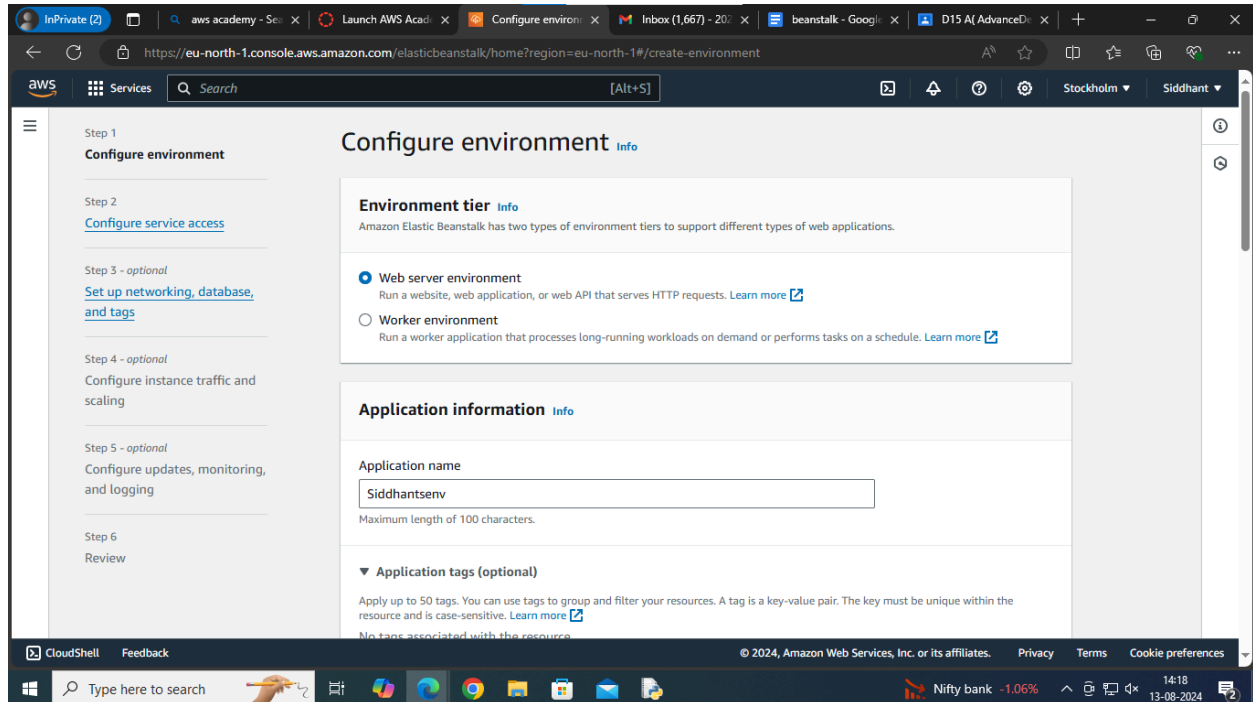


Aim: To build your application using AWS Codebuild and deploy on S3 using AWS CodePipeline
deploy sample application on EC2 instance using AWS codedeploy.

Code and Output :

Using elastic beanstalk:



Environment information [Info](#)

Choose the name, subdomain and description for your environment. These cannot be changed later.

Environment name

Must be from 4 to 40 characters in length. The name can contain only letters, numbers, and hyphens. It can't start or end with a hyphen. This name must be unique within a region in your account.

Domain

.eu-north-1.elasticbeanstalk.com

[Check availability](#)

Environment description

Application code [Info](#)

- ☒ Sample application
- ☐ Existing version
Application versions that you have uploaded.
- ☐ Upload your code
Upload a source bundle from your computer or copy one from Amazon S3.

Presets [Info](#)

Start from a preset that matches your use case or choose custom configuration to unset recommended values and use the service's default values.

Configuration presets

- ☐ Single instance (free tier eligible)
- ☐ Single instance (using spot instance)
- ☐ High availability
- ☐ High availability (using spot and on-demand instances)
- ☒ Custom configuration

[Cancel](#)

[Next](#)

Codepipeline

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

 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☐ Superseded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.

