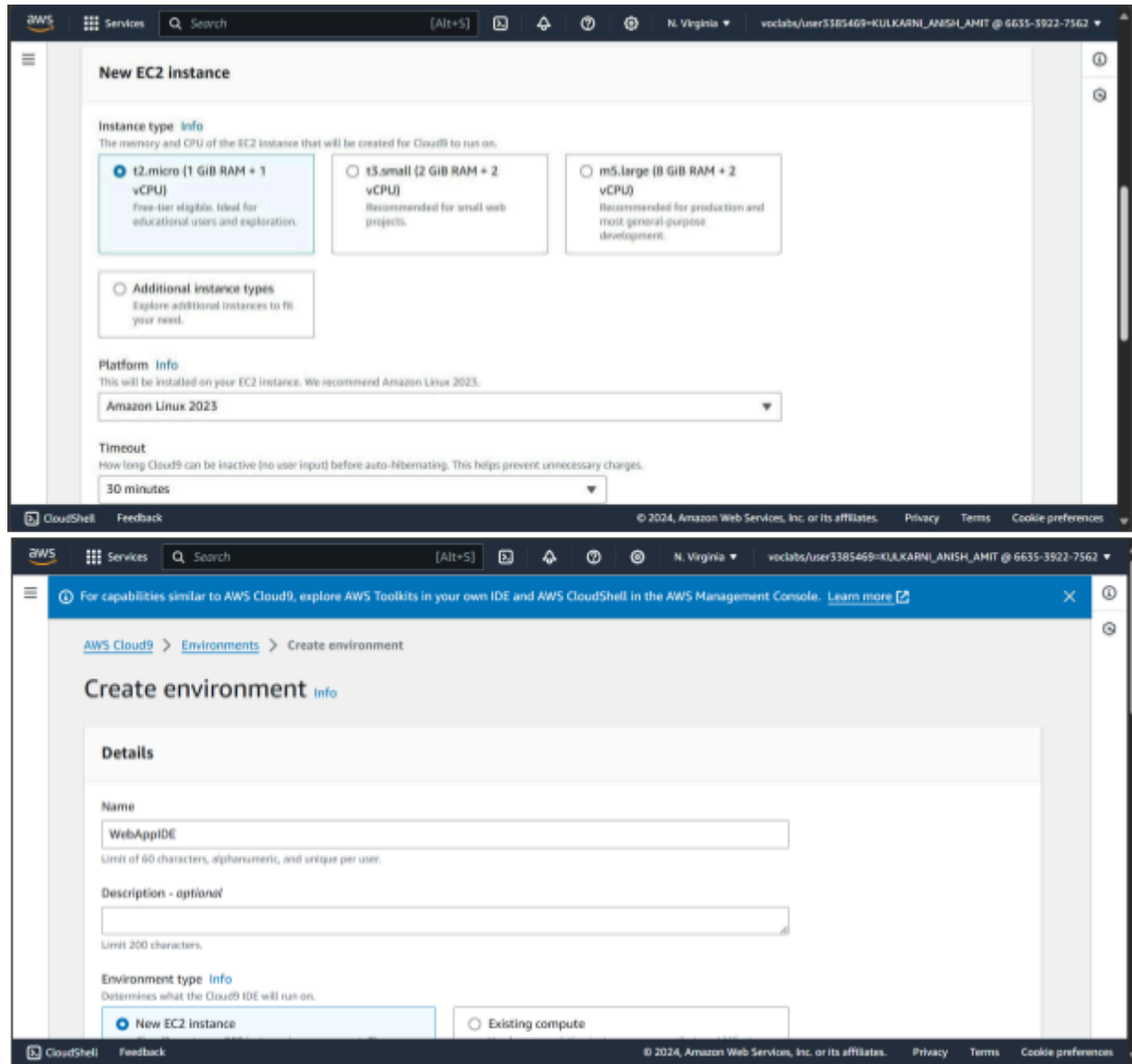


Aim: To understand the benefits of Cloud Infrastructure and Setup AWS Cloud9 IDE, Launch AWS Cloud9 IDE and Perform Collaboration Demonstration.

Step 1:



The image displays two screenshots from the AWS Management Console, illustrating the steps to create a new EC2 instance and then a new AWS Cloud9 environment.

