

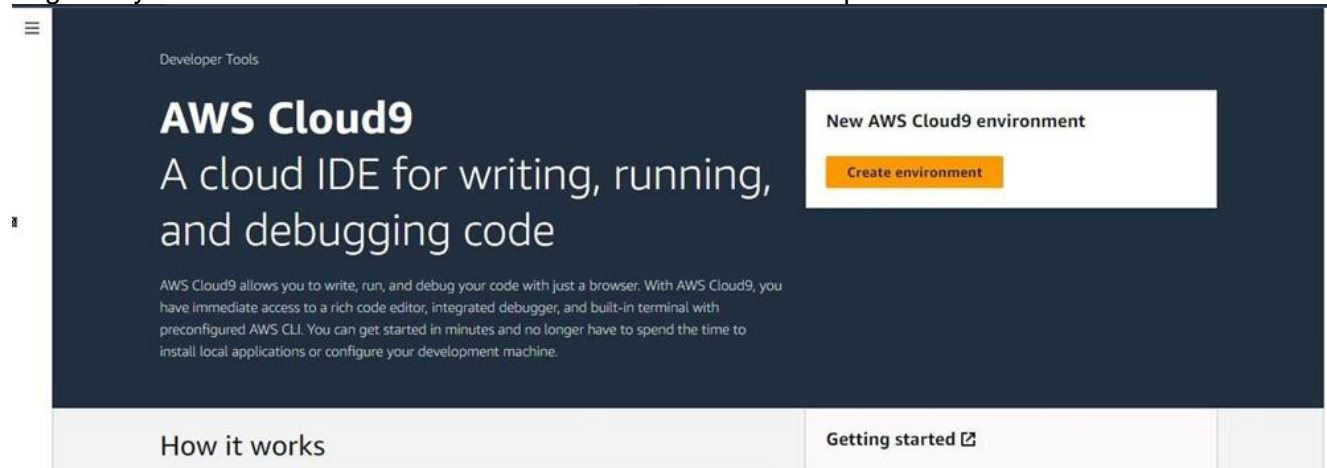
Name: Nishant S Khetal

D15C

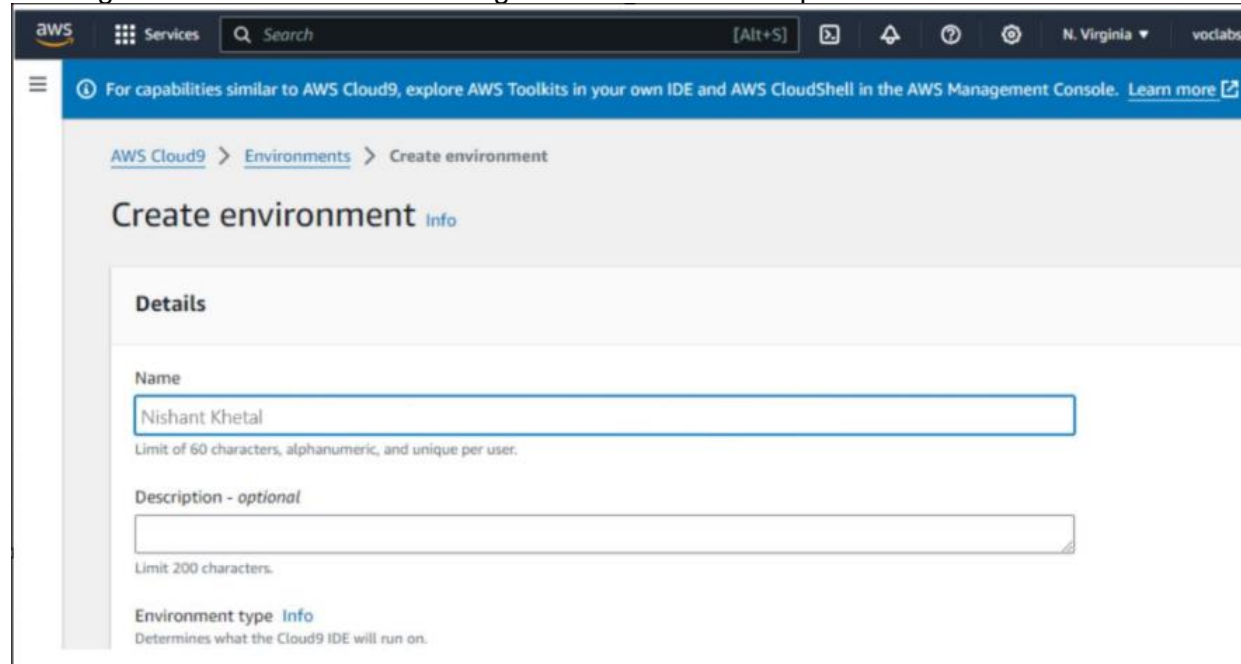
Roll No:24

Experiment No. 1B

Log in to your AWS account and search for Cloud9. Select the option to create a new environment.



