

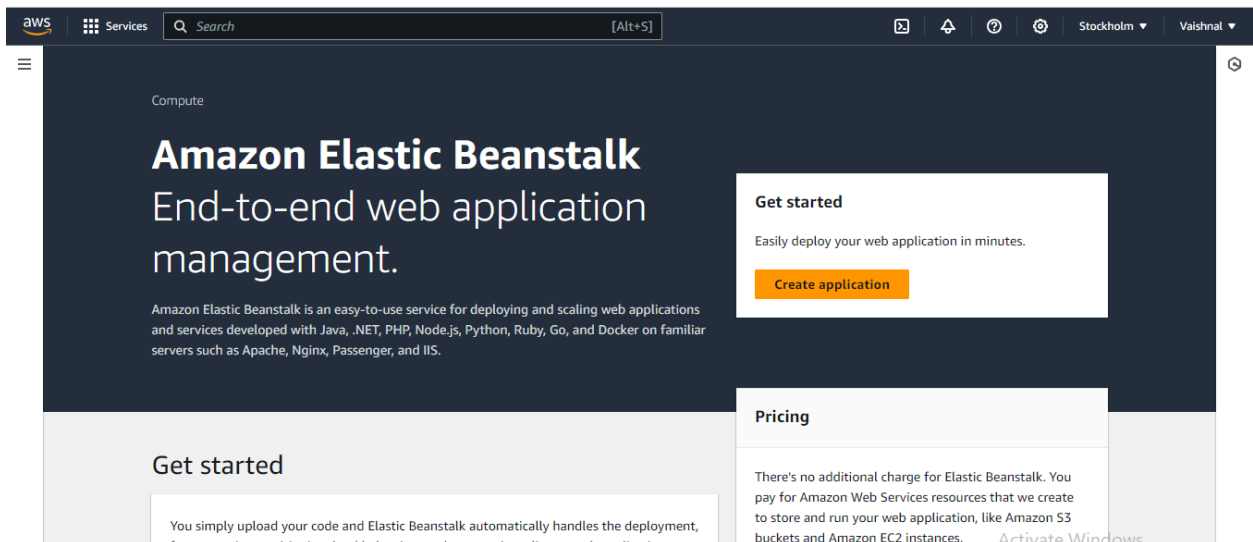
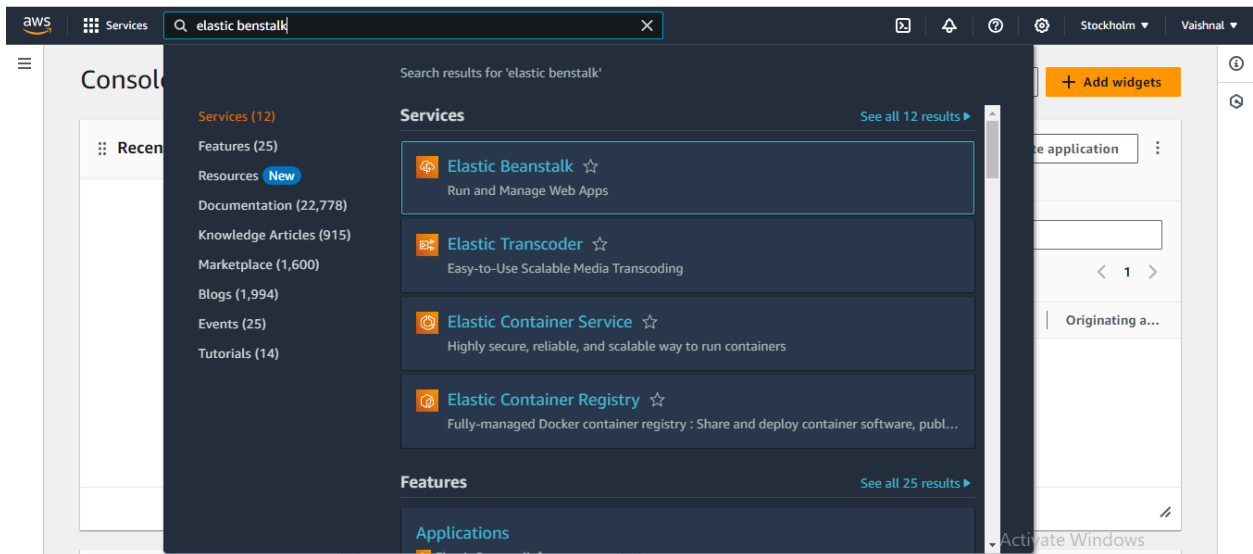
NAME:VAISHNAL MALI

DIV:D15A

ADVANCED DEV-OPS EXPERIMENT-02

AIM:To Build Your Application using AWS CodeBuild and Deploy on S3 / SEBS using AWS CodePipeline, deploy Sample Application on EC2 instance using AWS CodeDeploy.