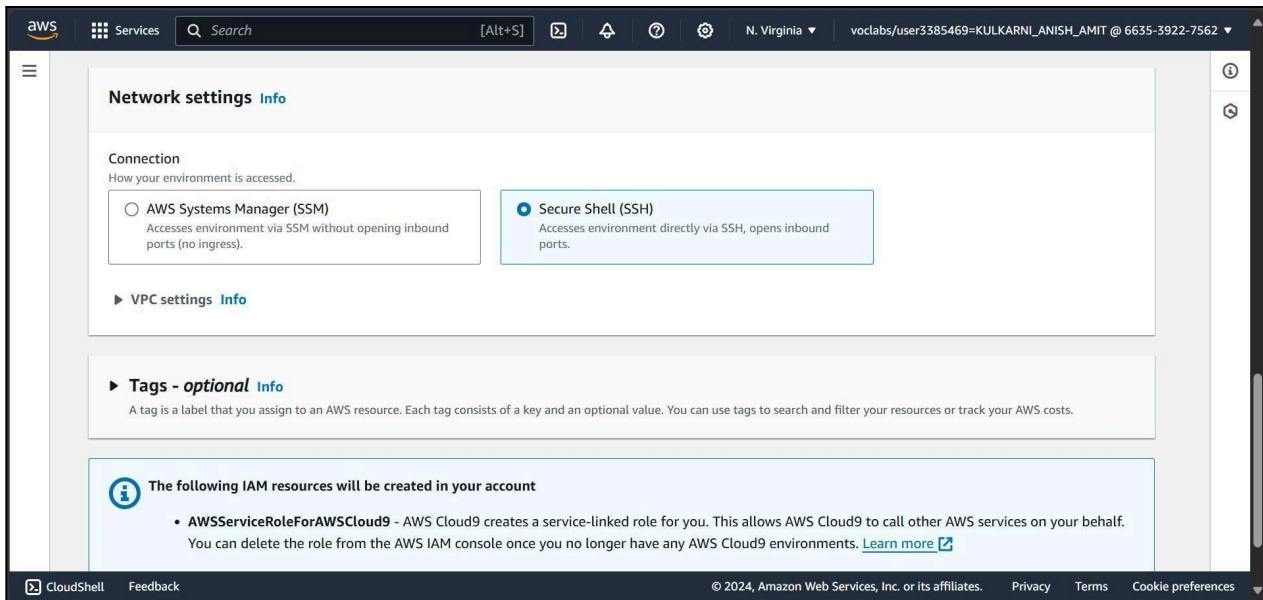
Top Screenshot: New EC2 instance

- Instance type:** The memory and CPU of the EC2 instance that will be created for Cloud9 to run on. Three options are shown:
 - ☒ **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.
- Platform:** This will be installed on your EC2 instance. We recommend Amazon Linux 2023. The dropdown menu shows **Amazon Linux 2023**.
- Timeout:** How long Cloud9 can be inactive (no user input) before auto-hibernating. This helps prevent unnecessary charges. The dropdown menu shows **30 minutes**.

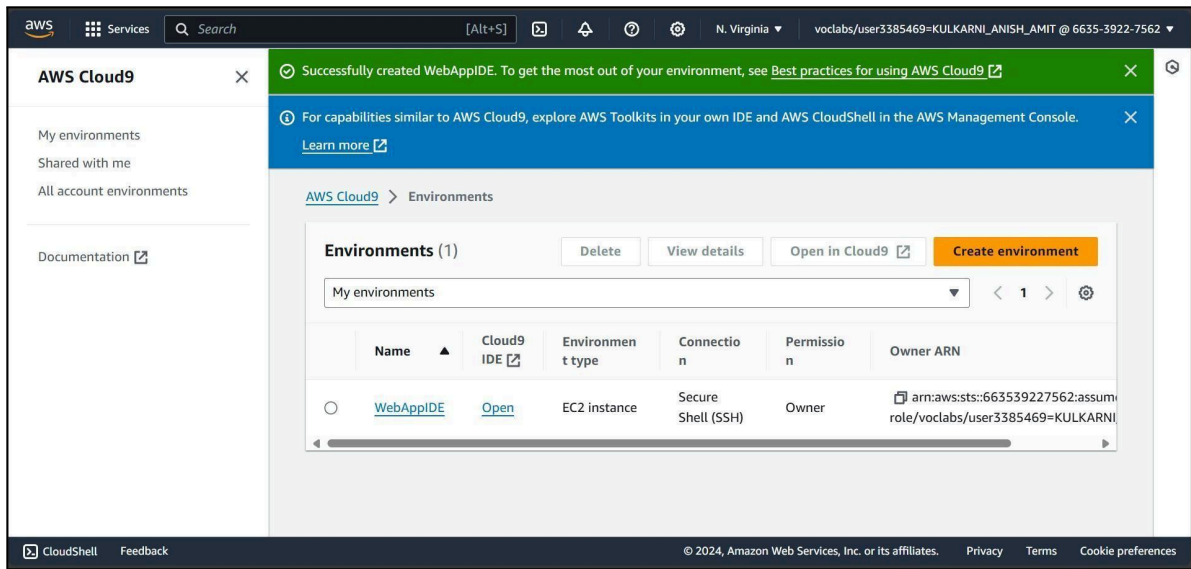
Bottom Screenshot: Create environment

- Details:**
 - Name:** (Limit of 60 characters, alphanumeric, and unique per user).
 - Description - optional:** (Limit 200 characters).
 - Environment type:** Determines what the Cloud9 IDE will run on. Two options are shown:
 - ☒ **New EC2 instance**
 - ☐ **Existing compute**

