

CI/CD pipeline with AWS Services

Let's Start:-

STEP-1:

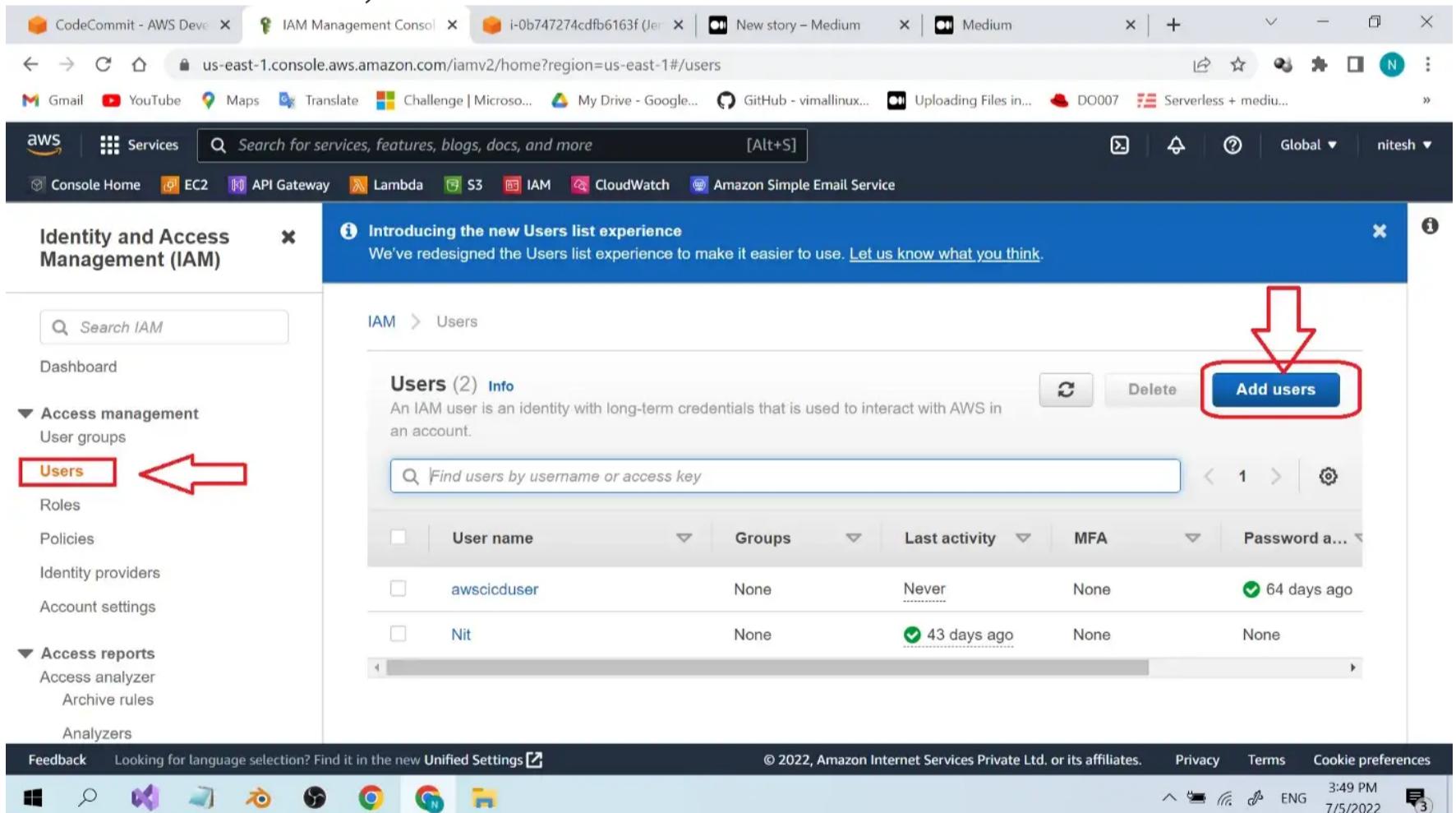
Firstly we make a repo in CodeCommit as our workspace, and to get access to that repo we need to clone that repo and push our files from the local pc with git or EC2 server

git clone <HTTP URL>

STEP-2:

If it is for the first time you are accessing to CodeCommit, you need user access so we will create a user in AWS with the IAM service.

In the IAM service, as shown below click on Users then add a user.



Name the user → Next → Attach policies → AdministratorAccess → Next
→ Next → Create User → close

AWS Services Search for services, features, blogs, docs, and more [Alt+S] Global nitesh

Console Home EC2 API Gateway Lambda S3 IAM CloudWatch Amazon Simple Email Service

Add user

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name* RepoUser

[Add another user](#)

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Select AWS credential type* Access key - Programmatic access
Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.

Password - AWS Management Console access
Enables a password that allows users to sign-in to the AWS Management Console.

Console password* Autogenerated password Custom password

* Required [Cancel](#) [Next: Permissions](#)

Feedback Looking for language selection? Find it in the new [Unified Settings](#) © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

aws Services Search for services, features, blogs, docs, and more [Alt+S] Global nitesh

Console Home EC2 API Gateway Lambda S3 IAM CloudWatch Amazon Simple Email Service

Add user

Set permissions

[Add user to group](#) [Copy permissions from existing user](#) [Attach existing policies directly](#) [Create policy](#)

[Filter policies](#) [Search](#) Showing 766 results

Policy name	Type	Used as
<input checked="" type="checkbox"/> AdministratorAccess	Job function	Permissions policy (2)
<input type="checkbox"/> AdministratorAccess-Amplify	AWS managed	None
<input type="checkbox"/> AdministratorAccess-AWSElasticBeanstalk	AWS managed	None
<input type="checkbox"/> AlexaForBusinessDeviceSetup	AWS managed	None
<input type="checkbox"/> AlexaForBusinessFullAccess	AWS managed	None
<input type="checkbox"/> AlexaForBusinessGatewayExecution	AWS managed	None
<input type="checkbox"/> AlexaForBusinessIfaceSizeDelegatedAccessPolicy	AWS managed	None

[Cancel](#) [Previous](#) [Next: Tags](#)

Feedback Looking for language selection? Find it in the new [Unified Settings](#) © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the 'Review' step of the 'Add user' wizard. At the top, there's a search bar and navigation links for various AWS services like EC2, API Gateway, Lambda, S3, IAM, CloudWatch, and Amazon Simple Email Service. Below the search bar, a breadcrumb trail shows 'Console Home > IAM > Add user'. A progress bar at the top right indicates step 4 of 5. The main content area is titled 'Review' and contains a section for 'User details' and a 'Permissions summary'.

User details

User name	RepoUser
AWS access type	AWS Management Console access - with a password
Console password type	Autogenerated
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	AdministratorAccess
Managed policy	IAMUserChangePassword

Buttons at the bottom include 'Cancel', 'Previous', and a prominent blue 'Create user' button.

The screenshot shows the 'Success' page after a user has been created. It features a success message box, a download CSV button, and a table showing the newly created user's details.

Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://718871632185.signin.aws.amazon.com/console>

Download .csv

User	Password	Email login instructions
RepoUser	***** Show	<input checked="" type="checkbox"/> Send email

Buttons at the bottom include 'Close' and standard footer links for Feedback, Unified Settings, Privacy, Terms, and Cookie preferences.

After that click on the user and goto summary, then click on *generate credentials and save the username and password.*

Servic... Search for services, features, blogs, docs, and more [Alt+S] Global nitesh

Console Home EC2 API Gateway Lambda S3 IAM CloudWatch Amazon Simple Email Service

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
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Users (3) Info

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

User name	Groups	Last activity	MFA	Password a...
awsciduser	None	Never	None	65 days ago
Nit	None	44 days ago	None	None
RepoUser	None	Never	None	Now

Add users

https://us-east-1.console.aws.amazon.com/iam/home#/users/RepoUser Edit Settings

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

aws Services Search for services, features, blogs, docs, and more [Alt+S]

Console Home EC2 API Gateway Lambda S3 IAM CloudWatch Amazon Simple Email Service

Identity and Access Management (IAM)

Dashboard

Access management

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

Access reports

- Access analyzer
- Archive rules
- Analyzers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

New feature to generate a policy based on CloudTrail events.

AWS uses your CloudTrail events to identify the services and actions used and generate a least privileged policy that you can attach to this user.

Users > RepoUser

Summary

User ARN: arn:aws:iam::718871632185:user/RepoUser

Path: /

Creation time: 2022-07-06 08:40 UTC+0530

Permissions Groups Tags Security credentials Access Advisor

Permissions policies (2 policies applied)

Add permissions Add inline policy

Policy name	Policy type
AdministratorAccess	AWS managed policy
IAMUserChangePassword	AWS managed policy

Attached directly

in the new Unified Settings

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS Identity and Access Management (IAM) service. On the left, the navigation menu includes options like Dashboard, Access management, Users, Roles, Policies, Identity providers, Account settings, Access reports, Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, and Service control policies (SCPs). The main content area is titled "SSH keys for AWS CodeCommit" and contains a sub-section "Use SSH public keys to authenticate access to AWS CodeCommit repositories." It features a "Upload SSH public key" button and a table with columns "SSH key ID", "Uploaded", and "Status". A message "No results" is displayed below the table. Below this, there's a section for "HTTPS Git credentials for AWS CodeCommit" with a "Generate credentials" button and a message "No credentials have been generated." Finally, there's a section for "Credentials for Amazon Keyspaces (for Apache Cassandra)" with a "Generate credentials" button and a similar "No credentials have been generated." message.

This screenshot shows a modal dialog box titled "Generate credentials" from the AWS IAM service. The dialog contains a green success message: "Your new credentials are available". Below this, it says "Save your user name and password now (or download a credentials file)." It provides the user name "RepoUser-at-718871632185" and a redacted password. There is a "Download credentials" button with a download icon. At the bottom right of the dialog is a blue "Close" button. The background shows the same IAM interface as the first screenshot, with the "Generate credentials" button highlighted.

Now let's create a repo for our project for this we are going to use CodeCommit (AWS service) as SCM tool(Source Code Management tool).

CodeCommit (SCM tool)

CodeCommit is a secure, highly scalable, managed source control service that hosts private Git repositories. CodeCommit eliminates the need for you to manage your source control system or worry about scaling its infrastructure.

You can use CodeCommit to store anything from code to binaries. It supports the standard functionality of Git, so it works seamlessly with your existing Git-based tools.

STEP-3:

Search CodeCommit in the search bar, Click on Repositories and Create a repository

. Name the repo and click create:

Copy the HTTPS URL by clicking on clone URL then click on Clone HTTPS

Now we can access the repo with a user that we created before.

git clone <HTTPS URL>

prompt will ask for Username and Password :



After go to that directory and put your files(package) there and push it:

git add.

git commit . -m “1st commit”

git push

You can see your files on CodeCommit now.



STEP-4:

Code Build (Build and Test Tool)

AWS CodeBuild is a fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy. CodeBuild eliminates the need to provision, manage, and scale your build servers.