Service role

☒ New service role

Create a service role in your account

☐ Existing service role

Choose an existing service role from your account

Role name

Type your service role name

☒ Allow AWS CodePipeline to create a service role so it can be used with this new pipeline

Create connection | CodePipeline | eu-north-1 - Personal - Microsoft Edge

https://eu-north-1.console.aws.amazon.com/codesuite/settings/connecti...

aws Services 🔍 📄 🔔 ⓘ ⚙️ Stockholm ▼ Siddhant ▼

☰

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

ⓘ

🔍

Create a connection Info

Create GitHub App connection Info

Connection name

githubapp1

▶ Tags - optional

Connect to GitHub

CloudShell Feedback Privacy Terms Cookie preferences

© 2024, Amazon Web Services, Inc. or its affiliates.

Default branch will be used only when pipeline execution starts from a different branch.



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

Beginning July 1, 2024, the console will create connections with codeconnections in the resource ARN. Resources with both service prefixes will continue to display in the console. [Learn more](#)

Connect to GitHub

GitHub connection settings [Info](#)

Connection name

githubapp1

App installation - *optional*

Install GitHub App to connect as a bot. Alternatively, leave it blank to connect as a GitHub user, which can be used in AWS CodeBuild projects.

🔍 53746808



or

[Install a new app](#)

► **Tags - *optional***

[Connect](#)



CloudShell

[Feedback](#)

[Privacy](#)

[Terms](#)

[Cookie preferences](#)

© 2024, Amazon Web Services, Inc. or its affiliates.

Source

Source provider

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

GitHub (Version 2) ▼



New GitHub version 2 (app-based) action

To add a GitHub version 2 action in CodePipeline, you create a connection, which uses GitHub Apps to access your repository. Use the options below to choose an existing connection or create a new one. [Learn more](#)

Connection

Choose an existing connection that you have already configured, or create a new one and then return to this task.

Q am:aws:codeconnections:eu-north-1:010928222259:connection/0b5d0b9a-7 X

or

Connect to GitHub



Ready to connect

Your GitHub connection is ready for use.

Repository name

Choose a repository in your GitHub account.

Q SiddhantSathe/aws-codepipeline-s3-codedeploy-linux-2.0 X

You can type or paste the group path to any project that the provided credentials can access. Use the format 'group/subgroup/project'.

Default branch

Default branch will be used only when pipeline execution starts from a different source or manually started.

Q master X

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.

Trigger

Trigger type

Choose the trigger type that starts your pipeline.

- ☒ **No filter**
Starts your pipeline on any push and clones the HEAD.
- ☐ **Specify filter**
Starts your pipeline on a specific filter and clones the exact commit. Pipeline type V2 is required.
- ☐ **Do not detect changes**
Don't automatically trigger the pipeline.

 You can add additional sources and triggers by editing the pipeline after it is created.

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](#) 

SourceArtifact

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.

 Siddhantbeanstalk

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.

 Siddhantbeanstalk-env

Siddhantbeanstalk-env

Success

Congratulations! The pipeline pipeline1 has been created.

Create a notification rule for this pipeline

Developer Tools > CodePipeline > Pipelines > pipeline1

pipeline1

Notify Edit Stop execution Clone pipeline Release change

Pipeline type: V2 Execution mode: QUEUED

Source Succeeded

Pipeline execution ID: 750da3e1-adc9-48a6-b1c2-396aa25fc160

Source

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

Succeeded - 9 minutes ago

[8fd5da54](#)

View details

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

Disable transition

Deploy Succeeded

Pipeline execution ID: 750da3e1-adc9-48a6-b1c2-396aa25fc160

Start rollback

Deploy

[AWS Elastic Beanstalk](#)

Succeeded - 9 minutes ago

Environments (1) Info

Filter environments

Environment name

Health

Application name

Platform

Domain

Running versions

Tier name

Date created

Siddhantbeanstalk-env

Green

Siddhantbeanstalk

PHP 8.3 running on...

Siddhantbeanstalk-env.eba-r3...

code-pipeline-1723...