Provide the name and other necessary configurations to create the environment. When configuring network settings, attempting to use the AWS Systems Manager may result in an error. The error message indicates a failure in creating the IAM resources required 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:

After completing the configuration, click on 'Create Environment' to set up the 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](#) [↗](#)

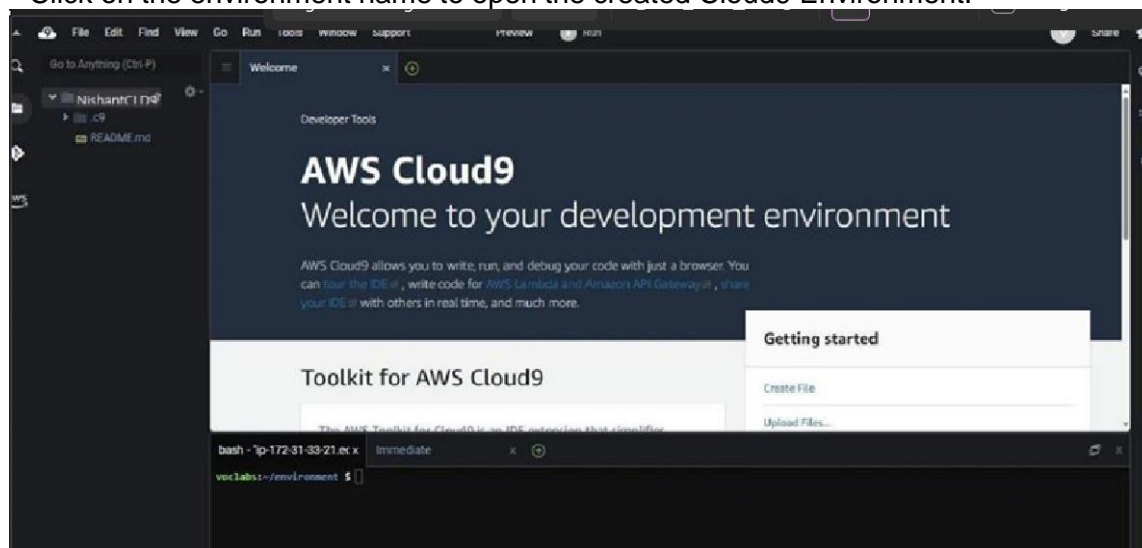
[AWS Cloud9](#) > Environments

Environments (1) Delete View details Open in Cloud9 Create environment

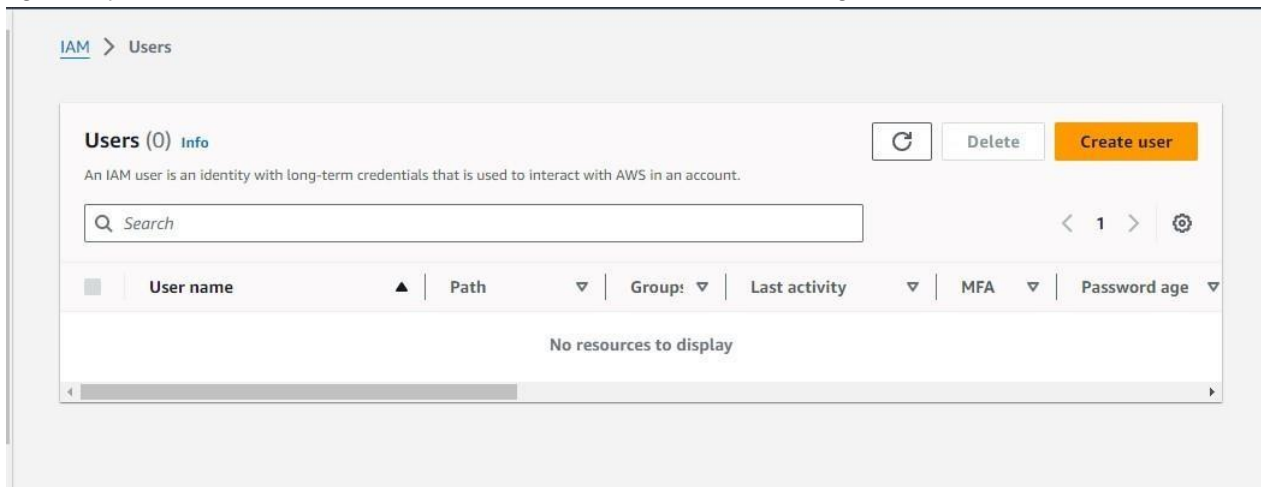
My environments

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