It provides prepackaged build environments for popular programming languages and builds tools such as Apache Maven, Gradle, and more. You can also customize build environments in CodeBuild to use your build tools. For more details you can visit the below-mentioned link :

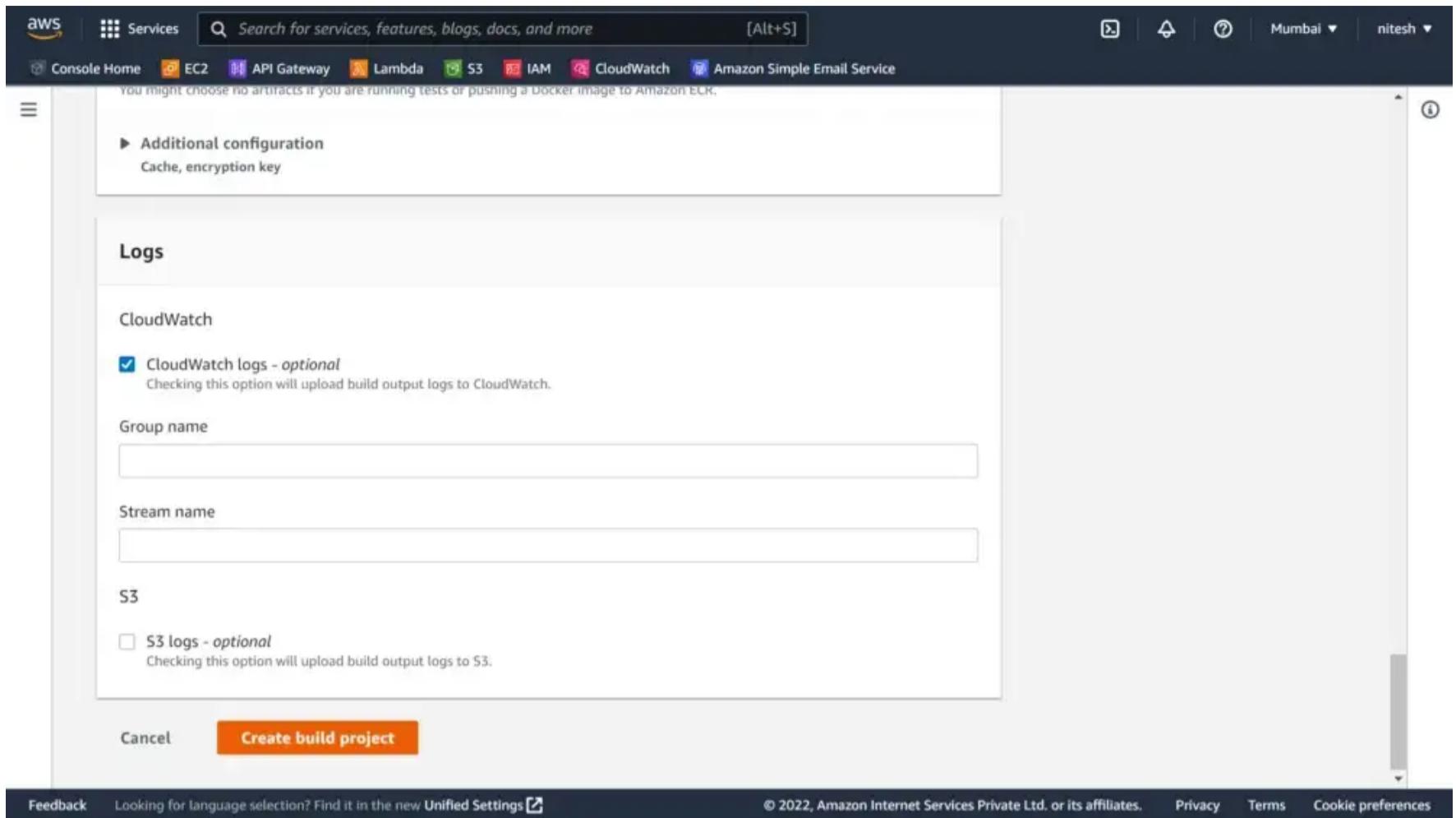
Search CodeBuild with the search bar, click on *Build Projects*, and then click on *Create build project*.

Type the name of the project → Source provider: AWS CodeCommit → Repository: <CodeCommit Repo> → Branch: master → **Insert build command** → Buildspec name: grep <Text> index.html → Cloud watch logs → create build project

The screenshot shows the 'Create build project' configuration page in the AWS Management Console. The 'Project configuration' section includes fields for 'Project name' (cicd_aws_build), 'Description - optional' (empty), 'Build badge - optional' (unchecked), 'Enable concurrent build limit - optional' (unchecked), and an 'Additional configuration' section for tags.

The 'Source 1 - Primary' configuration section includes fields for 'Source provider' (AWS CodeCommit), 'Repository' (cicdwithaws_Repo), 'Reference type' (Branch selected), 'Branch' (master), 'Commit ID - optional' (empty), 'Source version' (refs/heads/master, 2814e671 2nd commit), and an 'Additional configuration' section for Git clone depth and Git submodules.

Both screenshots show the AWS navigation bar at the top with services like EC2, API Gateway, Lambda, S3, IAM, CloudWatch, and Amazon Simple Email Service.



Feedback Looking for language selection? Find it in the new Unified Settings [?](#) © 2022, Amazon Internet Services Private Ltd. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#) Create CodeBuild project

Here we have two options for build spec, either we can use a **buildspec.yml file** or tell the commands for practice purposes we will go with **Insert build commands**.

As a command, we are using **grep <Text> index.html** → will gives exit code 0 if the file index.html contains the Text else exit code 1.

We can start building by just clicking the *Start build* button.

For Edit Buildspec : Click on Edit → Buildspec → Update buildspec

In the second image if we click on Switch to the editor we can see the buildspec file that is generated automatically. Always we should use the buildspec.yml file for the build because it gives more benefits. The third image shows the outcome.

We can create notification features with Create notification rule.

AWS Services Search for services, features, blogs, docs, and more [Alt+S] Mumbai nitesh

Console Home EC2 API Gateway Lambda S3 IAM CloudWatch Amazon Simple Email Service

Developer Tools CodeBuild

Source • CodeCommit Artifacts • CodeArtifact Build • CodeBuild Getting started Build projects Build project Settings Build history Report groups Report history Account metrics Deploy • CodeDeploy Pipeline • CodePipeline Settings

Project created You have successfully created the following project: cicd_aws_build Create a notification rule for this project

Developer Tools > CodeBuild > Build projects > cicd_aws_build

cicd_aws_build

Notify Share Edit Delete build project Start build with overrides Start build

Configuration

Source provider AWS CodeCommit	Primary repository cicdwithaws_Repo	Artifacts upload location -	Build badge Disabled
Public builds Disabled			

Build history Batch history Build details Build triggers Metrics

Feedback Looking for language selection? Find it in the new Unified Settings © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

AWS Services Search for services, features, blogs, docs, and more [Alt+S] Mumbai nitesh

Console Home EC2 API Gateway Lambda S3 IAM CloudWatch Amazon Simple Email Service

Developer Tools CodeBuild

Source • CodeCommit Artifacts • CodeArtifact Build • CodeBuild Getting started Build projects Build project Settings Build history Report groups Report history Account metrics Deploy • CodeDeploy Pipeline • CodePipeline Settings

Build logs Phase details Reports Environment variables Build details Resource utilization

Name	Status	Context	Duration	Start time	End time
SUBMITTED	✓ Succeeded	-	<1 sec	Jul 6, 2022 1:34 PM (UTC+5:30)	Jul 6, 2022 1:34 PM (UTC+5:30)
QUEUED	✓ Succeeded	-	103 secs	Jul 6, 2022 1:34 PM (UTC+5:30)	Jul 6, 2022 1:36 PM (UTC+5:30)
PROVISIONING	✓ Succeeded	-	20 secs	Jul 6, 2022 1:36 PM (UTC+5:30)	Jul 6, 2022 1:36 PM (UTC+5:30)
DOWNLOAD_SOURCE	✓ Succeeded	-	6 secs	Jul 6, 2022 1:36 PM (UTC+5:30)	Jul 6, 2022 1:37 PM (UTC+5:30)
INSTALL	✓ Succeeded	-	<1 sec	Jul 6, 2022 1:37 PM (UTC+5:30)	Jul 6, 2022 1:37 PM (UTC+5:30)
PRE_BUILD	✓ Succeeded	-	<1 sec	Jul 6, 2022 1:37 PM (UTC+5:30)	Jul 6, 2022 1:37 PM (UTC+5:30)
BUILD	✓ Succeeded	-	<1 sec	Jul 6, 2022 1:37 PM (UTC+5:30)	Jul 6, 2022 1:37 PM (UTC+5:30)
POST_BUILD	✓ Succeeded	-	<1 sec	Jul 6, 2022 1:37 PM (UTC+5:30)	Jul 6, 2022 1:37 PM (UTC+5:30)
UPLOAD_ARTIFACTS	✓ Succeeded	-	<1 sec	Jul 6, 2022 1:37 PM (UTC+5:30)	Jul 6, 2022 1:37 PM (UTC+5:30)

Feedback Looking for language selection? Find it in the new Unified Settings © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

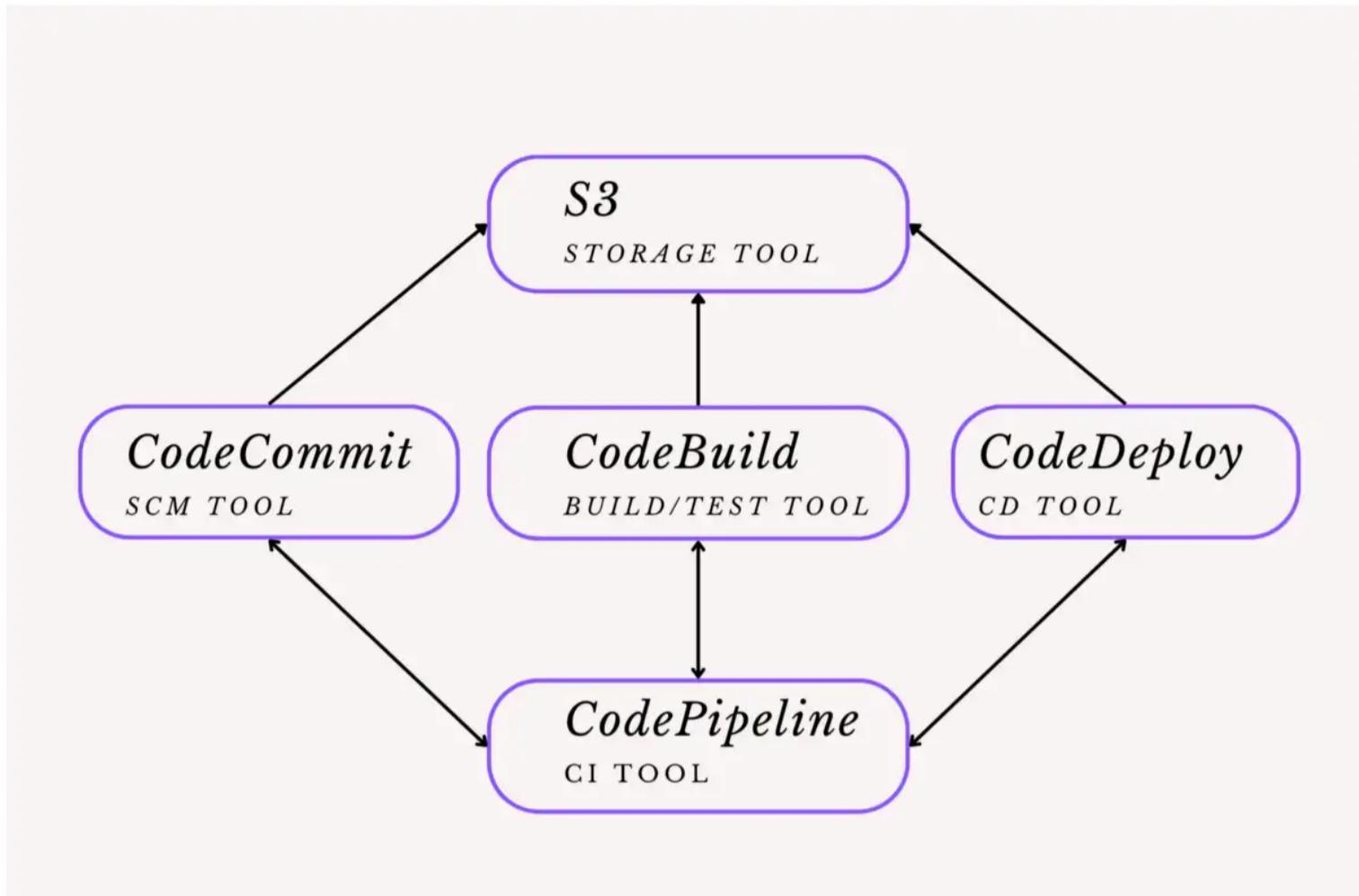
The screenshot shows the AWS CodeBuild console. The left sidebar has a 'CodeBuild' section with 'Build projects' selected. The main area shows a table of build projects:

Name	Source provider	Repository	Latest build status	Description	Last Modified
cicd_aws_build	AWS CodeCommit	cicdwithaws_Repo	Succeeded	-	4 minutes ago
cicd03_build	AWS CodeCommit	cicd_03_repo	Succeeded	-	2 months ago
cicdbuild02	AWS CodeCommit	cicdpipeline02	Succeeded	-	2 months ago

Now every time developers push the code, we have to click the build button to build the project. And it's very time-consuming, to make it automated we will going to use the CodePipeline service of AWS.

STEP-5: S3 (Storage Service)

Before integration with CodePipeline, we need centralized storage where we can put our code for use.



Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. For more details you can visit the below-mentioned link :

Now let's create a bucket(storage) in s3 with versioning enabled and the name of the bucket should be unique.

