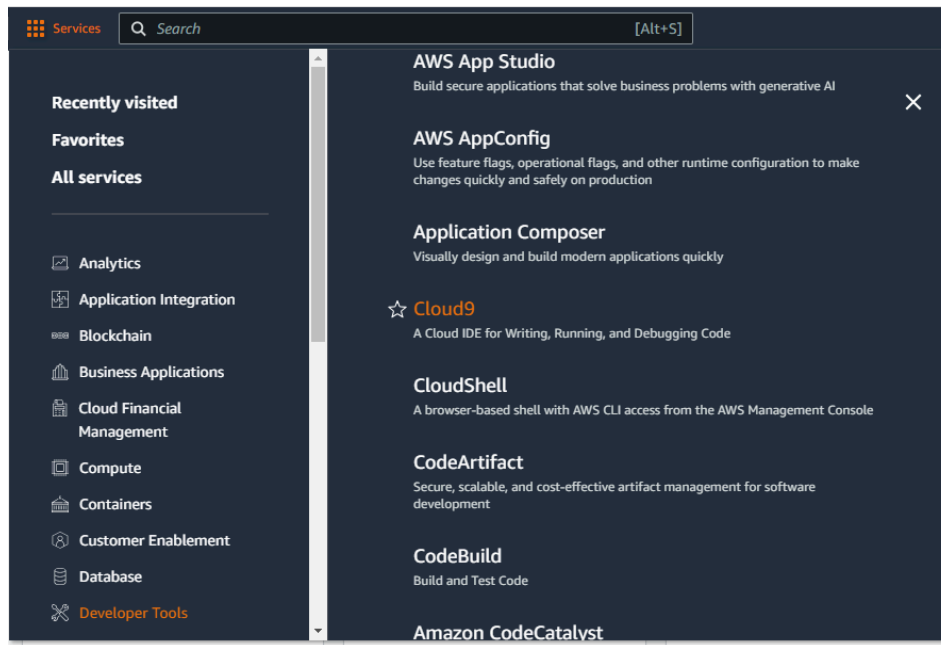


**Aim:** To understand the benefits of Cloud Infrastructure and Setup AWS Cloud9 IDE, Launch AWS Cloud9 IDE and Perform Collaboration Demonstration.

