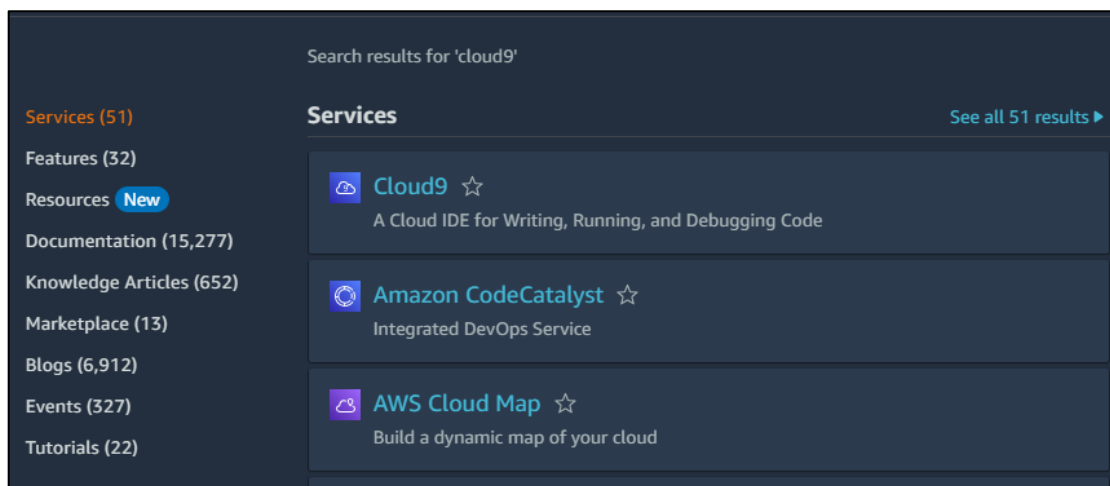


## Advance DevOps

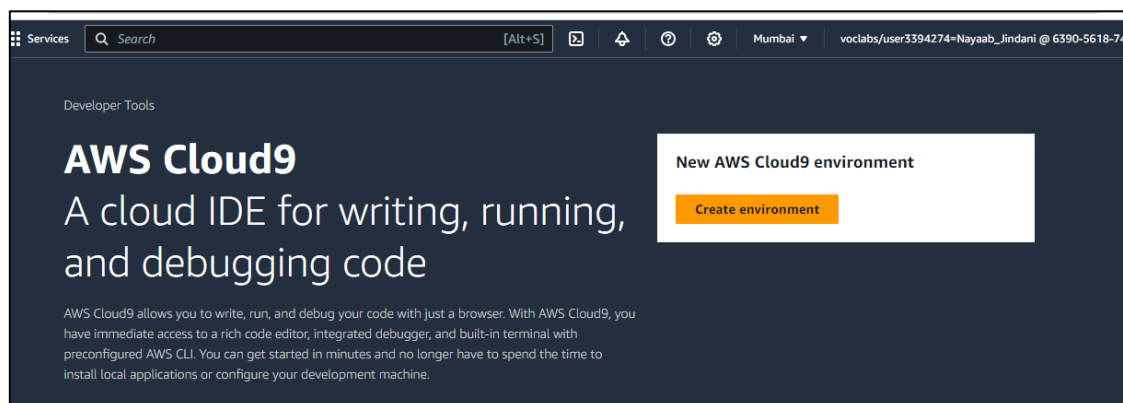
### Experiment 1b

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.



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.

