

ADVANCE DEVOPS EXP-2

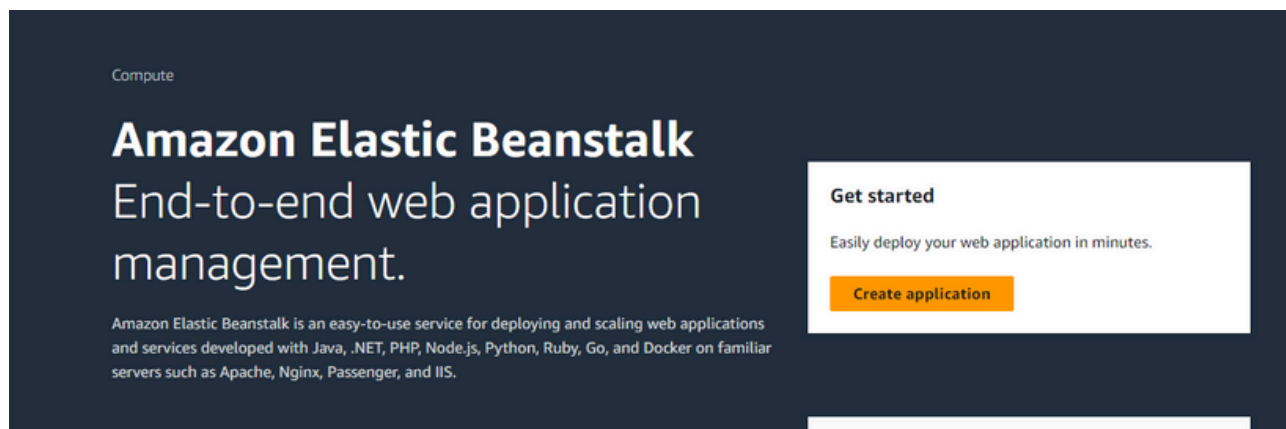
Aditi Taksale

D15A/60

Aim: To build your application using AWS Codebuild and deploy on S3 using AWS CodePipeline deploy sample application on EC2 instance using AWS codedeploy.

Code and Output :

Using elastic beanstalk:




The image shows the Amazon Elastic Beanstalk landing page. It features a dark blue header with the word 'Compute' in the top left. The main heading is 'Amazon Elastic Beanstalk' in large white font, followed by 'End-to-end web application management.' Below this, a paragraph describes the service: 'Amazon Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS.' On the right side, there is a white box titled 'Get started' with the text 'Easily deploy your web application in minutes.' and an orange button labeled 'Create application'.


Environment tier [Info](#)

Amazon Elastic Beanstalk has two types of environment tiers to support different types of web applications.

☒ **Web server environment**

Run a website, web application, or web API that serves HTTP requests. [Learn more](#) 

☐ **Worker environment**

Run a worker application that processes long-running workloads on demand or performs tasks on a schedule. [Learn more](#) 

Application information [Info](#)

Application name

Maximum length of 100 characters.

► **Application tags (optional)**

Platform [Info](#)

Platform type

☒ Managed platform

Platforms published and maintained by Amazon Elastic Beanstalk. [Learn more](#)

☐ Custom platform

Platforms created and owned by you. This option is unavailable if you have no platforms.

Platform

PHP

Platform branch

PHP 8.3 running on 64bit Amazon Linux 2023

Platform version

4.3.2 (Recommended)

Environment properties

Key



Value



No environment properties

There are no environment properties defined

Cancel

Previous

Submit

Aditibean-evn [Info](#)



Actions

Upload and deploy

Environment overview

Health

Unknown

Environment ID

e-vbcjjswjbp

Domain

-

Application name

Vedangbean

Platform

Change version

Platform

PHP 8.3 running on 64bit Amazon Linux 2023/4.3.2

Running version

-

Platform state

Supported

[Developer Tools](#) > [CodePipeline](#) > Pipelines

Introducing the new V2 pipeline type with improved release safety, pipeline triggers, parameterized pipelines, and a new billing model. [Learn more](#)

Pipelines [Info](#)



Notify

View history

Release change

Delete pipeline

Create pipeline

Q

< 1 > @

Name

Latest execution status

Latest source revisions

Latest execution started

Most recent executions

No results

There are no results to display.

