451:assumed-role/voclabs/user3394274=Nayaab_Jindani

6. Now we will create user. For that go to IAM -> Users -> Create user.



7. Enter user details like user name, password and click on next.

User details

User name

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.

Console password

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

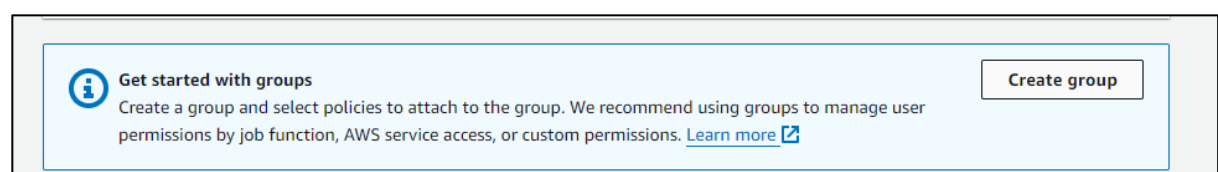
☒ Custom password
Enter a custom password for the user.

- 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) = [] { } | ' "

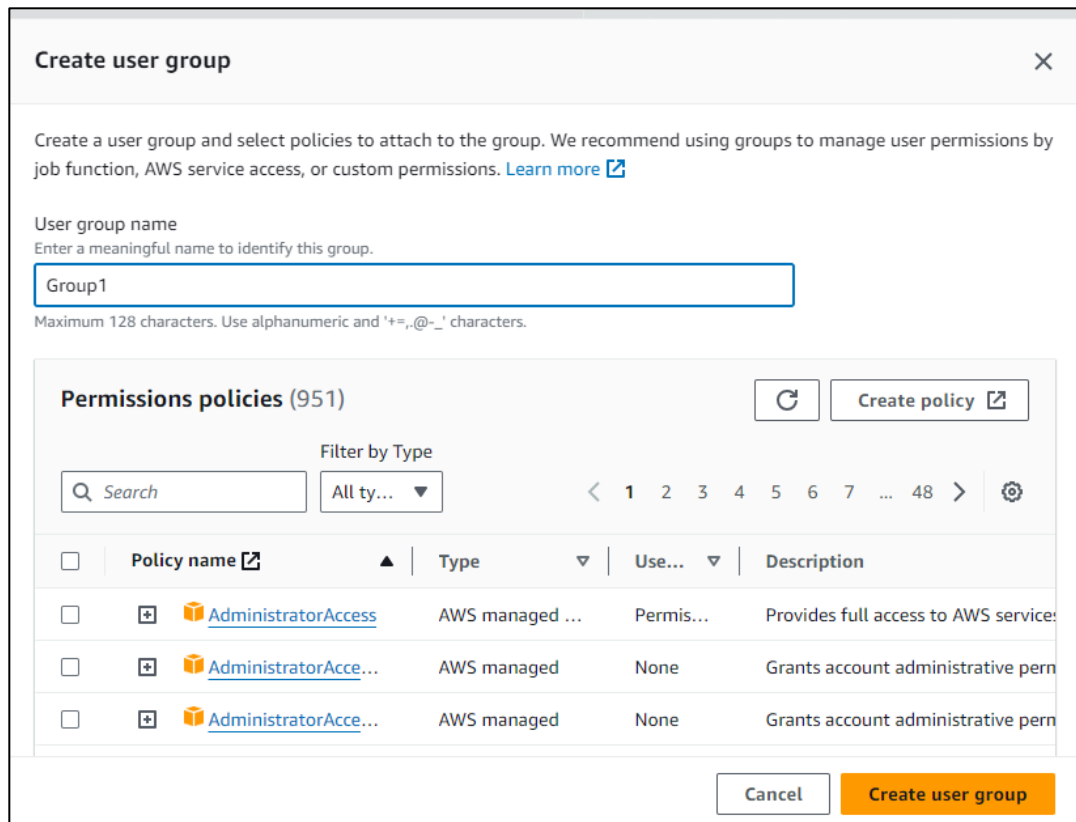
☐ Show password

☐ 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.

8. Select create group in the next section.



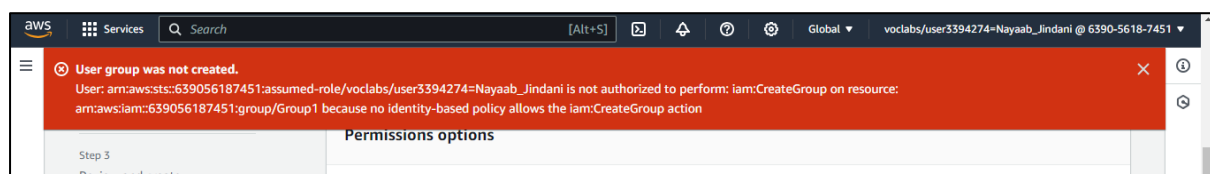
9. Enter group name, select permission policies and select create user group.