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

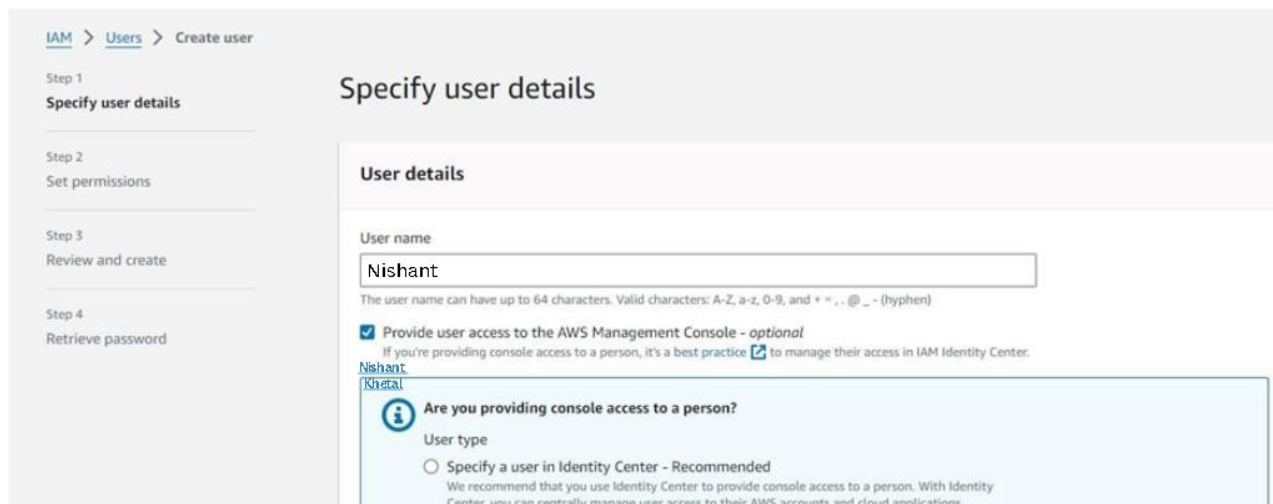


Log in to your AWS account and search for the IAM service. Navigate to the 'Users' tab and click on



'Create User' to add 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.



- ☒ 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 permissions by job function. [AWS recommends creating groups instead of users.](#) [Learn more](#) [☑](#)

[Create group](#)

Next, click on 'Add User to Group.' If no existing group is available, choose 'Create Group.' Assign a name to the group, select any necessary policies, and then create the 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