Elastic Beanstalk



aws

Services

Search

[Alt+S]

Stockholm

Vaishnal

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 [Info](#)

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

Vaishnal27

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

Python

Platform branch

Python 3.11 running on 64bit Amazon Linux 2023

Platform version

4.1.3 (Recommended)

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

iam

×

🔍

🔔

?

⚙️

Search results for 'iam'

Services (11)

Features (24)

Resources New

Documentation (59,485)

Knowledge Articles (461)


Marketplace (860)

Blogs (1,844)


Events (12)

Tutorials (1)


Services

 IAM ☆


Manage access to AWS resources

 IAM Identity Center ☆

Manage workforce user access to multiple AWS accounts and cloud applications

 Resource Access Manager ☆

Share AWS resources with other accounts or AWS Organizations

 AWS App Mesh ☆

Easily monitor and control microservices

Features

See all 11 results ▶

See all 24 results ▶

aws

Services

Search

[Alt+S]

Global

Vaishnal

IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity Info

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.

Service or use case

EC2

Choose a use case for the specified service.

Use case

☒ **EC2**
Allows EC2 instances to call AWS services on your behalf.

☐ **EC2 Role for AWS Systems Manager**
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

☐ **EC2 Spot Fleet Role**
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.

☐ **EC2 - Spot Fleet Auto Scaling**
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.

☐ **EC2 - Spot Fleet Tagging**
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.

☐ **EC2 - Spot Instances**
Allows EC2 Spot Instances to launch and manage spot instances on your behalf.

☐ **EC2 - Spot Fleet**
Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.

Activate Windows

Go to Settings to activate Windows

Filter by Type			
<input type="text" value="beanstalk"/>		All types	14 matches
Policy name	Type	Description	
<input type="checkbox"/> AdministratorAccess-AWS...	AWS managed	Grants account administrative permissions. Explicitly allows developers and administrators t...	
<input type="checkbox"/> AWSElasticBeanstalkCust...	AWS managed	Provide the instance in your custom platform builder environment permission to launch EC...	
<input type="checkbox"/> AWSElasticBeanstalkEnha...	AWS managed	AWS Elastic Beanstalk Service policy for Health Monitoring system	
<input type="checkbox"/> AWSElasticBeanstalkMan...	AWS managed	This policy is for the AWS Elastic Beanstalk service role used to perform managed updates o...	
<input checked="" type="checkbox"/> AWSElasticBeanstalkMulti...	AWS managed	Provide the instances in your multicontainer Docker environment access to use the Amazon ...	
<input type="checkbox"/> AWSElasticBeanstalkRead...	AWS managed	Grants read-only permissions. Explicitly allows operators to gain direct access to retrieve inf...	
<input type="checkbox"/> AWSElasticBeanstalkRole...	AWS managed	AWSElasticBeanstalkRoleCore (Elastic Beanstalk operations role) Allows core operation of a ...	
<input type="checkbox"/> AWSElasticBeanstalkRole...	AWS managed	(Elastic Beanstalk operations role) Allows an environment to manage Amazon CloudWatch L...	
<input type="checkbox"/> AWSElasticBeanstalkRole...	AWS managed	(Elastic Beanstalk operations role) Allows a multicontainer Docker environment to manage ...	
<input type="checkbox"/> AWSElasticBeanstalkRole...	AWS managed	(Elastic Beanstalk operations role) Allows an environment to integrate an Amazon RDS insta...	
<input type="checkbox"/> AWSElasticBeanstalkRole...	AWS managed	(Elastic Beanstalk operations role) Allows an environment to enable Amazon SNS topic inte...	
<input type="checkbox"/> AWSElasticBeanstalkRole...	AWS managed	(Elastic Beanstalk operations role) Allows a worker environment tier to create an Amazon D...	
<input checked="" type="checkbox"/> AWSElasticBeanstalkWeb...	AWS managed	Provide the instances in your web server environment access to upload log files to Amazon S3.	
<input checked="" type="checkbox"/> AWSElasticBeanstalkWor...	AWS managed	Provide the instances in your worker environment access to upload log files to Amazon S3, t...	

Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

Maximum 64 characters. Use alphanumeric and '+,=, @, -, _' characters.

Description

Add a short explanation for this role.

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=, @-/[\[\]]!#\$%^&*()~:~''`

Service role

- ☐ Create and use new service role
- ☒ Use an existing service role

Existing service roles

Choose an existing IAM role for Elastic Beanstalk to assume as a service role. The existing IAM role must have the required IAM managed policies.

