

# ADVANCE DEVOPS EXP-2

Pranav Titambe

D15A/62

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:

Step 1

Configure environment

Step 2

Configure service access

Step 3 - optional

Set up networking, database, and tags

Step 4 - optional

Configure instance traffic and scaling

Step 5 - optional

Configure updates, monitoring, and logging

Step 6

Review

Configure environment

Environment tier

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

Application name

pranavbean

Maximum length of 100 characters.

Application tags (optional)

Platform

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

Node.js

Platform branch

Node.js 20 running on 64bit Amazon Linux 2023

Platform version

6.2.0 (Recommended)

Application code

☒ Sample application

Step 1

[Configure environment](#)

Step 2

[Configure service access](#)

Step 3 - optional

**Set up networking, database, and tags**

Step 4 - optional

[Configure instance traffic and scaling](#)

Step 5 - optional

[Configure updates, monitoring, and logging](#)

Step 6

[Review](#)

## Set up networking, database, and tags - optional [Info](#)

### Virtual Private Cloud (VPC)

VPC

Launch your environment in a custom VPC instead of the default VPC. You can create a VPC and subnets in the VPC management console. [Learn more](#)

vpc-0e67c568f893e22c0 | (172.31.0.0/16)

[Create custom VPC](#)

### Instance settings

Choose a subnet in each AZ for the instances that run your application. To avoid exposing your instances to the Internet, run your instances in private subnets and load balancer in public subnets. To run your load balancer and instances in the same public subnets, assign public IP addresses to the instances. [Learn more](#)

### Public IP address

Assign a public IP address to the Amazon EC2 instances in your environment.

☒ Activated

CloudShellFeedback© 2024, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

aws

Services

Search

[Alt+S]

Stockholm

pranav\_titambe

Developer Tools

**CodePipeline**

Source • CodeCommit

Artifacts • CodeArtifact

Build • CodeBuild

Deploy • CodeDeploy

Pipeline • CodePipeline

Getting started

Pipelines

Pipeline

History

Settings

Settings

Go to resource

Feedback

Developer Tools > CodePipeline > Pipelines > pranav-pipeline

pranav-pipeline

Notify Edit Stop execution Clone pipeline Release change

Pipeline type: V2 Execution mode: QUEUED

Source Succeeded

Pipeline execution ID: c0f42bbd-966a-4851-ba7b-c5ecf72bbab1

Source

[GitHub \(Version 2\)](#)

Succeeded - 4 days ago

[8fd5da54](#)

View details

[8fd5da54](#) Source: Update README.md

Disable transition

Deploy Succeeded

Pipeline execution ID: c0f42bbd-966a-4851-ba7b-c5ecf72bbab1

Start rollback

CloudShellFeedback© 2024, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

Step 1

Configure environment

Step 2

Configure service access

Step 3 - optional

Set up networking, database, and tags

Step 4 - optional

Configure instance traffic and scaling

Step 5 - optional

Configure updates, monitoring, and logging

Step 6

Review

Configure instance traffic and scaling - optional

Info

▼ Instances

Info

Configure the Amazon EC2 instances that run your application.

Root volume (boot device)

Root volume type

(Container default)

Size

The number of gigabytes of the root volume attached to each instance.

8

GB

IOPS

Input/output operations per second for a provisioned IOPS (SSD) volume.

100

IOPS

Throughput

The desired throughput to provision for the Amazon EBS root volume attached to your environment's EC2 instance

125

MIB/s

Architecture

The processor architecture determines the instance types that are made available. You can't change this selection after you create the environment. [Learn more](#)

☒ x86\_64

This architecture uses x86 processors and is compatible with most third-party tools and libraries.

☐ arm64 - new

This architecture uses AWS Graviton2 processors. You might have to recompile some third-party tools and libraries.

Instance types

Add instance types for your fleet. Change the order that the instances are in to set the preferred launch order. This only affects On-Demand instances. We recommend you include at least two instance types. [Learn more](#)

Choose x86 instance types

t3.micro X t3.small X

AMI ID

Elastic Beanstalk selects a default Amazon Machine Image (AMI) for your environment based on the Region, platform version, and processor architecture that you choose. [Learn more](#)

ami-00de104c2f90581a8

Availability Zones

Number of Availability Zones (AZs) to use.

