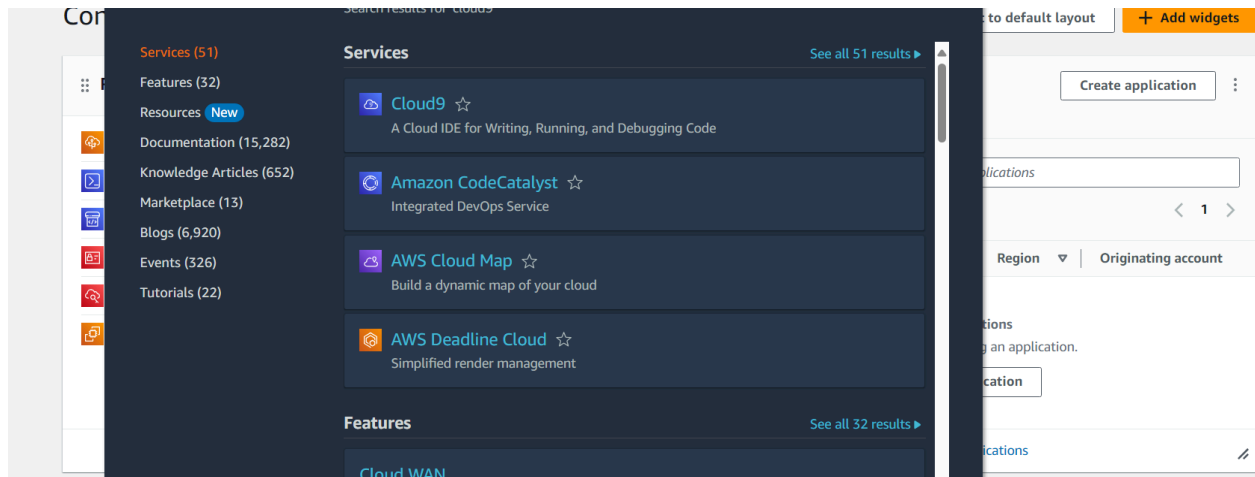


## Step 1: Set up Cloud9 environment.

1) Search Cloud9 in the services tab and open it



2) Click on Create Environment.

→Give a name to your Cloud9 Environment. You can add a description if needed.

→Select the option new EC2 instance if you do not have one ready for the environment. Give the specifications of that EC2 instance ahead

→On the AWS Academy account, if we select AWS System Manager(SSM) in Network settings, it gives an error as the account does not have permissions to use the setting. So we select Secure Shell (SSH). After that click on Create.

A screenshot of the AWS Cloud9 'Create environment' page. The breadcrumb navigation at the top reads 'AWS Cloud9 > Environments > Create environment'. The main heading is 'Create environment' with an 'Info' link. Below this is a 'Details' section. It contains three form fields: 'Name' with the value 'Ayush Maurya' and a note 'Limit of 60 characters, alphanumeric, and unique per user.'; 'Description - optional' with the value 'First Experience' and a note 'Limit 200 characters.'; and 'Environment type' with a note 'Determines what the Cloud9 IDE will run on.' There are two radio button options: 'New EC2 instance' (which is selected) and 'Existing compute'. The 'New EC2 instance' option has a sub-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 sub-note: 'You have an existing instance or server that you'd like to use.'

Details

Edit

Name Ayush Maurya	Owner ARN arn:aws:sts::217253764927:assumed-role/voclabs/user3385518=MAURYA_AYUSH_SUBHASHCHANDRA	Status Ready
Description First Experience	Number of members 1	Lifecycle status Created
Environment type EC2 instance		

EC2 instance

Network settings

Tags

EC2 instance

Manage EC2 instance

ARN arn:aws:cloud9:us-east-1:217253764927:environment:b096c95b7bb94be4bb2220da1765f6f6	Instance type t2.micro (1 GiB RAM + 1 vCPU)
Platform Amazon Linux 2023	Storage EBS only

## 6) The environment is being created.

For capabilities similar to AWS Cloud9, explore AWS Toolkits in your own IDE and AWS CloudShell in the AWS Management Console. [Learn more](#)