The screenshot shows the AWS search interface with the query 's3'. The results are categorized into 'Services' and 'Features'.

Services

- S3 ★ Scalable Storage in the Cloud
- S3 Glacier ☆ Archive Storage in the Cloud
- Athena ☆ Query Data in S3 using SQL
- AWS Snow Family ☆ Large Scale Data Transport

Features

- Amazon S3 File Gateway
- Storage Gateway feature

At the bottom right, there are two cards:

- Comp [17 mi ago]
- 25 mi ago

The screenshot shows the Amazon S3 buckets page. The sidebar includes links for Buckets, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, and Access analyzer for S3. It also has sections for Storage Lens and AWS Marketplace for S3.

The main area displays an account snapshot and a list of buckets:

Name	AWS Region	Access	Creation date
cicd03s3bucket	Asia Pacific (Mumbai) ap-south-1	Objects can be public	May 19, 2022, 16:41:22 (UTC+05:30)
cicdbucket02	Asia Pacific (Mumbai) ap-south-1	Objects can be public	May 2, 2022, 16:30:14 (UTC+05:30)
cicdpipeline01	Asia Pacific (Mumbai) ap-south-1	Objects can be public	May 2, 2022, 08:43:47 (UTC+05:30)

As shown below name the bucket that enables Bucket Versioning and click on create a bucket.

S | Services | Search for services, features, blogs, docs, and more | [Alt+S] | Global | nitesh

Console Home | EC2 | API Gateway | Lambda | S3 | IAM | CloudWatch | Amazon Simple Email Service

Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name: cicdawsstorage

Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region: Asia Pacific (Mumbai) ap-south-1

Copy settings from existing bucket - *optional*
Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Feedback | Looking for language selection? Find it in the new [Unified Settings](#) | © 2022, Amazon Internet Services Private Ltd. or its affiliates. | Privacy | Terms | Cookie preferences

aws | Services | Search for services, features, blogs, docs, and more | [Alt+S] | Global | nitesh

Console Home | EC2 | API Gateway | Lambda | S3 | IAM | CloudWatch | Amazon Simple Email Service

Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

ACLs disabled (recommended)
All objects in this bucket are owned by this account.
Access to this bucket and its objects is specified using only policies.

ACLs enabled
Objects in this bucket can be owned by other AWS accounts.
Access to this bucket and its objects can be specified using ACLs.

Object Ownership

Bucket owner enforced

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

Block public access to buckets and objects granted through new access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

Feedback | Looking for language selection? Find it in the new [Unified Settings](#) | © 2022, Amazon Internet Services Private Ltd. or its affiliates. | Privacy | Terms | Cookie preferences

The screenshot shows the 'Bucket Versioning' configuration page for an S3 bucket. At the top, there is a header bar with the AWS logo, a search bar, and navigation links for various AWS services like EC2, API Gateway, Lambda, S3, IAM, CloudWatch, and Amazon Simple Email Service. On the right side of the header, there are global settings and user information for 'nitesh'. Below the header, the main content area starts with a section titled 'Bucket Versioning' which explains the purpose of versioning. It includes a radio button for 'Enable' (which is selected) and a link to 'Learn more'. The next section is 'Tags (0) - optional', which allows tracking storage cost or other criteria by tagging the bucket. It shows a message 'No tags associated with this bucket.' and a 'Add tag' button. The final section is 'Default encryption', which automatically encrypts new objects stored in the bucket. It includes a radio button for 'Disable' (selected) and a link to 'Learn more'. At the bottom of the page, there is a feedback link, a copyright notice for 2022, and links for Privacy, Terms, and Cookie preferences.

This screenshot shows the 'Tags (0) - optional' configuration page for an S3 bucket. The layout is similar to the previous one, with the AWS logo, search bar, and service links at the top. The main content area features a section for 'Tags (0) - optional' with a note about tracking storage cost. It shows 'No tags associated with this bucket.' and an 'Add tag' button. Below this is the 'Default encryption' section, which is currently disabled. A 'Advanced settings' button is visible at the bottom left. A note at the bottom states: 'After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.' At the bottom right, there are 'Cancel' and 'Create bucket' buttons. The footer includes a feedback link, a copyright notice for 2022, and links for Privacy, Terms, and Cookie preferences.

Here CodeBuild needs access to S3 for files and to provide that we have to go to IAM → Roles → <CodeBuild Role >
Click: Add permissions → Attach policies → S3 Access (AmazonS3FullAccess)→ Click on Attach policies.

Servic... Search for services, features, blogs, docs, and more [Alt+S] Global nitesh

Console Home EC2 API Gateway Lambda S3 IAM CloudWatch Amazon Simple Email Service

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 Settings Credential report Organization activity Service control policies (SCPs)

IAM > Roles

Roles (37) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Search: cicd_aws_build

Role name	Trusted entities	Last ac...
codebuild-cicd_aws_build-service-role	AWS Service: codebuild	38 minutes ago

Create role

https://us-east-1.console.aws.amazon.com/iamv2/home#/roles/details/codebuild-cicd_aws_build-service-role © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

aws Services Search for services, features, blogs, docs, and more [Alt+S] Global nitesh

Console Home EC2 API Gateway Lambda S3 IAM CloudWatch Amazon Simple Email Service

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 Settings Credential report Organization activity Service control policies (SCPs)

IAM > Roles > codebuild-cicd_aws_build-service-role

codebuild-cicd_aws_build-service-role

Delete Edit

Summary

Creation date	ARN
July 06, 2022, 13:23 (UTC+05:30)	arn:aws:iam::718871632185:role/service-role/codebuild-cicd_aws_build-service-role
Last activity	Maximum session duration
38 minutes ago	1 hour

Permissions Trust relationships Tags Access Advisor Revoke sessions

Permissions policies (1)

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter

Policy name	Type	Description

Simulate Remove Add permissions

Feedback Looking for language selection? Find it in the new Unified Settings © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Servicenow

Search for services, features, blogs, docs, and more [Alt+S]

Console Home EC2 API Gateway Lambda S3 IAM CloudWatch Amazon Simple Email Service

Identity and Access Management (IAM)

Summary

Creation date: July 06, 2022, 13:23 (UTC+05:30) ARN: arn:aws:iam::718871632185:role/service-role/codebuild-cicd_aws_build-service-role

Last activity: 38 minutes ago Maximum session duration: 1 hour

Permissions Trust relationships Tags Access Advisor Revoke sessions

Permissions policies (1)

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter

Policy name	Type	Description
CodeBuildBasePolicy-cicd_aws_build-ap-sout...	Customer managed	Policy used in trust relationship with Co

Permissions boundary - (not set)

Feedback Looking for language selection? Find it in the new Unified Settings [?] © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Services Search for services, features, blogs, docs, and more [Alt+S]

Console Home EC2 API Gateway Lambda S3 IAM CloudWatch Amazon Simple Email Service

Search for policies by property or policy name and press enter 9 matches

"s3" X Clear filters

Policy name	Type	Description
AmazonDMSRedshiftS3Role	AWS managed	Provides access to mar
AmazonS3FullAccess	AWS managed	Provides full access to :
QuickSightAccessForS3StorageManagementAnalyticsReadOnly	AWS managed	Policy used by QuickS
AmazonS3ReadOnlyAccess	AWS managed	Provides read only acce
AmazonS3OutpostsFullAccess	AWS managed	Provides full access to /
AWSBackupServiceRolePolicyForS3Backup	AWS managed	Policy containing permi
AWSBackupServiceRolePolicyForS3Restore	AWS managed	Policy containing permi
AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	Provides AWS Lambda
AmazonS3OutpostsReadOnlyAccess	AWS managed	Provides read only acce

Feedback Looking for language selection? Find it in the new Unified Settings [?] © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Services Search for services, features, blogs, docs, and more [Alt+S]

Console Home EC2 API Gateway Lambda S3 IAM CloudWatch Amazon Simple Email Service

Filter policies by property or policy name and press enter

9 matches

"s3" X Clear filters

Policy name	Type	Description
AmazonDMSRedshiftS3Role	AWS managed	Provides access to mar
AmazonS3FullAccess	AWS managed	Provides full access to :
QuickSightAccessForS3StorageManagementAnalyticsReadOnly	AWS managed	Policy used by QuickS
AmazonS3ReadOnlyAccess	AWS managed	Provides read only acce
AmazonS3OutpostsFullAccess	AWS managed	Provides full access to /
AWSBackupServiceRolePolicyForS3Backup	AWS managed	Policy containing permi
AWSBackupServiceRolePolicyForS3Restore	AWS managed	Policy containing permi
AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	Provides AWS Lambda
AmazonS3OutpostsReadOnlyAccess	AWS managed	Provides read only acce

Cancel Attach policies

STEP-6:

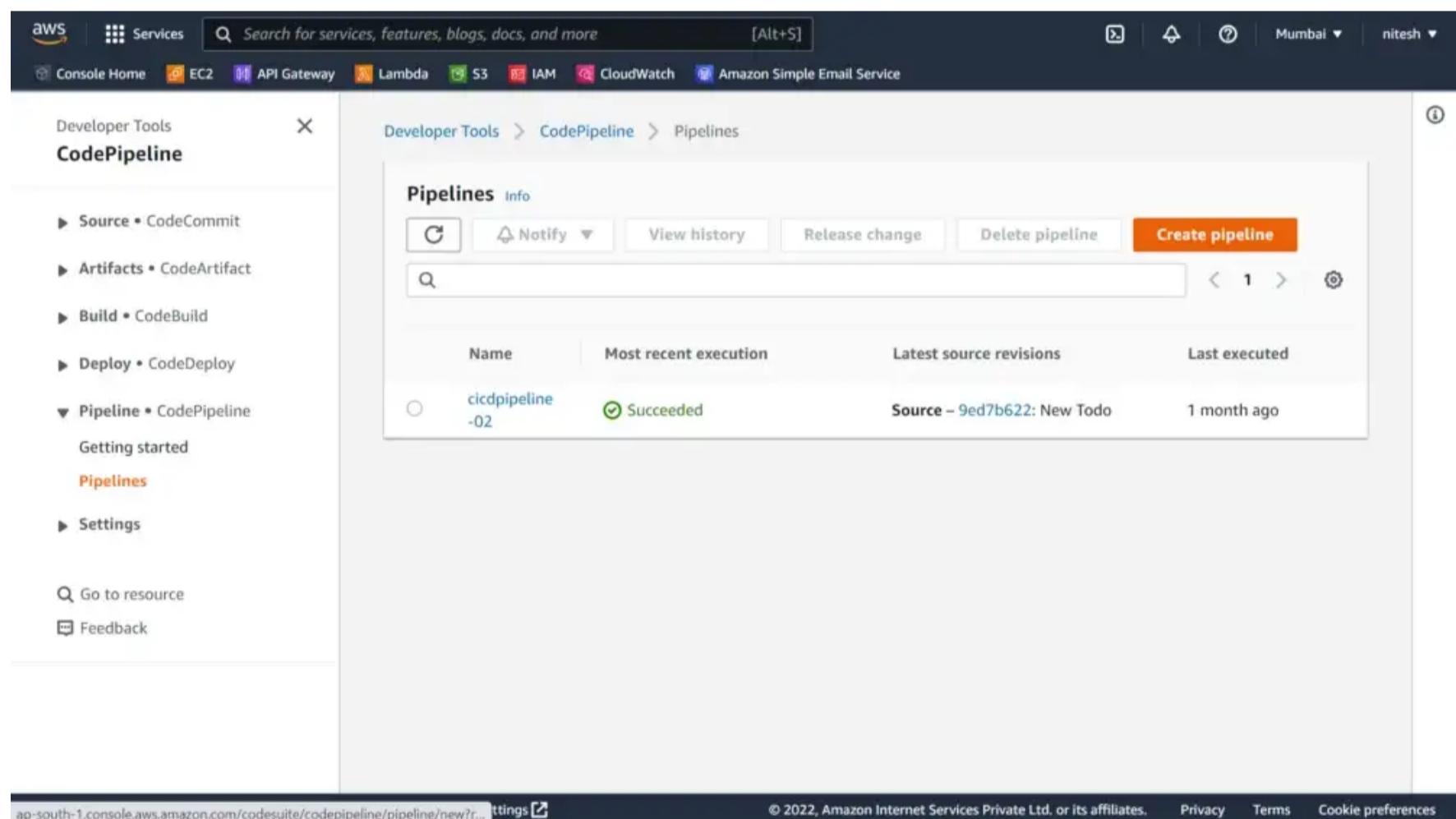
Code Pipeline (CI tool)

CodePipeline automates your release process's build, test, and deploy phases every time there is a code change, based on the release model you define. This enables you to rapidly and reliably deliver features and updates. For more details you can visit the below-mentioned link :

After creating the S3 bucket we need to integrate everything with CodePipeline.