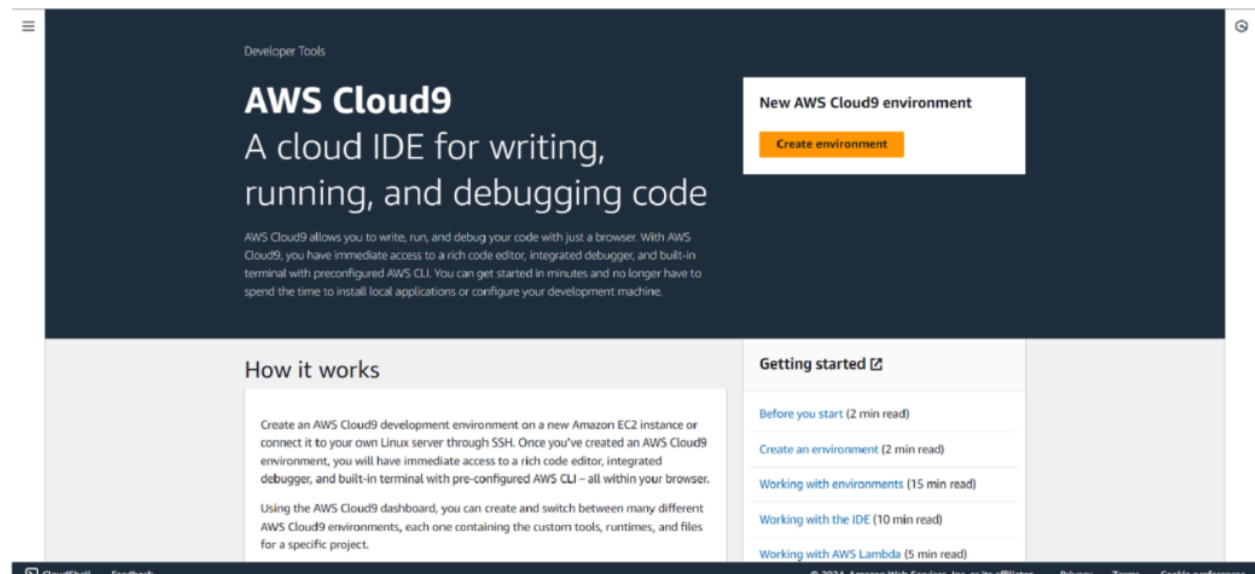
**Steps:**

**Step 1:** Set up a Cloud9 environment.

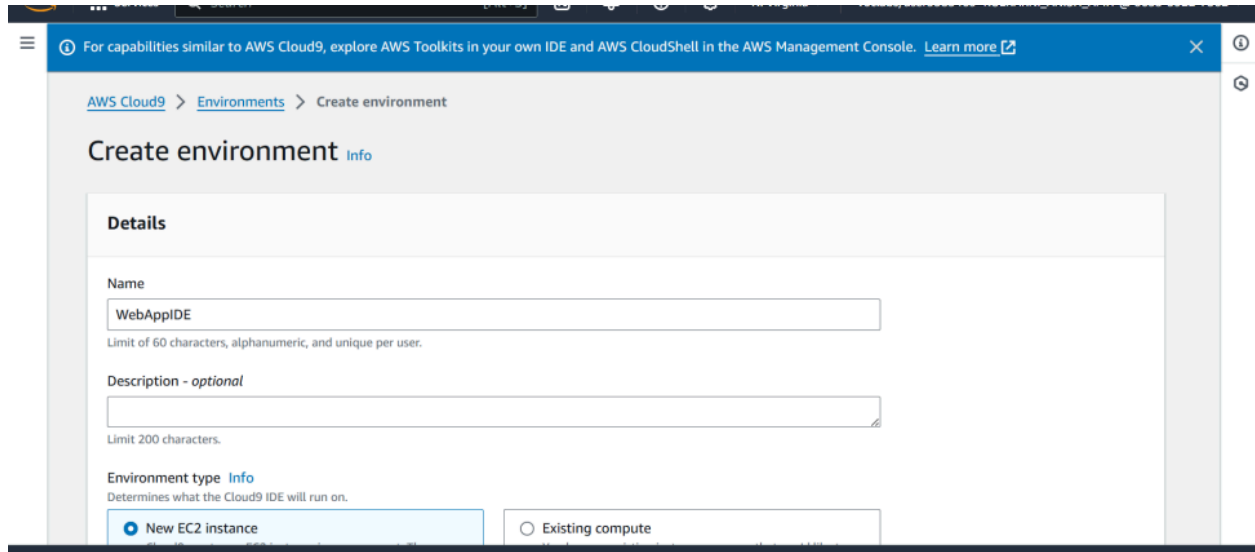
1) Search Cloud9 in the services tab and open it



2) Click on Create Environment.



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



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](#) > Create environment

## Create environment [Info](#)

**Details**

**Name**

WebAppIDE

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

**Description - optional**

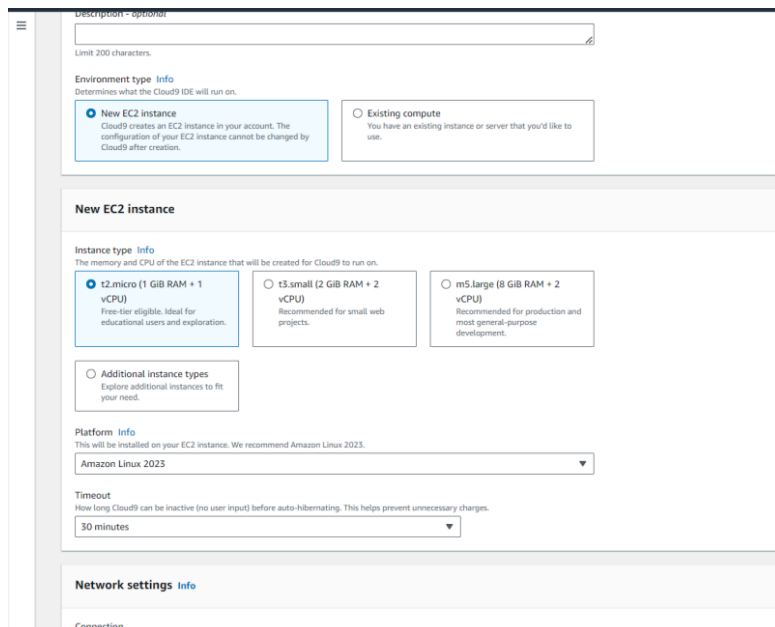
Limit 200 characters.

**Environment type** [Info](#)

Determines what the Cloud9 IDE will run on.

☒ New EC2 instance ☐ Existing compute

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



**Description - optional**

Limit 200 characters.

**Environment type** [Info](#)

Determines what the Cloud9 IDE will run on.

☒ New EC2 instance ☐ Existing compute

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

You have an existing instance or server that you'd like to use.

**New EC2 instance**

**Instance type** [Info](#)

The memory and CPU of the EC2 instance that will be created for Cloud9 to run on.

☒ 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 web projects.

☐ m5.large (8 GiB RAM + 2 vCPU)  
Recommended for production and most general-purpose development.

☐ Additional instance types  
Explore additional instances to fit your need.

**Platform** [Info](#)

This will be installed on your EC2 instance. We recommend Amazon Linux 2023.

Amazon Linux 2023

**Timeout**

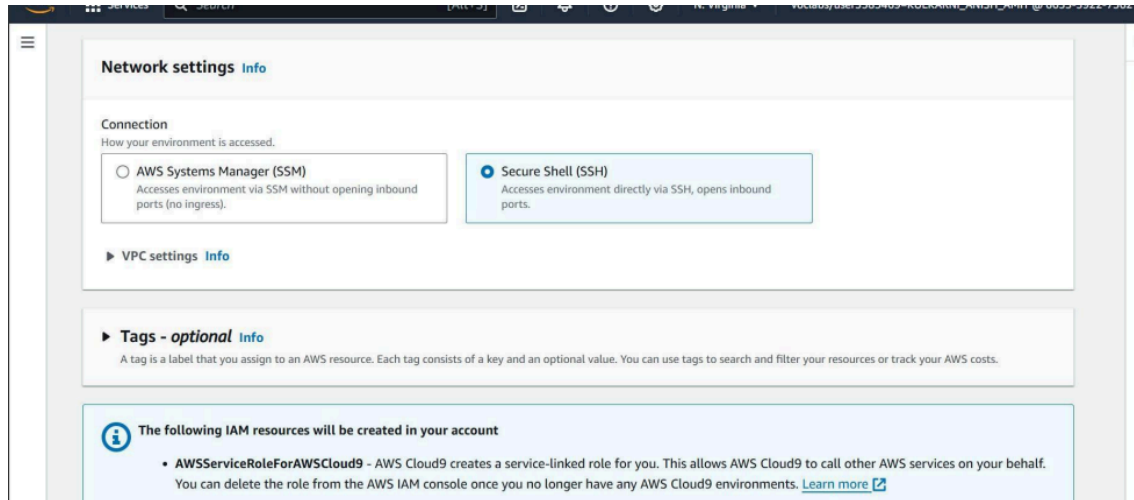
How long Cloud9 can be inactive (no user input) before auto-hibernating. This helps prevent unnecessary charges.

30 minutes

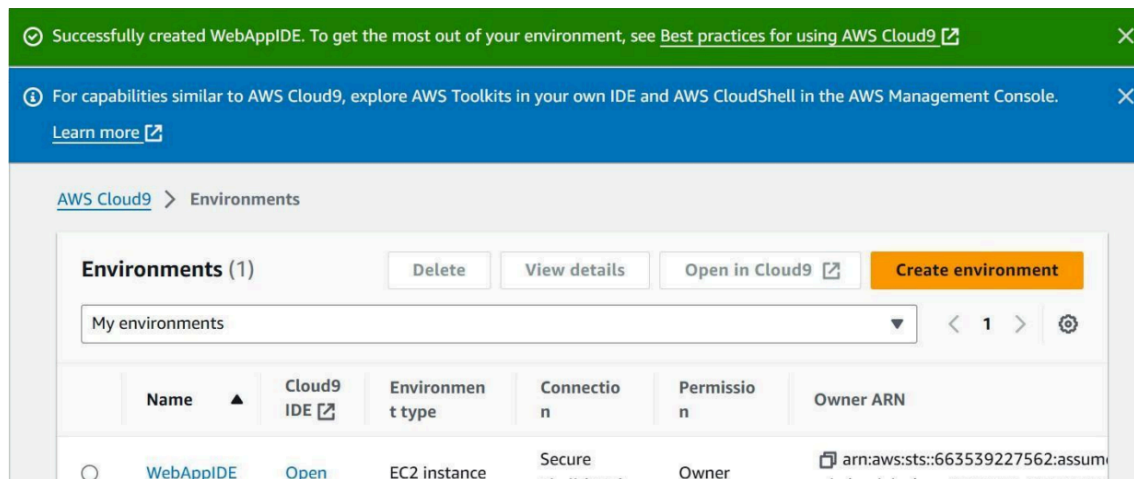
**Network settings** [Info](#)

