



Semester: V
Academic Year: 2023-24
Class / Branch: TE IT
Subject: Advanced Devops Lab (ADL)
Name of Instructor: Prof. Manjusha Kashilkar

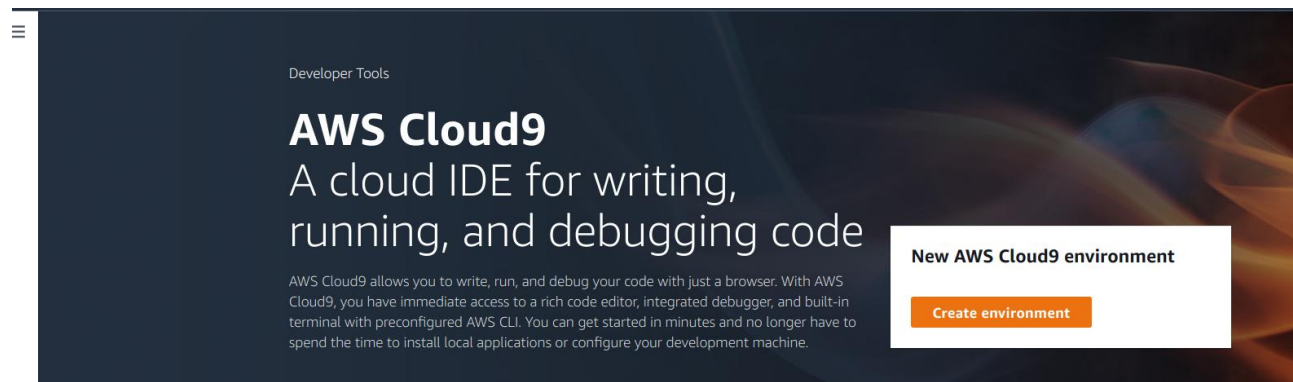
Name of Student:
Student ID:

EXPERIMENT NO. 01

Aim: To understand the benefits of Cloud Infrastructure and Setup AWS Cloud9 IDE, Launch AWS Cloud9 IDE and Perform Collaboration Demonstration.

Steps:

1. Login with your AWS account.
2. Navigate to Cloud 9 service from Developer tools section as below:
3. Click on Create Environment :



4. Provide name for the Environment (WebAppIDE) and click on next.



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



AWS Cloud9 > Environments > Create environment

Step 1
Name environment

Step 2
Configure settings

Step 3
Review

Name environment

Environment name and description

Name
The name needs to be unique per user. You can update it at any time in your environment settings.

Limit: 60 characters

Description - Optional
This will appear on your environment's card in your dashboard. You can update it at any time in your environment settings.

Limit: 200 characters

Cancel **Next step**

5. Keep all the Default settings as shown in below:



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



AWS Cloud9 X

Your environments
Shared with you
Account environments
How-to guide

AWS Cloud9 > Environments > Create environment

Step 1
Name environment

Step 2
Configure settings

Step 3
Review

Configure settings

Environment settings

Environment type [Info](#)
Run your environment in a new EC2 instance or an existing server. With EC2 instances, you can connect directly through Secure Shell (SSH) or connect via AWS Systems Manager (without opening inbound ports).

- ☒ **Create a new EC2 instance for environment (direct access)**
Launch a new instance in this region that your environment can access directly via SSH.
- ☐ Create a new no-ingress EC2 instance for environment (access via Systems Manager)
Launch a new instance in this region that your environment can access through Systems Manager.
- ☐ Create and run in remote server (SSH connection)
Configure the secure connection to the remote server for your environment.

Instance type

- ☒ **t2.micro (1 GiB RAM + 1 vCPU)**
Free-tier eligible. Ideal for educational users and exploration.
- ☐ t3.small (2 GiB RAM + 2 vCPU)
Recommended for small-sized web projects.
- ☐ m5.large (8 GiB RAM + 2 vCPU)
Recommended for production and general-purpose development.
- ☐ Other instance type
Select an instance type.

t3.nano

Platform

- ☒ **Amazon Linux 2 (recommended)**
- ☐ Amazon Linux AMI
- ☐ Ubuntu Server 18.04 LTS

Cost-saving setting
Choose a predetermined amount of time to auto-hibernate your environment and prevent unnecessary charges. We recommend a hibernation settings of half an hour of no activity to maximize savings.