Choose pipeline settings [Info](#)

Step 1 of 5

Pipeline settings

Pipeline name

Enter the pipeline name. You cannot edit the pipeline name after it is created.

No more than 100 characters

Pipeline type

- i** You can no longer create V1 pipelines through the console. We recommend you use the V2 pipeline type with improved release safety, pipeline triggers, parameterized pipelines, and a new billing model.

Execution mode

Choose the execution mode for your pipeline. This determines how the pipeline is run.

- ☐ Superseded
A more recent execution can overtake an older one. This is the default.
- ☒ Queued (Pipeline type V2 required)
Executions are processed one by one in the order that they are queued.
- ☐ Parallel (Pipeline type V2 required)
Executions don't wait for other runs to complete before starting or finishing.

eu-north-1.console.aws.amazon.com/codesuite/settings/connections/create?origi...



Services



Stockholm ▼

VedangWaije

[Developer Tools](#) > [Connections](#) > Create connection

Create a connection [Info](#)

Create GitHub App connection [Info](#)

Connection name

► Tags - optional

Connect to GitHub



Pipelines must have at least two stages. Your second stage must be either a build or deployment stage. Choose a provider for either the build stage or deployment stage.

Deploy

Deploy provider

Choose how you deploy to instances. Choose the provider, and then provide the configuration details for that provider.

AWS Elastic Beanstalk

Region

Europe (Stockholm)

Input artifacts

Choose an input artifact for this action. [Learn more](#)

No more than 100 characters

Application name

Choose an application that you have already created in the AWS Elastic Beanstalk console. Or create an application in the AWS Elastic Beanstalk console and then return to this task.

Aditibean

Environment name

Choose an environment that you have already created in the AWS Elastic Beanstalk console. Or create an environment in the AWS Elastic Beanstalk console and then return to this task.