Any

▼ Monitoring

Info

Health reporting

Enhanced health reporting provides free real-time application and operating system monitoring of the instances and other resources in your environment. The **EnvironmentHealth** custom metric is provided free with enhanced health reporting. Additional charges apply for each custom metric. For more information, see [Amazon CloudWatch Pricing](#)

System

☒ Basic

☐ Enhanced

Health event streaming to CloudWatch Logs

Configure Elastic Beanstalk to stream environment health events to CloudWatch Logs. You can set the retention up to a maximum of ten years and configure Elastic Beanstalk to delete the logs when you terminate your environment.

Log streaming

☒ Activated (standard CloudWatch charges apply.)

Retention

7

Lifecycle

Keep logs after terminating environment

Applications

Environments

Change history

▼ Application: my-web-app

Application versions

Saved configurations

▼ Environment: My-web-app-env

Go to environment

Configuration

Events

Health

Logs

Monitoring

Alarms

Managed updates

Tags

Elastic Beanstalk > Environments > My-web-app-env

My-web-app-env info

Environment overview

Health

Green

Environment ID

e-svs9jz6j3c

Domain

My-web-app-env.eba-zxe2ymzh.eu-north-1.elasticbeanstalk.com

Application name

my-web-app

Platform

Change version

Platform

PHP 8.3 running on 64bit Amazon Linux 2023/4.3.2

Running version

code-pipeline-1723541626202-8fd5da544b5da402627a6a01ed1fccf5b491c879

Platform state

Supported

Events

Health

Logs

Monitoring

Alarms

Managed updates

Tags

Events (21) info

Filter events by text, property or value

https://eu-north-1.console.aws.amazon.com/console/home?region=eu-north-1

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

my-web-app-env.eba-zxe2ymzh.eu-north-1.elasticbeanstalk.com

Not secure

Import favorites

YouTube

WhatsApp

Sigma Web Develo...

Pranavlovescode (Pr...

Google

Download Custom...

BIP39 - Mnemonic...

Text structures - Pre...

Other favorites

Congratulations!

You have successfully created a pipeline that retrieved this source application from an Amazon S3 bucket and deployed it to three Amazon EC2 instances using AWS CodeDeploy.

For next steps, read the AWS CodePipeline Documentation. Incoedge 2020

# Using S3 Bucket:

Amazon S3

Buckets

Access Grants

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

Storage Lens groups

AWS Organizations settings

Feature spotlight

Amazon S3 > Buckets

Account snapshot - updated every 24 hours

View Storage Lens dashboard

General purpose buckets

Directory buckets

General purpose buckets (2)

Find buckets by name

| Name                            | AWS Region                      | IAM Access Analyzer                         | Creation date                         |
|---------------------------------|---------------------------------|---|---------------------------------------|
| <a href="#">pranavawsbucket</a> | US East (N. Virginia) us-east-1 | <a href="#">View analyzer for us-east-1</a> | August 12, 2024, 14:47:03 (UTC+05:30) |
| <a href="#">pranavitambe</a>    | US East (N. Virginia) us-east-1 | <a href="#">View analyzer for us-east-1</a> | August 12, 2024, 14:29:10 (UTC+05:30) |

https://us-east-1.console.aws.amazon.com/s3/access?region=us-east-1

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Amazon S3

Buckets

Access Grants

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

Storage Lens groups

AWS Organizations settings

Feature spotlight

pranavawsbucket

Objects

Properties

Permissions

Metrics

Management

Access Points

Objects (3)

Find objects by prefix

| Name                       | Type   | Last modified                         | Size   | Storage class |
|----------------------------|--------|---------------------------------------|--------|---------------|
| <a href="#">index.html</a> | html   | August 12, 2024, 19:58:14 (UTC+05:30) | 4.0 KB | Standard      |
| <a href="#">public/</a>    | Folder | -                                     | -      | -             |
| <a href="#">style.css</a>  | css    | August 12, 2024, 19:58:15 (UTC+05:30) | 1.1 KB | Standard      |

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Amazon S3

Buckets

Access Grants

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

Storage Lens groups

AWS Organizations settings

Feature spotlight 7

Object Lock

Disabled

Requester pays

When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. [Learn more](#)