▼

↺

EC2 key pair

Select an EC2 key pair to securely log in to your EC2 instances. [Learn more](#)

Choose a key pair

▼

↺

EC2 instance profile

Choose an IAM instance profile with managed policies that allow your EC2 instances to perform required operations.

aws-elasticbeanstalk-role

▼

↺

[View permission details](#)

Cancel

Skip to review

Previous

Next

[Elastic Beanstalk](#) > [Environments](#) > Vaishnal27-env

Vaishnal27-env [Info](#)



Actions ▼

Upload and deploy

Environment overview

Health

⌚ Pending

Domain

—

Environment ID

📄 e-5gujukvgkpa

Application name

Vaishnal27

Platform

[Change version](#)

Platform

Python 3.11 running on 64bit Amazon Linux 2023/4.1.3

Running version

—

Platform state

✅ Supported

cloud formation

Search results for 'cloud formation'

Services (66)

Features (110)

Resources New

Documentation (116,209)

Knowledge Articles (1,064)

Marketplace (724)

Blogs (10,144)

Events (374)

Tutorials (26)

Services

See all 66 results

CloudFormation

☆

Create and Manage Resources with Templates

Application Composer

☆

Visually design and build modern applications quickly

Athena

☆

Serverless interactive analytics service

AWS Supply Chain

☆

Supply chain management application to manage your supply chain systems.

Features

See all 110 results

IaC Generator

CloudFormation > Stacks

Stacks (1)

Delete

Update

Stack actions

Create stack

Filter by stack name

Filter status

Active

View nested

< 1 >

Stack name	Status	Created time	Description
<div><div></div><div>awseb-e-5gujukvgkpa-stack</div></div>	<div><div></div><div>CREATE_COMPLETE</div></div>	2024-08-21 17:42:52 UTC+0530	AWS Elastic Beanstalk environment (Name: 'Vaishna127-env' Id: '5gujukvgkpa')

Instances (1) Info

Last updated less than a minute ago

Connect

Instance state

Actions

Launch instances

Find Instance by attribute or tag (case-sensitive)