WebServer

August 13, 2024 14

← ↻ ⚠ Not secure | siddhantbeanstalk-env.eba-r33erg9p.eu-north-1.elasticbeanstalk.com

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. Incodex 2020

Using S3 bucket: Create S3 bucket

Account snapshot - updated every 24 hours [All AWS Regions](#) [View Storage Lens dashboard](#)

Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

General purpose buckets Directory buckets

General purpose buckets (2) [Info](#) [All AWS Regions](#)

Buckets are containers for data stored in S3.

Find buckets by name

Name	AWS Region	IAM Access Analyzer	Creation date
siddhantsbucket	US East (N. Virginia) us-east-1	View analyzer for us-east-1	July 30, 2024, 15:08:55 (UTC+05:30)
sids3bucke	US East (N. Virginia) us-east-1	View analyzer for us-east-1	August 12, 2024, 14:33:49 (UTC+05:30)

Upload File

siddhantsbucket [Info](#)

Objects Properties Permissions Metrics Management Access Points

Objects (1) [Info](#) [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

Name	Type	Last modified	Size	Storage class
index.html	html	August 12, 2024, 14:27:18 (UTC+05:30)	5.3 KB	Standard

Edit block public access

Amazon S3 > Buckets > siddhantsbucket > Edit Block public access (bucket settings)

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**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

[Cancel](#) [Save changes](#)

Edit object ownership

[Amazon S3](#) > [Buckets](#) > [siddhantsbucket](#) > Edit Object Ownership

Edit Object Ownership [Info](#)

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.

Object Ownership

☒ **Bucket owner preferred**
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

☐ **Object writer**
The object writer remains the object owner.

ℹ If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. [Learn more](#)

[Cancel](#) [Save changes](#)

Make file public using ACL

[Amazon S3](#) > [Buckets](#) > [siddhantsbucket](#)

siddhantsbucket [Info](#)

[Objects](#) | [Properties](#) | [Permissions](#) | [Metrics](#) | [Management](#) | [Access Points](#)

Objects (1) [Info](#)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions.

🔄 Copy S3 URI Copy URL Download Open Delete Actions Create folder Upload

🔍 Find objects by prefix

<input checked="" type="checkbox"/>	Name	Type	Last modified	Size
<input checked="" type="checkbox"/>	index.html	html	August 12, 2024, 14:27:18 (UTC+05:30)	

Download as

Share with a presigned URL

Calculate total size

Copy

Move

Initiate restore

Query with S3 Select

Edit actions

Rename object

Edit storage class

Edit server-side encryption

Edit metadata

Edit tags

Make public using ACL

[Amazon S3](#) > [Buckets](#) > siddhantsbucket

siddhantsbucket

Info

[Objects](#) | [Properties](#) | [Permissions](#) | [Metrics](#) | [Management](#) | [Access Points](#)

Objects (1) Info

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

< 1 >

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	index.html	html	August 12, 2024, 14:27:18 (UTC+05:30)	5.3 KB	Standard

Google

Inbox (1,664)

ADV devops S3

S3 bucket - Go

WhatsApp

aws academy

Launch AWS Ac

Make objects p

index.html - Ob

https://us-east-1.console.aws.amazon.com/s3/buckets/siddhantsbucket/object/edit_public_read_access?region=us-east-1&bucketType=gener...

N. Virginia

voclabs/user3387498=SATHE_SIDDHANT_SANJAY @ 1929-0520-1551

Successfully edited public access

View details below.

Make public: status

Close

The information below will no longer be available after you navigate away from this page.

Summary

Source

s3://siddhantsbucket

Successfully edited public access

1 object, 5.3 KB

Failed to edit public access

0 objects

Failed to edit public access

Configuration

When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.

