

## Experiment 4

**Aim:-**To study AWS code pipeline and deploy web application using code pipeline

### **Theory:-**

AWS CodePipeline is a fully managed continuous delivery service that helps automate the release pipelines for fast and reliable application and infrastructure updates. It allows you to model, visualize, and automate the steps required to release your software. Here are some key points about AWS CodePipeline:

**Automation of Software Release Process:** AWS CodePipeline automates the build, test, and deployment phases of your release process every time there is a code change, based on the release model you define.

**Integration with Different Services:** It integrates with a variety of third-party services and AWS services such as AWS CodeBuild, AWS CodeDeploy, and AWS CloudFormation, enabling you to have a fully automated release process for your applications.

**Customizable Pipeline:** CodePipeline allows you to build custom release workflows with multiple stages and actions. Each stage can have one or more actions, and you can define the actions to be performed at each stage, such as source code versioning, building, testing, and deployment.

**Visual Workflow:** It provides a visual representation of your release process, allowing you to see the stages and actions in the pipeline and monitor the progress of each release.

**Integration with Third-Party Tools:** It supports integration with a wide range of third-party tools and services through its extensible architecture, enabling you to incorporate your favorite tools into the release process.

**Flexibility and Control:** CodePipeline provides flexibility and control over the release process, allowing you to define custom rules for the execution of each action and the transition between stages.

**Security:** It integrates with AWS Identity and Access Management (IAM) to control access to your pipelines, ensuring that only authorized users have the necessary permissions to view or modify the pipelines.

**Monitoring and Logging:** AWS CodePipeline provides monitoring and logging capabilities, allowing you to track the execution of each action and stage in the pipeline and quickly identify any issues or failures.

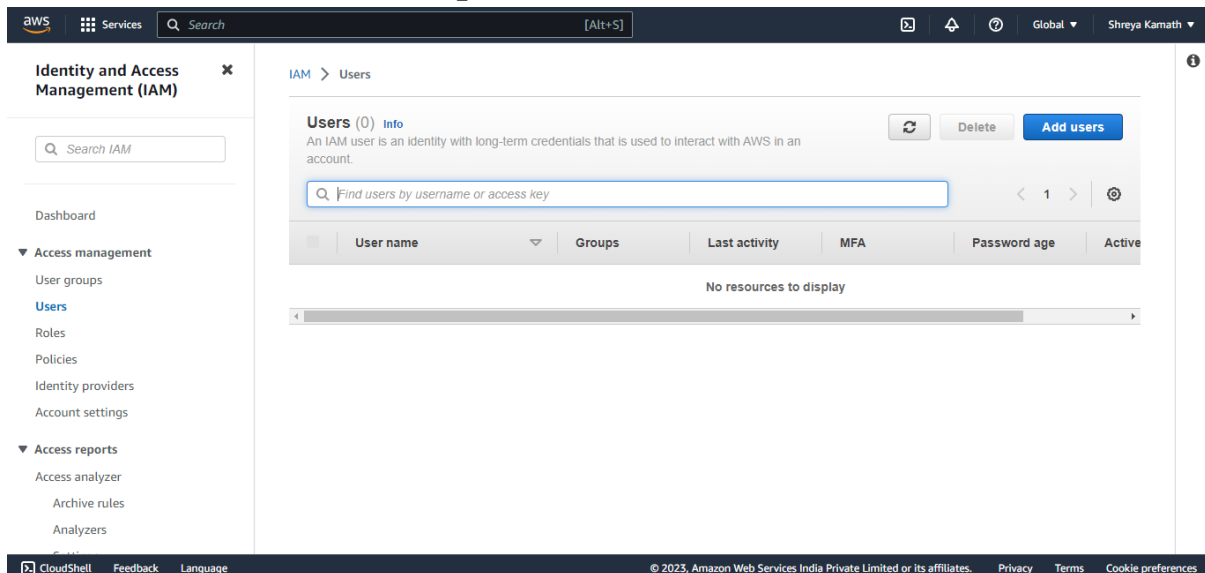
**Scalability and Availability:** As a fully managed service, AWS CodePipeline offers scalability and high availability, ensuring that your release pipelines can handle any workload and are always accessible.

**Cost-Effective:** With a pay-as-you-go pricing model, AWS CodePipeline helps you optimize costs by charging only for the resources you use.