[AWS Cloud9](#) > Environments

Environments (1)

Delete

View details

Open in Cloud9

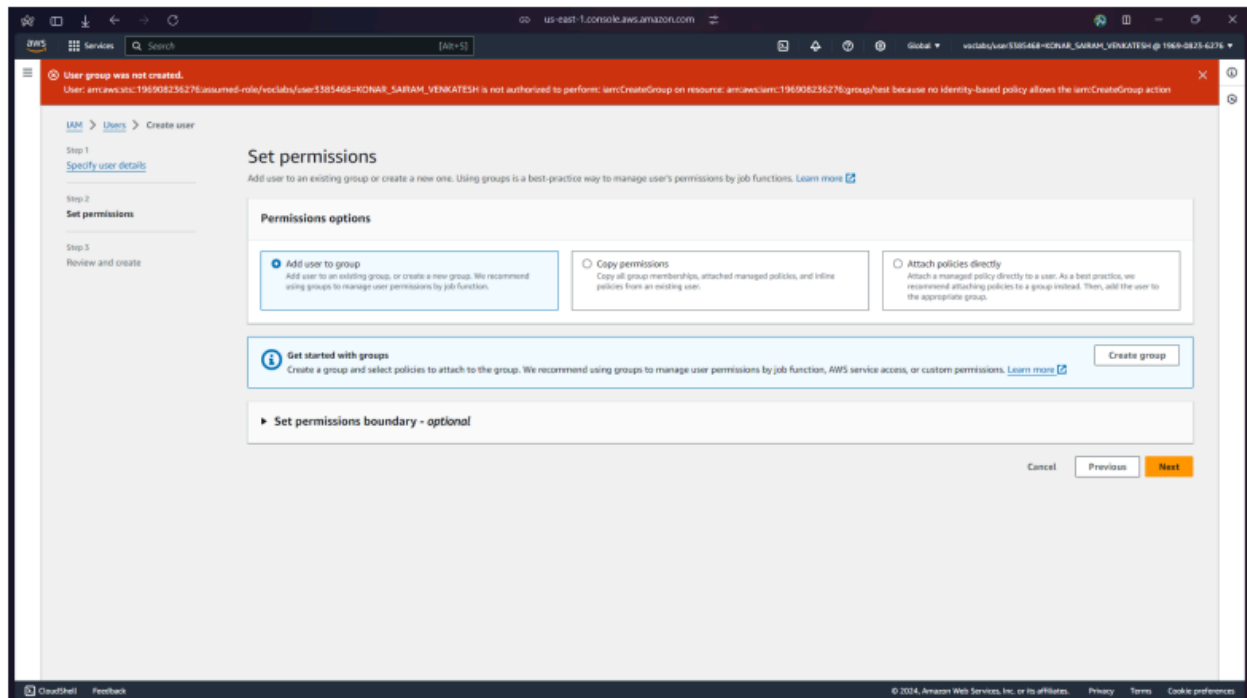
Create environment

My environments

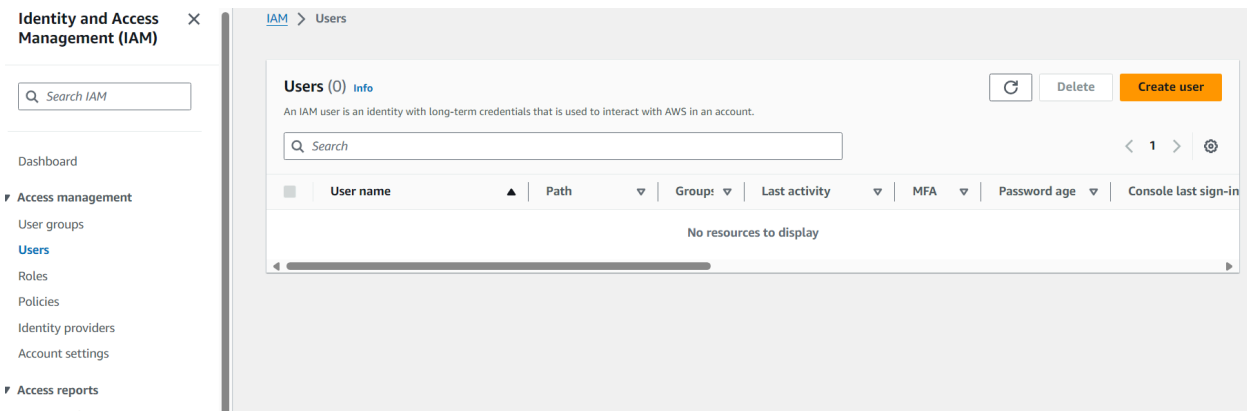
	Name	Cloud9 IDE	Environment type	Connection	Permission	Owner ARN
<input type="radio"/>	<a href="#">Ayush Maurya</a>	<a href="#">Open</a>	EC2 instance	Secure Shell (SSH)	Owner	arn:aws:sts::217253764927:assumed-role/voclabs/user3385518=MAURYA_AYUSH_SUBHASHCHANDRA

## Step 2: Creating IAM user.

When we go to add user to a group, the AWS Academy account throws an error as we do not have the permissions to create a group. So we have to use our personal AWS account for this part. ‘



1) Search IAM on the services search bar and open it. Click on Create User.



2) Give a username to your user and click Next.

IAM > Users > Create user

Step 1  
Specify user details

Step 2  
Set permissions

Step 3  
Review and create

## Specify user details

### 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.

**i** 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

3) Select add User to Group. If there are no user groups on your accounts, you will have to create one. Click on Create Group.

IAM > Users > Create user

Step 1  
[Specify user details](#)

Step 2  
Set permissions

Step 3  
Review and create

## 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.

**i** 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](#)

Create group

► Set permissions boundary - *optional*

Cancel Previous Next

#### 4) Give a name to your user group. Then click on Create User Group.

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.  

ayushGroup

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

Permissions policies (955)

Search

Filter by Type  
All ty...

< 1 2 3 4 5 6 7 ... 48 >

<input type="checkbox"/>	Policy name	Type	Use...	Description
<input type="checkbox"/>	AdministratorAccess	AWS managed ...	None	Provides full access to AWS service...
<input type="checkbox"/>	AdministratorAcce...	AWS managed	None	Grants account administrative perm...
<input type="checkbox"/>	AdministratorAcce...	AWS managed	None	Grants account administrative perm...
<input type="checkbox"/>	AlexaForBusinessD...	AWS managed	None	Provide device setup access to Alex...
<input type="checkbox"/>	AlexaForBusinessF...	AWS managed	None	Grants full access to AlexaForBusin...
<input type="checkbox"/>	AlexaForBusinessG...	AWS managed	None	Provide gateway execution access t...

Cancel

Create user group

#### 5) The group is created and shown under the groups area, select the group by clicking on the checkbox. Then click Next.

Services

Search

[Alt+S]

Global

ayushGroup user group created.

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](#)

Step 2  
Set permissions

Step 3  
Review and create

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)

Search

< 1 >

<input type="checkbox"/>	Group name	Users	Attached policies	Created
<input type="checkbox"/>	ayushGroup	0	-	2024-08-11 ()

Set permissions boundary - optional

Cancel

Previous

Next

6) Review all the Information, then click on Create user.

The screenshot shows the 'Review and create' step in the AWS IAM console. A green banner at the top states 'ayushGroup user group created.' The left sidebar shows 'Step 3 Review and create'. The main content area is divided into three sections: 'User details', 'Permissions summary', and 'Tags - optional'. The 'User details' section shows 'User name' as 'ayush', 'Console password type' as 'None', and 'Require password reset' as 'No'. The 'Permissions summary' section shows 'No resources'. The 'Tags - optional' section shows 'No tags associated with the resource' and an 'Add new tag' button.

Step 1

Review and create

Services Search [Alt+S]

ayushGroup user group created.

Step 3 Review and create

User details

User name: ayush

Console password type: None

Require password reset: No

Permissions summary

No resources

Tags - optional

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

7) Open User Groups tab from the left side option. Click on the name of your group.