Aditibean-evn

☐ Configure automatic rollback on stage failure

Cancel

Previous

Next

Step 4: Add deploy stage

Deploy action provider

Deploy action provider

AWS Elastic Beanstalk

ApplicationName

Aditibean

EnvironmentName

Aditibean-evn

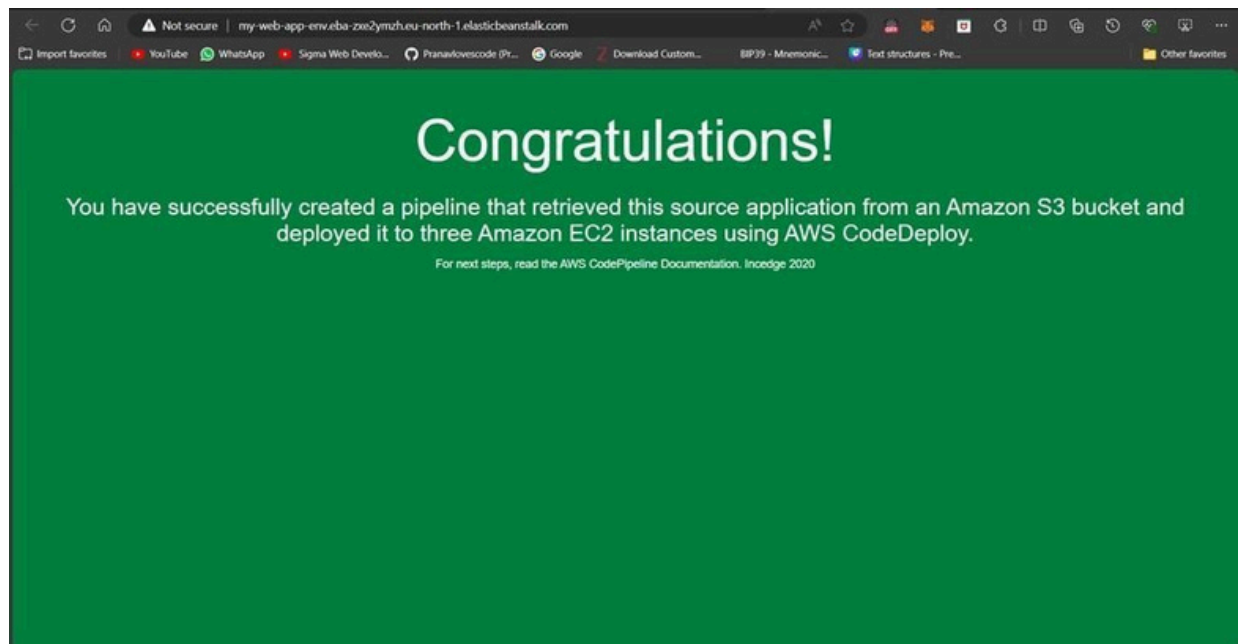
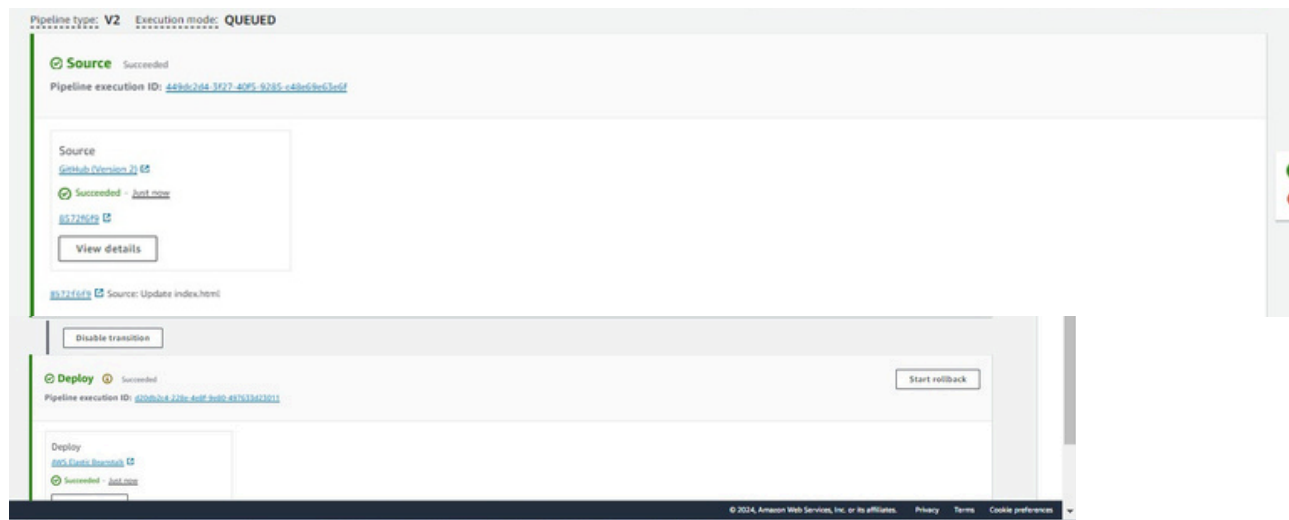
Configure automatic rollback on stage failure

Disabled

Cancel

Previous

Create pipeline



Using S3 Bucket:

Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region

Europe (Stockholm) eu-north-1

Bucket type Info

☒ General purpose

Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

☐ Directory - New

Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name Info

Aditibean

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Choose bucket

Format: s3://bucket/prefix

Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

Files and folders (1 Total, 315.0 B)

Remove

Add files

Add folder

All files and folders in this table will be uploaded.