After 30 minutes (default)

IAM role
AWS Cloud9 creates a service-linked role for you. This allows AWS Cloud9 to call other AWS services on your behalf. You can delete the role from the AWS IAM console once you no longer have any AWS Cloud9 environments. [Learn more](#)

AWSServiceRoleForAWSCloud9

► **Network settings (advanced)**

No tags associated with the resource.

Add new tag

You can add 50 more tags.

Cancel

Previous step

Next step

6. Review the Environment name and Settings and click on Create Environment:



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



AWS Cloud9



Your environments
Shared with you
Account environments
How-to guide

AWS Cloud9 > Environments > Create environment

Step 1
[Name environment](#)
Step 2
[Configure settings](#)
Step 3
Review

Review

Environment name and settings

Name
WebApplIDE

Description
No description provided

Environment type
EC2

Instance type
t2.micro

Subnet

Platform
Amazon Linux 2 (recommended)

Cost-saving settings
After 30 minutes (default)

IAM role
AWSServiceRoleForAWSCloud9 (generated)



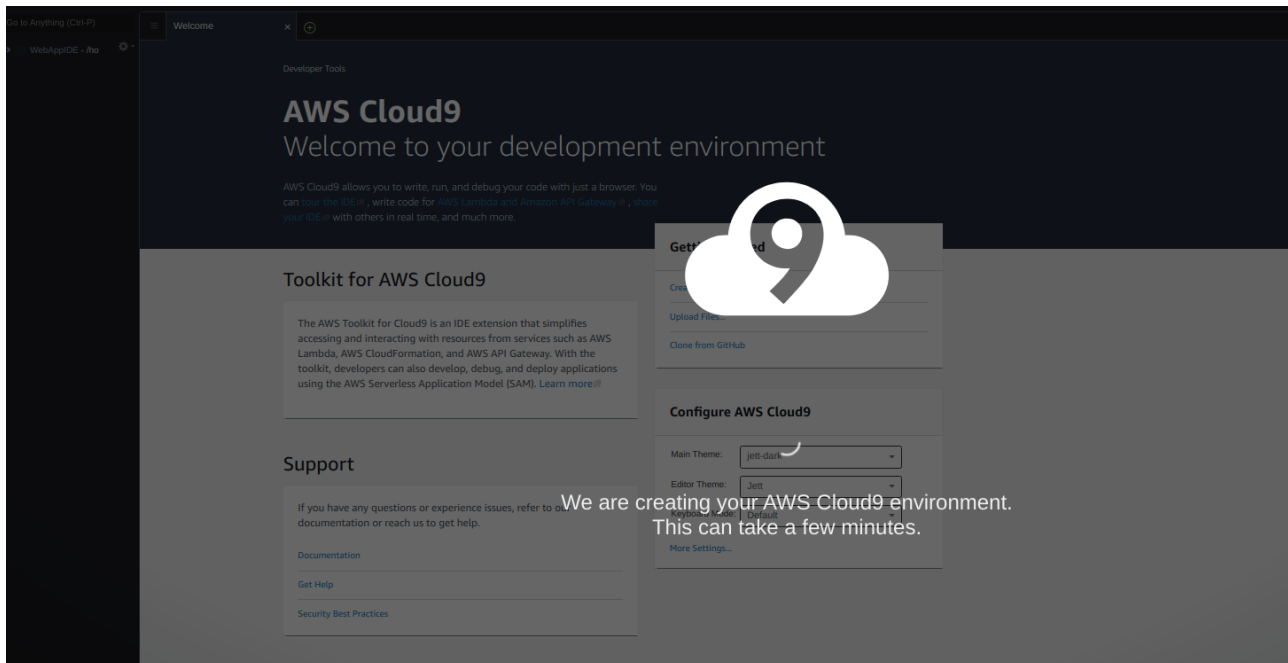
We recommend the following best practices for using your AWS Cloud9 environment