Search for CodePipeline, go to **Pipelines**, and click on **Create pipeline**. In Advance Settings click on **Custom Location** with the bucket name and click on Next. Select AWS CodeCommit → Repo Name → master (Branch) → Next.

Select AWS CodeBuild → Region → Project Name → Next. Skip the Deploy stage for now. Review the pipeline and **Create pipeline**.



The screenshot shows the AWS CodePipeline console interface. On the left, there is a navigation sidebar with sections for Source (CodeCommit), Artifacts (CodeArtifact), Build (CodeBuild), Deploy (CodeDeploy), and Pipeline (CodePipeline). Under Pipeline, there are links for Getting started and Pipelines. The Pipelines section is currently selected, showing a list of existing pipelines. One pipeline is listed: "cicdpipeline-02", which has a status of "Succeeded", was triggered by "Source - 9ed7b622: New Todo", and was last executed "1 month ago". At the top right of the main content area, there is a prominent orange "Create pipeline" button. The top navigation bar includes links for Services, Search, and various AWS services like EC2, API Gateway, Lambda, S3, IAM, CloudWatch, and Amazon Simple Email Service. The top right also shows the location as "Mumbai" and the user as "nitesh".

The screenshot shows the AWS CodePipeline 'Create new pipeline' interface. At the top, there's a navigation bar with links like 'Console Home', 'EC2', 'API Gateway', 'Lambda', 'S3', 'IAM', 'CloudWatch', and 'Amazon Simple Email Service'. Below the navigation is a breadcrumb trail: 'Developer Tools > CodePipeline > Pipelines > Create new pipeline'. The main title 'Choose pipeline settings' is at the top left of the form. On the left, a vertical sidebar lists steps: Step 1 'Choose pipeline settings' (selected), Step 2 'Add source stage', Step 3 'Add build stage', Step 4 'Add deploy stage', and Step 5 'Review'. The 'Pipeline settings' section contains fields for 'Pipeline name' (set to 'cicdawspipeline'), 'Service role' (radio button selected for 'New service role' with a note to 'Create a service role in your account'), and 'Role name' (set to 'AWSCodePipelineServiceRole-ap-south-1-cicdawspipeline'). A checkbox 'Allow AWS CodePipeline to create a service role so it can be used with this new pipeline' is checked.

This screenshot shows the 'Advanced settings' step of the pipeline creation process. It includes sections for 'Artifact store', 'Bucket', and 'Encryption key'. In the 'Artifact store' section, 'Custom location' is selected with a note to 'Choose an existing S3 location from your account in the same region and account as your pipeline'. The 'Bucket' section shows a search input with 'cicdawsstorage' and a clear button 'X'. The 'Encryption key' section has 'Default AWS Managed Key' selected with a note to 'Use the AWS managed customer master key for CodePipeline in your account to encrypt the data in the artifact store.' A 'Customer Managed Key' option is also available with a note to 'To encrypt the data in the artifact store under an AWS KMS customer managed key, specify the key ID, key ARN, or alias ARN.' At the bottom right are 'Cancel' and 'Next' buttons.

Step 3

Add build stage

Step 4

Add deploy stage

Step 5

Review

Source provider

This is where you stored your input artifacts for your pipeline. Choose the provider and then provide the connection details.

AWS CodeCommit

Repository name

Choose a repository that you have already created where you have pushed your source code.

cicdwithaws_Repo

Branch name

Choose a branch of the repository

master

Change detection options

Choose a detection mode to automatically start your pipeline when a change occurs in the source code.

Amazon CloudWatch Events (recommended)
Use Amazon CloudWatch Events to automatically start my pipeline when a change occurs

AWS CodePipeline
Use AWS CodePipeline to check periodically for changes

Output artifact format

Choose the output artifact format.

CodePipeline default
AWS CodePipeline uses the default zip format for artifacts in the pipeline. Does not include git metadata about the repository.

Full clone
AWS CodePipeline passes metadata about the repository that allows subsequent actions to do a full git clone. Only supported for AWS CodeBuild actions.

Cancel Previous Next

Feedback Looking for language selection? Find it in the new Unified Settings [\[?\]](#)

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Console Home EC2 API Gateway Lambda S3 IAM CloudWatch Amazon Simple Email Service

Step 2

Add source stage

Step 3

Add build stage

Step 4

Add deploy stage

Step 5

Review

Build - optional

Build provider

This is the tool of your build project. Provide build artifact details like operating system, build spec file, and output file names.

AWS CodeBuild

Region

Asia Pacific (Mumbai)

Project name

Choose a build project that you have already created in the AWS CodeBuild console. Or create a build project in the AWS CodeBuild console and then return to this task.

cicd aws build

or [Create project \[?\]](#)

Environment variables - optional

Choose the key, value, and type for your CodeBuild environment variables. In the value field, you can reference variables generated by CodePipeline. [Learn more \[?\]](#)

Add environment variable

Build type

Single build
Triggers a single build.

Batch build
Triggers multiple builds as a single execution.

Cancel Previous Skip build stage Next

Feedback Looking for language selection? Find it in the new Unified Settings [\[?\]](#)

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS CodePipeline 'Create new pipeline' wizard, Step 4: Add deploy stage. The 'Deploy - optional' section is displayed, which includes a 'Deploy provider' dropdown menu. Below the dropdown is a note: 'Choose how you deploy to instances. Choose the provider, and then provide the configuration details for that provider.' Navigation buttons at the bottom include 'Cancel', 'Previous', 'Skip deploy stage' (highlighted in orange), and 'Next'.

For deployment we have 3 things to do :

- Creating web servers (Local or Cloud(AWS → EC2)).
- Configuration of the web server
- Deploy our code(files) to these web servers.

STEP-7:

EC2 (Web Server)

Amazon Elastic Compute Cloud (Amazon EC2) offers the broadest and deepest compute platform, with over 500 instances and a choice of the latest processor, storage, networking, operating system, and purchase model to help you best match the needs of your workload. For more details you can visit the below-mentioned link :

Creating EC2 instants :

Select the Amazon Linux → (Step: 2)t2 micro → (Step : 3)Number of instances: 2 → (Step: 4) Next → (Step: 5) Next → (Step: 6) Add Rule (HTTP: So everyone can visit our site) → (Step: 7) Launch

Services Search for services, features, blogs, docs, and more [Alt+S] Mumbai nitesh

Console Home EC2 API Gateway Lambda S3 IAM CloudWatch Amazon Simple Email Service

Next Step

⚠ This launch experience will soon be reaching end of life
We've introduced a new launch experience with new and updated features. You can opt in now by choosing Opt in to the new experience.
Currently, you can opt out to the old experience at any time. Please send us your feedback about the new experience so that we can continue to improve it.

Opt in to the new experience

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 1: Choose an Amazon Machine Image (AMI)

Search for an AMI by entering a search term e.g. "Windows"

Cancel and Exit

Search by Systems Manager parameter

Quick Start

My AMIs

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type - ami-08df646e18b182346 (64-bit x86) / ami-0e0aaaf29e73155b91 (64-bit Arm)

Select
64-bit (x86)
64-bit (Arm)

AWS Marketplace

Community AMIs

Free tier only ⓘ

Amazon Linux 2 AMI (HVM) - Kernel 4.14, SSD Volume Type - ami-09de362f44ba0a166 (64-bit x86) / ami-044ba583062cb113b (64-bit Arm)

Select
64-bit (x86)
64-bit (Arm)

Feedback Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Services Search for services, features, blogs, docs, and more [Alt+S] Mumbai nitesh

Console Home EC2 API Gateway Lambda S3 IAM CloudWatch Amazon Simple Email Service

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance families Current generation Show/Hide Columns

Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes
	t2	t2.xlarge	4	16	EBS only	-	Moderate	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

Feedback Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances	<input type="text" value="2"/>	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-0bf168604dc074cc9 (default)	<input type="button" value="Create new VPC"/>
Subnet	No preference (default subnet in any Availability Zone)	<input type="button" value="Create new subnet"/>
Auto-assign Public IP	<input type="button" value="Use subnet setting (Enable)"/>	
Hostname type	<input type="button" value="Use subnet setting (IP name)"/>	
DNS Hostname	<input type="checkbox"/> Enable IP name IPv4 (A record) DNS requests <input checked="" type="checkbox"/> Enable resource-based IPv4 (A record) DNS requests <input type="checkbox"/> Enable resource-based IPv6 (AAAA record) DNS requests	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	<input type="button" value="Open"/>	

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-08bbaef4a42ffdca4	<input type="text" value="8"/>	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	<input type="button" value="Not Encrypted"/>

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Shared file systems

You currently don't have any file systems on this instance. Select "Add file system" button below to add a file system.

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Tags](#)

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.

A copy of a tag can be applied to volumes, instances or both.

Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (128 characters maximum) Value (256 characters maximum)

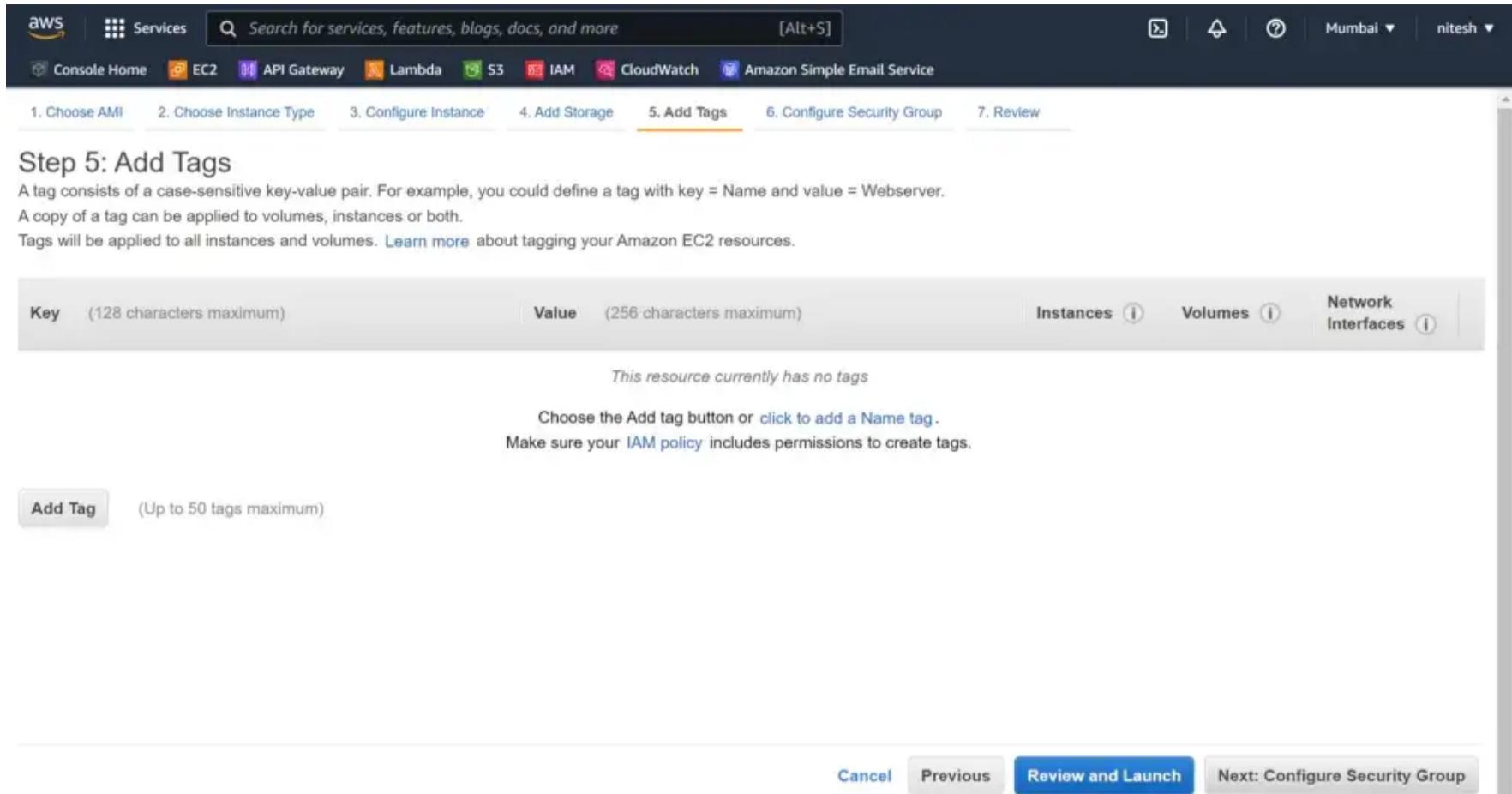
Instances (i) Volumes (i) Network Interfaces (i)

This resource currently has no tags

Choose the Add tag button or click to add a Name tag.
Make sure your IAM policy includes permissions to create tags.