< 1 >

<input type="checkbox"/>	Name	Folder	Type
<input type="checkbox"/>	index.html	-	text/html

Edit Block public access (bucket settings) [Info](#)

Block public access (bucket settings)

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 all your S3 buckets and 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 your buckets 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.

☐ Block public access to buckets and objects granted through *any* access control lists (ACLs)

S3 will ignore all ACLs that grant public access to buckets and objects.

☐ Block public access to buckets and objects granted through *new* public bucket or access point policies

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☐ Block public and cross-account access to buckets and objects through *any* public bucket or access point policies

Object Ownership


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.

 We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.

Enabling ACLs turns off the bucket owner enforced setting for Object Ownership

Once the bucket owner enforced setting is turned off, access control lists (ACLs) and their associated permissions are restored. Access to objects that you do not own will be based on ACLs and not the bucket policy.

☒ I acknowledge that ACLs will be restored.

Upload succeeded
View details below.

Summary

Destination
s3://vedangbucket

Succeeded
1 file, 315.0 B (100.00%)

Failed
0 files, 0 B (0%)

Files and folders

Configuration

Files and folders (1 Total, 315.0 B)

Find by name

< 1 >

Name	Folder	Type	Size	Status	Error
index.html	-	text/html	315.0 B	Succeeded	-

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting

- ☐ Disable
- ☒ Enable

Hosting type

- ☒ Host a static website
Use the bucket endpoint as the web address. [Learn more](#)
- ☐ Redirect requests for an object
Redirect requests to another bucket or domain. [Learn more](#)

i For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see [Using Amazon S3 Block Public Access](#)

Index document

Specify the home or default page of the website.

index.html

Using EC2:

The screenshot shows the AWS Management Console 'Instances' page. The instance 'dynamic-server' (ID: i-Decbd8d07a55bd2e3) is in a 'Running' state. The console displays various details for this instance, including its public and private IP addresses, DNS names, and instance type (t2.micro).

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Put
dynamic-server	i-Decbd8d07a55bd2e3	Running	t2.micro	2/2 checks passed	View alarms	us-east-1c	ec2

i-Decbd8d07a55bd2e3 (dynamic-server)

- Instance ID: i-Decbd8d07a55bd2e3 (dynamic-server)
- IPv6 address: -
- Hostname type: IP name: ip-172-31-85-104.ec2.internal
- Answer private resource DNS name: IPv4 (A)
- Public IPv4 address: 34.201.70.101 | [open address](#)
- Instance state: Running
- Private IP DNS name (IPv4 only): ip-172-31-85-104.ec2.internal
- Instance type: t2.micro
- Private IPv4 addresses: 172.31.85.104
- Public IPv4 DNS: ec2-34-201-70-101.compute-1.amazonaws.com | [open address](#)
- Elastic IP addresses: -

Public IP address: 34.201.70.101

Username: ubuntu

Note: In most cases, the default username, ubuntu, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

You have insufficient IAM permissions to connect to an instance using EC2 Instance Connect

To connect to an instance via EC2 Instance Connect, you must have an attached IAM policy that grants the following permissions:

- ec2:instance-connect:SendSSHPublicKey
- ec2:DescribeInstances

Consider restricting access to specific EC2 instances using `ec2:osuser` condition, or specific resource tag. Visit [IAM Console](#) to verify if you have above permissions. For more information about IAM policy examples, see [Grant IAM permissions for EC2 Instance Connect](#).