The screenshot shows the 'User groups' tab in the AWS IAM console. The left sidebar shows 'Identity and Access Management (IAM)' and 'Access management' with 'User groups' selected. The main content area shows 'User groups (1)' with a search bar and a table. The table has columns: 'Group name', 'Users', 'Permissions', and 'Creation time'. The row for 'ayushGroup' shows 0 users, 'Not defined' permissions, and '2 minutes ago' creation time.

Identity and Access Management (IAM)

Search 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

IAM > User groups

User groups (1) Info

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

Search

Group name Users Permissions Creation time

ayushGroup 0 Not defined 2 minutes ago

8) Go to permissions and click on Add permissions. Click on Attach Policies.

The screenshot shows the 'Permissions' tab for the 'ayushGroup' user group in the AWS IAM console. The left sidebar shows 'Identity and Access Management (IAM)' and 'Access management' with 'User groups' selected. The main content area shows 'ayushGroup' with a 'Delete' button. Below is a 'Summary' section with 'User group name' as 'ayushGroup', 'Creation time' as 'August 11, 2024, 18:14 (UTC+05:30)', and 'ARN' as 'arn:aws:iam::011528263337:group/ayushGroup'. The 'Permissions policies (0)' section shows 'No resources to display'.

Identity and Access Management (IAM)

Search 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

IAM > User groups > ayushGroup

ayushGroup Info

Delete

Summary

Edit

User group name: ayushGroup

Creation time: August 11, 2024, 18:14 (UTC+05:30)

ARN: arn:aws:iam::011528263337:group/ayushGroup

Users Permissions Access Advisor

Permissions policies (0) Info

You can attach up to 10 managed policies.

Search

Filter by Type: All types

Policy name Type Attached entities

No resources to display

## 9) Search for AWSCloud9EnvironmentMember, select it and click on Attach policies

IAM > User groups > ayushGroup > Add permissions

### Attach permission policies to ayushGroup

► **Current permissions policies (0)**

**Other permission policies (1/953)**

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

Q: AWSCloud9 Filter by Type: All types 4 matches < 1 >

	Policy name ▲	Type ▼	Used as ▼	Description
<input type="checkbox"/>	<a href="#">AWSCloud9Administrator</a>	AWS managed	None	Provides administrator access to AWS Clo...
<input checked="" type="checkbox"/>	<a href="#">AWSCloud9EnvironmentMember</a>	AWS managed	None	Provides the ability to be invited into AW...
<input type="checkbox"/>	<a href="#">AWSCloud9SSMInstanceProfile</a>	AWS managed	Permissions policy (1)	This policy will be used to attach a role o...
<input type="checkbox"/>	<a href="#">AWSCloud9User</a>	AWS managed	None	Provides permission to create AWS Cloud...

## 10) The policies have been attached

Identity and Access Management (IAM)

Q Search 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

**Policies attached to this user group.**

IAM > User groups > ayushGroup

### ayushGroup [Info](#)

**Summary**

User group name	Creation time	ARN
ayushGroup	August 11, 2024, 18:14 (UTC+05:30)	arn:aws:iam::011528263337:group/ayushGroup