## Steps :-

1) Login to AWS account and in search bar search IAM and click on it

2) Dashboard of IAM user open and then create a new user



aws Services Search [Alt+S] Global Shreya Kamath

IAM > Users > Create user

Step 1  
Specify user details

Step 2  
Set permissions

Step 3  
Review and create

### Specify user details

#### User details

User name

shreyakamath

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and +, =, @, \_ (hyphen)

☐ 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.

**i** 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](#)

Cancel Next

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

## 2) Set the permissions for the new user

aws Services Search [Alt+S] Global Shreya Kamath

IAM > Users > Create user

Step 1  
Specify user details

Step 2  
Set permissions

Step 3  
Review and create

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.

**i** 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

► Set permissions boundary - *optional*

Cancel Previous Next

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

## 3) Create user and user name , usergroup will be visible on dashboard

awsServicesSearch

GlobalShreya Kamath

Step 2Set permissions

Step 3Review and create

### 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.

t13shreya

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

Permissions policies (871)

Create policy

Search

Filter by Type

All ty...

< 1 2 3 4 5 6 7 ... 44 >

<input type="checkbox"/>	Policy name	Type	Use...	Description
<input type="checkbox"/>	AdministratorAccess	AWS managed ...	None	Provides full access to AWS services
<input type="checkbox"/>	AdministratorAcce...	AWS managed	None	Grants account administrative perm
<input type="checkbox"/>	AdministratorAcce...	AWS managed	None	Grants account administrative perm
<input type="checkbox"/>	AlexaForBusinessD...	AWS managed	None	Provide device setup access to Alex

Cancel

Create user group

awsServicesSearch[Alt+S]

GlobalShreya Kamath

t13shreya user group created.

Review and create

☒ 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.

User groups (1)

Create group

Search

< 1 >

<input type="checkbox"/>	Group name	Users	Attached policies	Created
<input type="checkbox"/>	t13shreya	0	-	2023-08-08 (Now)

Set permissions boundary - optional

Cancel

Previous

Next

CloudShellFeedbackLanguage

© 2023, Amazon Web Services India Private Limited or its affiliates. PrivacyTermsCookie preferences

Type here to search

29°C Mostly cloudy

3:17 PM 8/8/2023

aws Services Search [Alt+S] Global Shreya Kamath

**Identity and Access Management (IAM)**

Search IAM

Dashboard

▼ Access management

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

▼ Access reports

- Access analyzer
- Archive rules
- Analizers

**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](#)

**IAM > Users**

**Users (1)** Info [Refresh](#) [Delete](#) [Add users](#)

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

Find users by username or access key

<input type="checkbox"/>	User name	Groups	Last activity	MFA	Password a...	Active
<input type="checkbox"/>	shreyakamath	None	Never	None	None	-