Specified objects

Find objects by name

Name

Type

Last modified

Size

[index.html](#)

html

August 12, 2024, 14:27:18 (UTC+05:30)

5.3 KB

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

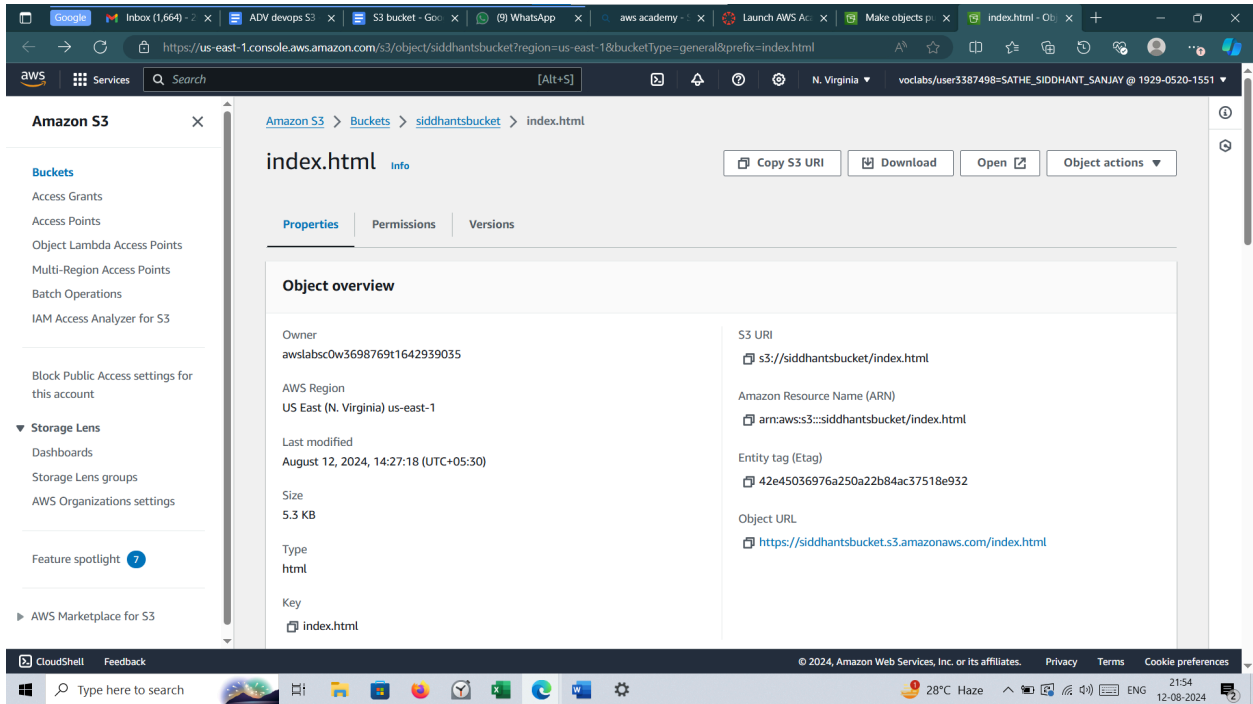
Cookie preferences

Type here to search

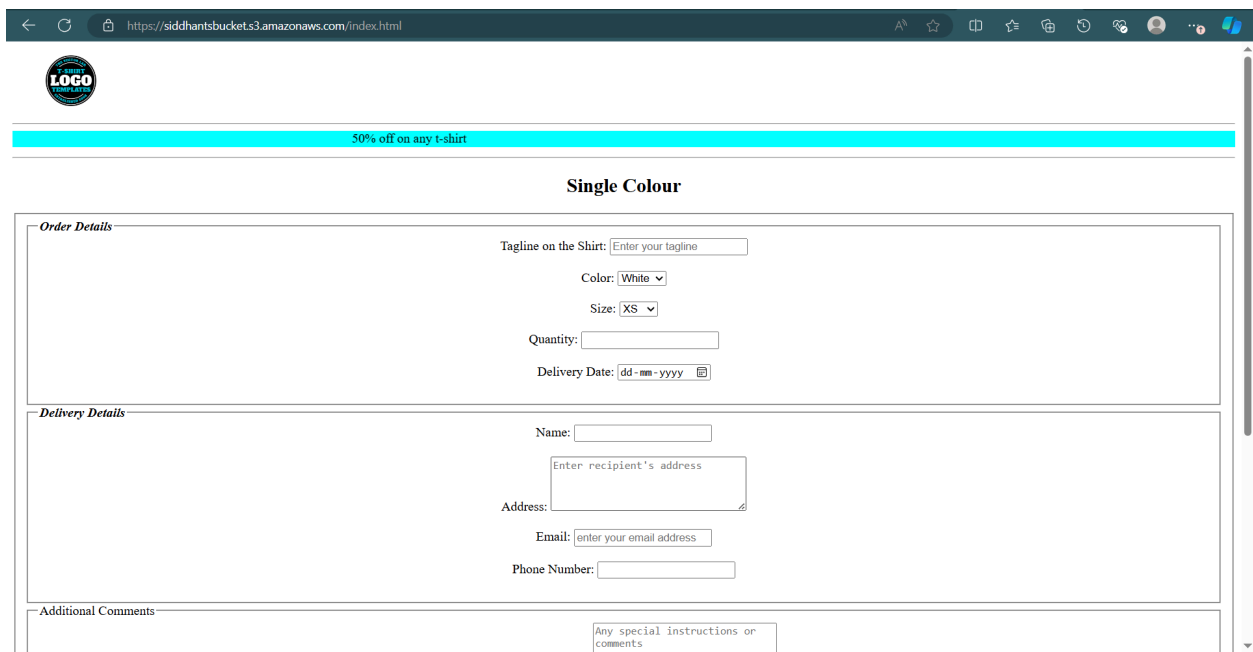
28°C Haze

21:54

12-08-2024



Hosted website




Using EC2:
Siddhant Sathe


D15A/51

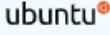
Aim: To build your application using AWS Codebuild and deploy on S3 using AWS CodePipeline, deploy sample application on EC2 instance using AWS codedeploy.


Code and Output :


Quick Start


Amazon Linux



macOS


Ubuntu


Windows


Red Hat


SUSE Linux



Browse more AMIs
Including AMIs from
AWS, Marketplace and
the Community

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type Free tier eligible ▼

ami-04a81a99f5ec58529 (64-bit (x86)) / ami-0c14ff330901e49ff (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Ubuntu Server 24.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Architecture

64-bit (x86) ▼

AMI ID

ami-04a81a99f5ec58529

Verified provider

▼ **Instance type** [Info](#) | [Get advice](#)

Instance type

t2.micro

Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand RHEL base pricing: 0.026 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour

☒ All generations

[Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

▼ **Network settings** [Info](#)

Edit

Network | [Info](#)

vpc-06c996635e2aef808

Subnet | [Info](#)