Users **Permissions** Access Advisor

**Permissions policies (1) [Info](#)**

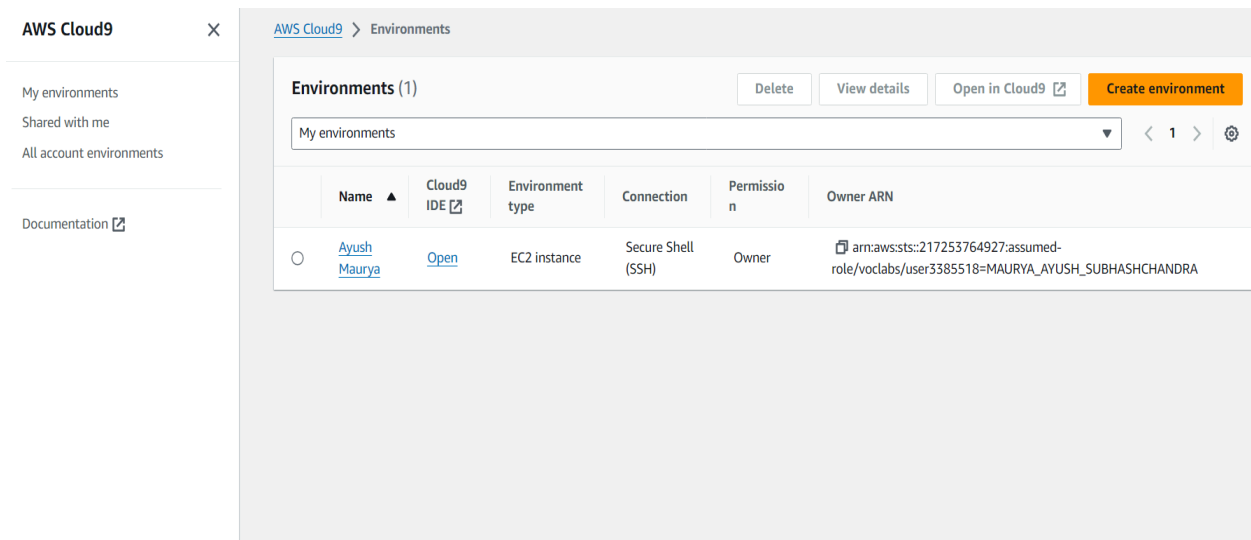
You can attach up to 10 managed policies.

Q Search Filter by Type: All types < 1 >

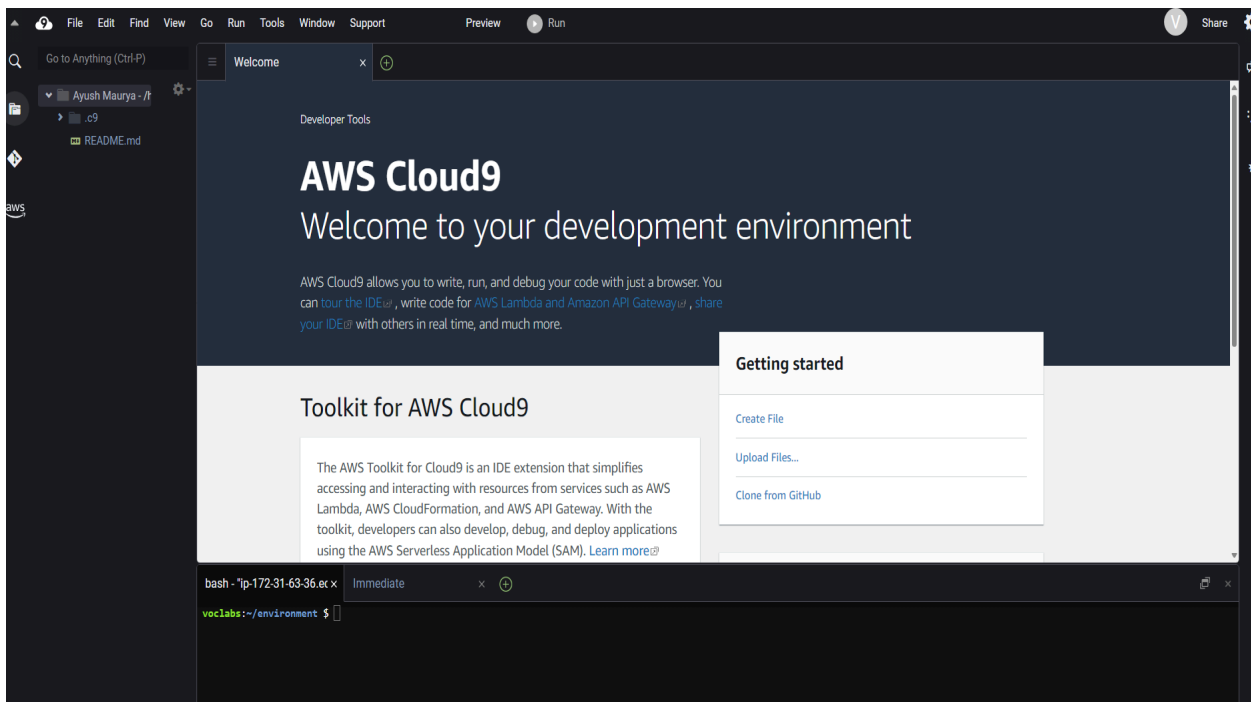
<input type="checkbox"/>	Policy name	Type ▼	Attached entities ▼
<input type="checkbox"/>	<a href="#">AWSCloud9EnvironmentMember</a>	AWS managed	1