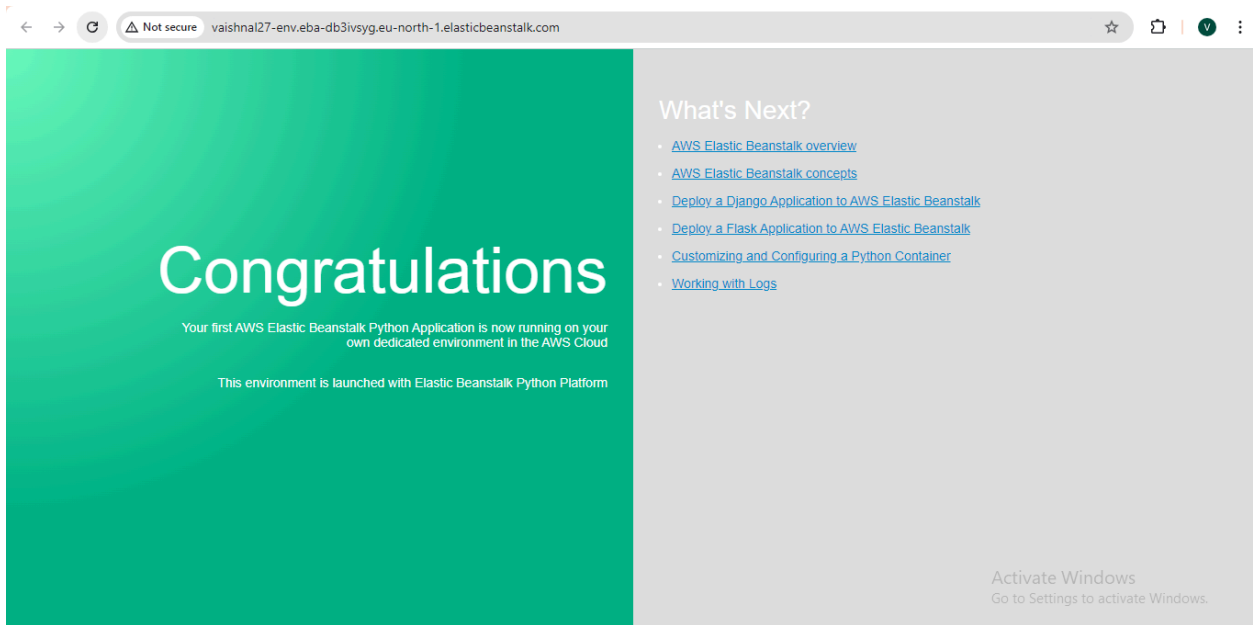
All states

Instance state: running

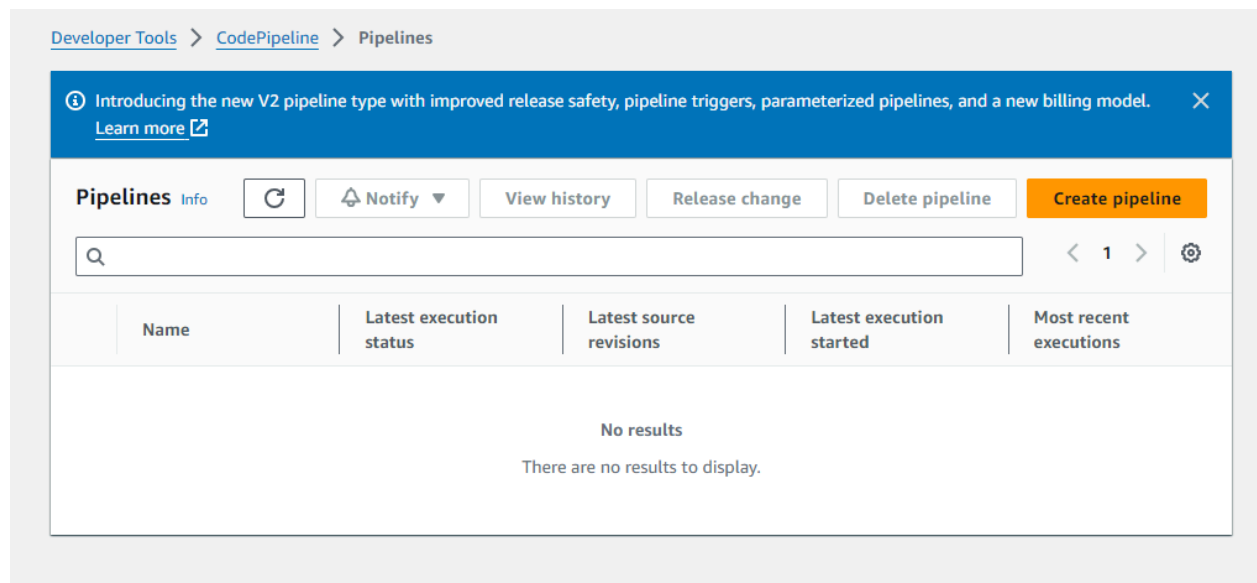
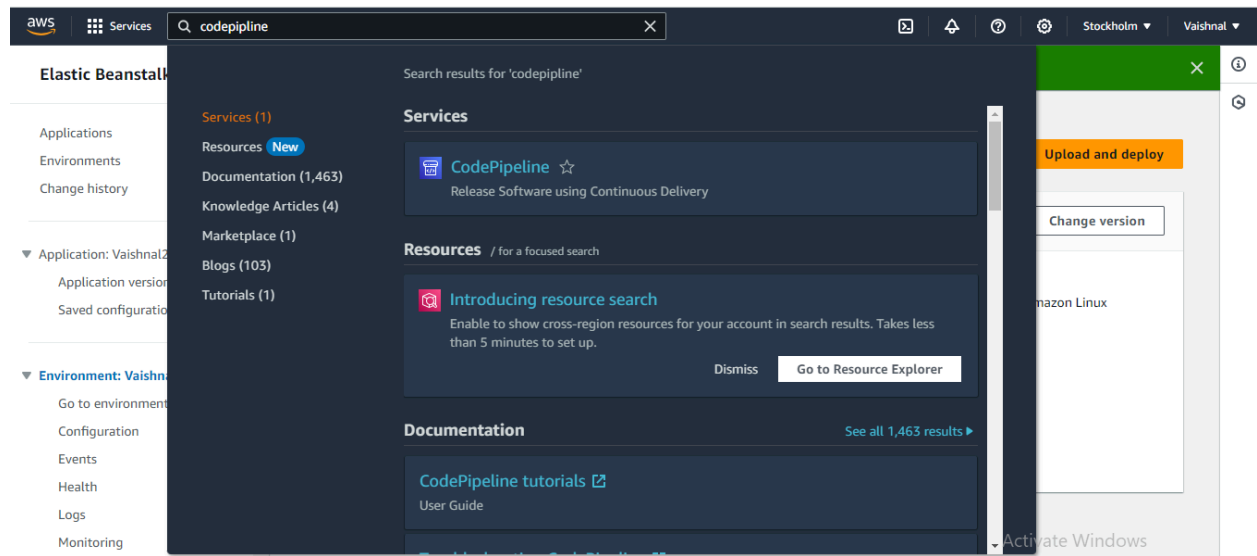
Clear filters

< 1 >

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability
<div><div></div><div></div></div>	Vaishna127-env	i-09ae763ea6085e5d4	<div><div></div><div>Running</div></div>	t3.micro	<div><div></div><div>2/2 checks passed</div></div>	<div><div>View alarms</div></div>	eu-north-1



Code Deployment using Codepipeline



Developer Tools > CodePipeline > Pipelines > Create new pipeline

Step 1
Choose pipeline settings

Step 2
Add source stage

Step 3
Add build stage

Step 4
Add deploy stage

Step 5
Review

Choose pipeline settings

Step 1 of 5

Pipeline settings

Pipeline name

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

Vaishnal-pipeline

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)

Activate Windows
Go to Settings to activate Windows.