Requester pays

Disabled

Edit

Static website hosting

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

Static website hosting

Enabled

Hosting type

Bucket hosting

Bucket website endpoint

When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. [Learn more](#)

<http://pranavawsbucket.s3-website-us-east-1.amazonaws.com>

Edit

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Amazon S3

Buckets

Access Grants

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

Storage Lens groups

AWS Organizations settings

Feature spotlight 7

Amazon S3 > Buckets > pranavawsbucket

pranavawsbucket Info

Objects Properties Permissions Metrics Management Access Points

Permissions overview

Access finding

Access findings are provided by IAM external access analyzers. Learn more about [How IAM analyzer findings work](#)

[View analyzer for us-east-1](#)

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

Off

Individual Block Public Access settings for this bucket

Edit

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Amazon S3

Buckets

Access Grants

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

Storage Lens groups

AWS Organizations settings

Feature spotlight 7

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

Off

Individual Block Public Access settings for this bucket

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

```
{
  "Version": "2012-10-17",
  "Id": "Policy1723472714525",
  "Statement": [
    {
      "Sid": "Stmt1723472712792",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "s3:GetObject",

```

Copy

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Amazon S3

Buckets

Access Grants

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

Storage Lens groups

AWS Organizations settings

Feature spotlight 7

Individual Block Public Access settings for this bucket

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)


```
{
  "Version": "2012-10-17",
  "Id": "Policy1723472714525",
  "Statement": [
    {
      "Sid": "Stmt1723472712792",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::pranavawsbucket/*"
    }
  ]
}
```

Copy

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)



VIVEKANAND EDUCATION SOCIETY'S  
Institute of Technology

Welcome to Vivekanand Education Society's Institute of Technology

[About Us](#) | [Services](#) | [Contact Us](#)

## About Us


Watch our promotional video:


Vivekanand Education Society's Institute of Technology (VESIT) is a premier institution offering quality education and fostering research and innovation.

Listen to our introduction:

▶

0:00 / 2:42






Department of Information Technology , VESIT.

