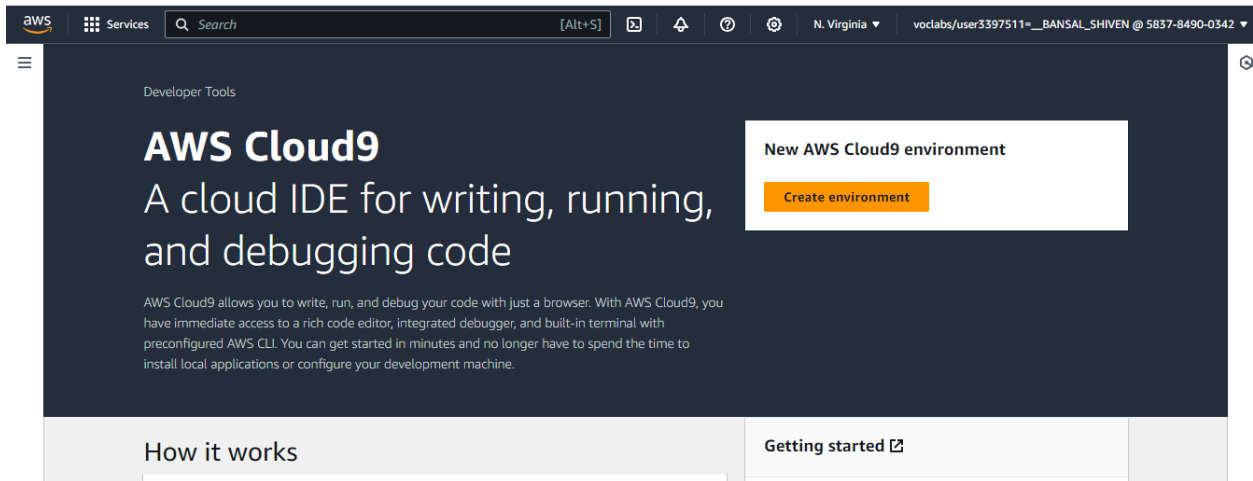
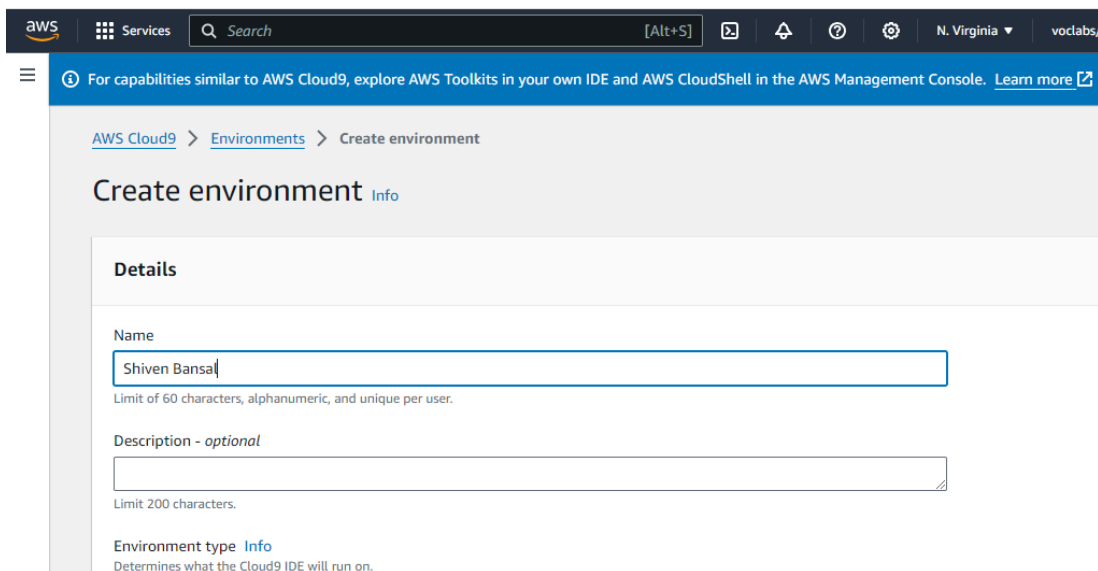


Open the AWS account and search for Cloud9. Click on create environment.



Enter the name and other required configuration for creating an environment. In network settings, using the AWS system manager gives an error while creating the environment. It states there was an error creating IAM resources needed for SSM.