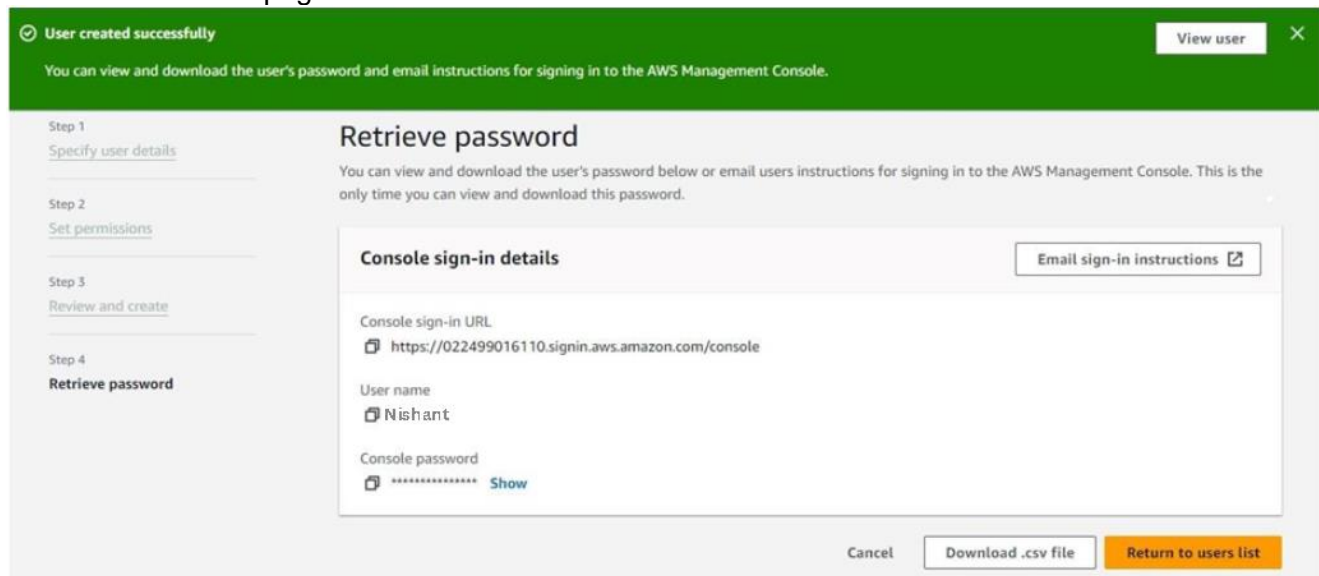
User name Nishant	Console password type Custom password	Require password reset No
----------------------	--	------------------------------

Permissions summary

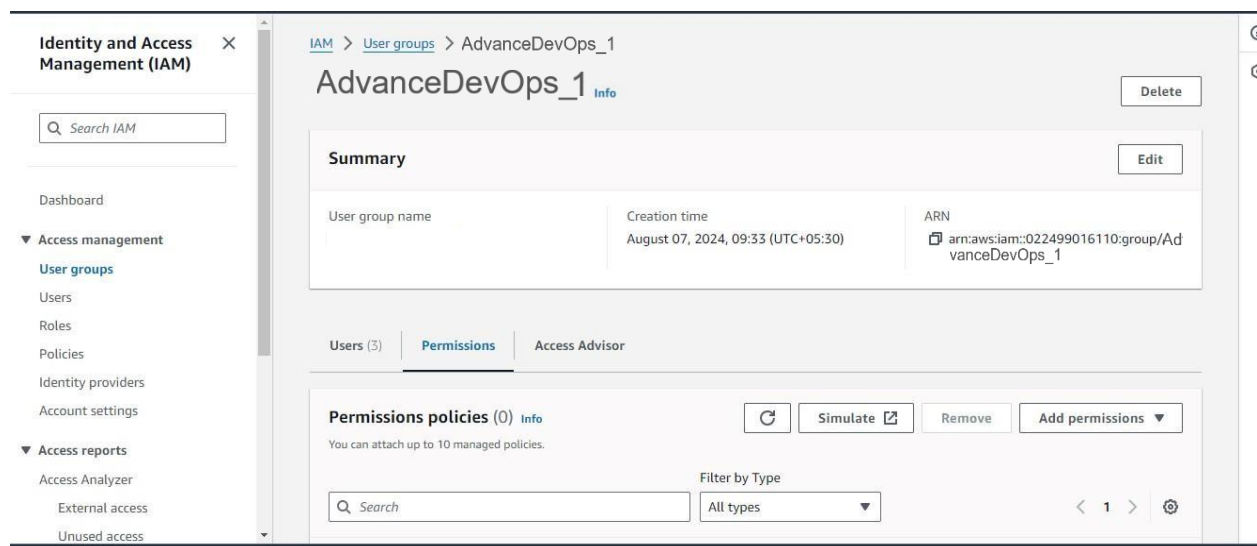
< 1 >

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

Review all the configurations and user details, then click on 'Create User.' Afterward, you will be directed to the next page.



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.




Search for the 'AWSCloud9EnvironmentMember' policy and attach it.


IAM > User groups > AdvanceDevOps_3_21_9 > Add permissions





Attach permission policies to AdvanceDevOps_1

► Current permissions policies (0)


Other permission policies (945) Nishant 

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


Search Filter by Type All types < 1 2 3 4 5 6 7 ... 48 > 





<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.

Search X Filter by Type All types 4 matches < 1 > 

<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...

Identity and Access Management (IAM) X

Search IAM


Dashboard

▼ Access management

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


▼ Access reports

- Access Analyzer
- External access
- Unused access





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)    

You can attach up to 10 managed policies.

Search Filter by Type All types < 1 > 

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