- Use **source control and backup** your environment frequently. AWS Cloud9 does not perform automatic backups.
- Perform regular **updates of software** on your environment. AWS Cloud9 does not perform automatic updates on your behalf.
- **Turn on AWS CloudTrail** in your AWS account to track activity in your environment. [Learn more](#)
- Only share your environment with **trusted users**. Sharing your environment may put your AWS access credentials at risk. [Learn more](#)

Cancel

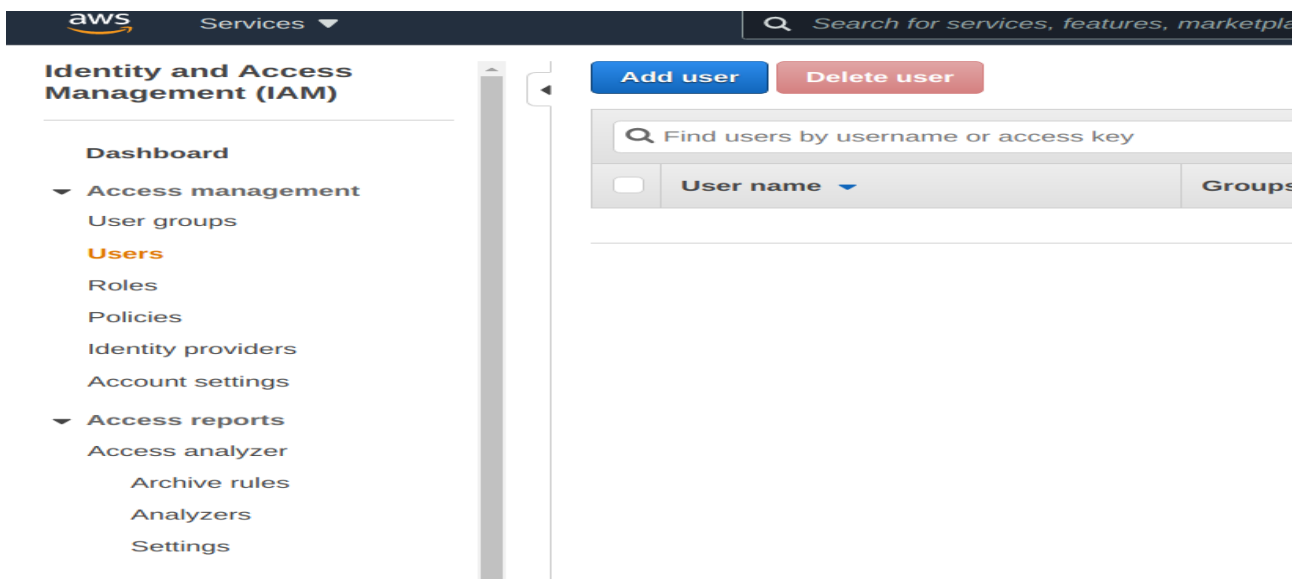
Previous step

Create environment



It will take few minutes to create aws instance for your Cloud 9 Enviornment.

7. Till that time open IAM Identity and Access Management in order to Add user In other tab.



8. Add user provide manual password if you want and click on Next permission tab.



Add user

1 2 3 4 5

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

[+ Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type* ☐ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☒ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password* ☐ Autogenerated password
☒ Custom password

☐ Show password

Require password reset ☐ User must create a new password at next sign-in
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

* Required

[Cancel](#)

[Next: Permissions](#)

9. Click on Create group

Add user

1

▼ Set permissions



Add user to group



Copy permissions from existing user



Attach existing policies directly



Get started with groups

You haven't created any groups yet. Using groups is a best-practice way to manage users' permissions by job access, or your custom permissions. Get started by creating a group. [Learn more](#)

[Create group](#)

► Set permissions boundary

10. Provide group name and click on create group.



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



Create group

Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. [Learn more](#)