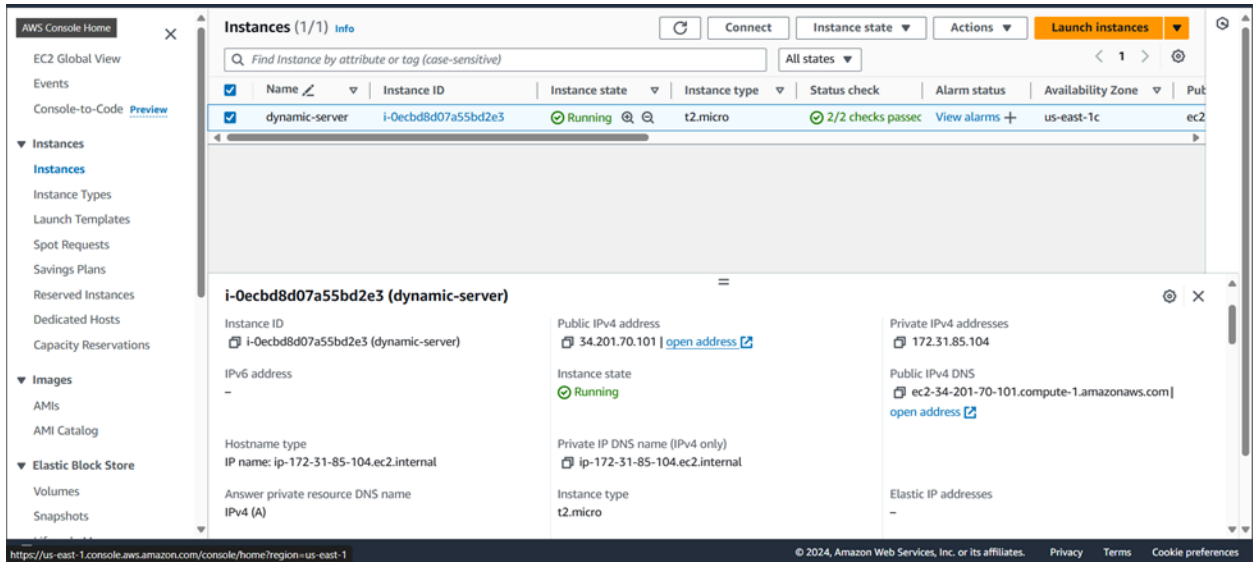
Watch later

Share

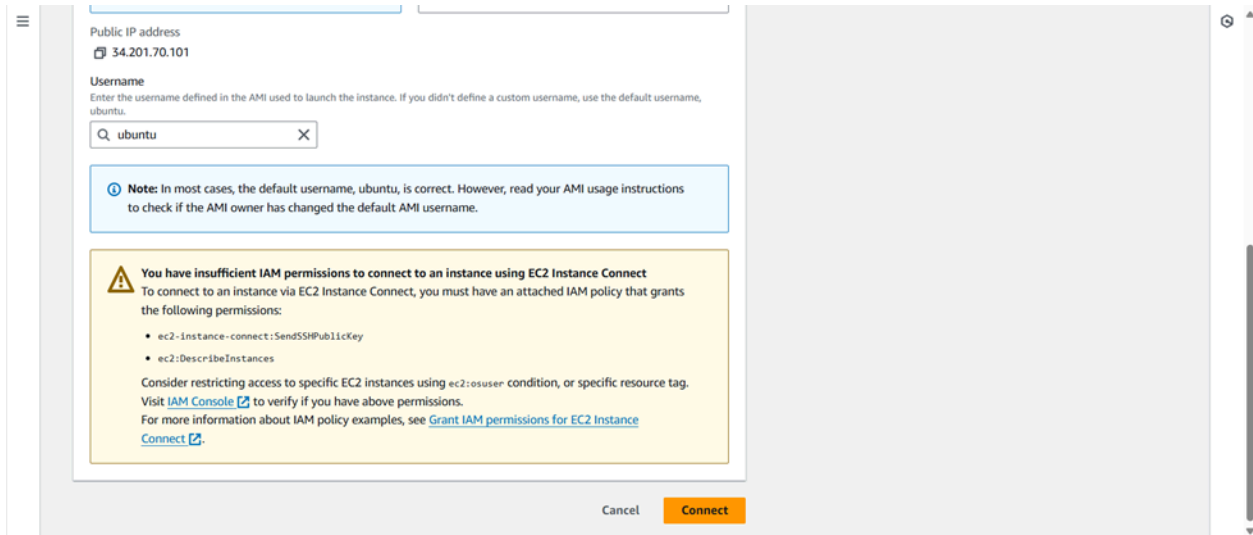




## Using EC2:



The screenshot shows the AWS Management Console for the 'us-east-1' region. The 'Instances' page is active, displaying a table with one instance: 'dynamic-server' (ID: i-0ecbd8d07a55bd2e3), which is in a 'Running' state. Below the table, the details for this instance are shown, including its Public IPv4 address (34.201.70.101), Private IPv4 address (172.31.85.104), and Instance type (t2.micro).



The screenshot shows the EC2 Instance Connect dialog box. It displays the Public IP address (34.201.70.101) and the Username (ubuntu). A note indicates that the default username 'ubuntu' is correct. A warning message states that the user has insufficient IAM permissions to connect to the instance using EC2 Instance Connect, listing the required permissions: `ec2:instance-connect:SendSSHPublicKey` and `ec2:DescribeInstances`.

```
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
```

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

Security group name

launch-wizard-2

Security group ID

sg-0816efec751fcad96

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

Outbound rules

Tags

Inbound rules (4)

↺

Manage tags

Edit inbound rules

Q Search

< 1 > ⚙

| 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-0baf94a6c403d52a8   | 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-0dd4c1c56f9eb78a7

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:

Not secure | 34.201.70.101:3000

Import favorites | YouTube | WhatsApp | Sigma Web Develo... | Pranavlovescode (Pr... | Google | Download Custom... | BIP39 - Mnemonic... | Text structures - Pre... | Other favorites

Hey this is Dynamic Website.

Not secure | 34.201.70.101:3000/about

Import favorites | YouTube | WhatsApp | Sigma Web Develo... | Pranavlovescode (Pr... | Google | Download Custom... | BIP39 - Mnemonic... | Text structures - Pre... | Other favorites

Hey this is about page.