3. Provide the name, description (optional).

**Connection**  
How your environment is accessed.

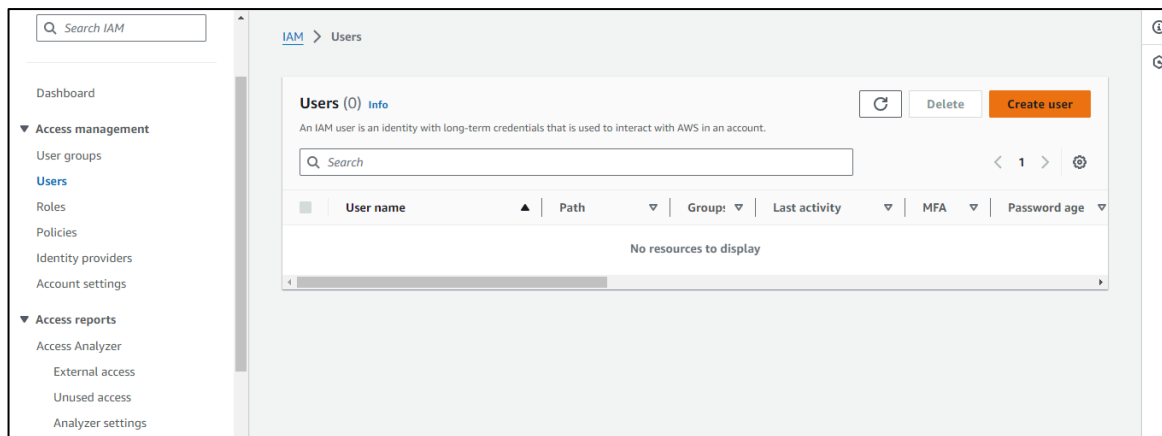
☐ **AWS Systems Manager (SSM)**  
Accesses environment via SSM without opening inbound ports (no ingress).

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

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

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

5. Your Cloud9 IDE has been created.



### 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.

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.

### Create user group

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](#)

User group name  
Enter a meaningful name to identify this group.

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

#### Permissions policies (951)

Filter by Type  
All ty... ▼

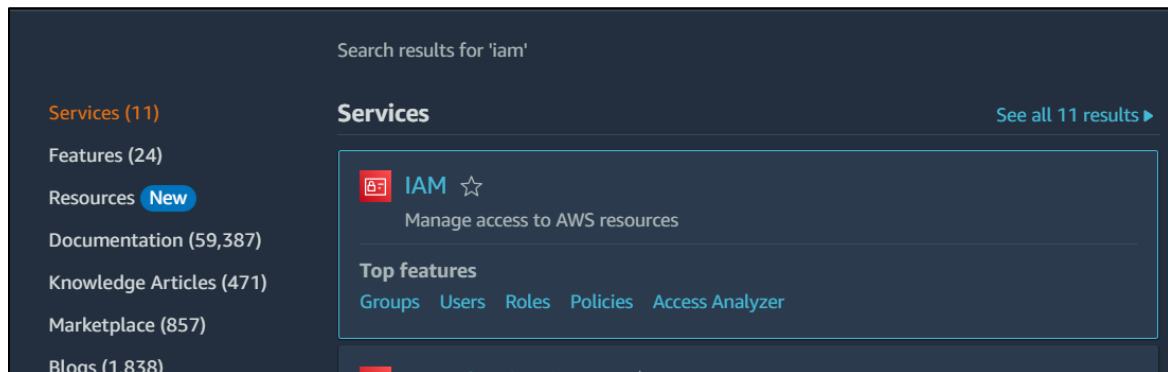
< 1 2 3 4 5 6 7 ... 48 > ⚙

<input type="checkbox"/>	Policy name	Type	Use...	Description
<input type="checkbox"/>	<a href="#">AdministratorAccess</a>	AWS managed ...	Permis...	Provides full access to AWS service:
<input type="checkbox"/>	<a href="#">AdministratorAcce...</a>	AWS managed	None	Grants account administrative per...
<input type="checkbox"/>	<a href="#">AdministratorAcce...</a>	AWS managed	None	Grants account administrative per...