Developer Tools > CodePipeline > Pipelines > Create new pipeline

Step 1
Choose pipeline settings

Step 2
Add source stage

Step 3
Add build stage

Step 4
Add deploy stage

Step 5
Review

Add source stage

Step 2 of 5

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 1)

Grant AWS CodePipeline access to your GitHub repository. This allows AWS CodePipeline to upload commits from GitHub to your pipeline.

Connected

You have successfully configured the action with the provider.

Repository

vaishnal16/IP-lab-Exp-2

Branch

main

main

Change detection options

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



GitHub webhooks (recommended)

Use webhooks in GitHub to automatically start my pipeline when a change occurs



AWS CodePipeline

Use AWS CodePipeline to check periodically for changes

Cancel

Previous

Next

Developer Tools > CodePipeline > Pipelines > Create new pipeline

Step 1

Choose pipeline settings

Step 2

Add source stage

Step 3

Add build stage

Step 4

Add deploy stage

Step 5

Review

Add build stage

Info

Step 3 of 5

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.

Cancel

Previous

Skip build stage

Next

Developer Tools > CodePipeline > Pipelines > Create new pipeline

Step 1

Choose pipeline settings

Step 2

Add source stage

Step 3

Add build stage

Step 4

Add deploy stage

Step 5

Review

Add deploy stage

Info

Step 4 of 5



You cannot skip this stage

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)

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.



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.



Vaishnal27-env

Cancel

Previous

Next

Developer Tools > CodePipeline > Pipelines > Create new pipeline

Step 1
Choose pipeline settings

Step 2
Add source stage

Step 3
Add build stage

Step 4
Add deploy stage

Step 5
Review

Review

[Info](#)

Step 5 of 5

Step 1: Choose pipeline settings

Pipeline settings

Pipeline name

Vaishnal-pipeline

Pipeline type

V2

Execution mode

QUEUED

Artifact location

A new Amazon S3 bucket will be created as the default artifact store for your pipeline

Service role name

AWSCodePipelineServiceRole-eu-north-1-Vaishnal-pipeline

Activate Windows

Go to Settings to activate Windows.

aws Services Search [Alt+S]

Developer Tools **CodePipeline**

- Source • CodeCommit
- Artifacts • CodeArtifact
- Build • CodeBuild
- Deploy • CodeDeploy
- Pipeline • CodePipeline
 - Getting started
 - Pipelines
 - Pipeline**
 - History
 - Settings
- Settings

Success
Congratulations! The pipeline Vaishnal-pipeline has been created.

Create a notification rule for this pipeline

Developer Tools > CodePipeline > Pipelines > Vaishnal-pipeline

Vaishnal-pipeline

Notify Edit Stop execution Clone pipeline Release change

Pipeline type: V2 Execution mode: QUEUED

Source Succeeded


Pipeline execution ID: [914dbdae-9746-43a0-917c-96f15484b6e0](#)

Source
[GitHub \(Version 1\)](#)

Succeeded - Just now
[2f65ba7d](#)

View details

< → ↻ Not secure vaishnal27-env.eba-db3ivsyg.eu-north-1.elasticbeanstalk.com ☆ 📄 🔒