No preference (Default subnet in any availability zone)

Auto-assign public IP | [Info](#)

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) | [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group

☐ Select existing security group

We'll create a new security group called 'launch-wizard-1' with the following rules:

☒ Allow SSH traffic from
Helps you connect to your instance

Anywhere
0.0.0.0/0



☐ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

☐ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

▼ Configure storage [Info](#)


[Advanced](#)

1x GiB ▼ Root volume (Not encrypted)

 Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage 

Add new volume

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance

 Click refresh to view backup information




The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems

[Edit](#)

[EC2](#) > [Instances](#) > Launch an instance

 **Success**
Successfully initiated launch of instance ([i-01fe3a23a4a6d901c](#))

► Launch log

Instances (1/1) [Info](#)




Connect

Instance state ▼

Actions ▼







Launch instances ▼

All states ▼

Instance ID = [i-0afa557e0e5b49a50](#) 

Clear filters

< 1 > 

<input checked="" type="checkbox"/>	Name 	Instance ID	Instance state ▼	Instance type ▼	Status check	Alarm status	Availabili
<input checked="" type="checkbox"/>	Siddhant's Ser...	i-0afa557e0e5b49a50	 Running  	t2.micro	 Initializing	View alarms 	us-east-1

Instance summary for i-0afa557e0e5b49a50 (Siddhant's Server) [Info](#)

[Refresh](#) [Connect](#) [Instance state ▼](#) [Actions ▼](#)

