

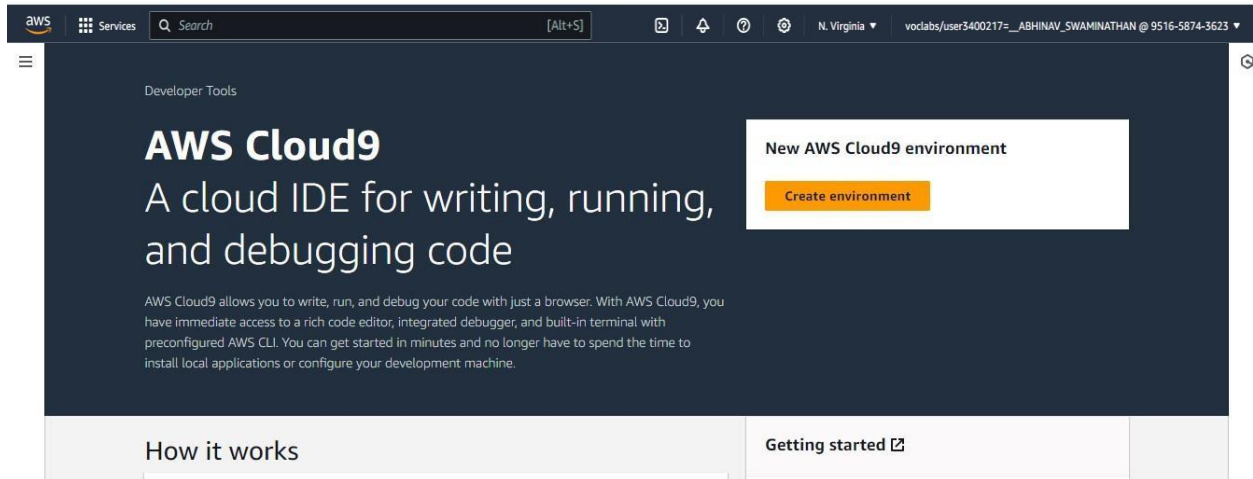
Name: Laukik Padgaonkar

D15C

Roll No:37

Experiment No. 1B

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.

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

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.

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.

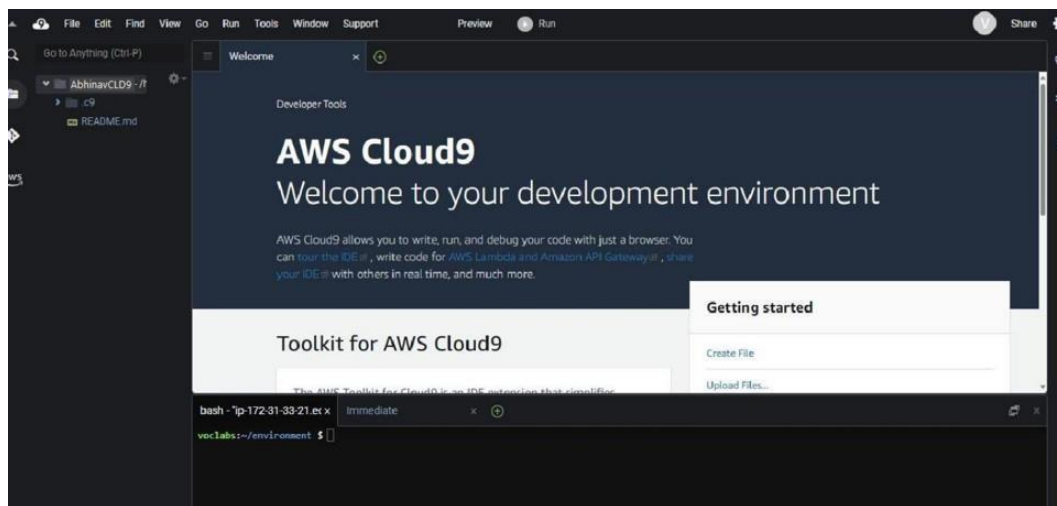
[VPC settings](#) [Info](#)

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.