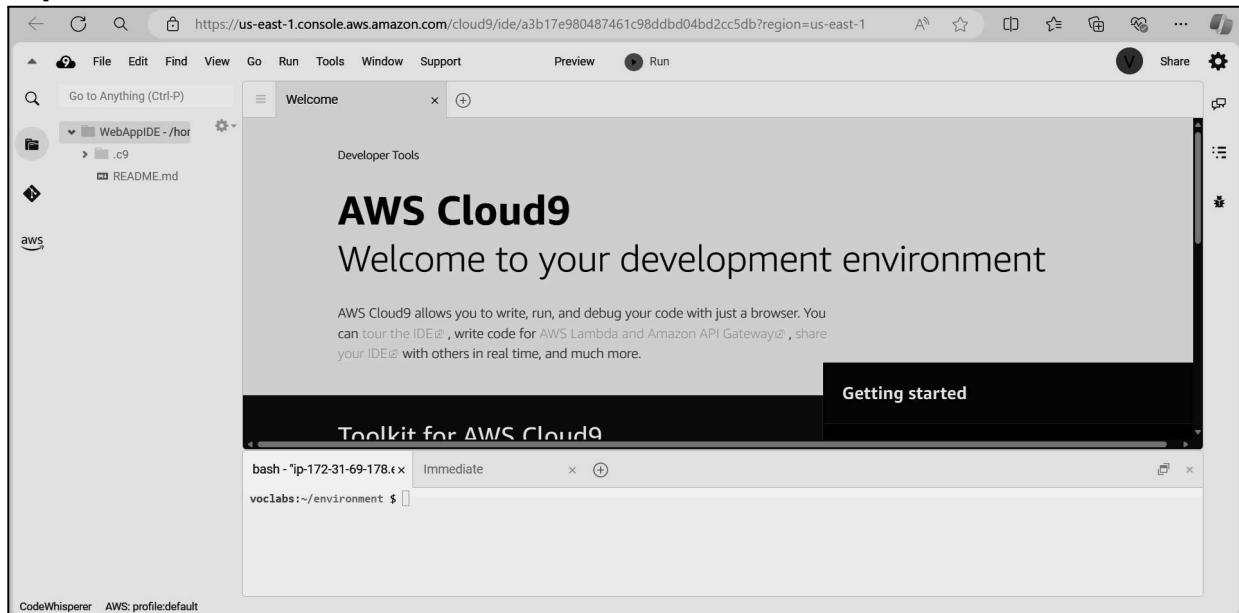
Step 2:



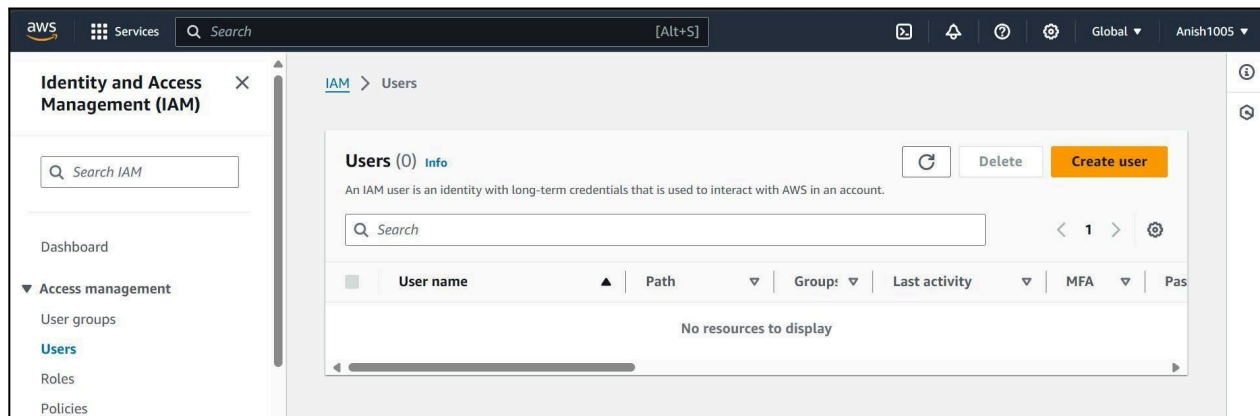
Step 3:



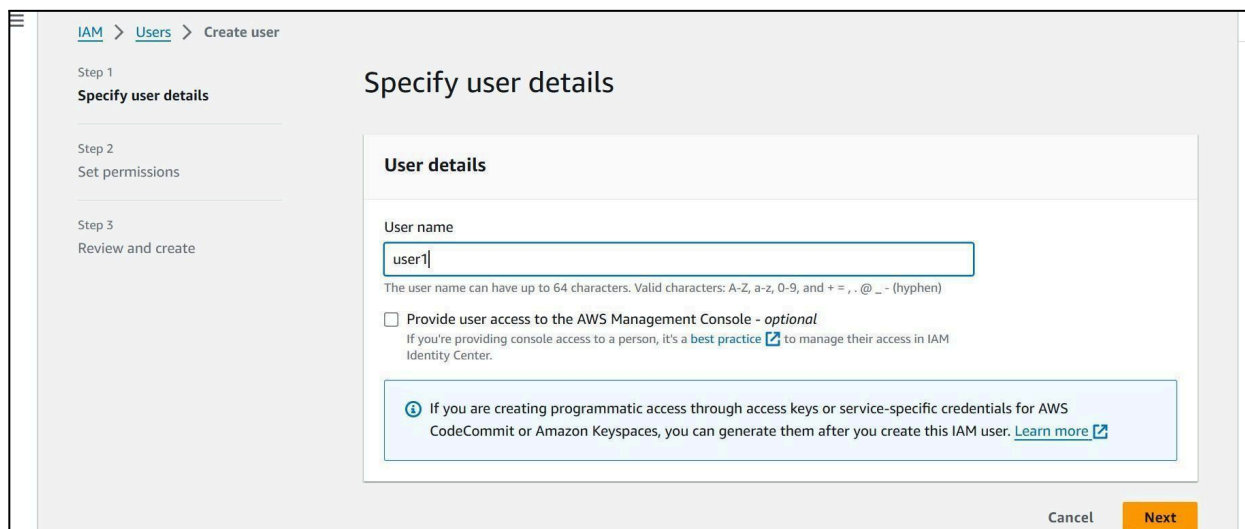
Step 4:



Step 5:



Step 6:



Step 7:

The screenshot shows the AWS IAM console interface. The breadcrumb navigation is IAM > Users > Create user. The left sidebar shows the progress: Step 1 Specify user details, Step 2 Set permissions (active), and Step 3 Review and create. The main heading is 'Set permissions' with a subtext: '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](#)'. Below this, there are three radio button options under 'Permissions options': 'Add user to group' (selected), 'Copy permissions', and 'Attach policies directly'. Each option has a brief description. At the bottom, there 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](#)

The screenshot shows the 'Create user group' modal. It has a close button (X) in the top right. The main text says: '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 the 'User group name' section with a text input field containing 'group1' and a note: 'Maximum 128 characters. Use alphanumeric and '+=,.-_' characters.' The 'Permissions policies (947)' section features a search bar, a 'Filter by Type' dropdown set to 'All ty...', and a pagination bar showing 1 to 48. A table lists policies with columns for checkboxes, policy names, types, use cases, and descriptions. The first two rows are '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.

group1

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

Permissions policies (947)

Filter by Type

Search 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

Cancel Create user group

Step 8:

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

Step 9:

✔ 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.

IAM > Users

Users (1) Info

Refresh

Delete

Create user

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Search

< 1 >

⚙

☐

User name

▲

☐

Path

▼

☐

Group

▼

☐

Last activity

▼

☐

MFA

▼

☐

P

☐

[user1](#)

/

0

-

-

-

User groups (1) Info

Refresh

Delete

Create group

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Search

< 1 >

⚙

☐

Group name

▲

☐

Users

▼

☐

Permissions

▼

☐

Creation time

▼

☐

[group1](#)

⚠ 0

⌚ Pending

5 minutes ago

Step 10:

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

IAM > User groups > group1

group1

Summary

User group name

group1

Creation time

August 04, 2024, 16:59 (UTC+05:30)

ARN

arn:aws:iam::010928206130:group/group1

Users

Permissions

Access Advisor

Permissions policies (0)

You can attach up to 10 managed policies.

Simulate

Remove

Add permissions

Step 11:

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 AWSCloud9

All types

4 matches

Policy name	Type	Used as	Description
<input type="checkbox"/> AWSCloud9Administ...	AWS managed	None	Provides administrator access to AWS ...
<input checked="" type="checkbox"/> AWSCloud9Environ...	AWS managed	None	Provides the ability to be invited into A...
<input type="checkbox"/> AWSCloud9SSMInsta...	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...