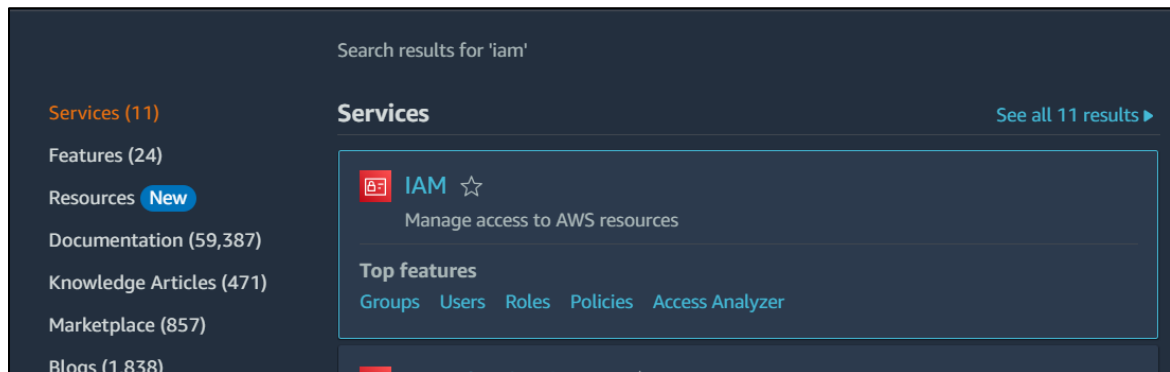
The screenshot shows the 'Create user group' console window. At the top, it says 'Create user group' with a close button. Below is a description: 'Create a user group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)'. The 'User group name' field is set to 'Group1'. Below the field, it says 'Maximum 128 characters. Use alphanumeric and '+','=','@_- ' characters.' The 'Permissions policies (951)' section shows a search bar, a 'Filter by Type' dropdown set to 'All ty...', and a table of policies. The table has columns: Policy name, Type, Use..., and Description. Three policies are listed, all starting with 'AdministratorAccess'. At the bottom, there are 'Cancel' and 'Create user group' buttons.

Policy name	Type	Use...	Description
AdministratorAccess	AWS managed ...	Permis...	Provides full access to AWS service:
AdministratorAcce...	AWS managed	None	Grants account administrative perm
AdministratorAcce...	AWS managed	None	Grants account administrative perm

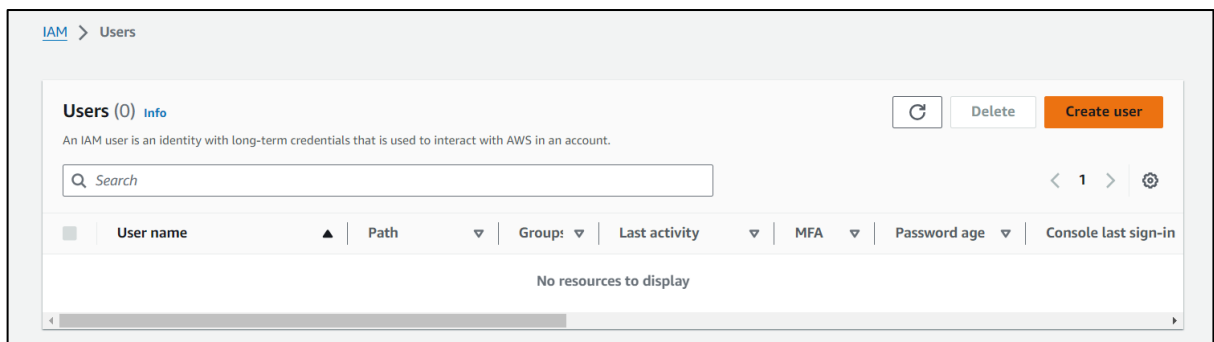
10. Due to authorization issues the group was not created and the below given error was displayed.



11. Now we will sign in to the AWS account to continue with the further procedure and sign out from the console we were working on earlier. After logging in search for IAM in services and click on it.



12. Now again we will follow the same procedure to create user and group as done above.



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.

- 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.