Home About Us Services Portfolio Blog Careers Contact

Welcome to Service Samurai

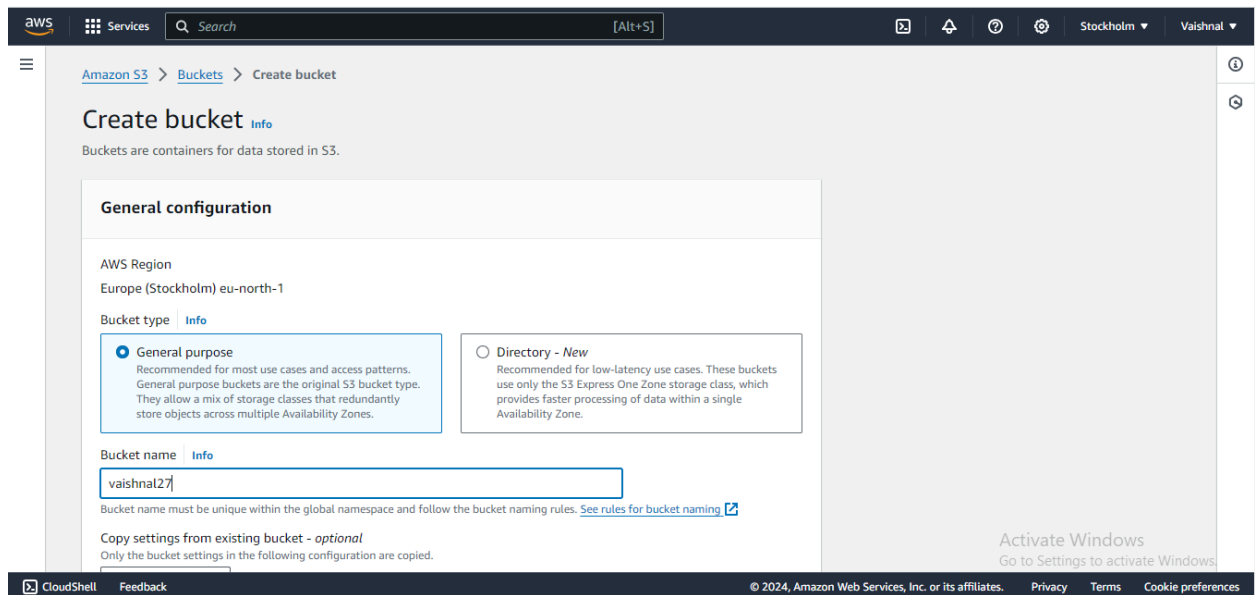
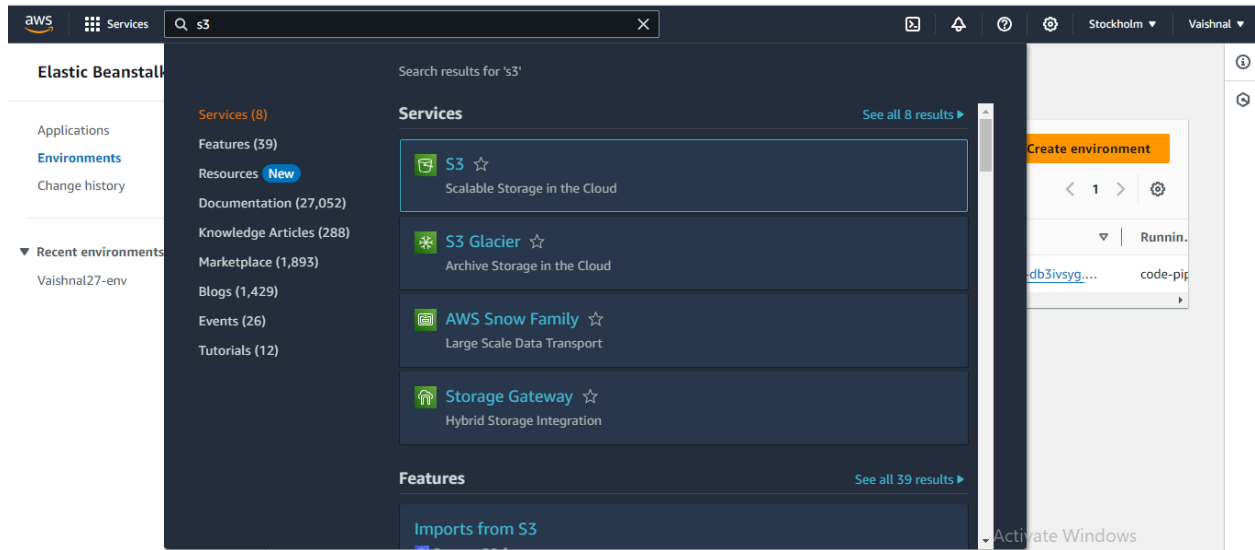
Innovating the future with cutting-edge technology products.

Explore Our Services

Our Story

Activate Windows
Go to Settings to activate Windows.

Code Deployment Using S3 Bucket :



aws

Services

Search

[Alt+S]

Stockholm

Vaishnal

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

CloudShell

Feedback

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

Privacy

Terms

Cookie preferences

Activate Windows
Go to Settings to activate Windows.

aws

Services

Search

[Alt+S]

Stockholm

Vaishnal

Default encryption

Info

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type

Info

Server-side encryption with Amazon S3 managed keys (SSE-S3)

Server-side encryption with AWS Key Management Service keys (SSE-KMS)

Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the [Storage](#) tab of the [Amazon S3 pricing page](#).

Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

Disable

Enable

Advanced settings

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

CloudShell

Feedback

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

Privacy

Terms

Cookie preferences

Activate Windows
Go to Settings to activate Windows.

aws

Services

Search

[Alt+S]

Stockholm

Vaishnal

Successfully created bucket "vaishnal27"

To upload files and folders, or to configure additional bucket settings, choose [View details](#).

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 (3)

Info

All AWS Regions

Copy ARN

Empty

Delete

Create bucket

Buckets are containers for data stored in S3.