Add Tag (Up to 50 tags maximum)

Cancel Previous Review and Launch Next: Configure Security Group



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: Create a new security group
 Select an existing security group

Security group name: launch-wizard-8

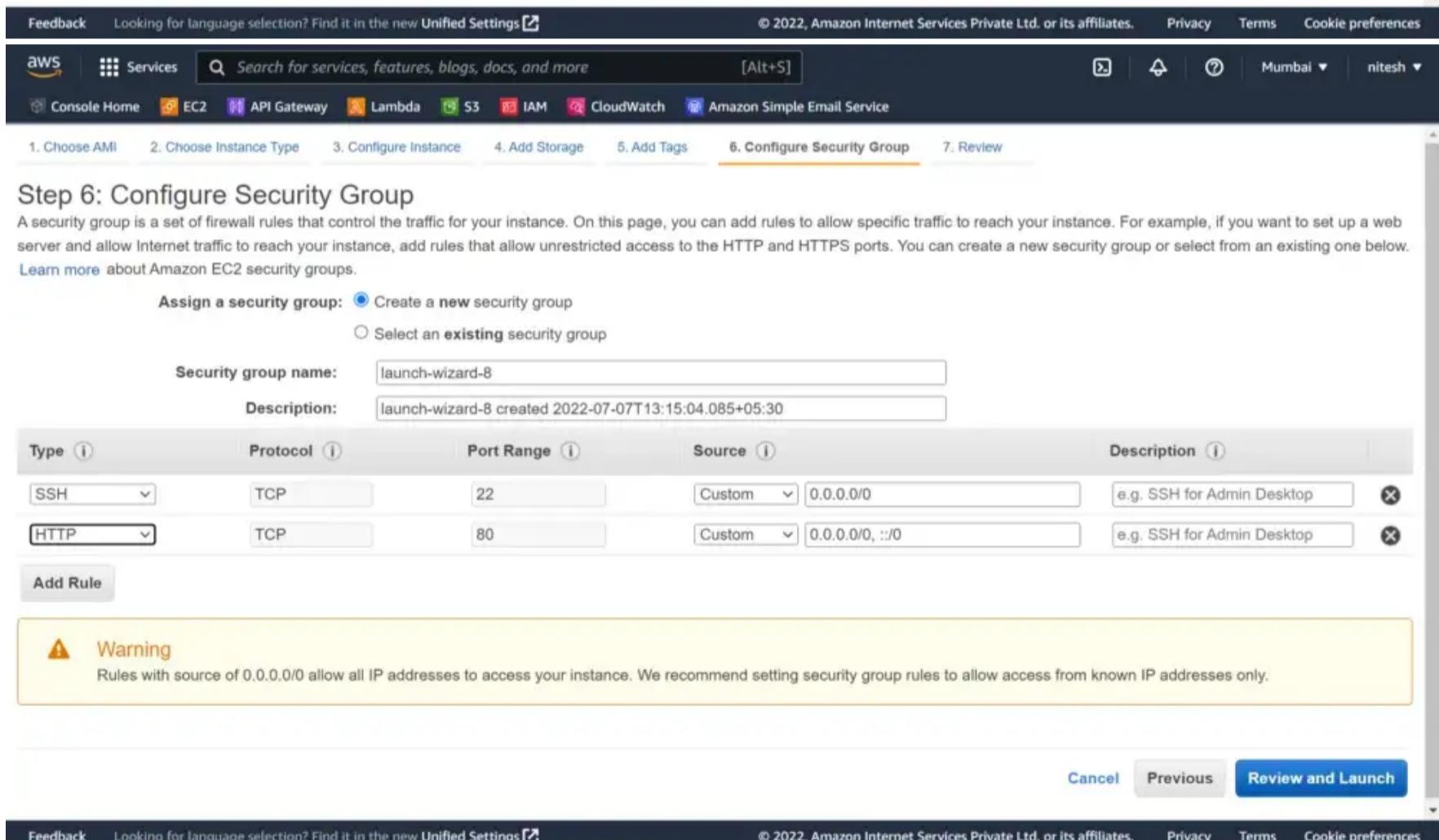
Description: launch-wizard-8 created 2022-07-07T13:15:04.085+05:30

Type (i)	Protocol (i)	Port Range (i)	Source (i)	Description (i)
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
HTTP	TCP	80	Custom 0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop

Add Rule

Warning
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel Previous Review and Launch



Review the details and view Instances, here we can tag them by selecting them and selecting the tag option. Name instances.

The screenshot shows the AWS Management Console interface. At the top, there's a search bar with placeholder text "Search for services, features, blogs, docs, and more". To its right is a keyboard shortcut "[Alt+S]". On the far right of the top bar are icons for notifications, help, and user "nitesh". Below the top bar, a horizontal menu bar contains links for "Console Home", "EC2", "API Gateway", "Lambda", "S3", "IAM", "CloudWatch", and "Amazon Simple Email Service".

Launch Status

i Get notified of estimated charges

Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click [View Instances](#) to monitor your instances' status. Once your instances are in the **running** state, you can [connect](#) to them from the Instances screen. [Find out](#) how to connect to your instances.

▼ Here are some helpful resources to get you started

- [How to connect to your Linux instance](#)
- [Learn about AWS Free Usage Tier](#)
- [Amazon EC2: User Guide](#)
- [Amazon EC2: Discussion Forum](#)

While your instances are launching you can also

- [Create status check alarms](#) to be notified when these instances fail status checks. (Additional charges may apply)
- [Create and attach additional EBS volumes](#) (Additional charges may apply)
- [Manage security groups](#)

[View Instances](#)

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with various EC2-related options like EC2 Dashboard, Global View, Events, Tags, Limits, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, and Capacity Reservations. The main area shows a table of instances:

Name	env	Instance ID	Instance state
cicd02	Testing	i-033c92c36e0864ba3	Stopped
cicd2	Production	i-054e78dabf6286bb1	Stopped
JenkinsOS	-	i-0b747274cdfb6163f	Stopped
cicdaws-Testing	Testing	i-0d5690436b45d0e6b	Stopped
cicdaws-Production	Production	i-0da7ed8ca342c64e3	Stopped

A success message at the top of the main area says "Successfully stopped i-0da7ed8ca342c64e3,i-0d5690436b45d0e6b". There are buttons for "Connect", "Actions", and "Launch Instances".

Feedback Looking for language selection? Find it in the new [Unified Settings](#) i © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Now let's create a role for ec2 (EC2 → CodeDeploy) :

AWS Services Search for services, features, blogs, docs, and more [Alt+S] Global nitesh

Console Home EC2 API Gateway Lambda S3 IAM CloudWatch Amazon Simple Email Service

IAM > Roles > Create role

Step 1 Select trusted entity

Step 2 Add permissions

Step 3 Name, review, and create

Select trusted entity

Trusted entity type

AWS service Allow AWS services like EC2, Lambda, or others to perform actions in this account.

AWS account Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

Web identity Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

SAML 2.0 federation Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

Custom trust policy Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Common use cases

EC2 Allows EC2 Instances to call AWS services on your behalf.

Feedback Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

aws Services Search for services, features, blogs, docs, and more [Alt+S] Global nitesh

Console Home EC2 API Gateway Lambda S3 IAM CloudWatch Amazon Simple Email Service

Step 3 Name, review, and create

Trusted entity type

AWS service Allow AWS services like EC2, Lambda, or others to perform actions in this account.

AWS account Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

Web identity Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

SAML 2.0 federation Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

Custom trust policy Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Common use cases

EC2 Allows EC2 Instances to call AWS services on your behalf.

Lambda Allows Lambda functions to call AWS services on your behalf.

Use cases for other AWS services:

Choose a service to view use case

Cancel Next

The screenshot shows the 'Add permissions' step of creating a new IAM role. The top navigation bar includes links for Services, EC2, API Gateway, Lambda, S3, IAM, CloudWatch, and Amazon Simple Email Service. The search bar says 'Search for services, features, blogs, docs, and more'. The top right shows 'Global' and 'nitesh'. The main area has a sidebar with 'Step 1 Select trusted entity', 'Step 2 Add permissions' (which is selected), and 'Step 3 Name, review, and create'. The title 'Add permissions' is centered above a table. The table header is 'Permissions policies (Selected 1/768)' with columns 'Policy name', 'Type', and 'Description'. A search bar at the top of the table says 'Filter policies by property or policy name and press enter' with a placeholder '11 matches'. A filter bar below it shows a checked filter for 'codede' and a 'Clear filters' button. The table lists several policies, with the first one selected: 'AmazonEC2RoleforAWSCodeDeploy' (AWS managed, Provides EC2 access to S3 bucket to d...). Other listed policies include 'AWSCodeDeployRoleForECS', 'AWSCodeDeployReadOnlyAccess', 'AWSCodeDeployFullAccess', 'AWSCodeDeployRole', and 'AWSCodeDeployRoleForECSLimited'.

The screenshot shows the 'Name, review, and create' step of creating a new IAM role. The top navigation bar and search bar are identical to the previous screenshot. The main area has a sidebar with 'Step 1 Select trusted entity', 'Step 2 Add permissions' (selected), and 'Step 3 Name, review, and create'. The title 'Name, review, and create' is centered above a 'Role details' section. In the 'Role details' section, there is a 'Role name' field containing 'ec2codedeploysaws' with a note about character limits. Below it is a 'Description' field with the text 'Allows EC2 instances to call AWS services on your behalf.' and a note about character limits. At the bottom of the 'Role details' section is a 'Step 1: Select trusted entities' link and an 'Edit' button. The bottom of the page includes standard footer links for Feedback, Unified Settings, Copyright 2022, Privacy, Terms, and Cookie preferences.

Now attach the role to ec2 as follow :
Select instance → Actions → Security → Modify IAM role → Update IAM role.

The screenshot shows the AWS EC2 Instances page. In the left sidebar, under 'Instances', 'Instances' is selected. In the main content area, an instance named 'cicdaws-Testing' is selected. On the right, a context menu is open with the 'Modify IAM role' option highlighted. Below this, the instance details page is shown for 'i-0d5690436b45d0e6b'. The 'Details' tab is selected, showing the instance summary with fields like Instance ID, Public IPv4 address, Private IPv4 addresses, Instance state, Public IPv4 DNS, and Hostname type.

The screenshot shows the 'Modify IAM role' page for the instance 'i-0d5690436b45d0e6b'. The 'Instance ID' field is populated with 'i-0d5690436b45d0e6b (cicdaws-Testing)'. The 'IAM role' section contains a dropdown menu with 'eccodedeployaws' selected, and a 'Create new IAM role' button. At the bottom, there are 'Cancel' and 'Update IAM role' buttons.

We also have to set up Code Deploy Agent in our EC2 instance(webserver). For more details about the CodeDeploy agent you can visit the below-mentioned link :

STEP-8:

Connect to instant and paste the below code :

sudo yum update -y

sudo yum install -y ruby wget

wget https://aws-codedeploy-eu-west-1.s3.eu-west-1.amazonaws.com/latest/install

chmod +x ./install

sudo ./install auto

sudo service codedeploy-agent status

Here in step: 3 → change : eu-west-1 → to your region(ex. ap-south-1).

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with various EC2-related options like EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, and Capacity Reservations. The main area displays a table of instances:

Name	env	Instance ID	Instance state
cicd02	Testing	i-033c92c36e0864ba3	Stopped
cicd2	Poduction	i-054e78dabf6286bb1	Stopped
JenkinsOS	-	i-0b747274cdfb6163f	Stopped
cicdaws-Testing	Testing	i-0d5690436b45d0e6b	Running
cicdaws-Production	Production	i-0da7ed8ca342c64e3	Stopped

At the bottom of the page, there's a section for the selected instance: "Instance: i-0d5690436b45d0e6b (cicdaws-Testing)".