## Step 3: Working on Cloud9 IDE

1) Go to Cloud9 services. Click on Open under Cloud9 IDE.

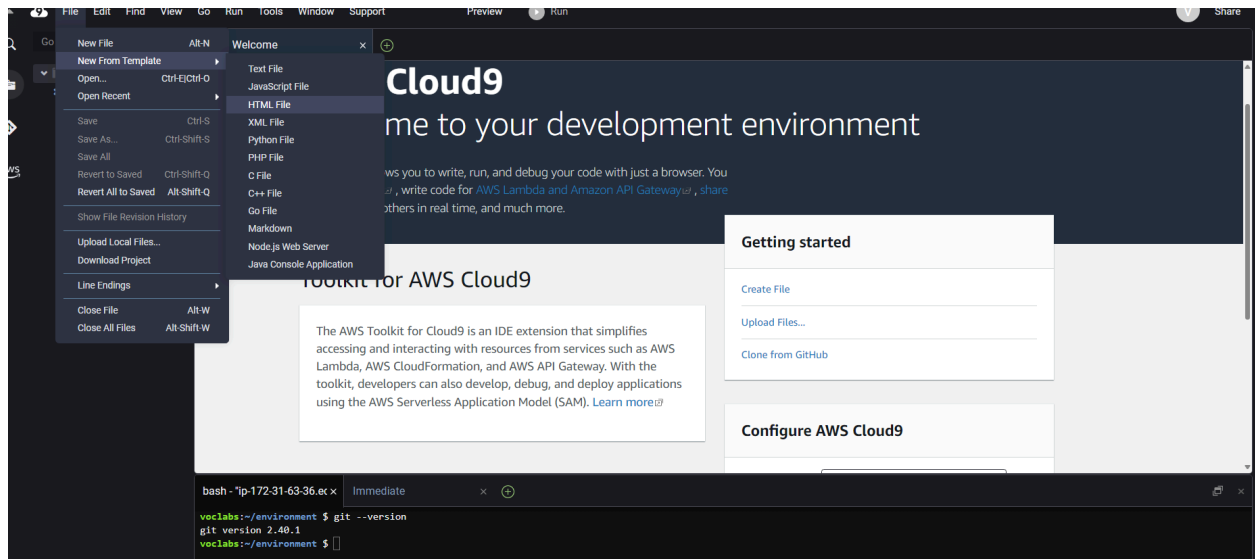


2) This is the Cloud9 IDE interface. The major part of the screen is the coding IDE. There is a command console just below it. For example, the command `git --version` is run.

