

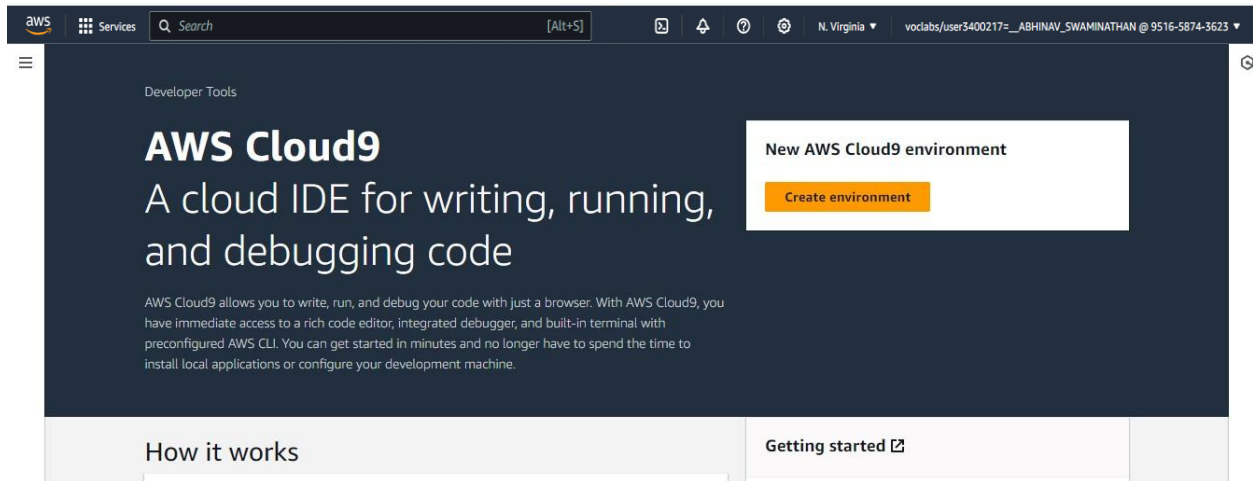
Name: Abhinav Swaminathan

D15C

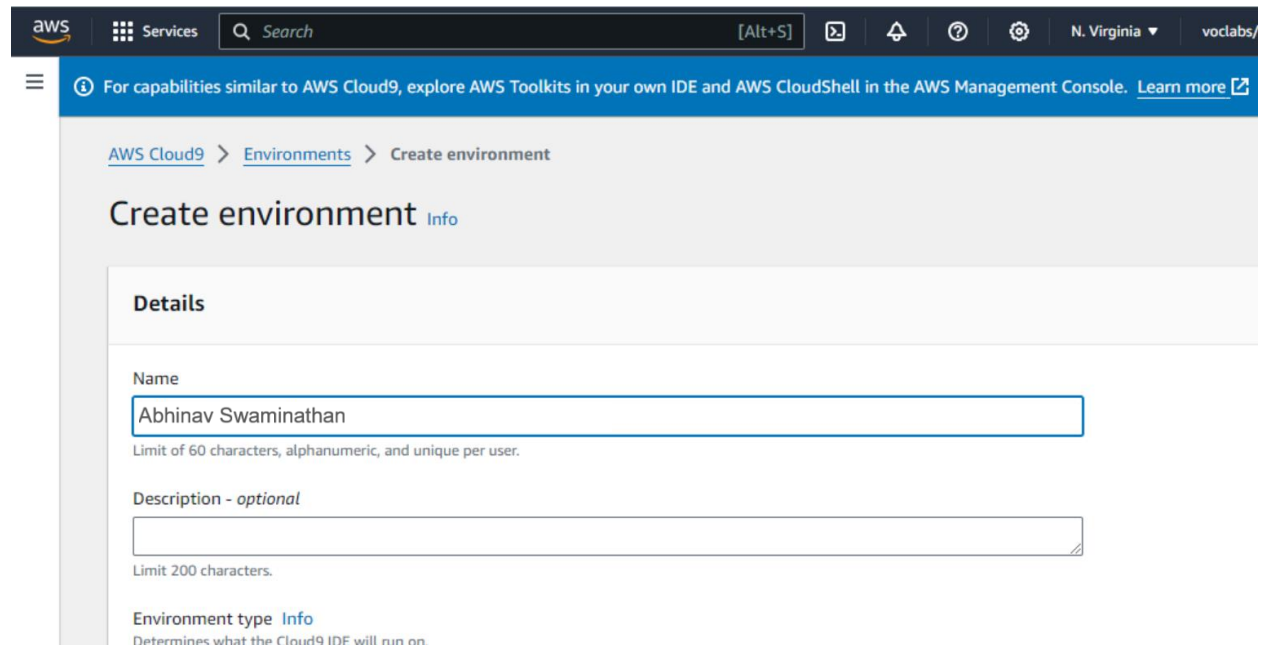
Roll No:01

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.