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

#### 4) See the summary of created user and usergroup

aws Services Search [Alt+S] Global Shreya Kamath

**Identity and Access Management (IAM)**

Search IAM

Dashboard

▼ Access management

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

▼ Access reports

- Access analyzer
- Archive rules
- Analizers

**Users added to this group.**

**IAM > User groups > t13shreya**

**t13shreya** [Delete](#)

**Summary** [Edit](#)

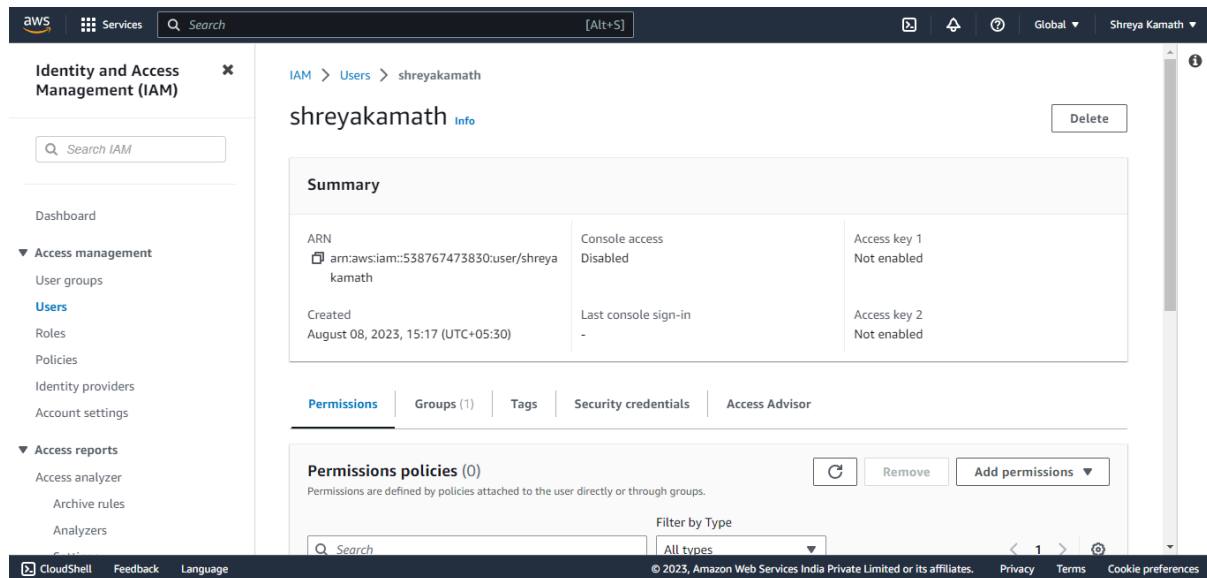
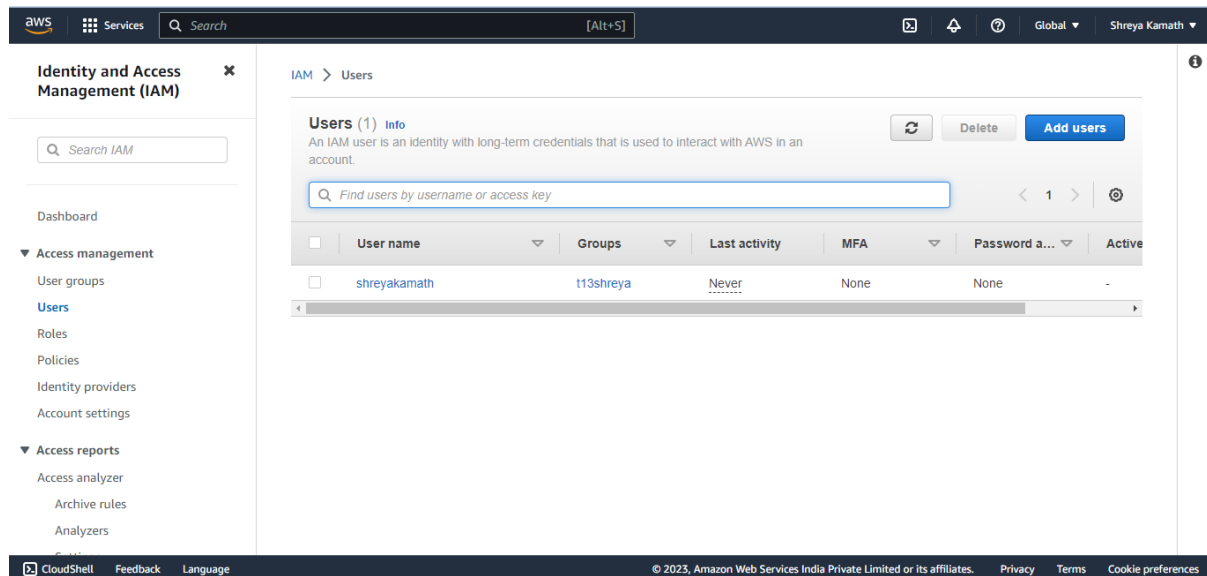
User group name	Creation time	ARN
t13shreya	August 08, 2023, 15:17 (UTC+05:30)	arn:aws:iam::538767473830:group/t13shreya

**Users** **Permissions** **Access Advisor**

**Users in this group (1)**

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. [Refresh](#) [Remove users](#) [Add users](#)

Search



**5) Go to security credentials tab and see for console password and other details, take screenshot of these details**

aws

Services

Search

[Alt+S]

Global

Shreya Kamath

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

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

Access reports

- Access analyzer
- Archive rules
- Analyzers

ARN

- am:aws:iam::538767473830:user/shreyakamath

Console access

- Disabled

Access key 1

- Not enabled

Created

- August 08, 2023, 15:17 (UTC+05:30)

Last console sign-in

-

Access key 2

- Not enabled

Permissions

Groups (1)

Tags

Security credentials

Access Advisor

Console sign-in

Enable console access

Console sign-in link

- https://538767473830.signin.aws.amazon.com/console

Console password

- Not enabled

Multi-factor authentication (MFA) (0)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

Remove

Resync

Assign MFA device

Device type

Identifier

Certifications

Created on

CloudShell

Feedback

Language

© 2023, Amazon Web Services India Private Limited or its affiliates.