Connection

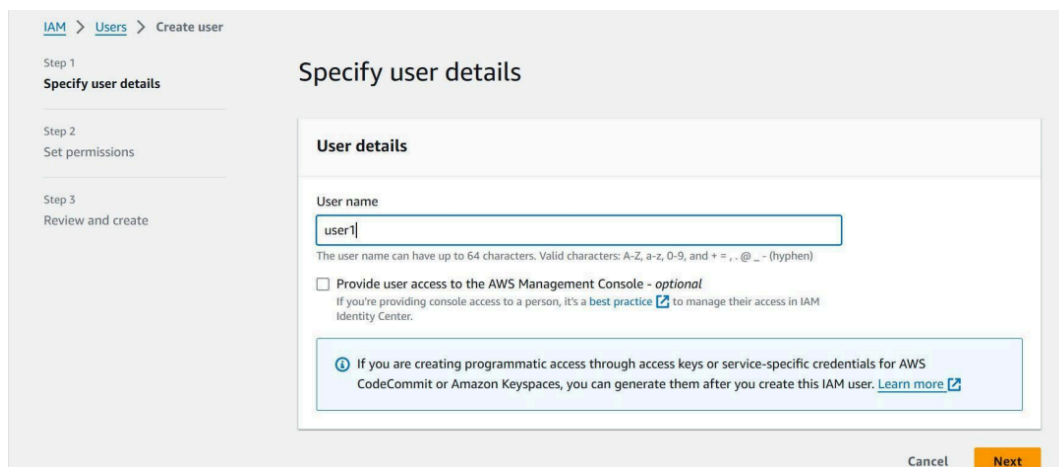
5) On the AWS Academy account, if we select AWS System Manager (SSM) in Network settings, it gives an error as the account does not have permissions to use the setting. So we select Secure Shell (SSH). After that click on Create.



6) The environment has been created.



7) Search IAM on the services search bar and open it. Click on Create User. Give a username to your user and click Next.



8) 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.

**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](#)

[Create 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.

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

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

[Specify user details](#)

Step 2  
[Set permissions](#)

Step 3  
**Review and create**

### 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 user1	Console password type None	Require password reset No
--------------------	-------------------------------	------------------------------

#### Permissions summary

< 1 >

Name	Type	Used as
No resources		

#### 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](#)

10) Go to permissions and click on Add permissions. Click on Attach Policies. Search for AWSCloud9EnvironmentMember, select it and click on Attach policies.

The screenshot displays the AWS IAM console interface. On the left, the 'Identity and Access Management (IAM)' sidebar is visible, with 'User groups' selected under 'Access management'. The main content area shows the details for 'group1'. The 'Summary' section indicates the group was created on August 04, 2024, at 16:59 UTC+05:30, with an ARN of 'arn:aws:iam::010928206130:group/group1'. The 'Permissions' tab is active, showing 'Permissions policies (0)' and an 'Add permissions' button. Below this, a search for 'AWSCloud9' yields 4 matches. The resulting table lists four AWS managed policies, with 'AWSCloud9EnvironmentMember' selected.

**group1** [Info](#) [Delete](#)

**Summary** [Edit](#)

User group name	Creation time	ARN
group1	August 04, 2024, 16:59 (UTC+05:30)	arn:aws:iam::010928206130:group/group1

[Users](#) **[Permissions](#)** [Access Advisor](#)

**Permissions policies (0)** [Info](#) [Refresh](#) [Simulate](#) [Remove](#) [Add permissions](#)

You can attach up to 10 managed policies.

**Other permission policies (1/945)** [Refresh](#)

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

[X](#) [All types](#) [4 matches](#) [<](#) [1](#) [>](#) [Settings](#)

<input type="checkbox"/>	Policy name	Type	Used as	Description
<input type="checkbox"/>	<a href="#">AWSCloud9Administrator</a>	AWS managed	None	Provides administrator access to AWS ...
<input checked="" type="checkbox"/>	<a href="#">AWSCloud9EnvironmentMember</a>	AWS managed	None	Provides the ability to be invited into A...
<input type="checkbox"/>	<a href="#">AWSCloud9SSMInstanceProfile</a>	AWS managed	None	This policy will be used to attach a rol...
<input type="checkbox"/>	<a href="#">AWSCloud9User</a>	AWS managed	None	Provides permission to create AWS Clo...