8. Select create group in the next section.

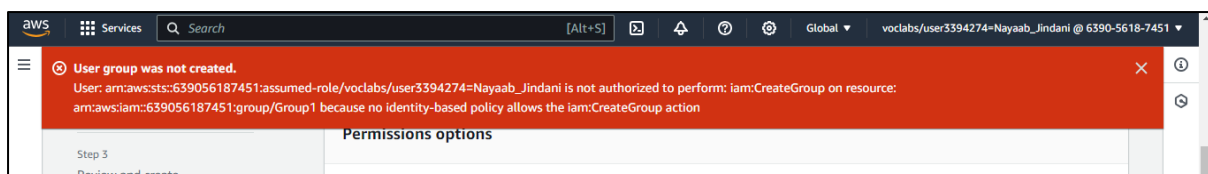
**Get started with groups**  
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

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



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.

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

The screenshot shows the 'Add user to group' step in the AWS IAM console. A green banner at the top says 'Group1 user group created.' Below it, a sidebar on the left lists steps: Step 2 (Set permissions), Step 3 (Review and create), and Step 4 (Retrieve password). The main area is titled 'Permissions options' and has three radio buttons: 'Add user to group' (selected), 'Copy permissions', and 'Attach policies directly'. Below this is a section 'User groups (1)' with a search bar and a table. The table has columns: Group name, Users, Attached policies, and Created. It shows one group, 'Group1', with 0 users and a creation date of '2024-08-08 (Now)'. At the bottom, there is a 'Set permissions boundary - optional' link and 'Cancel', 'Previous', and 'Next' buttons.

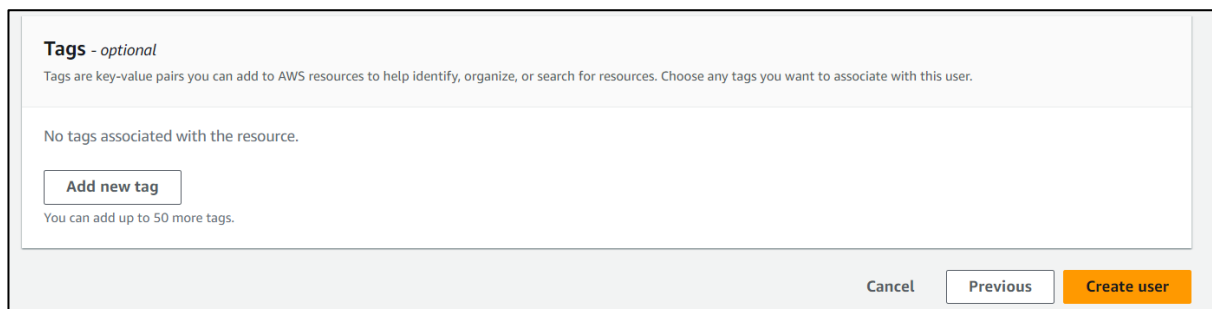
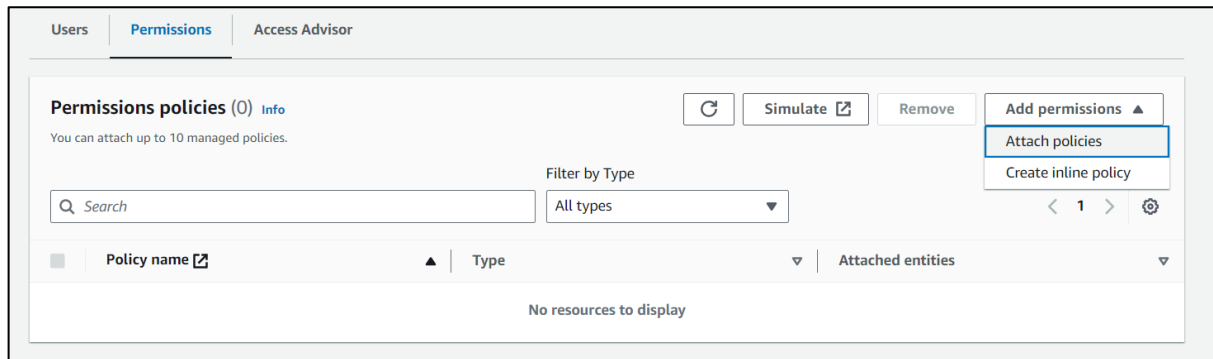
Group name	Users	Attached policies	Created
Group1	0	-	2024-08-08 (Now)