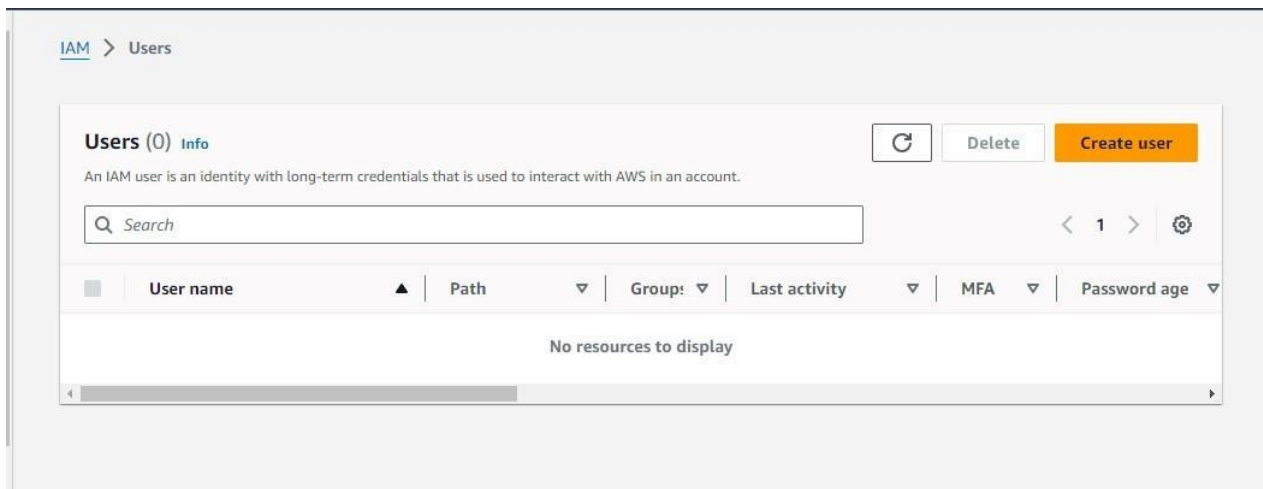
 The following IAM resources will be created in your account

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

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 'Specify user details' step of the 'Create user' wizard in the AWS IAM console. On the left, a sidebar lists the steps: 'Step 1: Specify user details' (active), 'Step 2: Set permissions', and 'Step 3: Review and create'. The main content area is titled 'Specify user details' and contains a 'User details' section. It features a 'User name' text input field with the value 'laukik'. Below the input, a note states: 'The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)'. There is an unchecked checkbox labeled 'Provide user access to the AWS Management Console - optional', with a sub-note: 'If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.' At the bottom of the form, there is an information box with a blue icon and text: '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'. At the bottom right of the form, there are 'Cancel' and 'Next' buttons.

- ☒ 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.



Are you providing console access to a person?

User type

- ☐ Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.
- ☒ I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

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



IAM > Users > Create user

Step 1

[Specify user details](#)

Step 2

Set permissions

Step 3

[Review and create](#)

Step 4

[Retrieve password](#)

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

[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.

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.

AdvanceDevOps

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

Permissions policies (947)

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 per
<input type="checkbox"/>	AdministratorAcce...	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.

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 Abhinav	Console password type Custom password	Require password reset No
----------------------	--	------------------------------

Permissions summary

Name	Type	Used as
AdvanceDevOps_1	Group	Permissions group
AdvanceDevOps_2	Group	Permissions group
AdvDevOpsLab_3	Group	Permissions group

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 displays the AWS IAM console interface. On the left, the 'Identity and Access Management (IAM)' sidebar is visible, containing a search bar and a navigation menu with categories like 'Access management' and 'Access reports'. The main content area shows the details for the 'AdvanceDevOps_1' user group. The 'Permissions' tab is active, displaying a section for 'Permissions policies (0)' with buttons for 'Simulate', 'Remove', and 'Add permissions'. A search bar and a 'Filter by Type' dropdown are also present in this section.

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

IAM > User groups > AdvanceDevOps_1

AdvanceDevOps_1 Info

Delete

Summary Edit

User group name	Creation time	ARN
	August 07, 2024, 09:33 (UTC+05:30)	arn:aws:iam::022499016110:group/AdvanceDevOps_1

Users (3) | Permissions | Access Advisor

Permissions policies (0) Info

You can attach up to 10 managed policies.

Refresh Simulate Remove Add permissions ▼

Search Filter by Type

All types ▼

< 1 > ⚙

Search for the “AWSCloud9EnvironmentMember” policy and attach it.

Attach permission policies to AdvanceDevOps_1

► **Current permissions policies (0)**

Other permission policies (945)

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: All types

<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...

► **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.

Filter by Type: All types

cloud9 X 4 matches

<input type="checkbox"/>	Policy name	Type	Used as	Description
<input type="checkbox"/>	AWSCloud9Administrator	AWS managed	None	Provides administrator access to AWS ...
<input checked="" type="checkbox"/>	AWSCloud9Environment...	AWS managed	None	Provides the ability to be invited into ...
<input type="checkbox"/>	AWSCloud9SSMInstanceP...	AWS managed	None	This policy will be used to attach a rol...
<input type="checkbox"/>	AWSCloud9User	AWS managed	None	Provides permission to create AWS Clo...

Cancel Attach policies

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_21_9

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

ARN: arn:aws:iam::022499016110:group/AdvanceDevOps_21_9

Users (3) | **Permissions** | Access Advisor

Permissions policies (1) Info

You can attach up to 10 managed policies.

Filter by Type: All types

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