Privacy

Terms

Cookie preferences

Console password

✓

You have successfully enabled the user's new password.  
This is the only time you can view this password. After you close this window, if the password is lost, you must create a new one.

Console sign-in URL

- https://538767473830.signin.aws.amazon.com/console

User name

- shreyakamath

Console password

- \*\*\*\*\* Show

Download .csv file

Close

6)Go to dashboard and search codecommit in search bar

The screenshot displays the AWS Management Console interface. At the top, the navigation bar includes the AWS logo, a search bar, and the user's profile (shreyakamath). The main content area shows the 'Console Home' dashboard with sections for 'Recently visited' (listing Cloud9 and EC2) and 'Welcome to AWS' (with links for getting started, training, and new services). Below this, there are tabs for 'AWS Health' and 'Cost and usage'. A green notification banner at the bottom states 'shreyat13 user group created.' and 'Step 2: Review'. The 'Permissions options' dialog is open, showing three radio button options: 'Add user to group' (selected), 'Copy permissions', and 'Attach policies directly'. Below the options, the 'User groups (1)' section shows a table with one entry: 'shreyat13' with 0 users and the 'AdministratorAccess' policy. The 'Create group' button is highlighted with a red box. The bottom of the console shows the footer with copyright information and links for privacy, terms, and cookie preferences.

Console Home [Info](#)

Reset to default layout [+ Add widgets](#)

**Recently visited** [Info](#)

- Cloud9
- EC2

[View all services](#)

**Welcome to AWS**

- [Getting started with AWS](#)  
Learn the fundamentals and find valuable information to get the most out of AWS.
- [Training and certification](#)  
Learn from AWS experts and advance your skills and knowledge.
- [What's new with AWS?](#)  
Discover new AWS services, features, and Regions.

**AWS Health** [Info](#) **Cost and usage** [Info](#)

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Type here to search

29°C Mostly cloudy 3:28 PM 8/8/2023

shreyat13 user group created.

Step 2: Review

**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, inline policies, and any existing permissions boundaries 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.

**User groups (1)** [Refresh](#) [Create group](#)

<input type="checkbox"/>	<a href="#">Group name</a>	<a href="#">Users</a>	<a href="#">Attached policies</a>	<a href="#">Created</a>
<input type="checkbox"/>	shreyat13	0	AdministratorAccess	2023-08-08 (Now)

[Cancel](#) [Next](#)

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

7) Go to repositories option and create a new repository , give a name to it



The image shows two screenshots of the AWS CodeCommit interface. The top screenshot displays the 'Repositories' page, which includes a sidebar with navigation options like 'Source', 'Artifacts', 'Build', 'Deploy', 'Pipeline', and 'Settings'. The main content area shows a list of repositories, currently empty, with a 'Create repository' button. The bottom screenshot shows the 'Repository settings' page for a repository named 'adv devops'. It includes fields for 'Repository name', 'Description', and 'Tags'. The 'Tags' section shows a key-value pair 'repo1' being added. There is also a checkbox for 'Enable Amazon CodeGuru Reviewer for Java and Python'.

**Top Screenshot: AWS CodeCommit Repositories**

Developer Tools > CodeCommit > Repositories

**Repositories** Info

Buttons: Refresh, Notify, Clone URL, View repository, Delete repository, **Create repository**

Search: [Q]

Name	Description	Last modified	Clone URL
No results There are no results to display.			

**Bottom Screenshot: Repository settings**

Repository name: adv devops  
100 characters maximum. Other limits apply.

Description - optional  
1,000 characters maximum

Tags

Key: Name Value - optional: repo1 Remove tag

Add tag

☐ Enable Amazon CodeGuru Reviewer for Java and Python - optional  
Get recommendations to improve the quality of the Java and Python code for all pull requests in this repository.  
A service-linked role will be created in IAM on your behalf if it does not exist.