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 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

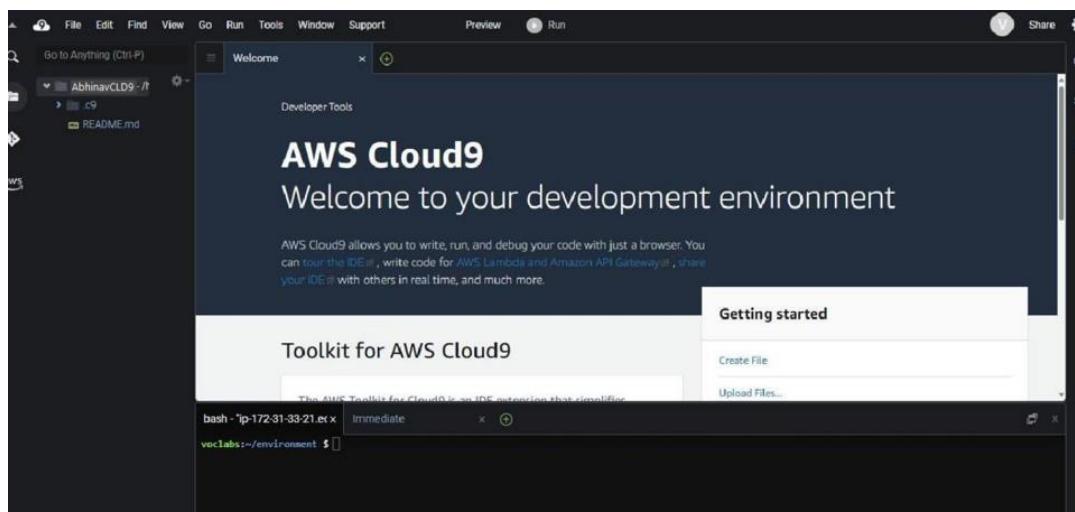
Environments (1)

Delete View details Open in Cloud9 **Create environment**

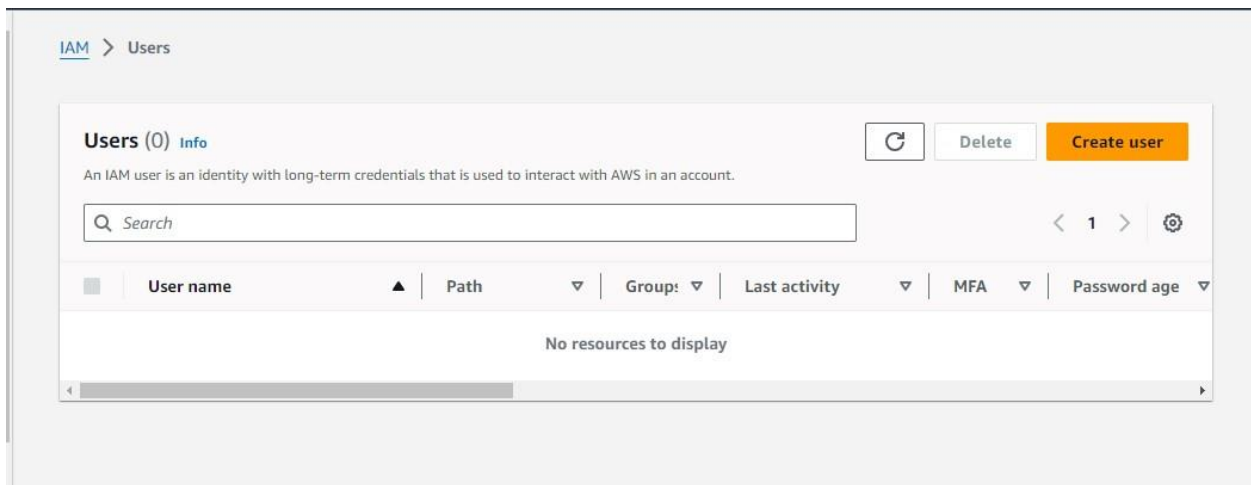
My environments

	Name	Cloud9 IDE	Environment type	Connection	Permission	Owner ARN
<input type="radio"/>	Abhinav Swaminathan	Open	EC2 instance	Secure Shell (SSH)	Owner	arn:aws:sts::583784900342:assumed-role/voclabs/user3397511:__Abhinav Swaminathan