Info 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

13. Select add user to group and click on next.

The screenshot shows the 'Add user to group' step in the AWS IAM console. The left sidebar indicates the current step is 'Set permissions'. The main content area has a green header 'Group1 user group created.' and a sub-header '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](#)'. Below this, there are three 'Permissions options' boxes: 'Add user to group' (selected), 'Copy permissions', and 'Attach policies directly'. The 'Add user to group' box contains the text: 'Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.' Below the options is a 'User groups (1)' section with a search bar and a table. The table has columns: 'Group name', 'Users', 'Attached policies', and 'Created'. It shows one group named 'Group1' with 0 users and policies, created on 2024-08-08 (Now). At the bottom, there is a 'Set permissions boundary - optional' section and buttons for 'Cancel', 'Previous', and 'Next'.

Group name	Users	Attached policies	Created
Group1	0	-	2024-08-08 (Now)

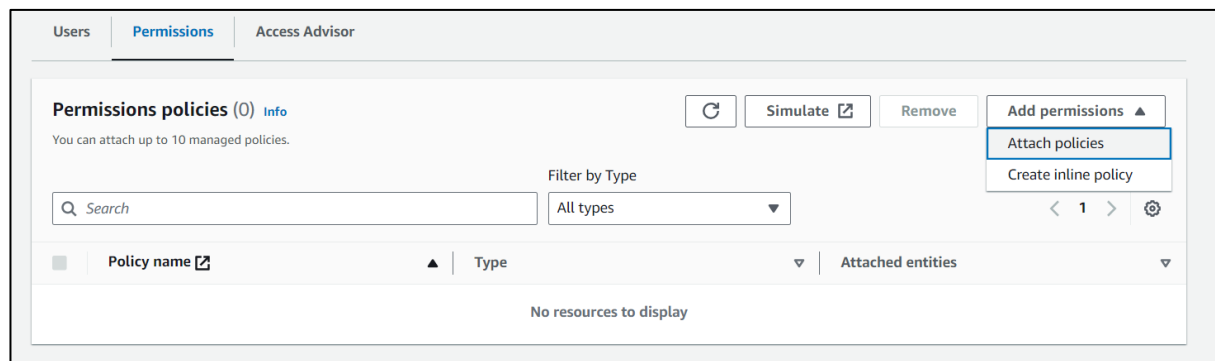
14. Add tags (optional) and select create user.

The screenshot shows the 'Tags - optional' step in the AWS IAM console. The section title is 'Tags - optional' with a sub-header: '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.' Below this, it says 'No tags associated with the resource.' and there is an 'Add new tag' button. A note states: 'You can add up to 50 more tags.' At the bottom, there are buttons for 'Cancel', 'Previous', and 'Create user'.

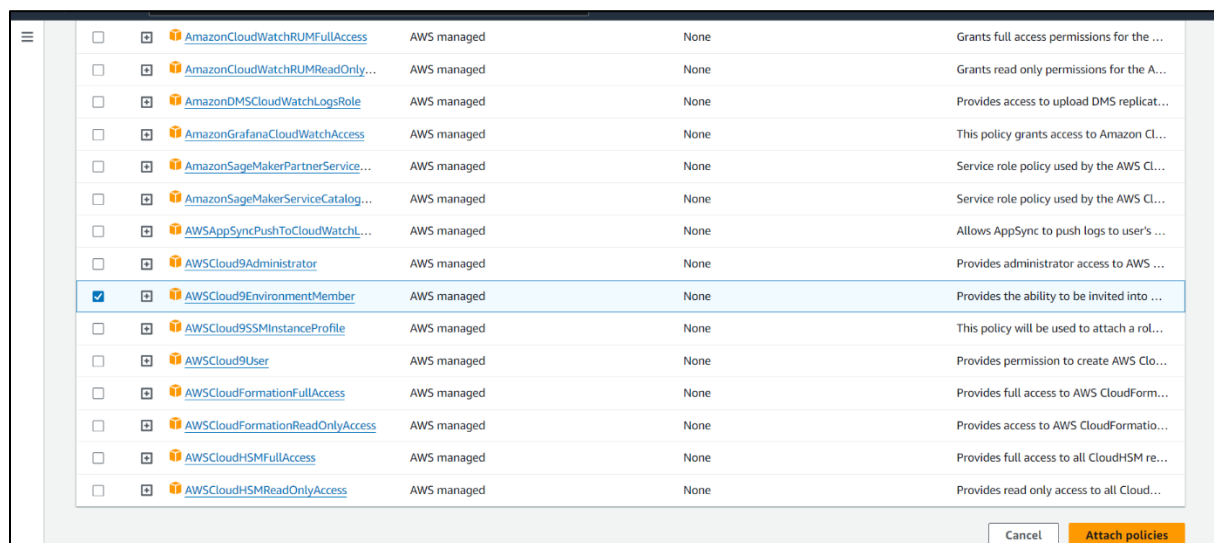
15. In the left pane select user groups.