Group name

Create policy

Refresh

Filter policies

Showing 669 results

| | Policy name | Type | Used as | Description |
|--------------------------|---|--------------|---------|--|
| <input type="checkbox"/> | AdministratorAccess | Job function | None | Provides full access to AWS services and resources. |
| <input type="checkbox"/> | AdministratorAccess-Amplify | AWS managed | None | Grants account administrative permissions while explicitly allowing direct access to resour... |
| <input type="checkbox"/> | AdministratorAccess-AWSElasticBeanst... | AWS managed | None | Grants account administrative permissions. Explicitly allows developers and administrators... |
| <input type="checkbox"/> | AlexaForBusinessDeviceSetup | AWS managed | None | Provide device setup access to AlexaForBusiness services |
| <input type="checkbox"/> | AlexaForBusinessFullAccess | AWS managed | None | Grants full access to AlexaForBusiness resources and access to related AWS Services |
| <input type="checkbox"/> | AlexaForBusinessGatewayExecution | AWS managed | None | Provide gateway execution access to AlexaForBusiness services |
| <input type="checkbox"/> | AlexaForBusinessLifesizeDelegatedAcc... | AWS managed | None | Provide access to Lifesize AVS devices |

Cancel

Create group

11. After that group is created click on next if u want to provide tag else click on Review for user settings and click on create user as shown in fig.

Add user

1 2 3 4 5

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

| | |
|------------------------|---|
| User name | apsit |
| AWS access type | AWS Management Console access - with a password |
| Console password type | Custom |
| Require password reset | No |
| Permissions boundary | Permissions boundary is not set |

Permissions summary

The user shown above will be added to the following groups.

| Type | Name |
|-------|---------------------------------|
| Group | WebApppsitgroup |

Tags

No tags were added.

[Cancel](#) [Previous](#) [Create user](#)

12. Now close that window and Navigate to user Groups from left pane in IAM.



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



Identity and Access Management (IAM) ✕

Introducing the new User groups experience
We've redesigned the User groups experience to make it easier to use. [Let us know what you think](#)

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analyzers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

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.

| <input type="checkbox"/> | Group name | Users | Permissions | Creation time |
|--------------------------|------------------|-------|-------------|---------------|
| <input type="checkbox"/> | WebAppapsitgroup | 1 | Not defined | 4 minutes ago |

13. click on your group name which you have created and nevigat to permission tab as shown:

Identity and Access Management (IAM) ✕

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analyzers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

IAM > User groups > WebAppapsitgroup

WebAppapsitgroup Delete

Summary Edit

| | | |
|------------------|----------------------------------|--|
| User group name | Creation time | ARN |
| WebAppapsitgroup | July 07, 2021, 12:07 (UTC+05:30) | arn:aws:iam::229296960472:group/WebAppapsitgroup |

Users **Permissions** Access advisor

Permissions policies (0) [Info](#)

You can attach up to 10 managed policies.

| <input type="checkbox"/> | Policy Name | Type | Attached entities |
|--------------------------|-------------|------|-------------------|
| No resources to display | | | |