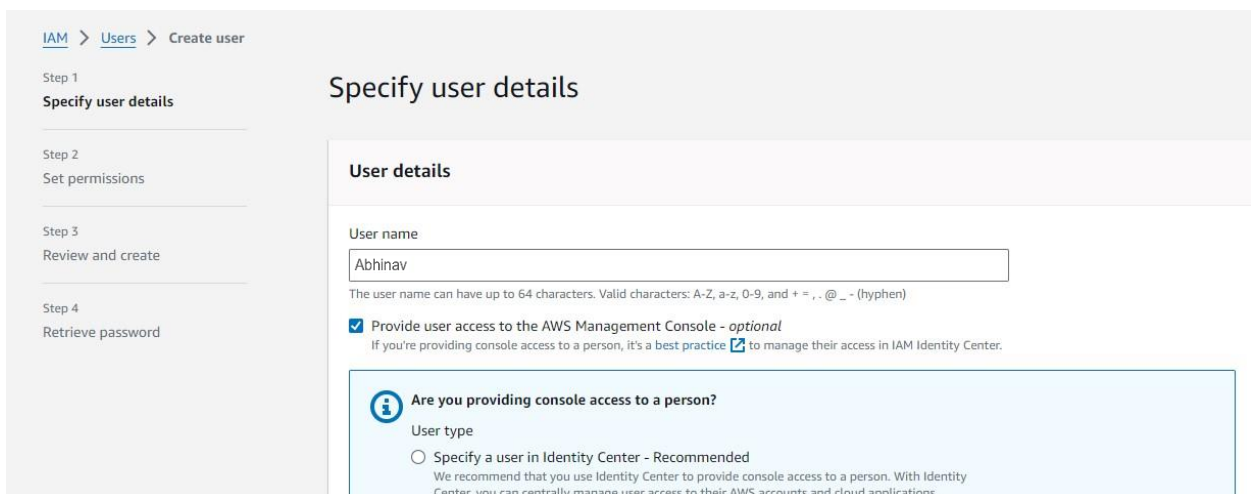
Click on the environment name to open the created Cloud9 Environment.



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.



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)

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

< 1 >

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

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

✔ User created successfully

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

View user

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

Abhinav

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.

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

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

ARN

arn:aws:iam::022499016110:group/AdvanceDevOps_1

Users (3)

Permissions

Access Advisor

Permissions policies (0)

Info

Refresh

Simulate

Remove

Add permissions

You can attach up to 10 managed policies.

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

Search: cloud9 All types 4 matches

Policy name	Type	Used as	Description
AdministratorAccess	AWS managed - job function	None	Provides full access to AWS services an...
AdministratorAccess-Amp...	AWS managed	None	Grants account administrative permis...
AdministratorAccess-AWS...	AWS managed	None	Grants account administrative permis...
AlexaForBusinessDeviceS...	AWS managed	None	Provide device setup access to AlexaFo...
AWSCloud9Environment...	AWS managed	None	Provides the ability to be invited into ...
AWSCloud9SSMInstanceP...	AWS managed	None	This policy will be used to attach a rol...
AWSCloud9User	AWS managed	None	Provides permission to create AWS Clo...

► 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

Search: cloud9 All types 4 matches

Policy name	Type	Used as	Description
AWSCloud9Administrator	AWS managed	None	Provides administrator access to AWS ...
AWSCloud9Environment...	AWS managed	None	Provides the ability to be invited into ...
AWSCloud9SSMInstanceP...	AWS managed	None	This policy will be used to attach a rol...
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_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

You can attach up to 10 managed policies.

Filter by Type

Search: All types 1

Policy name	Type	Attached entities
AWSCloud9EnvironmentMe...	AWS managed	3