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

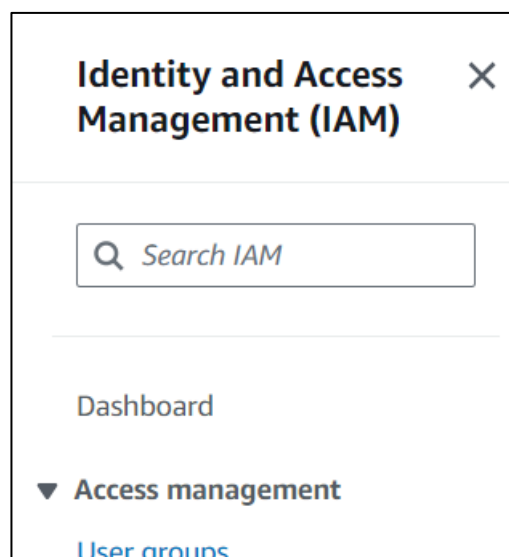
The screenshot shows the 'Users' page in the AWS IAM console. The breadcrumb is 'IAM > Users'. The main heading is 'Users (0) Info' with a 'Create user' button. Below the heading is a search bar and a table with columns: User name, Path, Group, Last activity, MFA, Password age, and Console last sign-in. The table is empty, showing 'No resources to display'.

The screenshot shows the 'Create user' wizard in the AWS IAM console. The first step is 'User type' with two options: 'Specify a user in Identity Center - Recommended' and 'I want to create an IAM user' (selected). The second step is 'Console password' with two options: 'Autogenerated password' and 'Custom password' (selected). The 'Custom password' option has a text input field with a password and a list of requirements: '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) = [ ] { } ' '. There is also a 'Show password' checkbox. The third step is 'Users must create a new password at next sign-in - Recommended' with a checkbox. At the bottom, there is a 'Cancel' button and a 'Next' button.