Updated less than a minute ago

Instance ID i-0afa557e0e5b49a50 (Siddhant's Server)	Public IPv4 address 34.200.231.88 open address	Private IPv4 addresses 172.31.7.177
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-34-200-231-88.compute-1.amazonaws.com open address
Hostname type IP name: ip-172-31-7-177.ec2.internal	Private IP DNS name (IPv4 only) ip-172-31-7-177.ec2.internal	Elastic IP addresses -
Answer private resource DNS name IPv4 (A)	Instance type t2.micro	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more
Auto-assigned IP address 34.200.231.88 [Public IP]	VPC ID vpc-06c996635e2aef808	

```
root@ip-172-31-90-124:/home/ubuntu/siddhant# git clone https://github.com/siddhantsathe/nodejs.git
Cloning into 'nodejs'...
remote: Enumerating objects: 647, done.
remote: Counting objects: 100% (647/647), done.
remote: Compressing objects: 100% (488/488), done.
remote: Total 647 (delta 125), reused 635 (delta 121), pack-reused 0
Receiving objects: 100% (647/647), 713.52 KiB | 12.09 MiB/s, done.
Resolving deltas: 100% (125/125), done.
root@ip-172-31-90-124:/home/ubuntu/siddhant#
```

```
root@ip-172-31-90-124:/home/ubuntu/siddhant/nodejs# npm i
```

```
added 36 packages, and audited 102 packages in 5s
```

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

```
2 moderate severity vulnerabilities
```

```
To address issues that do not require attention, run:
  npm audit fix
```

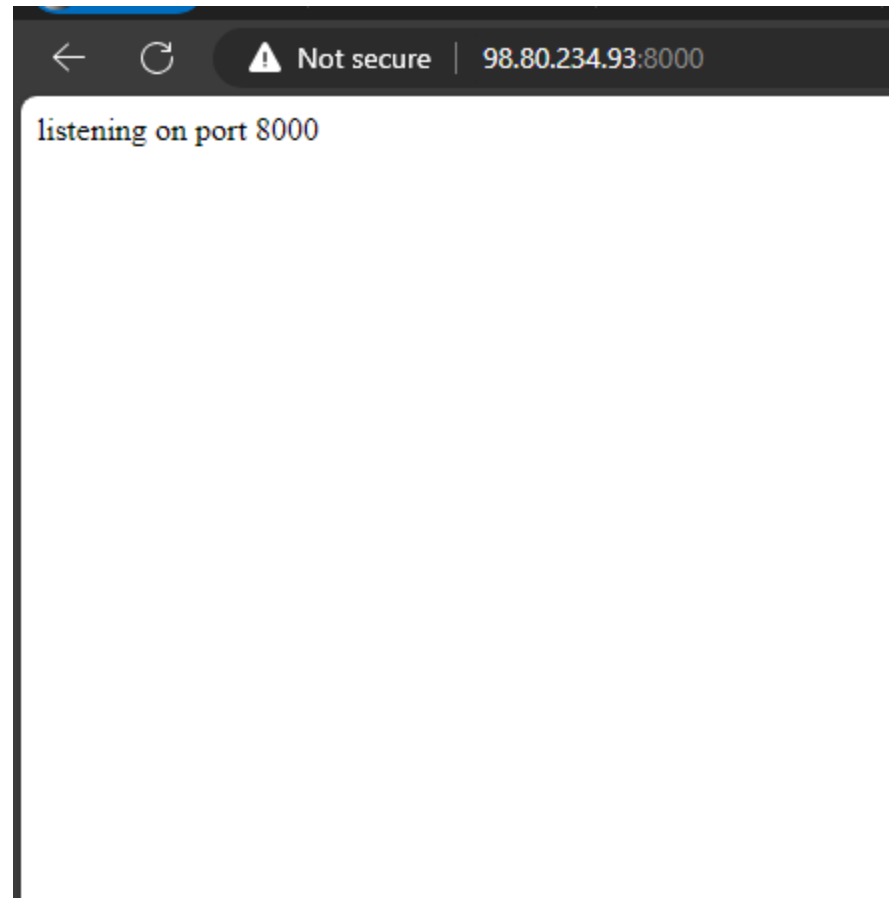
```
To address all issues, run:
  npm audit fix --force
```

```
Run `npm audit` for details.
```

```
root@ip-172-31-90-124:/home/ubuntu/siddhant/nodejs# npm start

> nodejs@1.0.0 start
> node index.js

listening on port 8000
```





Not secure

98.80.234.93:8000/about

about page