8) Go to code option in left sidebar and select https there

aws

Services

Search

[Alt+S]

Stockholm

shreyakamath @ 5387-6747-3830

Repository settings

Repository name

adv devops

100 characters maximum. Other limits apply.

Description - optional

1,000 characters maximum

Tags

Key

Name

Value - optional

repo1

Remove tag

Add tag

☐ Enable Amazon CodeGuru Reviewer for Java and Python - optional

Get recommendations to improve the quality of the Java and Python code for all pull requests in this repository.

A service-linked role will be created in IAM on your behalf if it does not exist.

Developer Tools

CodeCommit

Source • CodeCommit

Getting started

Repositories

Code

Pull requests

Commits

Branches

Git tags

Settings

Approval rule templates

Artifacts • CodeArtifact

Build • CodeBuild

Deploy • CodeDeploy

Pipeline • CodePipeline

Success

Repository successfully created

Create a notification rule for this repository

Developer Tools > CodeCommit > Repositories > advdevops

advdevops

Clone URL

Connection steps

HTTPS

SSH

HTTPS (GRC)

Step 1: Prerequisites

You must use a Git client that supports Git version 1.7.9 or later to connect to an AWS CodeCommit repository. If you do not have a Git client, you can install one from Git downloads. [View Git downloads page](#)

You must have an AWS CodeCommit managed policy attached to your IAM user, belong to a CodeStar project team, or have the equivalent permissions. [Learn how to create and configure an IAM user for accessing AWS CodeCommit.](#) | [Learn how to add team members to an AWS CodeStar Project.](#)

Step 2: Git credentials

Developer Tools

CodeCommit

Source • CodeCommit

Getting started

Repositories

Code

Pull requests

Commits

Branches

Git tags

Settings

Approval rule templates

Artifacts • CodeArtifact

Build • CodeBuild

Deploy • CodeDeploy

Pipeline • CodePipeline

Step 1: Prerequisites

You must use a Git client that supports Git version 1.7.9 or later to connect to an AWS CodeCommit repository. If you do not have a Git client, you can install one from Git downloads. [View Git downloads page](#)

You must have an AWS CodeCommit managed policy attached to your IAM user, belong to a CodeStar project team, or have the equivalent permissions. [Learn how to create and configure an IAM user for accessing AWS CodeCommit.](#) | [Learn how to add team members to an AWS CodeStar Project.](#)

Step 2: Git credentials

Create Git credentials for your IAM user, if you do not already have them. Download the credentials and save them in a secure location. [Generate Git Credentials](#)

Step 3: Clone the repository

Clone your repository to your local computer and start working on code. Run the following command:

git clone https://git-codecommit.eu-north-1.amazonaws.com/v1/repos/advdevops

Copy

Additional details

You can find more detailed instructions in the documentation. [View documentation](#)

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

## 9) Create a new application and give name to it , create a deployment group for deployment of application created

The image shows two screenshots of the AWS Management Console interface. The top screenshot displays the 'Create application' page, and the bottom screenshot displays the 'Create deployment group' page.