14. Now click on Add permission and select Attach Policy after that search for Cloud9



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

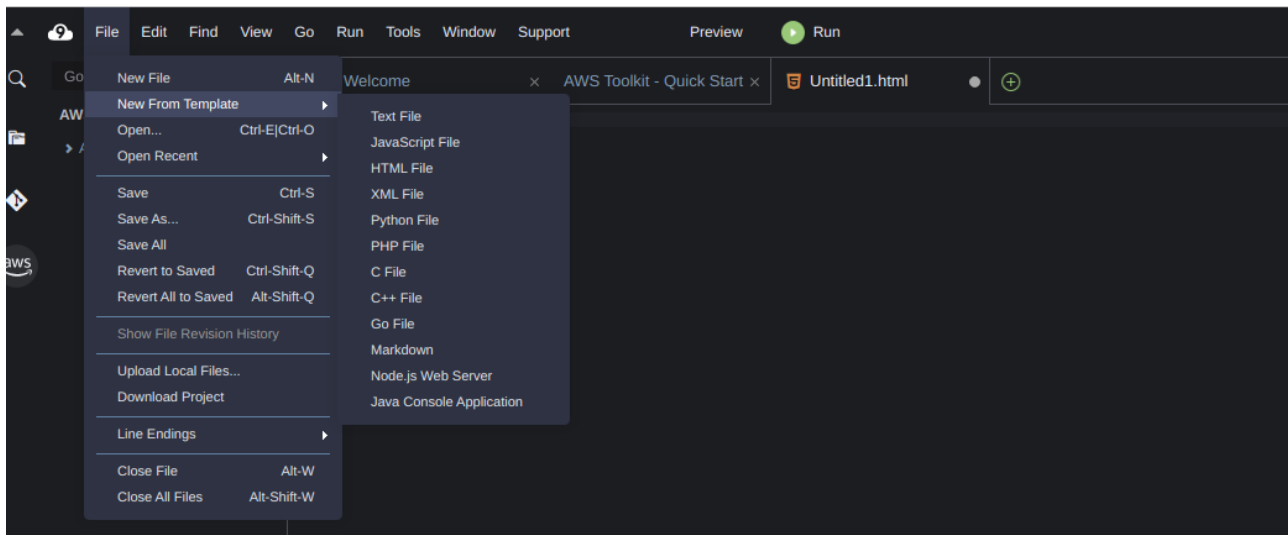
Department of Information Technology

(NBA Accredited)



```
bash - "ip-172-31-10-50.a x
ec2-user:~/environment $ git --version
git version 2.23.4
ec2-user:~/environment $ aws iam get-user
{
  "User": {
    "PasswordLastUsed": "2021-07-07T05:34:24Z",
    "CreateDate": "2021-06-03T18:03:54Z",
    "UserId": "229296960472",
    "Arn": "arn:aws:iam::229296960472:root"
  }
}
```

17. Now we will setup collaborative environment Click on File you can create new file or choose from template, here m opting html file to collaborate.



18. Edit html file and save it

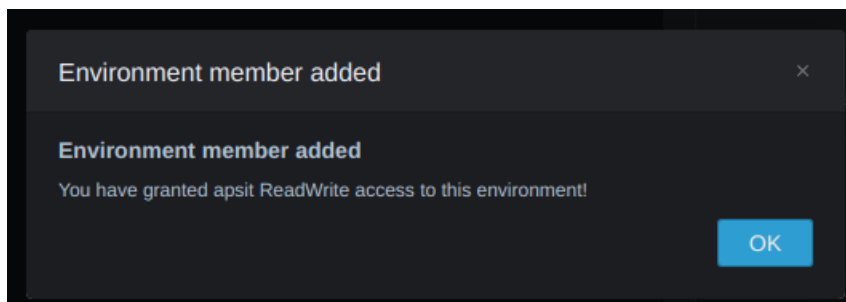
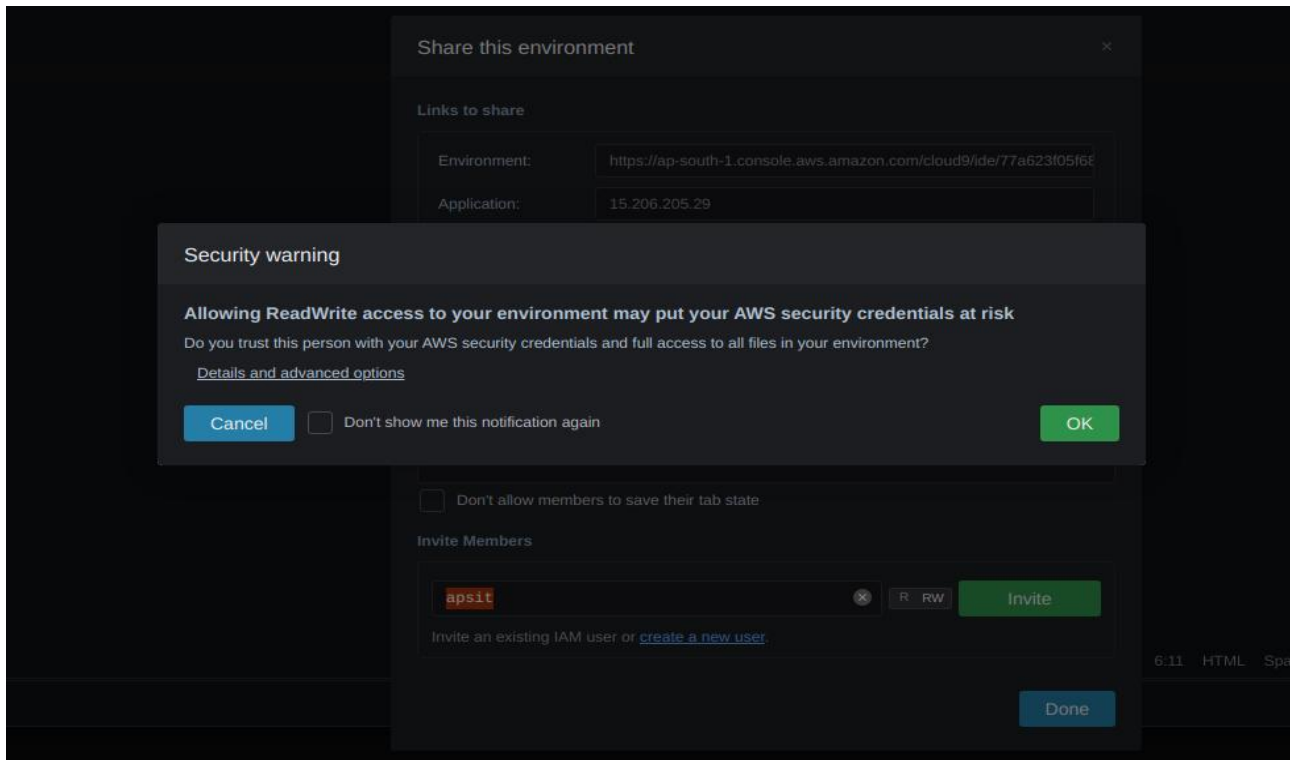


PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



```
1 <!DOCTYPE html>
2 <html>
3   <head>
4     <title> Welcome to A.P.Shah Institute of Technology </title>
5   </head>
6   <body>
7
8   </body>
9 </html>
```

19. now in order to share this file to collaborate with other members of your team click on Share option on Right Pane and username which you created in IAM before into Invite members and enable permission as RW (Read and Write) and click on Done. Click OK for Security warning.



20. Now Open your Browsers Incognito Window and login with IAM user which you configured before.



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Sign in



Root user

Account owner that performs tasks requiring unrestricted access. [Learn more](#)



IAM user

User within an account that performs daily tasks. [Learn more](#)

Account ID (12 digits) or account alias

229296960472

☐ Remember this account

Next

By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

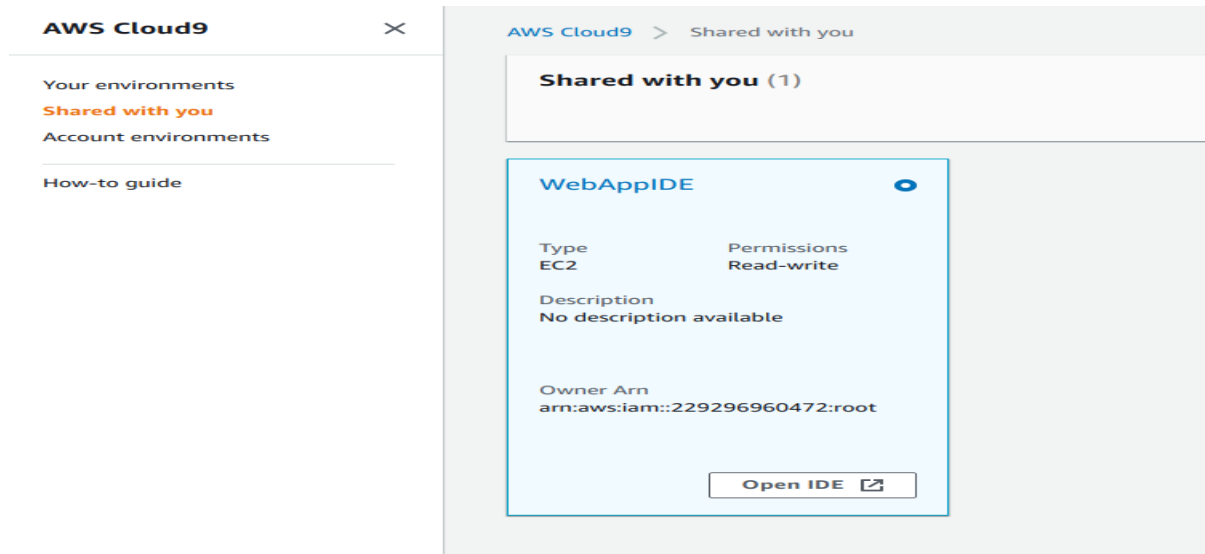
— New to AWS? —

Create a new AWS account

21. After Successful login with IAM user open Cloud9 service from dashboard services and click on shared with you environment to collaborate.