15. In the left pane select user groups.



16. Click on policies

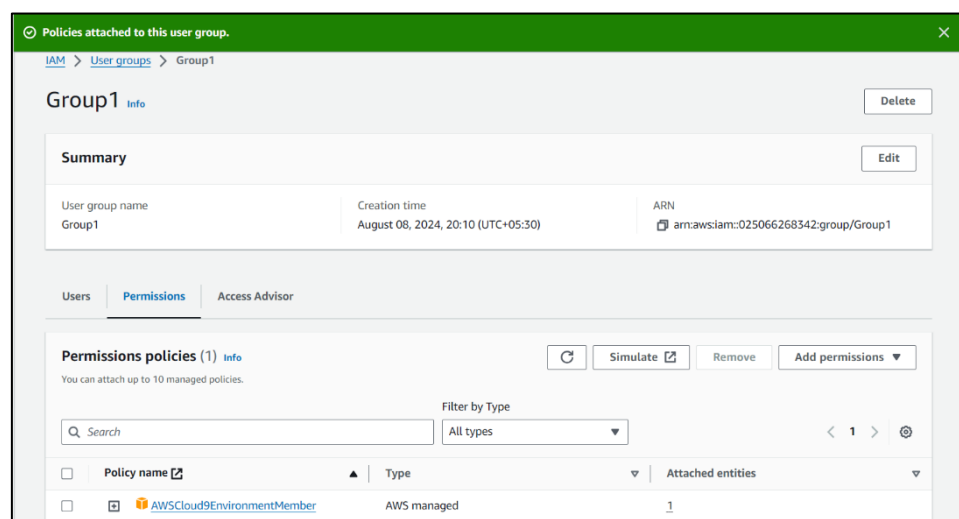
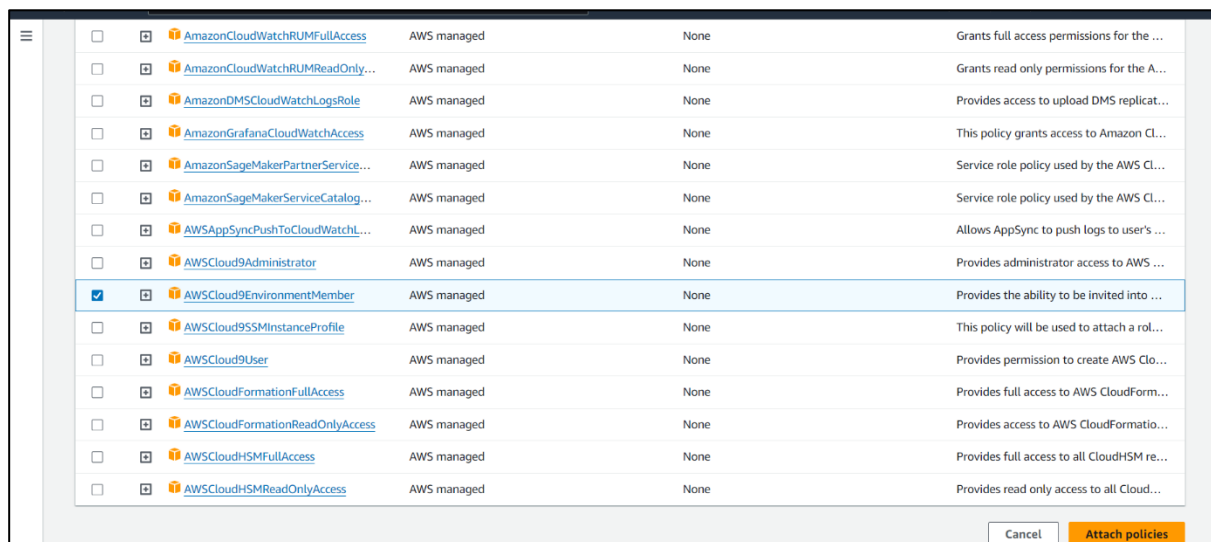


the group you created and go to permissions tab and select attach from add permissions.

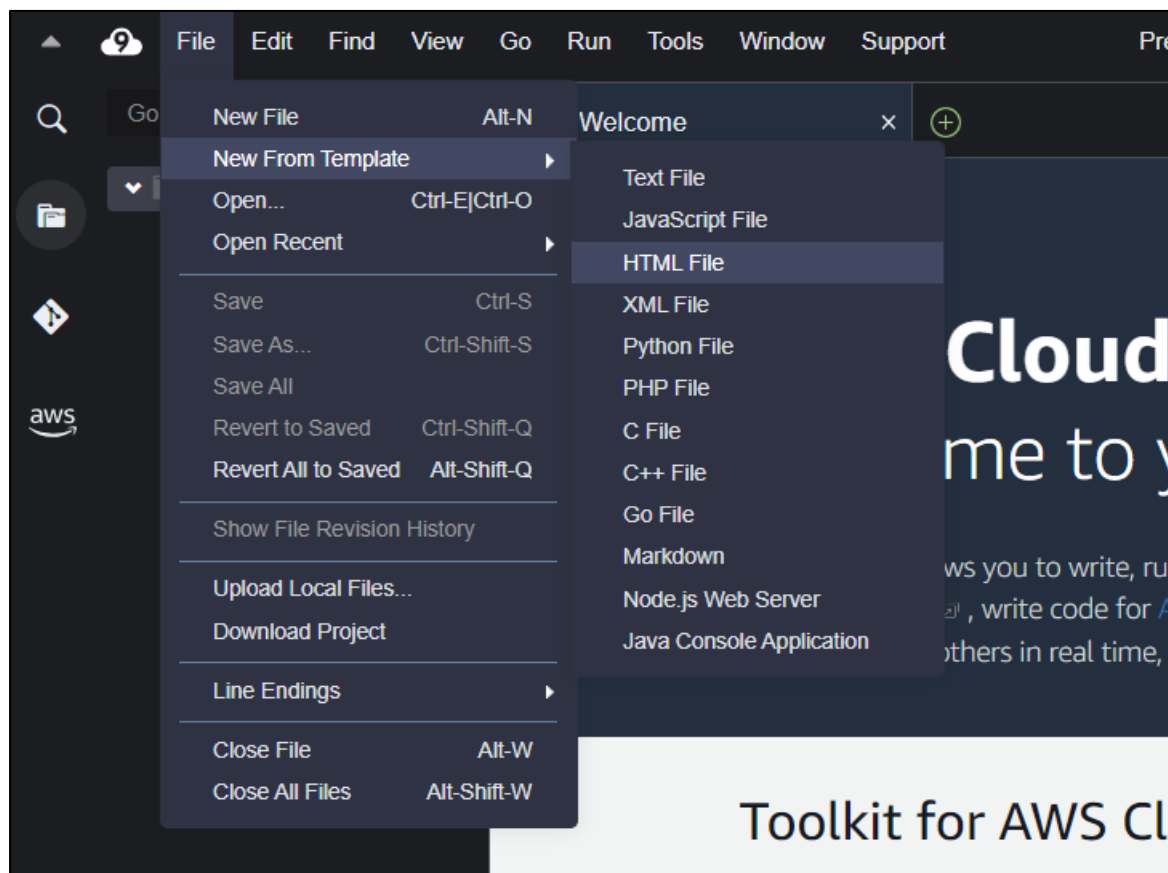
17. Attach the policy `AWSCloud9EnvironmentMember` by selecting it and click on attach policies.