Screenshot of the AWS EC2 Connect interface showing connection details for instance i-0d5690436b45d0e6b. The 'EC2 Instance Connect' tab is selected. The instance ID is i-0d5690436b45d0e6b, the public IP address is 13.235.19.229, and the user name is ec2-user. A note states: 'Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.' Below the connection details is a terminal window showing the deployment of the 'codedeploy-agent' package. The terminal output includes:

```

ap-south-1.console.aws.amazon.com/ec2/v2/connect/.../i-0d5690436b45d0e6b
codedeploy-agent      noarch      1.3.2-1902      /codedeploy-agent-1.3.2-1902.noarch.tmp-20220707-3724-1t122bp      11 M
Transaction Summary
=====
Install 1 Package
=====
Total size: 11 M
Installed size: 11 M
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction

pre hook : 1
Checking the ruby version.
Checking if there is already a process named codedeploy-agent running.
  Installing : codedeploy-agent-1.3.2-1902.noarch
  1/1

post hook : 1
Check if there is a codedeployagent config file.
Start codedeploy-agent in post hook if this is a first install.
  Verifying  : codedeploy-agent-1.3.2-1902.noarch
  1/1

Installed:
  codedeploy-agent.noarch 0:1.3.2-1902

Complete!
I, [2022-07-07T08:01:43.135596 #3724] INFO -- : Update check complete.
I, [2022-07-07T08:01:43.135691 #3724] INFO -- : Stopping updater.
[ec2-user@ip-172-31-36-88 ~]$ sudo service codedeploy-agent status
The AWS CodeDeploy agent is running as PID 3806
[ec2-user@ip-172-31-36-88 ~]$ sudo service codedeploy-agent status

```

The terminal shows the deployment of the 'codedeploy-agent' package, which includes checking the ruby version, installing the package, verifying it, and starting the service. The final status shows the service is running with PID 3806.

STEP-9:

Code Deploy (CD tool)

AWS CodeDeploy is a fully managed deployment service that automates software deployments to a variety of computing services such as Amazon EC2, AWS Fargate, AWS Lambda, and your on-premises servers. For more details you can visit the below-mentioned link :

CodeDeploy will configure our web servers and deploy our code. Let's first create a role for CodeDeploy (CodeDeploy → EC2):

Select the role and attach the EC2Access policy to it.

The screenshot shows the AWS IAM service console. A role named "AWSCodeDeployRole" is being created. The "Attached as" section shows the "EC2Access" policy is attached. Below this, the "Tags" section is shown, with an "Add tag" button and a note indicating up to 50 tags can be added. At the bottom right, there are "Cancel", "Previous", and "Create role" buttons.

AWSCodeDeployRole AWS managed Permissions policy

Tags

Add tags (Optional)

No tags associated with the resource.

Add tag You can add up to 50 more tags

Create role

The screenshot shows the "Identity and Access Management (IAM)" service console. The "Roles" section is selected. A list of roles is displayed, including "build03-role", "codebuild-cicdbuild02-service-role", "codebuild-cicdwithaws-service-role", "codebuild-cicd_aws_build-service-role", "codedeploytoec2", "codedeploytoec202", "codedeploytoec2AWS", "codedeploytoec2_cicd03", and "codedeploypermissionrole". The "codedeploytoec2AWS" role is currently selected. The "Manage" button is visible at the bottom right of the role card.

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

Roles Anywhere

Manage

https://us-east-1.console.aws.amazon.com/iamv2/home#/roles/details/codedeploytoec2AWS

Screenshot of the AWS IAM console showing the 'Permissions policies' section for a role named 'AWSCodeDeployRole'. The role has one managed policy attached.

Permissions policies (1)

You can attach up to 10 managed policies.

AWSCodeDeployRole AWS managed Provides CodeDeploy service access to expand tags and int...

Permissions boundary - (not set)

Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting but can be used to delegate permission management to others.

Set permissions boundary

Screenshot of the AWS IAM console showing the 'Current permissions policies' section for a role named 'AWSCodeDeployRole'. The role has one managed policy attached.

Current permissions policies (1)

Other permissions policies (Selected 1/767)

Filter policies by property or policy name and press enter

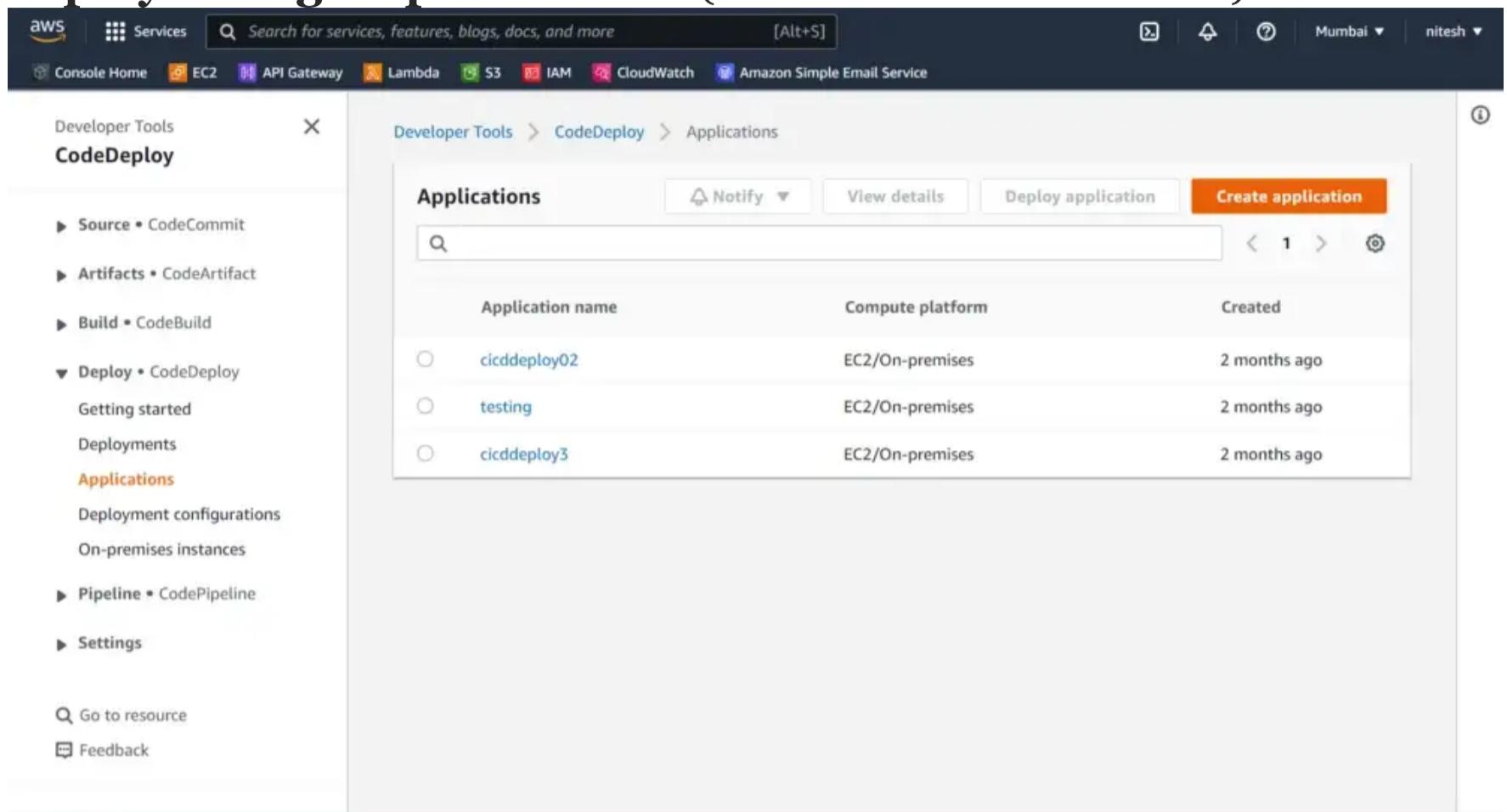
26 matches

"ec2" X Clear filters

Policy name	Type	Description
AmazonEC2FullAccess	AWS managed	Provides full access to Amazon EC2 via the AWS Manage...
AmazonEC2RoleforSSM	AWS managed	This policy will soon be deprecated. Please use AmazonS...
AmazonEC2RoleforAWSCodeDeploy	AWS managed	Provides EC2 access to S3 bucket to download revision. ...
AmazonEC2ContainerRegistryFullAccess	AWS managed	Provides administrative access to Amazon ECR resources
AmazonEC2ContainerRegistryReadOnly	AWS managed	Provides read-only access to Amazon EC2 Container Reg...

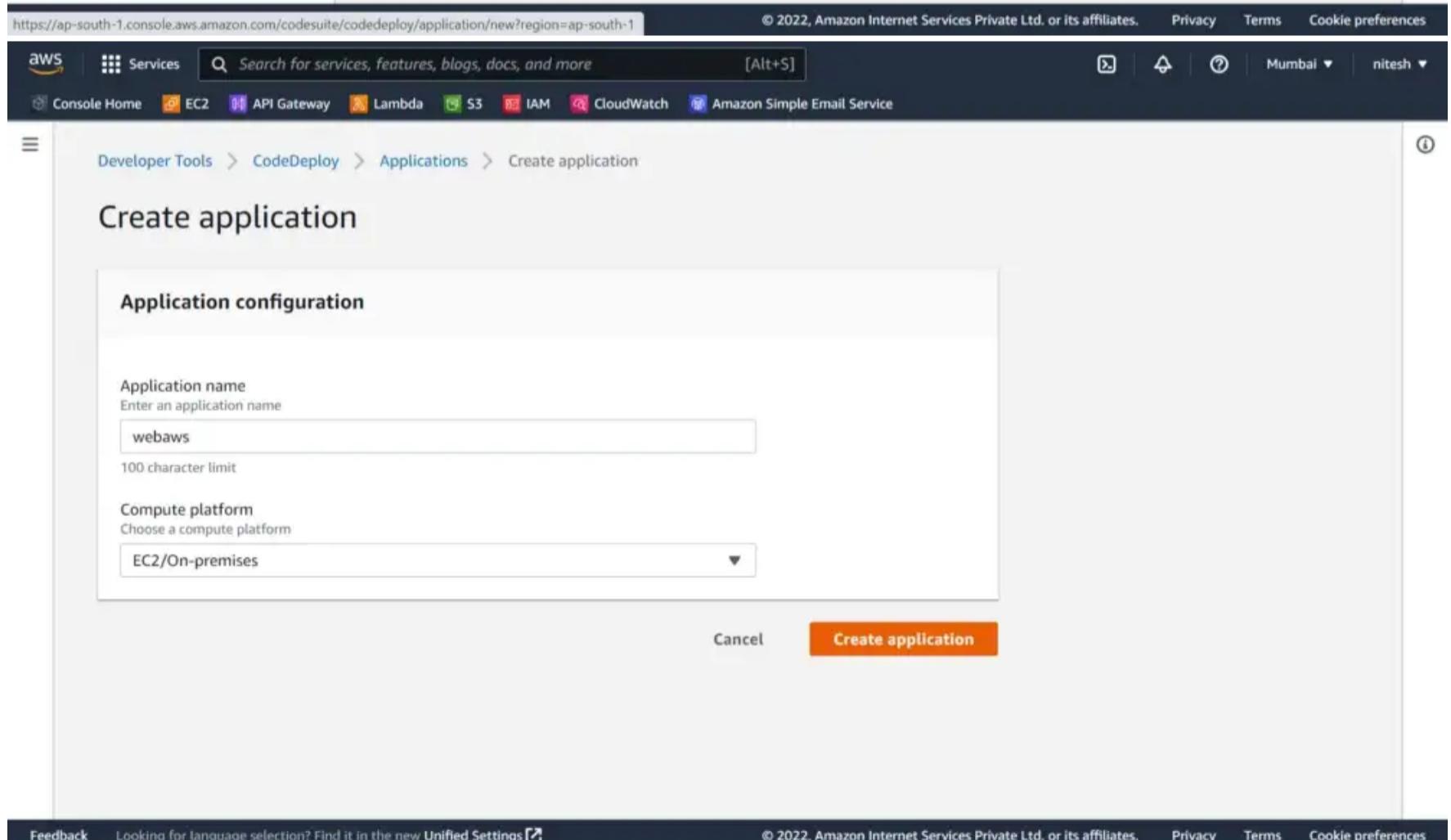
STEP-10:

In CodeDeploy: Create Application and after that Create deployment group with the role(the role we created before).