## Use the Secure Shell option in Network settings

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

**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.

► **VPC settings** [Info](#)

► **Tags - optional** [Info](#)  
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

The following IAM resources will be created in your account

Once the configuration is complete, click on create environment to create a Cloud9 environment.

aws

Services

Search

[Alt+S]

N. Virginia

voclabs/user3397511=\_\_BANSAL\_SHIVEN @ 5837-8490-0342

**AWS Cloud9**

My environments

Shared with me

All account environments

Documentation

Successfully created Shiven Bansal. To get the most out of your environment, see [Best practices for using AWS Cloud9](#)

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

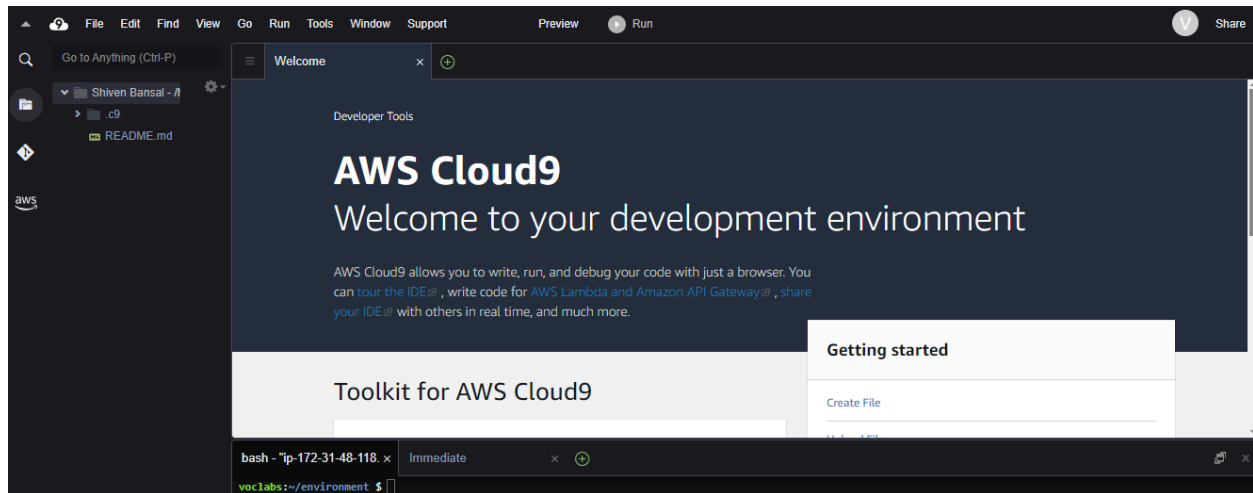
Environments (1)

Delete View details Open in Cloud9 Create environment

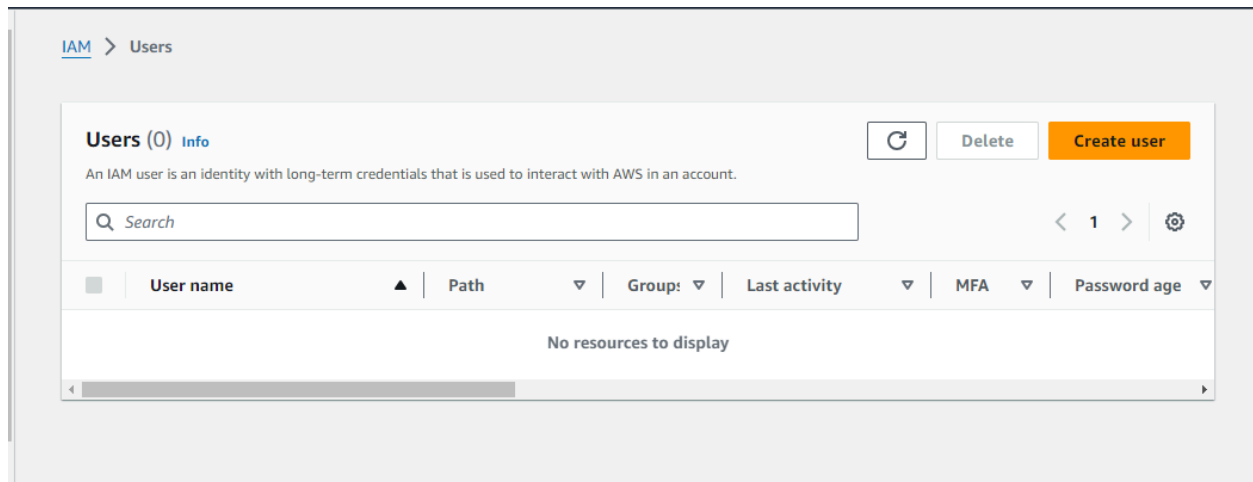
My environments

	Name ▲	Cloud9 IDE	Environment type	Connection	Permission	Owner ARN
<input type="radio"/>	<a href="#">Shiven Bansal</a>	<a href="#">Open</a>	EC2 instance	Secure Shell (SSH)	Owner	<code>arn:aws:sts::583784900342:assumed-role/voclabs/user3397511=__BANSAL_SHIVEN</code>

Click on the environment name to open the created Cloud9 Environment.



Open the aws account and search for IAM service. Then go to users tab and click on create user to create a new user.



Give the user name, select the “provide user access” checkbox. Also select the option “I want to create an IAM user”. Otherwise we will have to enable the Identity center and specify a user there.



The screenshot shows the 'Set permissions' step of the AWS IAM 'Create user' wizard. The left sidebar lists the steps: Step 1: Specify user details, Step 2: Set permissions (active), Step 3: Review and create, and Step 4: Retrieve password. The main content area is titled 'Set permissions' and includes a sub-header 'Permissions options'. There are three radio button options: 'Add user to group' (selected), 'Copy permissions', and 'Attach policies directly'. Below these options is a 'Get started with groups' section with a 'Create group' button.