Cancel Connect

```
ubuntu@ip-172-31-85-104:~$ pwd
/home/ubuntu
ubuntu@ip-172-31-85-104:~$ mkdir pranav
ubuntu@ip-172-31-85-104:~$ cd pranav
ubuntu@ip-172-31-85-104:~/pranav$ git clone https://github.com/Pranavlovescode/Dynamic-website-hosting-sample.git
Cloning into 'Dynamic-website-hosting-sample'...
remote: Enumerating objects: 6, done.
remote: Counting objects: 100% (6/6), done.
remote: Compressing objects: 100% (5/5), done.
remote: Total 6 (delta 0), reused 6 (delta 0), pack-reused 0
Receiving objects: 100% (6/6), 11.16 KiB | 5.58 MiB/s, done.
```

```
ubuntu@ip-172-31-85-104:~/pranav$ ls
Dynamic-website-hosting-sample
ubuntu@ip-172-31-85-104:~/pranav$ cd Dynamic-website-hosting-sample/
ubuntu@ip-172-31-85-104:~/pranav/Dynamic-website-hosting-sample$ ls
index.js package-lock.json package.json
ubuntu@ip-172-31-85-104:~/pranav/Dynamic-website-hosting-sample$ npm i

added 93 packages, and audited 94 packages in 3s

16 packages are looking for funding
  run `npm fund` for details

found 0 vulnerabilities
npm notice
npm notice New patch version of npm available! 10.8.1 -> 10.8.2
npm notice Changelog: https://github.com/npm/cli/releases/tag/v10.8.2
npm notice To update run: npm install -g npm@10.8.2
npm notice
```

```
ubuntu@ip-172-31-85-104:~/pranav/Dynamic-website-hosting-sample$ npm start

> hosting-dynamic-website@1.0.0 start
> nodemon index.js

[nodemon] 3.1.4
[nodemon] to restart at any time, enter `rs`
[nodemon] watching path(s): *.*
[nodemon] watching extensions: js,mjs,cjs,json
[nodemon] starting `node index.js`
Server is running on port 3000
```

The screenshot displays the AWS Management Console interface for a Security Group. The left sidebar shows navigation options like Savings Plans, Reserved Instances, Elastic Block Store, and Network & Security. The main content area shows the details for the Security Group 'launch-wizard-2'.

Security Group Details:

- Security group name:** launch-wizard-2
- Security group ID:** sg-0816efec751fad96
- Description:** launch-wizard-2 created 2024-08-12T15:09:38.633Z
- VPC ID:** vpc-0dd4c1c56f9eb78a7
- Owner:** 433618061107
- Inbound rules count:** 4 Permission entries
- Outbound rules count:** 1 Permission entry

Inbound rules (4):

Security group rule...	IP version	Type	Protocol	Port range	Source
sg-09762f34ff97dc77a	IPv4	Custom TCP	TCP	3000	0.0.0.0/0
sg-05780e80302575...	IPv4	SSH	TCP	22	0.0.0.0/0
sg-0f28e3996f5f4c2d0	IPv4	HTTP	TCP	80	0.0.0.0/0
sg-0ba194a6c403d52a8	IPv4	HTTPS	TCP	443	0.0.0.0/0

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

▼ Images

AMIs

AMI Catalog

▼ Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

▼ Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

▼ Load Balancing

Load Balancers

Target Groups

Security group name

launch-wizard-1

Security group ID

sg-09444ecdb8b403eb6

Description

launch-wizard-1 created 2024-07-23T09:30:42.912Z

VPC ID

vpc-0dd44c1c56f9eb78a7

Owner

433618061107

Inbound rules count

4 Permission entries

Outbound rules count

1 Permission entry

Inbound rules

Outbound rules

Tags

Inbound rules (4)

Manage tags

Edit inbound rules

Search

< 1 >

▼	Security group rule...	▼	IP version	▼	Type	▼	Protocol	▼	Port range	▼
	sgr-033434d2717167...		IPv4		HTTP		TCP		80	
	sgr-0810859d39a92a...		IPv4		HTTPS		TCP		443	
	sgr-08756637bd2e26fe7		IPv4		SSH		TCP		22	
	sgr-05bbf31ac11f942fe		IPv4		Custom TCP		TCP		3000	

Hosting:

