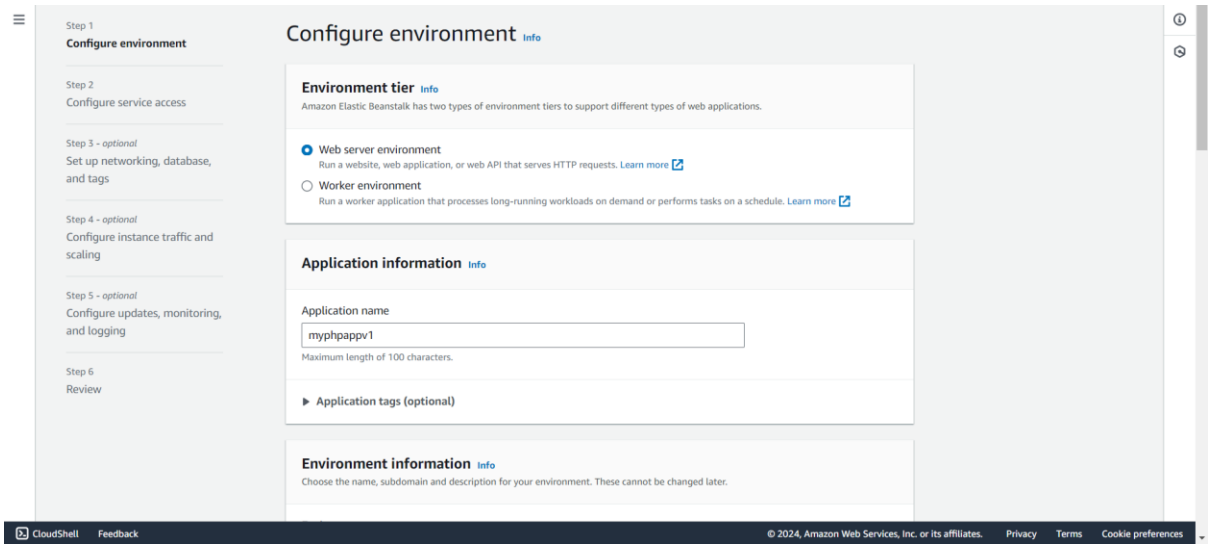
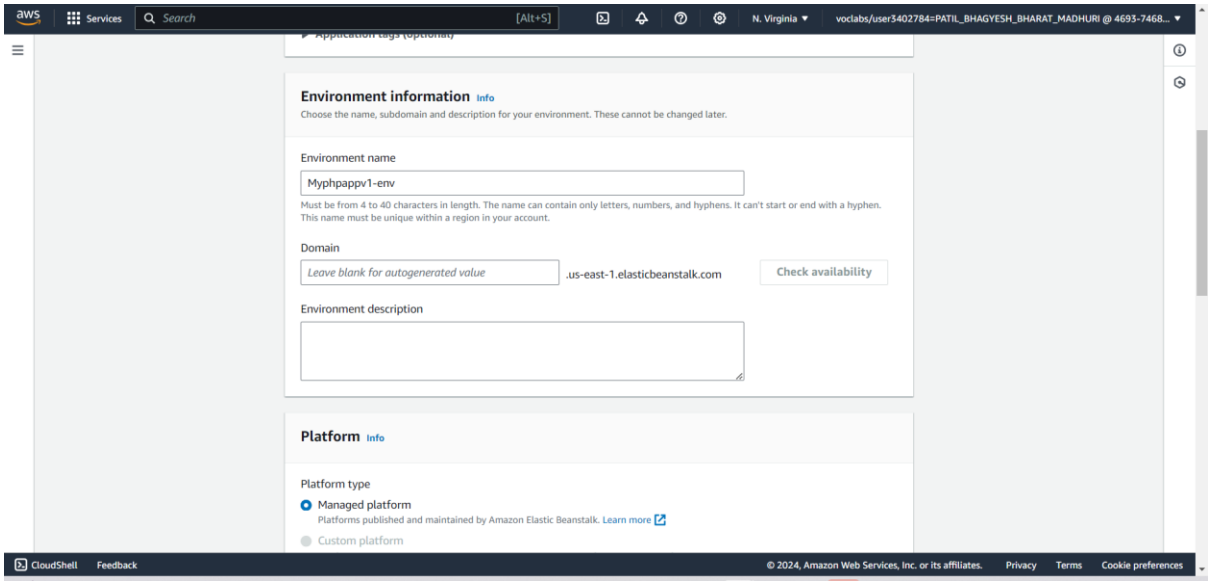
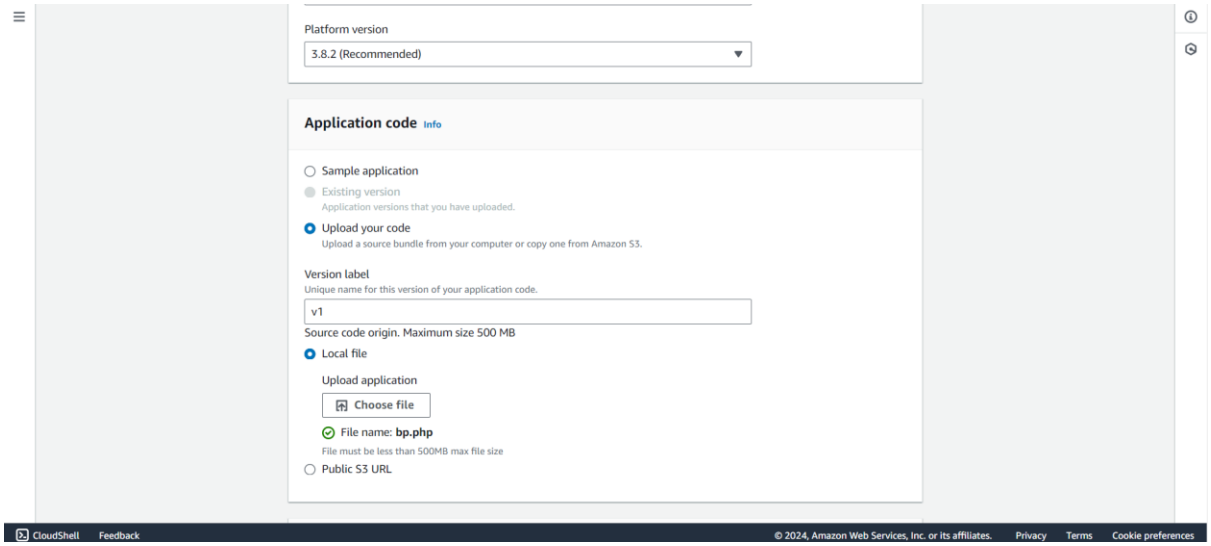
ADVANCE DEVOPS EXPERIMENT NO.2

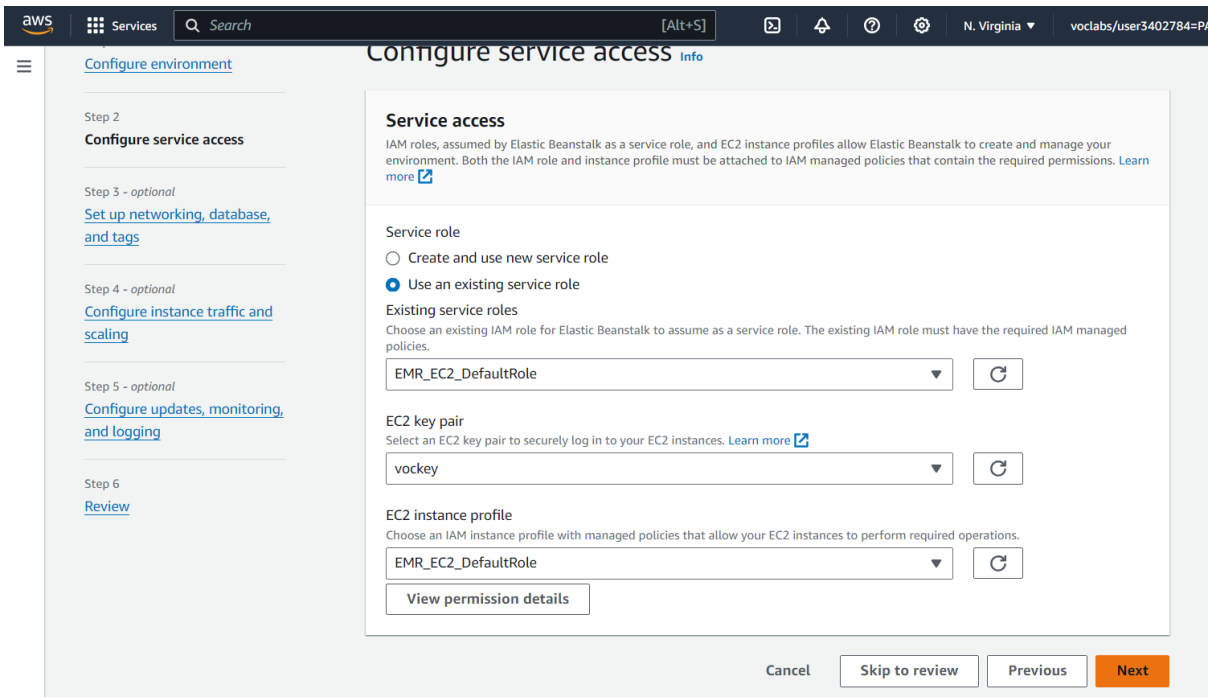
Name: Bhagyesh Patil
Class:D15A
Roll No:36

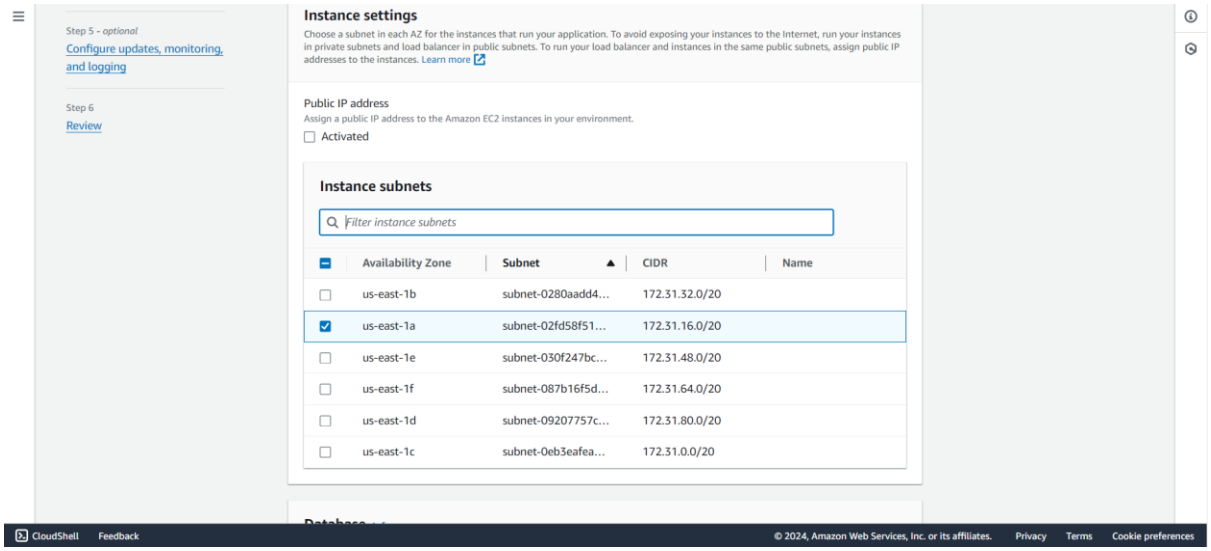
Aim:-
To Build Your Application using AWS CodeBuild and Deploy on S3 / SEBS using AWSCodePipeline, deploy Sample Application on EC2 instance using AWS CodeDeploy