**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 more](#)

[Create group](#)

Next click on add user to group. If you do not have an existing group, select create group. Then Give the group name and policies if required, and create a group.

The screenshot shows the 'Create user group' dialog box. It has a title bar 'Create user group' with a close button. The main content area has a heading '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](#)'. Below this is a section for 'User group name' with a text input field containing 'AdvanceDevOps\_3\_21\_9' and a note 'Maximum 128 characters. Use alphanumeric and '+','=','@','- ' characters. Below the input field is a section for 'Permissions policies (947)' with a 'Filter by Type' dropdown set to 'All ty...', a search bar, and a table of policies. The table has columns: Policy name, Type, Use..., and Description. The first three rows show 'AdministratorAccess' policies. At the bottom are 'Cancel' and 'Create user group' buttons.

**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 (947)**

[Refresh](#) [Create policy](#)

Filter by Type

< 1 2 3 4 5 6 7 ... 48 > [Settings](#)

<input type="checkbox"/>	Policy name <a href="#">↗</a>	Type	Use...	Description
<input type="checkbox"/>	<a href="#">+ AdministratorAccess</a>	AWS managed ...	None	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

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

Once the group is created, select the group in which the user should be added.

✔ AdvanceDevOps\_3\_21\_9 user group created.

Users

Create user

Step 1

[Specify user details](#)

Step 2

[Set permissions](#)

Step 3

**Review and create**

Step 4

Retrieve password

## 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

Shiven

Console password type

Custom password

Require password reset

No

**Permissions summary**

< 1 >

Name	Type	Used as
<a href="#">AdvanceDevOps_21_3_9</a>	Group	Permissions group
<a href="#">AdvanceDevOps_3_21_9</a>	Group	Permissions group
<a href="#">AdvDevOpsLab_9</a>	Group	Permissions group

Recheck all the configuration and details of the user and click on create user. Then you will see this page.

✔ User created successfully

View user

✕

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Step 1

[Specify user details](#)

Step 2

[Set permissions](#)

Step 3

[Review and create](#)

Step 4

**Retrieve password**

## Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

**Console sign-in details**

Email sign-in instructions

Console sign-in URL

<https://022499016110.signin.aws.amazon.com/console>

User name

Shiven

Console password

\*\*\*\*\* [Show](#)

Cancel

Download .csv file

Return to users list

After creation of the user, go to the user groups tab and select the group in which the user has been added. Navigate to the permissions tab. Click on add permissions and attach policy.

The screenshot shows the AWS IAM console interface. On the left is a navigation sidebar with 'Identity and Access Management (IAM)' selected. The main content area shows the 'AdvanceDevOps\_3\_21\_9' user group. The 'Permissions' tab is active, displaying 'Permissions policies (0)'. A search bar and a 'Filter by Type' dropdown are visible. Buttons for 'Add permissions', 'Simulate', and 'Remove' are present.

Search for the “AWSCloud9EnvironmentMember” policy and attach it.

The screenshot shows the 'Attach permission policies to AdvanceDevOps\_3\_21\_9' dialog in the AWS IAM console. It displays 'Current permissions policies (0)' and 'Other permission policies (945)'. A search bar and a 'Filter by Type' dropdown are visible. Below is a table of available policies.

<input type="checkbox"/>	Policy name	Type	Used as	Description
<input type="checkbox"/>	AdministratorAccess	AWS managed - job function	None	Provides full access to AWS services an...
<input type="checkbox"/>	AdministratorAccess-Amp...	AWS managed	None	Grants account administrative permis...
<input type="checkbox"/>	AdministratorAccess-AWS...	AWS managed	None	Grants account administrative permis...
<input type="checkbox"/>	AlexaForBusinessDeviceS...	AWS managed	None	Provide device setup access to AlexaFo...

aws

Services

Search

[Alt+S]

Global

VedantD

Attach permission policies to AdvanceDevOps\_3\_21\_9

► Current permissions policies (0)

Other permission policies (1/945)

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

cloud9

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 ...
<input checked="" type="checkbox"/>	<a href="#">AWSCloud9EnvironmentMe...</a>	AWS managed	None	Provides the ability to be invited into ...
<input type="checkbox"/>	<a href="#">AWSCloud9SSMInstanceP...</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...

Cancel

Attach policies

aws

Services

Search

[Alt+S]

Global

VedantD

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

✔ Policies attached to this user group.

Summary

User group name

AdvanceDevOps\_3\_21\_9

Creation time

August 07, 2024, 09:33 (UTC+05:30)

ARN

arn:aws:iam::022499016110:group/AdvanceDevOps\_3\_21\_9

Users (3)

Permissions

Access Advisor

Permissions policies (1)

Info

Simulate

Remove

Add permissions

You can attach up to 10 managed policies.

Search

Filter by Type

All types

< 1 >

	Policy name	Type	Attached entities
<input type="checkbox"/>	<a href="#">AWSCloud9EnvironmentMe...</a>	AWS managed	3