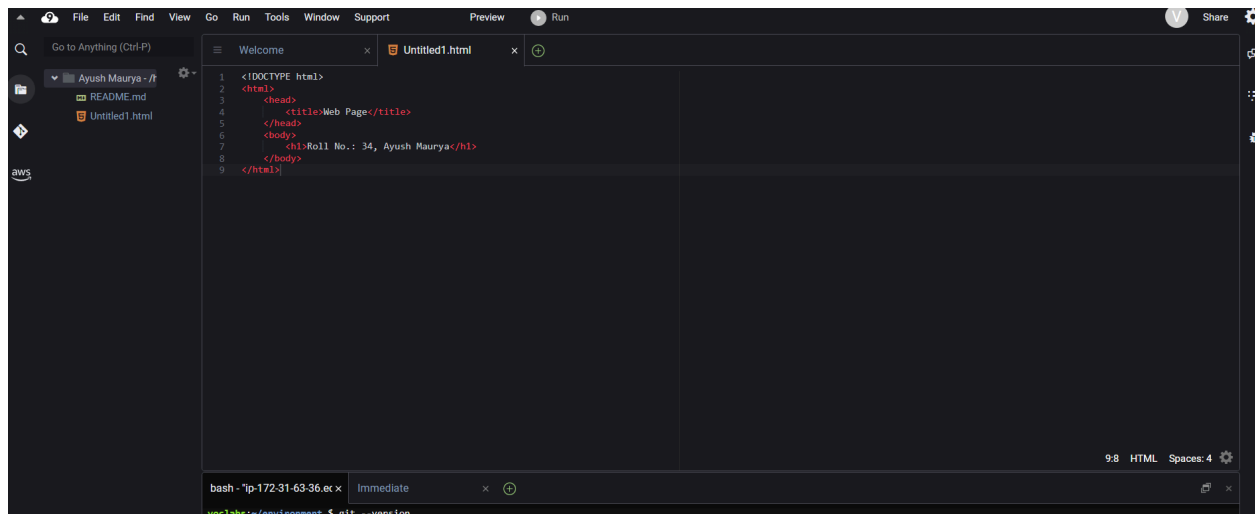




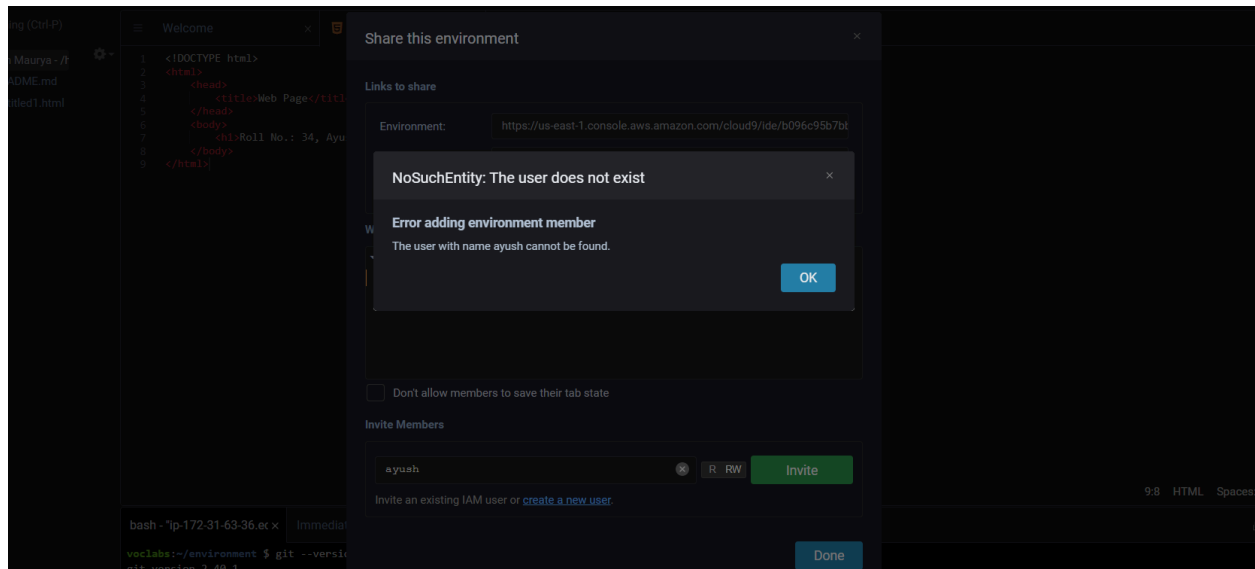
3) To add a file, click on file. For this experiment, we are to add an HTML file. So go to File → New From Template → HTML file. This gives a basic HTML template on the coding IDE.



4) Make a basic website on the HTML template and save it.



After saving, on the toolbar towards the far right, click on Share. Then put the username that you had put during creating IAM user.



Here, it gives an error as Cloud9 was created on the academy account where creating an IAM group is not available, meanwhile on the personal account, the services of Cloud9 have been deprecated. So currently, it is not possible to integrate the cloud9 and IAM parts of the experiment.