**Create application**

**Application configuration**

Application name  
Enter an application name  
shreyaT13  
100 character limit

Compute platform  
Choose a compute platform  
EC2/On-premises

Tags  
Key  
Name  
Value - optional  
webapp1  
Remove tag  
Add tag

Cancel Create application

**Create deployment group**

**Deployment group name**

Enter a deployment group name  
webappdeploygroup1  
100 character limit

**Service role**

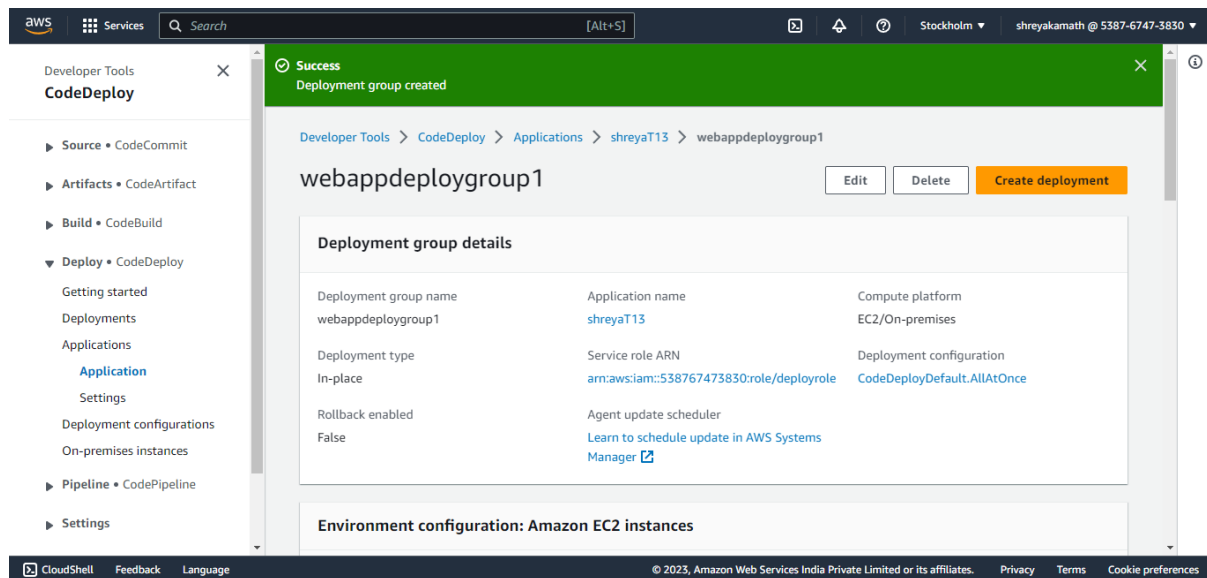
Enter a service role  
Enter a service role with CodeDeploy permissions that grants AWS CodeDeploy access to your target instances.  
service1

**Deployment type**

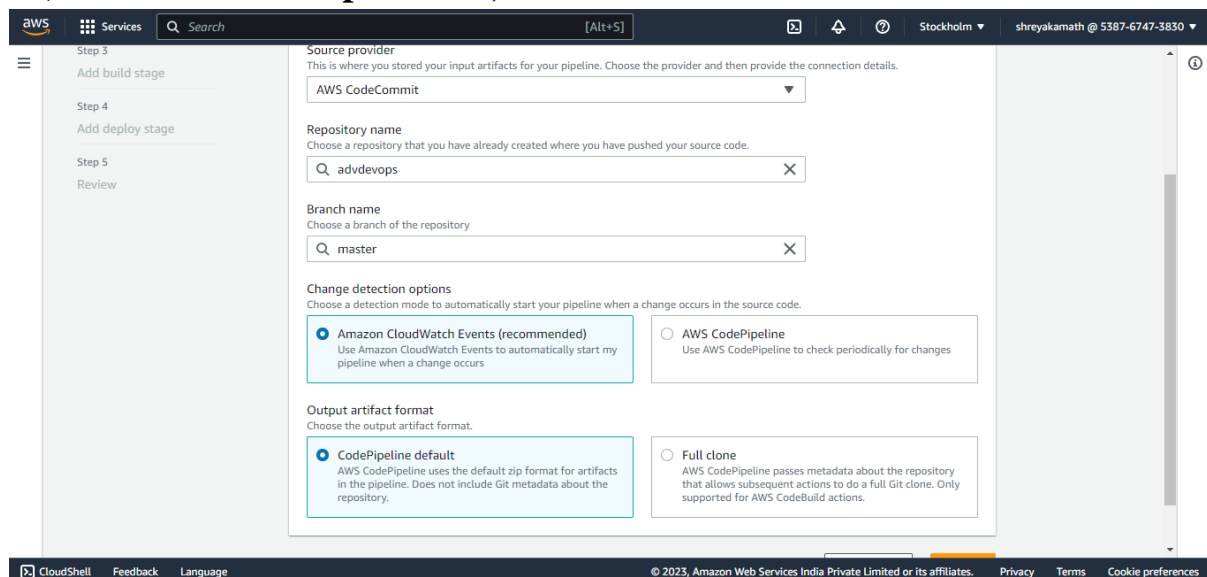
Choose how to deploy your application

☒ In-place  
Updates the instances in the deployment group with the new version of the application.