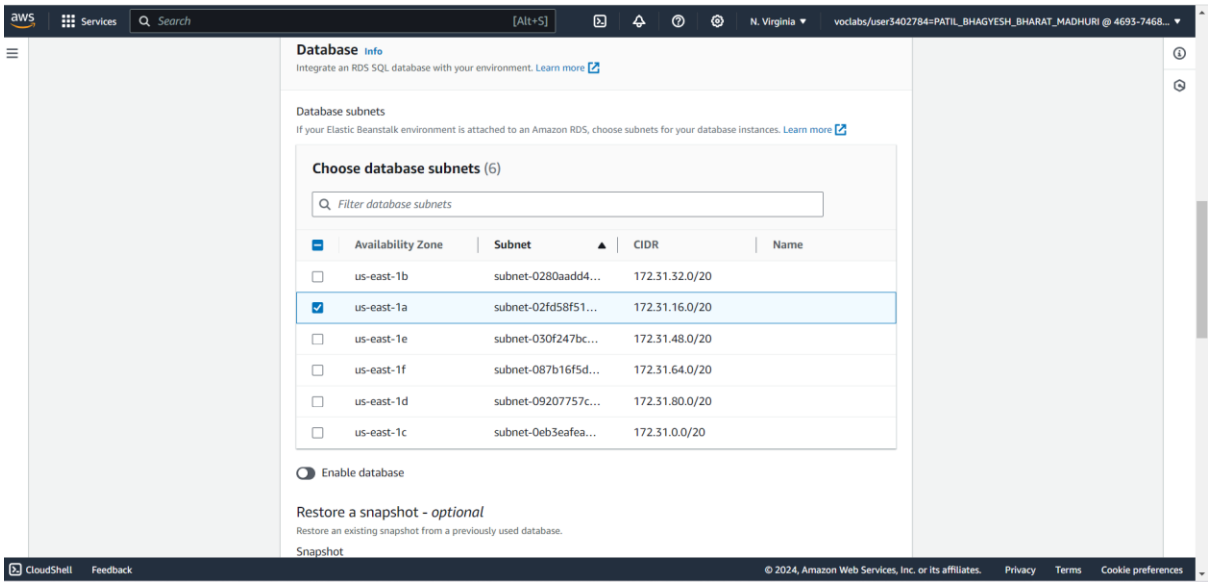


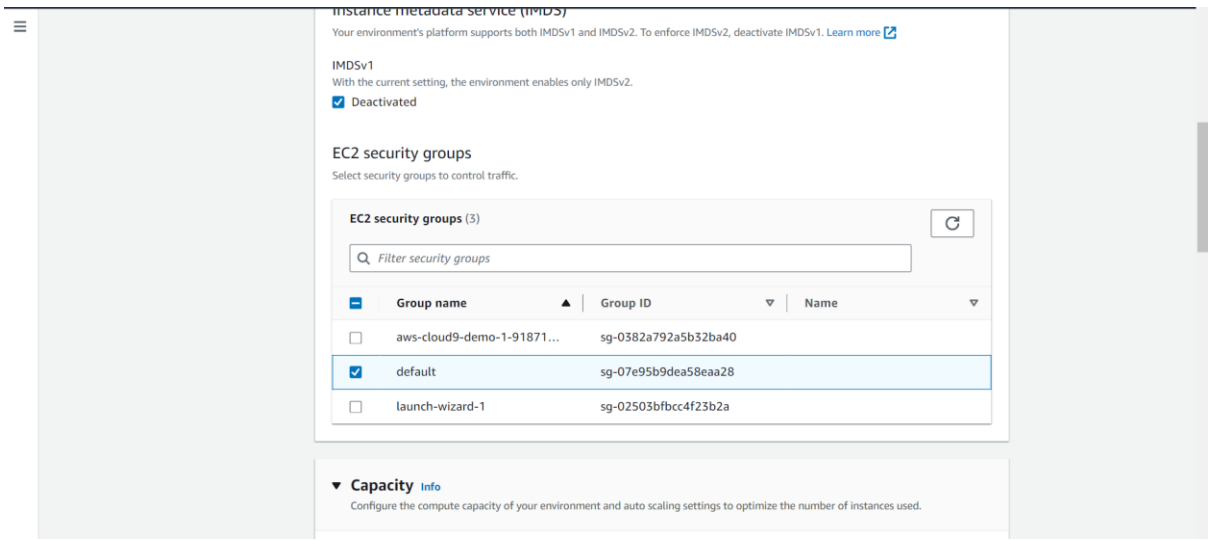


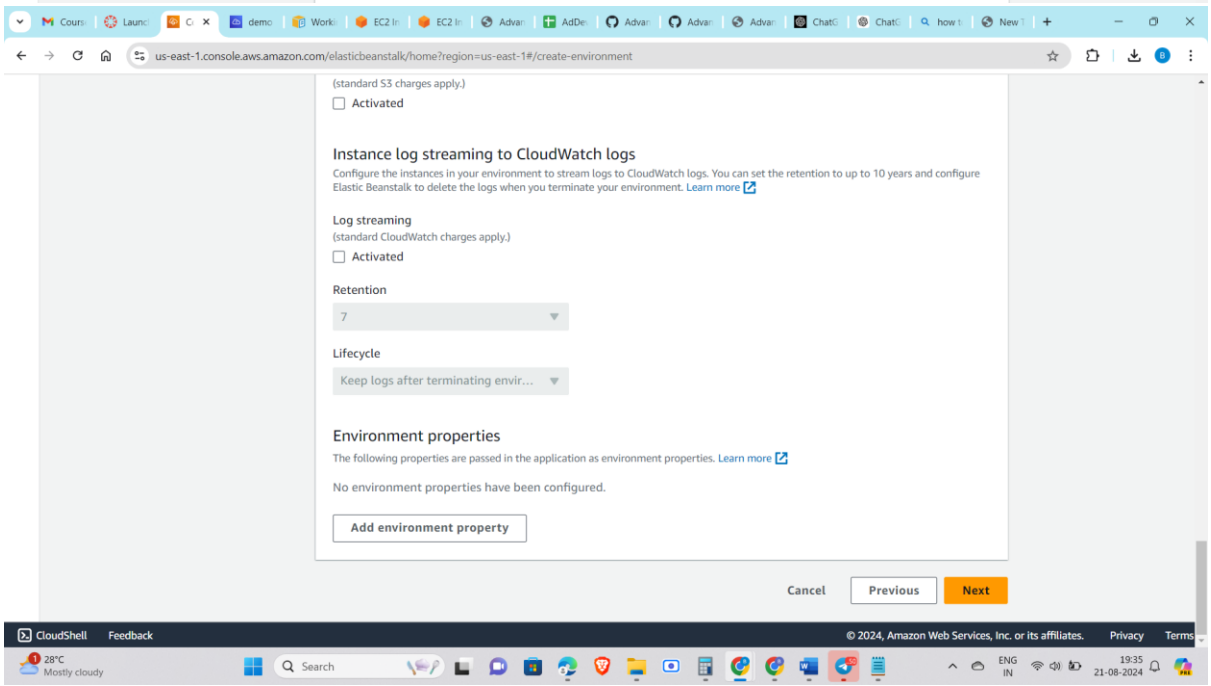

Platform version
3.8.2 (Recommended)
Application code Info
Sample application
Existing version
Application versions that you have uploaded.
Upload your code
Upload a source bundle from your computer or copy one from Amazon S3.
Version label
Unique name for this version of your application code.
v1
Source code origin. Maximum size 500 MB
Local file
Upload application
Choose file
File name: bp.php
File must be less than 500MB max file size
Public S3 URL
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
N. Virginia
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 service access Info
Service access
IAM roles, assumed by Elastic Beanstalk as a service role, and EC2 instance profiles allow Elastic Beanstalk to create and manage your environment. Both the IAM role and instance profile must be attached to IAM managed policies that contain the required permissions. Learn more
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.
EMR_EC2_DefaultRole
EC2 key pair
Select an EC2 key pair to securely log in to your EC2 instances. Learn more
vockey
EC2 instance profile
Choose an IAM instance profile with managed policies that allow your EC2 instances to perform required operations.
EMR_EC2_DefaultRole
View permission details
Cancel
Skip to review
Previous
Next