The screenshot shows the left sidebar of the AWS IAM console. The title is 'Identity and Access Management (IAM)'. Below the title is a search bar labeled 'Search IAM'. The sidebar menu includes 'Dashboard' and 'Access management'. Under 'Access management', 'User groups' is highlighted in blue.

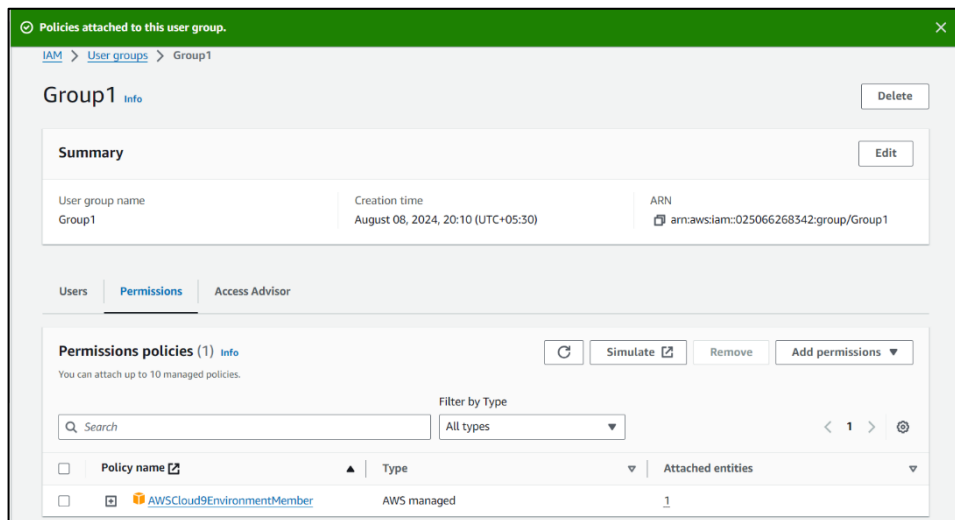
16. Click on the group you created and go to permissions tab and select attach policies from add permissions.



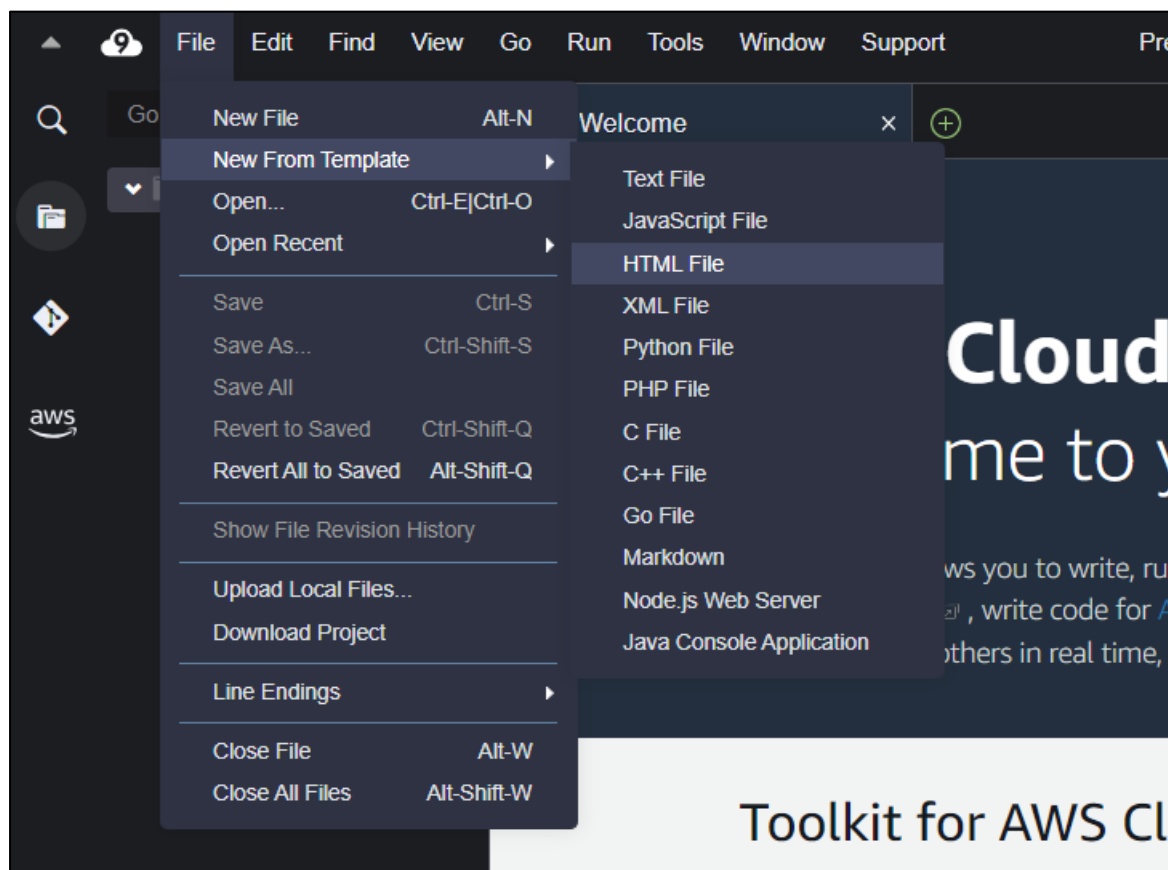
17. Attach the policy `AWSCloud9EnvironmentMember` by selecting it and click on attach policies.