Find buckets by name

< 1 >

	Name	AWS Region	IAM Access Analyzer	Creation date
<input type="radio"/>	codepipeline-eu-north-1-282300822552	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1	August 21, 2024, 18:50:19 (UTC+05:30)
<input type="radio"/>	elasticbeanstalk-eu-north-1-108782066834	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1	August 21, 2024, 17:26:41 (UTC+05:30)
<input type="radio"/>	vaishnal27	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1	August 22, 2024, 20:56:15 (UTC+05:30)

CloudShell Feedback

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

aws

Services

Search

[Alt+S]

Stockholm

Vaishnal

Amazon S3

Buckets

vaishnal27

Upload

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, 2.5 KB)

Remove

Add files

Add folder

All files and folders in this table will be uploaded.

Find by name

< 1 >

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

Destination

Info

Activate Windows
Go to Settings to activate Windows.

CloudShell Feedback

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

aws

Services

Search

[Alt+S]

Stockholm

Vaishnal

Upload succeeded

View details below.

Summary

Destination

s3://vaishnal27

Succeeded

1 file, 2.5 KB (100.00%)

Failed

0 files, 0 B (0%)

Files and folders

Configuration

Files and folders (1 Total, 2.5 KB)

Find by name

Name	Folder	Type	Size	Status	Error
index.html	-	text/html	2.5 KB	Succeeded	-

CloudShell

Feedback

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

Privacy

Terms

Cookie preferences

aws

Services

Search

[Alt+S]

Stockholm

Vaishnal

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

Amazon S3

Buckets

vaishnal27

index.html

index.html

Info

Copy S3 URI

Download

Open

Object actions

Properties

Permissions

Versions

Object overview

Owner

2a2d4731449a9a279eef4456196a2cf4eb9ffa8e7796cbbac73abfe103264d2

AWS Region

Europe (Stockholm) eu-north-1

Last modified

August 22, 2024, 21:04:51 (UTC+05:30)

Size

2.5 KB

S3 URI

s3://vaishnal27/index.html

Amazon Resource Name (ARN)

arn:aws:s3:::vaishnal27/index.html

Entity tag (Etag)

c07652731061bfca2575fa2fde413cdb

Object URL

https://vaishnal27.s3.eu-north-1.amazonaws.com/index.html

CloudShell

Feedback

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

Privacy

Terms

Cookie preferences

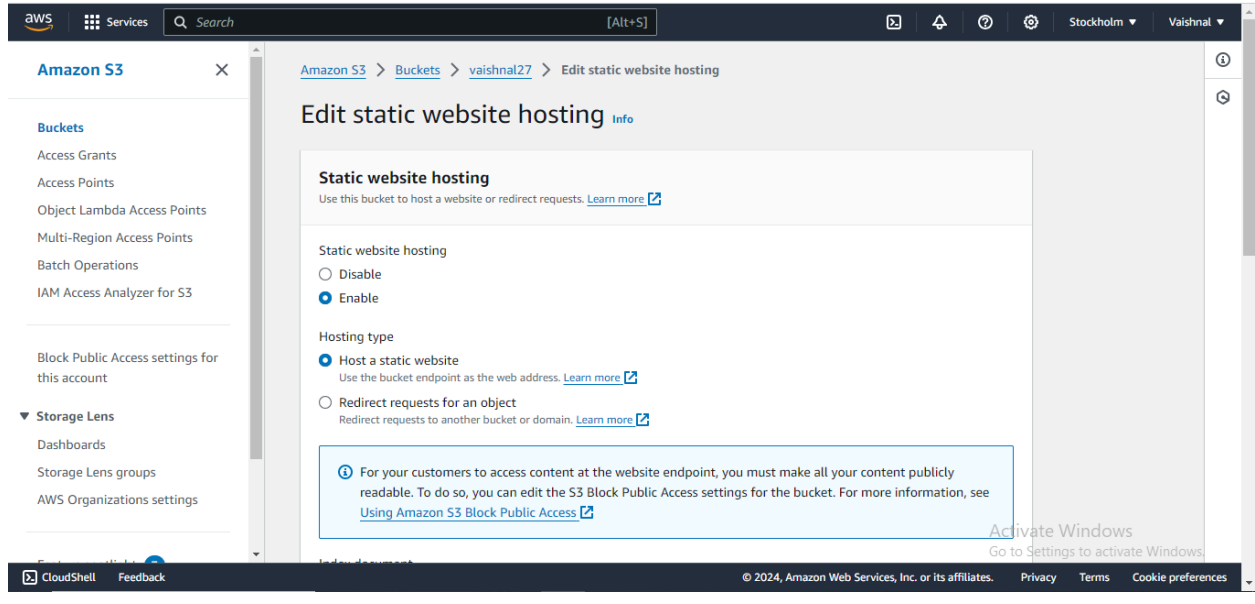
Static website hosting

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

Static website hosting

Disabled

Edit



Index document

Specify the home or default page of the website.