18. Policy has been successfully attached to the user group

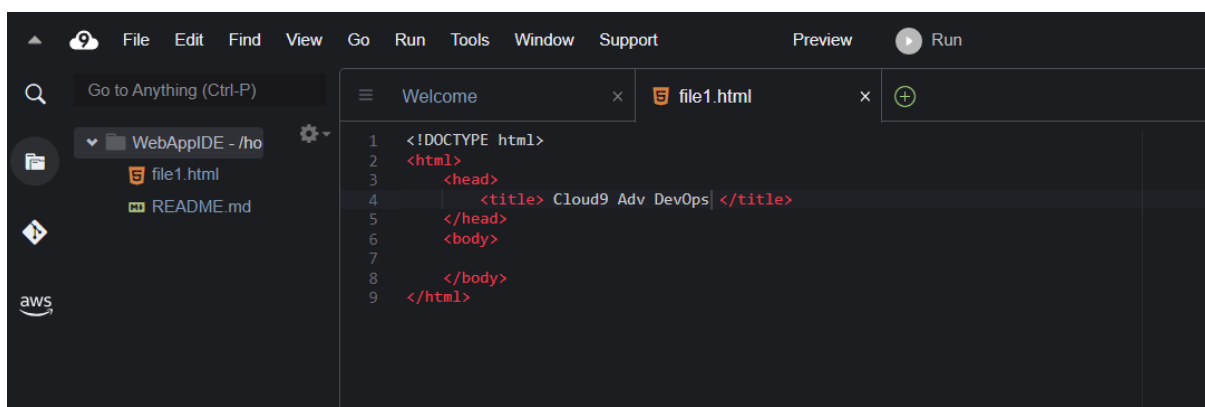
19. Now we will open the Cloud9 IDE we created earlier. Then go to file -> new from template -> HTML file (any file type can be selected).







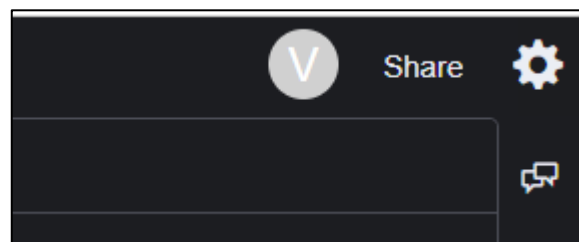
20. You can now edit the html file and save it.



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  
invite in



teammate will get an  
“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