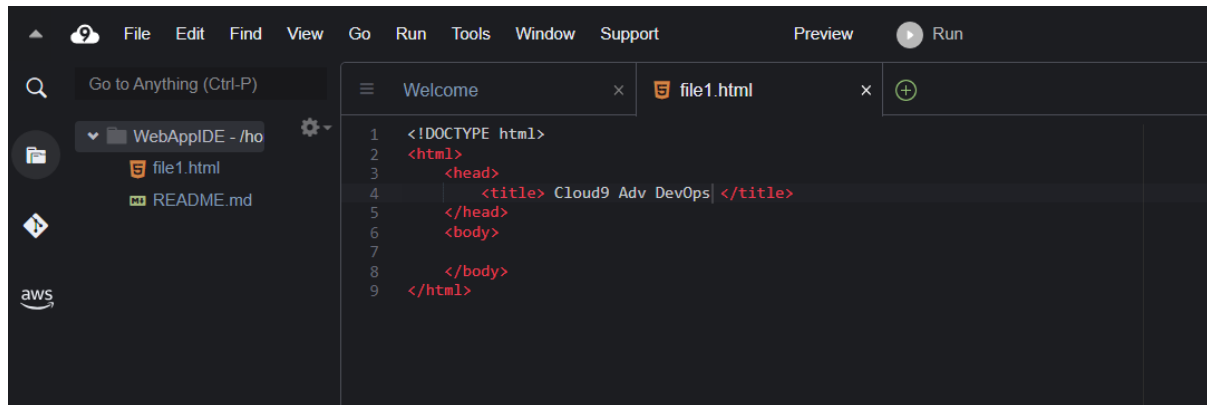
18. Policy has been successfully attached to the user group



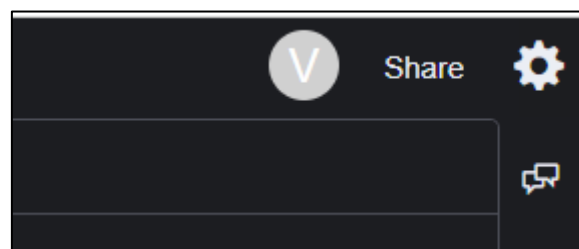
19. Now we will open the Cloud9 IDE we created earlier. Then go to file -> new from template -> HTML file (any file type can be selected).



20. You can now edit the html file and save it.



21. We can collaborate with other members by sharing this file. To do so click on the share option to the top right of the screen.



22. Here you can give read or read/write permission to your team members and click on invite.

Your teammate will get an invite in “shared with you” and after he/she selects open IDE they will be able to see the same interface as yours and now you and your team members can collaborate in real time.

Share this environment

Links to share

Environment:

https://us-east-1.console.aws.amazon.com/cloud9/ide/9448d4b73ea8

Application:

54.165.13.44

To make your application accessible from the internet, please follow [our documentation](#).

Who has access

ReadWrite

You (online)

RW

☐ Don't allow members to save their tab state

Invite Members

Nayaab

R RW

Invite

Invite an existing IAM user or [create a new user](#).

Done