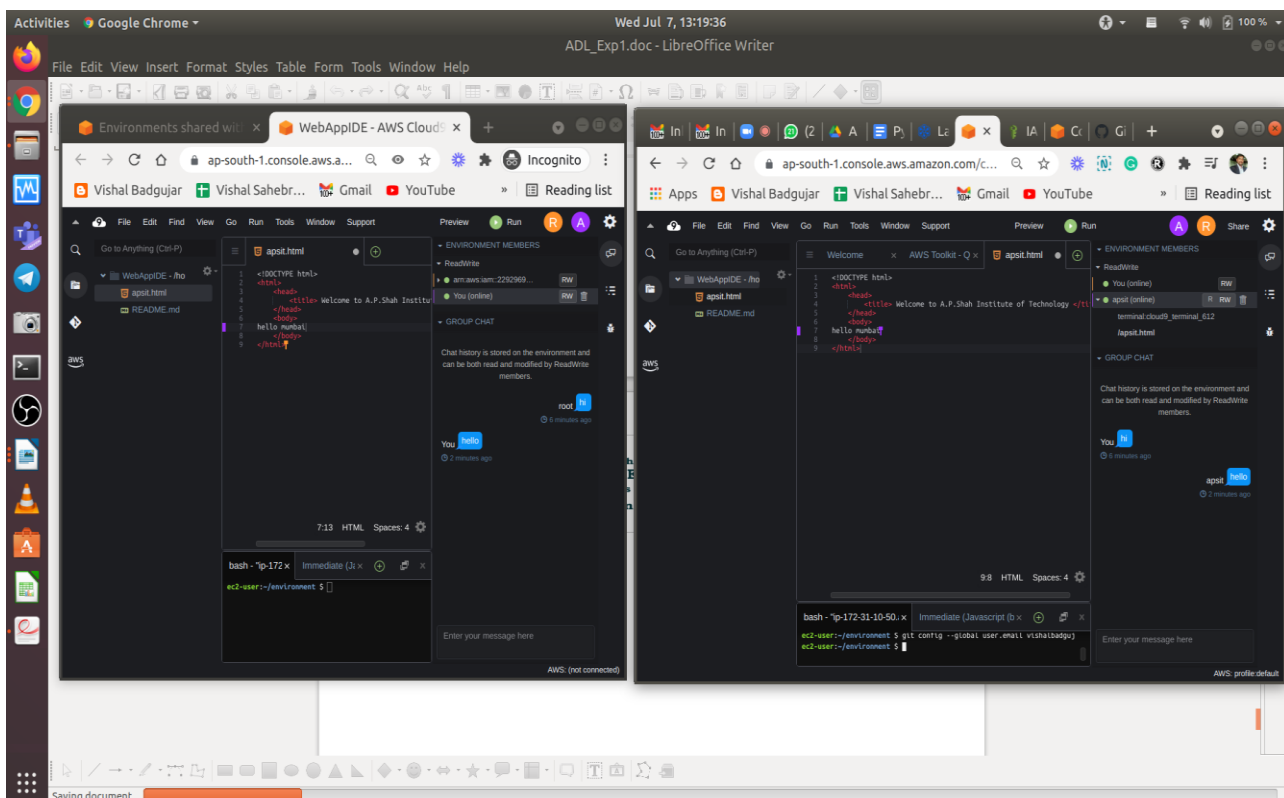
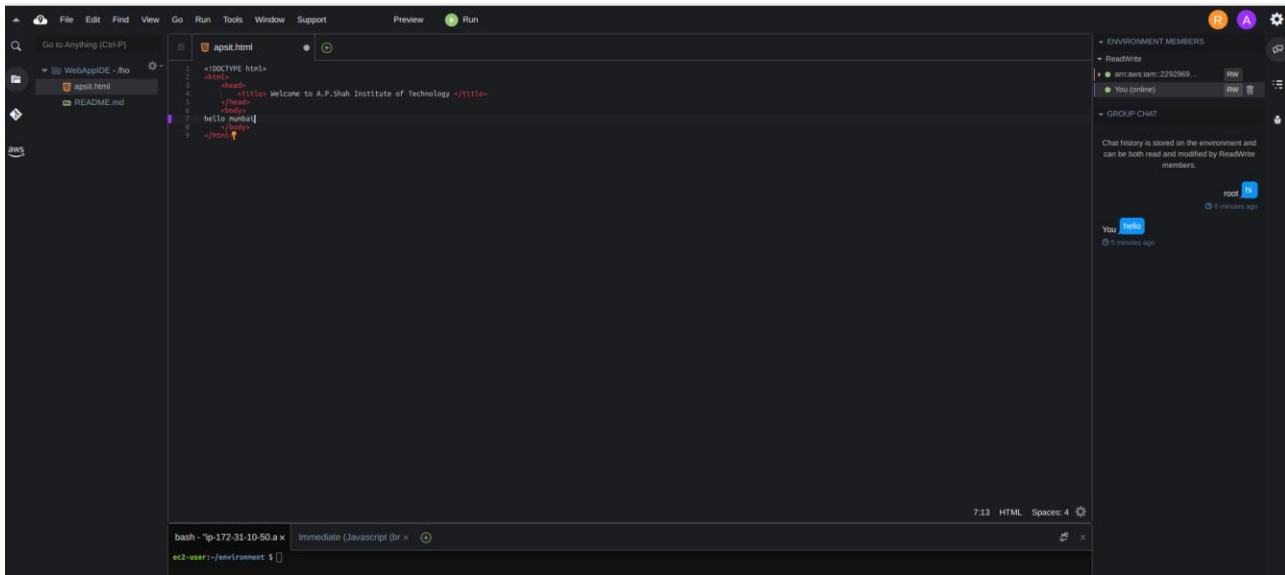
PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