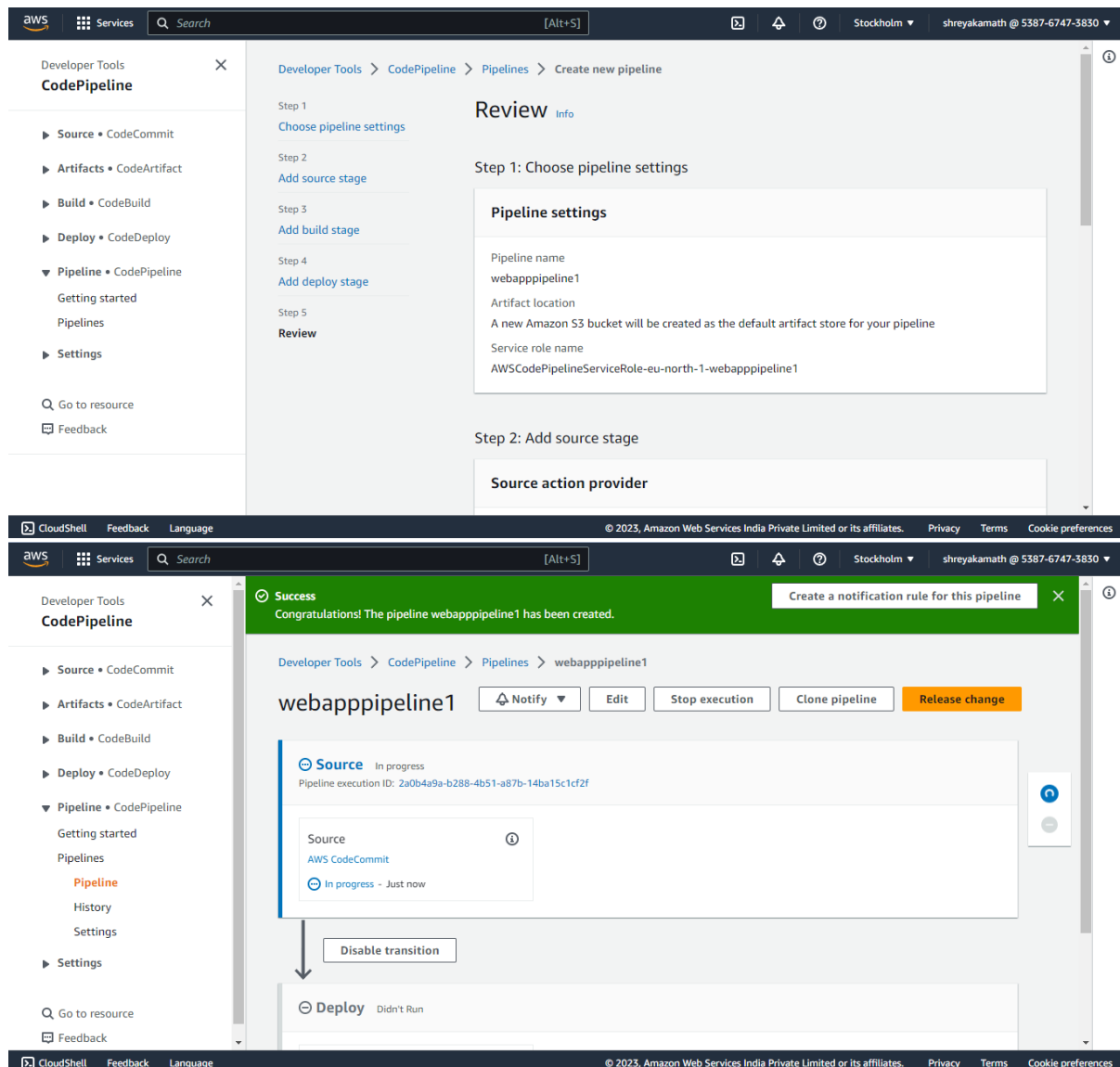
☐ Blue/green  
Replaces the instances in the deployment group with new instances.



## 10) Select the source provider , artifact



## 11) Review the application and then click on deploy , after deploying success message is displayed on screen



## Conclusion :-

Learnt about creation and deployment of web application using AWS codepipeline ,hence learnt about basic components of codepipeline in AWS such as codebuild , codecommit , codedeploy and built , committed and deployed a web application using codepipeline