The screenshot shows the AWS CodeDeploy Applications page. On the left, there's a sidebar with navigation links for Source (CodeCommit), Artifacts (CodeArtifact), Build (CodeBuild), Deploy (CodeDeploy), Pipeline (CodePipeline), and Settings. Under Deploy, 'Applications' is selected. The main content area displays a table of existing applications. The columns are Application name, Compute platform, and Created. The data is as follows:

Application name	Compute platform	Created
cicdddeploy02	EC2/On-premises	2 months ago
testing	EC2/On-premises	2 months ago
cicdddeploy3	EC2/On-premises	2 months ago



The screenshot shows the 'Create application' dialog box. At the top, it says 'Create application'. Below that is a section titled 'Application configuration'. It has two main fields: 'Application name' with a value of 'webaws' and 'Compute platform' set to 'EC2/On-premises'. At the bottom right of the dialog are 'Cancel' and 'Create application' buttons.

Services Search for services, features, blogs, docs, and more [Alt+S] Mumbai nitesh

Console Home EC2 API Gateway Lambda S3 IAM CloudWatch Amazon Simple Email Service

Developer Tools CodeDeploy

Source • CodeCommit
Artifacts • CodeArtifact
Build • CodeBuild
Deploy • CodeDeploy
Getting started
Deployments
Applications Application Settings Deployment configurations On-premises instances Pipeline • CodePipeline Settings Go to resource

Developer Tools > CodeDeploy > Applications > webaws

webaws

Notify Delete application

Application details

Name	Compute platform
webaws	EC2/On-premises

Deployments Deployment groups Revisions

Deployment groups

Name	Status	Last attempted deployment	Last successful deployment	Trigger count
No deployment groups				

View details Edit Create deployment group

No deployment groups

Before you can deploy your application using CodeDeploy, you must create a deployment group.

ap-south-1.console.aws.amazon.com/codesuite/codedeploy/applications/.../ne... © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

CodeCommit CodeBuild - Al... CodeDeploy - IAM Manager IAM Manager i-0d5690436b IAM Manager Update

Gmail YouTube Maps Translate Challenge | Microso... My Drive - Google... GitHub - vimallinux... Uploading Files in... DO007 Serverless + mediu...

aws Services Search for services, features, blogs, docs, and more [Alt+S] Mumbai nitesh

Console Home EC2 API Gateway Lambda S3 IAM CloudWatch Amazon Simple Email Service

Developer Tools > CodeDeploy > Applications > webaws > Create deployment group

Create deployment group

Application

Application	webaws
Compute type	EC2/On-premises

Deployment group name

Enter a deployment group name

100 characters limit

Feedback Looking for language selection? Find it in the new Unified Settings © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences 11:28 AM 7/8/2022

The screenshot shows the AWS CodeDeploy application configuration page. In the 'Service role' section, a service role with ARN `arn:aws:iam::718871632185:role/codedeploytoec2AWS` is selected. The 'Deployment type' section is expanded, showing two options: 'In-place' (selected) and 'Blue/green'. Under 'Deployment groups', it says 'Select any combination of Amazon EC2 Auto Scaling groups, Amazon EC2 instances, and on-premises instances to add to this deployment'. Under 'Amazon EC2 instances', there is a checked checkbox for 'Amazon EC2 instances' with a note: '1 unique matched instance. Click here for details'. Below this, there is a 'Tag group 1' section with a 'Key' input field containing 'Name' and a 'Value - optional' input field containing 'cicdaws-Testing'. A 'Remove tag' button is also present.

The screenshot shows the continuation of the AWS CodeDeploy application configuration page. It lists 'Instances | EC2' and 'i-0d5690436b' as target instances. The 'Tag group 1' section is still visible at the bottom left. The status bar at the bottom right shows the time as 11:28 AM and the date as 7/8/2022.

The screenshot shows the final configuration summary of the AWS CodeDeploy application. It includes sections for 'Service role', 'Deployment type', 'Deployment groups', and 'Tags'. The status bar at the bottom right shows the time as 11:30 AM and the date as 7/8/2022.

Before updating CodePipeline for deployment, we are adding some files.
Files :

- `Buildspec.yml` : For CodeBuild
- `Appspec.yml` : For CodeDeploy
- Scripts(Folder) : For Confirmation (described in `Appspec.yml`)

For files go to the below-mentioned link:

Update CodeBuild: Got to Build the project Click on Edit and then click on Buildspec → Use buildspec file → Update buildspec.

Buildspec.yml file :

Here grep -i LW index.html command will look for the LW word in index.html

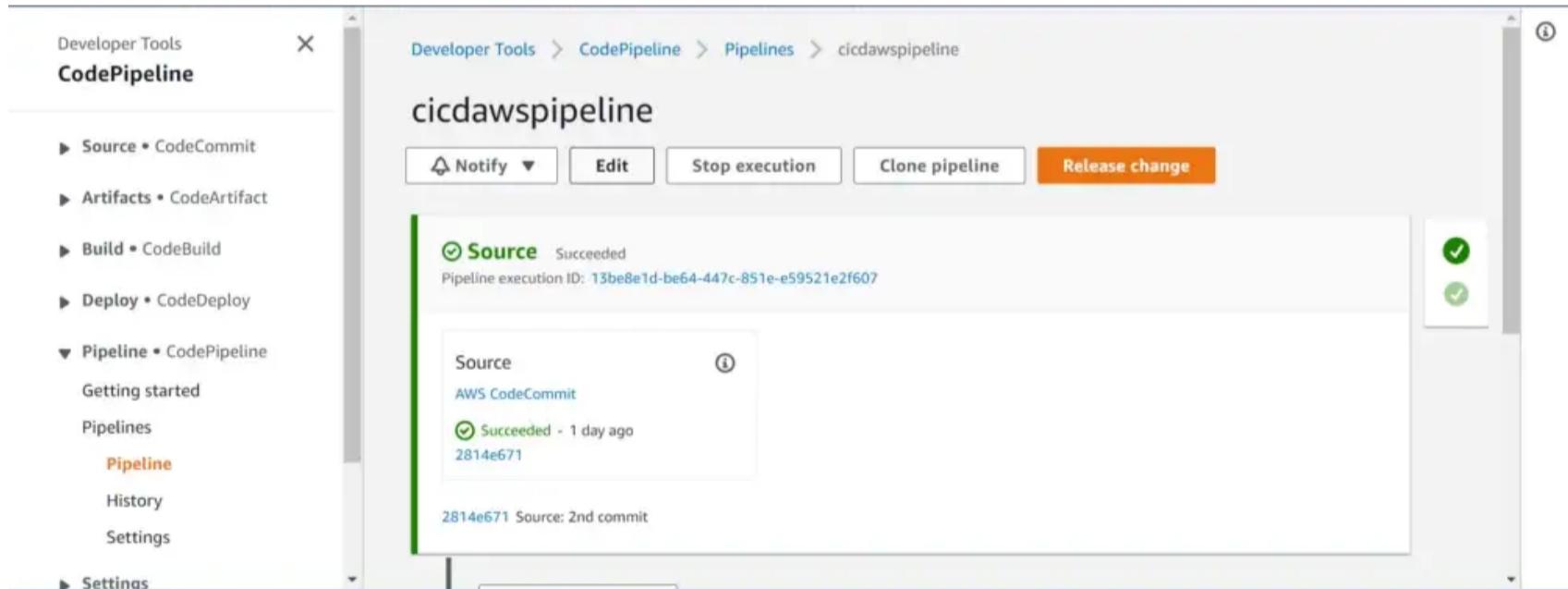
Appspec.yml file:

Scripts you will find at:<https://github.com/devopsoo14/cicd-with-aws.git>

Now add all files and the Script folder with your code then commit it and push it.

Now let's add the deploy stage with CodePipeline :

CodePipeline: Pipeline → Edit (Button) → Add Stage (Below Build Stage) → Stage Name → Add Action Group → Edit it → Save → Release Change (For testing)



The screenshot shows the AWS CodePipeline console interface. On the left, a sidebar menu is open under the 'CodePipeline' heading, listing various stages: Source, Artifacts, Build, Deploy, Pipeline, Getting started, Pipelines, Pipeline (selected), History, Settings, and Settings. The main area displays the 'Source' stage, which is configured to use 'AWS CodeCommit'. Below it is the 'Edit: Build' stage, which is configured to use 'AWS CodeBuild'. A large 'Edit stage' button is visible next to the build stage. At the bottom of the main area, there is a '+ Add stage' button. The browser's address bar shows the URL: ap-south-1.console.aws.amazon.com/codesuite/codepipeline/pipelines/cicdawspipeline/edit?region=ap-south-1. The status bar at the bottom right indicates the time as 11:32 AM and the date as 7/8/2022.

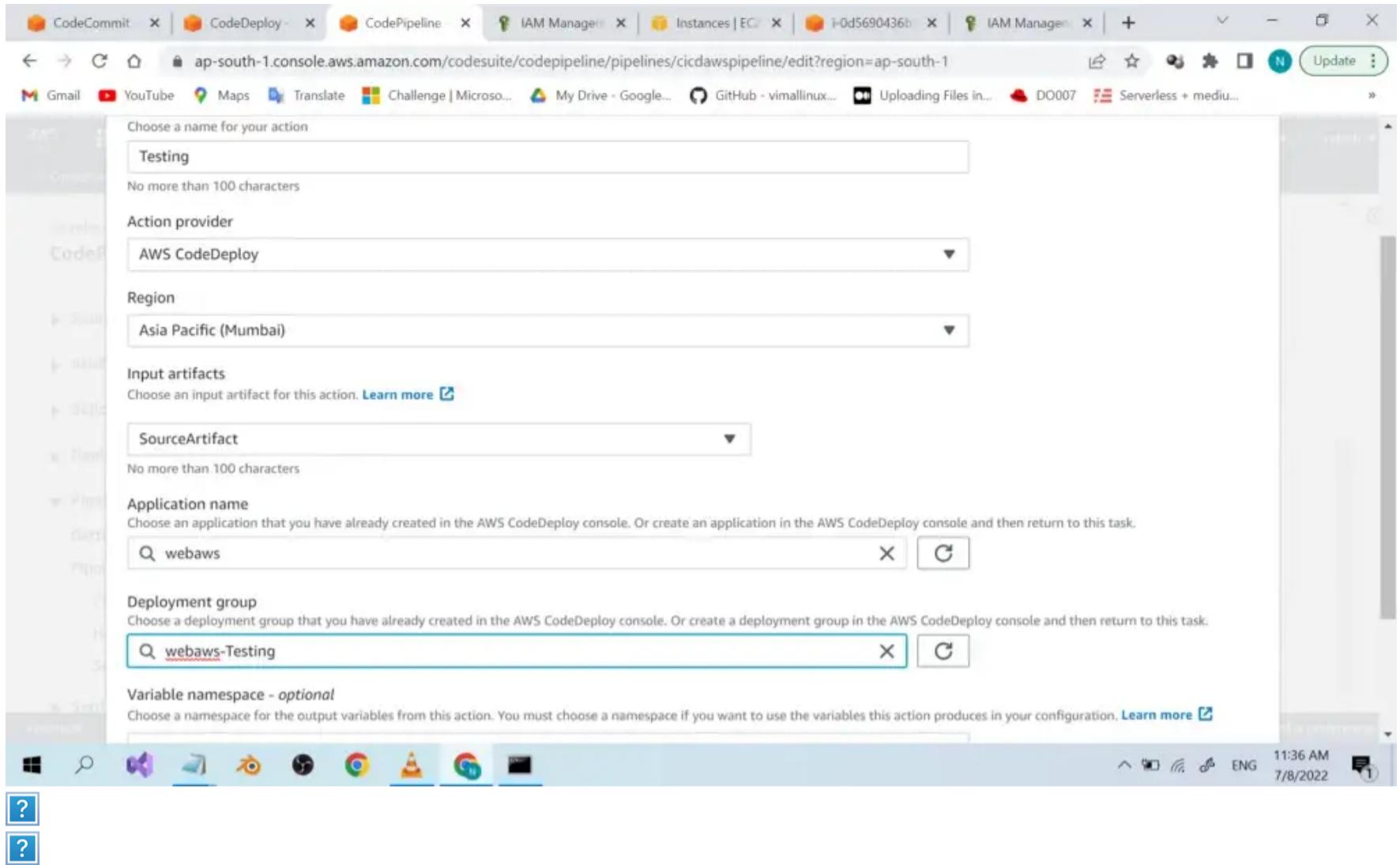
This screenshot shows the same AWS CodePipeline interface, but with a modal dialog box in the foreground titled 'Add stage'. The dialog box has a 'Stage name' input field where 'Deploy-Testing' is typed. There is also a note below the input field stating 'No more than 100 characters'. At the bottom of the dialog are 'Cancel' and 'Add stage' buttons. The background shows the same pipeline configuration as the previous screenshot, with the 'Source' and 'Build' stages already defined. The browser's address bar and status bar are identical to the first screenshot.