index.html

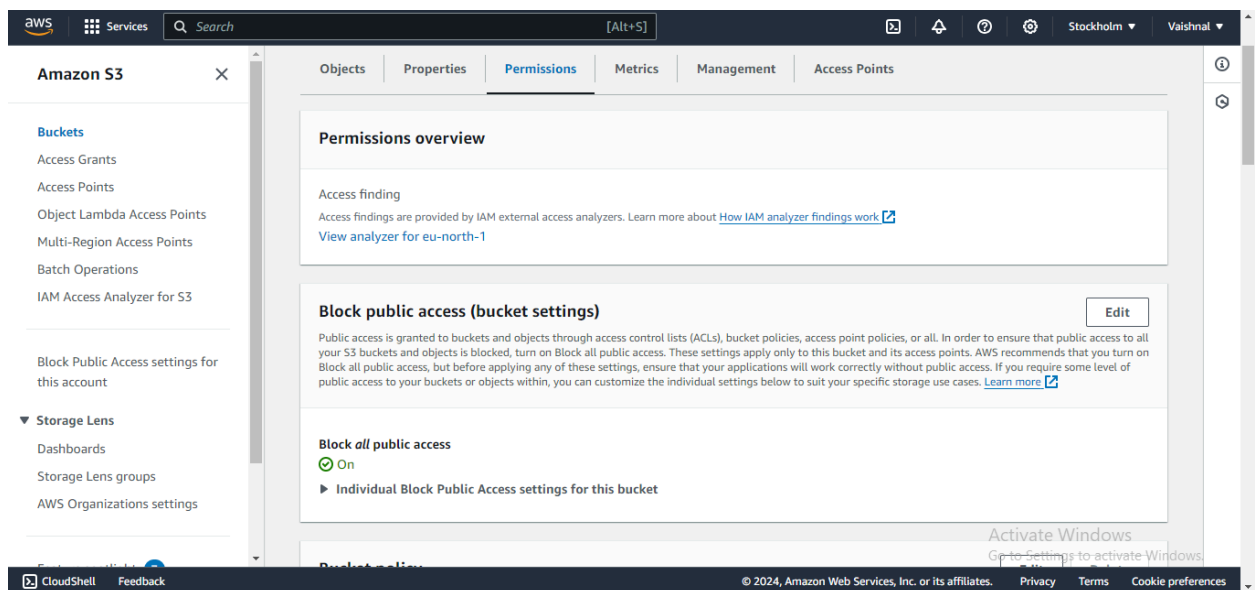
Error document - optional

This is returned when an error occurs.

error.html

Redirection rules – optional

Redirection rules, written in JSON, automatically redirect webpage requests for specific content. [Learn more](#)



aws

Services

Search

[Alt+S]

Stockholm

Vaishnal

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

Amazon S3

Buckets

vaishnal27

Edit Block public access (bucket settings)

Edit Block public access (bucket settings)

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

CloudShell

Feedback

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

Privacy

Terms

Cookie preferences

Edit Block public access (bucket settings)

⚠️ Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.

To confirm the settings, enter *confirm* in the field.

confirm

Cancel

Confirm

Object Ownership

Edit

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.

Object Ownership

Bucket owner enforced

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

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

AWS Marketplace for S3

Amazon S3 > Buckets > vaishnal27 > Edit Object Ownership

Edit Object Ownership

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.

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.

Activate Windows
Go to Settings to activate Windows.

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

Amazon S3 > Buckets > vaishnal27

vaishnal27

Objects Properties Permissions Metrics Management Access Points

Objects (1)

Refresh

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder Upload

Find objects by prefix Show versions

<input checked="" type="checkbox"/>	Name	Type	Last modified	Size
<input checked="" type="checkbox"/>	index.html	html	August 22, 2024, 21:04:51 (UTC+05:30)	

Initiate restore

Query with S3 Select

Edit actions

Rename object

Edit storage class

Edit server-side encryption

Edit metadata

Edit tags

Make public using ACLs

Activate Windows
Go to Settings to activate Windows.

CloudShell Feedback

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

Amazon S3 > Buckets > vaishnal27 > Make public

Make public

Info

The make public action enables public read access in the object access control list (ACL) settings. [Learn more](#).

⚠ 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 22, 2024, 21:04:51 (UTC+05:30)	2.5 KB

Cancel

Make public

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	Successfully edited public access	Failed to edit public access
s3://vaishnal27	✔ 1 object, 2.5 KB	0 objects

vaishnal27.s3.eu-north-1.amazonaws.com/index.html

Welcome to Service Samurai

Company Logo

Company Details

Name	Service Samurai
Address	123 Business Ave, Suite 100, City, Country
Contact Information	(123) 456-7890 contact@servicesamurai.com
Description	Service Samurai provides top-notch services in technology solutions, including consulting, development, and support.

Our Services

- Consulting Services
- Software Development
- Technical Support
- IT Infrastructure Management

Introduction Audio

0:00 / 0:00

Promotional Video

Activate Windows

Go to Settings to activate Windows.