22. Click on Open IDE you will same interface as your other member have to collaborate in real time, also you all within team can do group chats as shown below:



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)

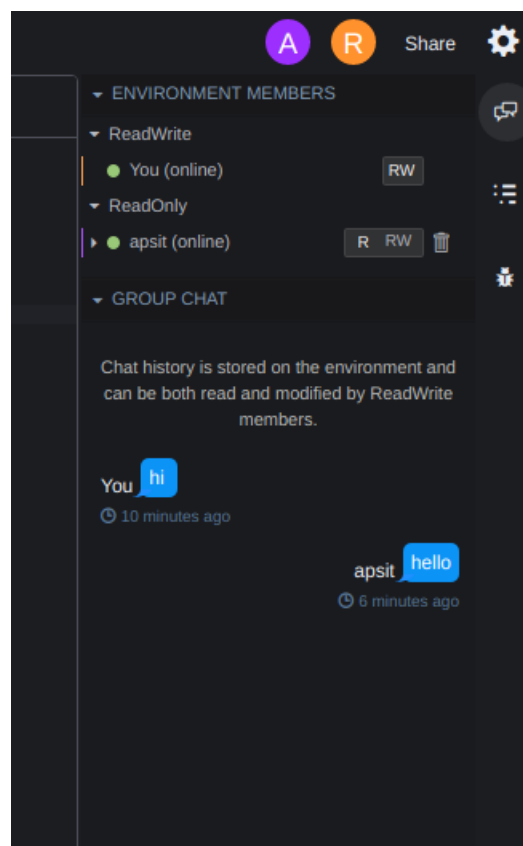




PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



24. you can also explore settings where you can update permissions of your temmates as from RW to R only or you can remove user too.



For more info related to AWS-Cloud 9 you all can refer following Docs.

<https://docs.aws.amazon.com/cloud9/latest/user-guide/aws-cloud9-ug.pdf>



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Conclusion: Write your own findings.