The screenshot shows the AWS CodePipeline console with the pipeline editor open. On the left, a sidebar menu is visible under the 'CodePipeline' heading, listing various stages and actions. The main area displays two stages: 'Build' (using AWS CodeBuild) and 'Deploy-Testing'. A modal window titled 'Edit: Deploy-Testing' is open, showing a button to '+ Add action group'. Below the stages, there are buttons for 'Edit stage', 'Delete', and 'Done'.

The screenshot shows the AWS CodeDeploy console with the 'Edit action' configuration dialog open. The dialog fields include:

- Action name: Testing
- Action provider: AWS CodeDeploy
- Region: Asia Pacific (Mumbai)
- Input artifacts: (empty dropdown)
- Application name: (empty search bar)

The background shows the AWS CodeDeploy console interface with various tabs and navigation elements.



QAT

The difference between Continuous Delivery and Continuous Deployment :

Continuous Delivery: Manual QAT Approval

Continuous Deployment: Automatic QAT Approval

Let's add a manual QAT stage :

CodePipeline: Pipeline → Edit (Button) → Add Stage (Below Deploy Stage) → Stage Name → Add Action Group → Edit action → Save → Release Change (For testing)

Edit action

Action name
Choose a name for your action **Approvals**
Manual Approval

No more than 100 characters

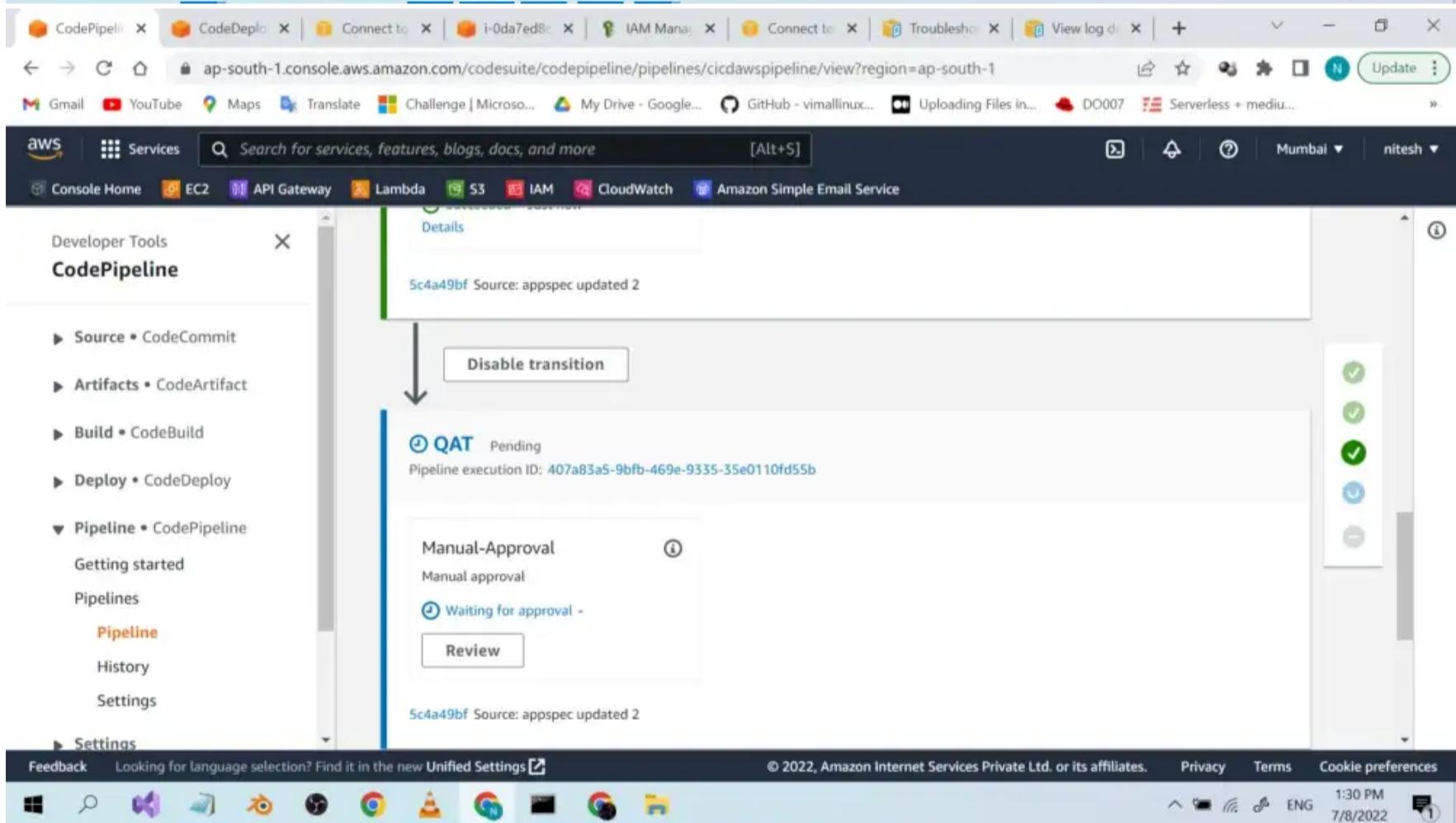
Action provider
Manual approval

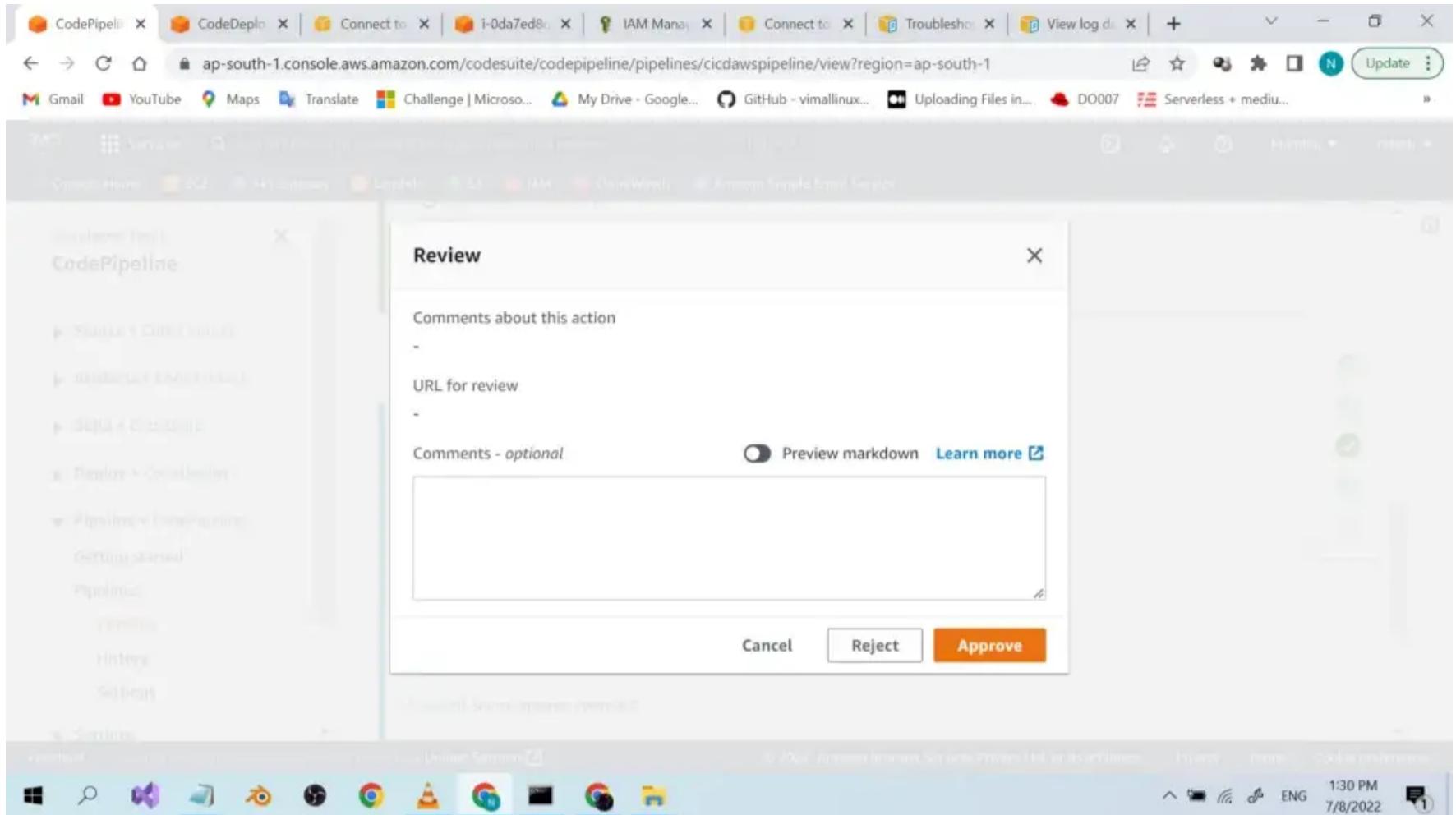
Configure the approval request.

SNS topic ARN - optional

URL for review - optional
Type the URL you want to provide to the reviewer as part of the approval request. The URL must begin with 'http://' or 'https://'.
[]

Comments - optional
Comments you type here display for the reviewer in email notifications or the console.
[]





Production Environment

In CodeDeploy: Click on Application and after that **Create deployment group** with the role(the role we created before), just like we created Testing deployment. Now add the agent and the role (EC2 → CodeDeploy) in the other EC2 instance.

Now create a new stage in CodePipeline for production.

In CodePipeline:

Pipeline → Edit (Button) → Add Stage (Below Deploy Stage) → Stage Name → Add Action Group → Edit action → Save → Release Change

The screenshot shows the AWS CodePipeline console. A modal window titled "Action Manual-Approval was approved" is displayed, indicating that the "Sc4a49bf Source: appspec updated 2" action has been approved. Below this, the "Deploy-Production" step is shown as "Succeeded" with Pipeline execution ID: 407a83a5-9bfb-469e-9335-35e0110fd55b. The status bar at the bottom right shows the date and time as 7/8/2022 1:31 PM.

Action Manual-Approval was approved

Sc4a49bf Source: appspec updated 2

Disable transition

Deploy-Production Succeeded

Pipeline execution ID: 407a83a5-9bfb-469e-9335-35e0110fd55b

Deploy-Production

AWS CodeDeploy

Succeeded - Just now

Details

Sc4a49bf Source: appspec updated 2

Instances (1/5)

Instances (1/5) Info

Search

Name	env	Instance ID	Instance state
JenkinsOS	-	i-0b747274cd86163f	Stopped
cicdaws-Testing	Testing	i-0d5690436b45d0e6b	Running
cicdaws-Production	Production	i-0da7ed8ca342c64e3	Running

Instance: i-0da7ed8ca342c64e3 (cicdaws-Production)

Details Security Networking Storage Status checks Monitoring Tags

Instance summary

Instance ID: i-0da7ed8ca342c64e3 (cicdaws-Production)

Public IPv4 address copied: 15.206.92.134 | open address

Private IPv4 addresses: 172.31.44.35

Feedback Looking for language selection? Find it in the new Unified Settings © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Instances (1/5) Info

Search

Name	env	Instance ID	Instance state
JenkinsOS	-	i-0b747274cd86163f	Stopped
cicdaws-Testing	Testing	i-0d5690436b45d0e6b	Running
cicdaws-Production	Production	i-0da7ed8ca342c64e3	Running

Instance: i-0da7ed8ca342c64e3 (cicdaws-Production)

Details Security Networking Storage Status checks Monitoring Tags

Instance summary

Instance ID: i-0da7ed8ca342c64e3 (cicdaws-Production)

Public IPv4 address copied: 15.206.92.134 | open address

Private IPv4 addresses: 172.31.44.35

Feedback Looking for language selection? Find it in the new Unified Settings © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