Step 5 - optional
Configure updates, monitoring, and logging
Step 6
Review
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
Instance subnets
Filter instance subnets
Availability Zone
Subnet
CIDR
Name
us-east-1b subnet-0280aadd4... 172.31.32.0/20
us-east-1a subnet-02fd58f51... 172.31.16.0/20
us-east-1e subnet-030f247bc... 172.31.48.0/20
us-east-1f subnet-087b16f5d... 172.31.64.0/20
us-east-1d subnet-09207757c... 172.31.80.0/20
us-east-1c subnet-0eb3eafea... 172.31.0.0/20
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Database Info
Integrate an RDS SQL database with your environment. Learn more
Database subnets
If your Elastic Beanstalk environment is attached to an Amazon RDS, choose subnets for your database instances. Learn more
Choose database subnets (6)
Filter database subnets
Availability Zone
Subnet
CIDR
Name
us-east-1b subnet-0280aadd4... 172.31.32.0/20
us-east-1a subnet-02fd58f51... 172.31.16.0/20
us-east-1e subnet-030f247bc... 172.31.48.0/20
us-east-1f subnet-087b16f5d... 172.31.64.0/20
us-east-1d subnet-09207757c... 172.31.80.0/20
us-east-1c subnet-0eb3eafea... 172.31.0.0/20
Enable database
Restore a snapshot - optional
Restore an existing snapshot from a previously used database.
Snapshot
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Your environment's platform supports both IMDSv1 and IMDSv2. To enforce IMDSv2, deactivate IMDSv1. Learn more
IMDSv1
With the current setting, the environment enables only IMDSv2.
Deactivated
EC2 security groups
Select security groups to control traffic.
EC2 security groups (3)
Filter security groups
Group name
Group ID
Name
aws-cloud9-demo-1-91871... sg-0382a792a5b32ba40
default sg-07e95b9dea58eaa28
launch-wizard-1 sg-02503bfbcc4f23b2a
Capacity Info
Configure the compute capacity of your environment and auto scaling settings to optimize the number of instances used.


us-east-1.console.aws.amazon.com/elasticbeanstalk/home?region=us-east-1#/create-environment
(standard S3 charges apply.)
Activated
Instance log streaming to CloudWatch logs
Configure the instances in your environment to stream logs to CloudWatch logs. You can set the retention to up to 10 years and configure Elastic Beanstalk to delete the logs when you terminate your environment. Learn more
Log streaming
(standard CloudWatch charges apply.)
Activated
Retention
7
Lifecycle
Keep logs after terminating envir...
Environment properties
The following properties are passed in the application as environment properties. Learn more
No environment properties have been configured.
Add environment property
Cancel
Previous
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms

Review Info

Step 1: Configure environment

Edit

Environment information

Environment tier
Web server environment

Application name
Aryan27

Environment name
Aryan27-env

Application code
Sample application

Platform
arn:aws:elasticbeanstalk:us-east-1::platform/PHP 8.3 running on 64bit Amazon Linux 2023/4.3.2

Step 2: Configure service access

Edit

Service access Info

Configure the service role and EC2 instance profile that Elastic Beanstalk uses to manage your environment. Choose an EC2 key pair to securely log in to your EC2 instances.

Service role
arn:aws:iam::405894863107:role/service-role/aws-elasticbeanstalk-service-role

EC2 instance profile
aws-elasticbeanstalk-ec2-role

Step 3: Set up networking, database, and tags

Edit

Networking, database, and tags Info

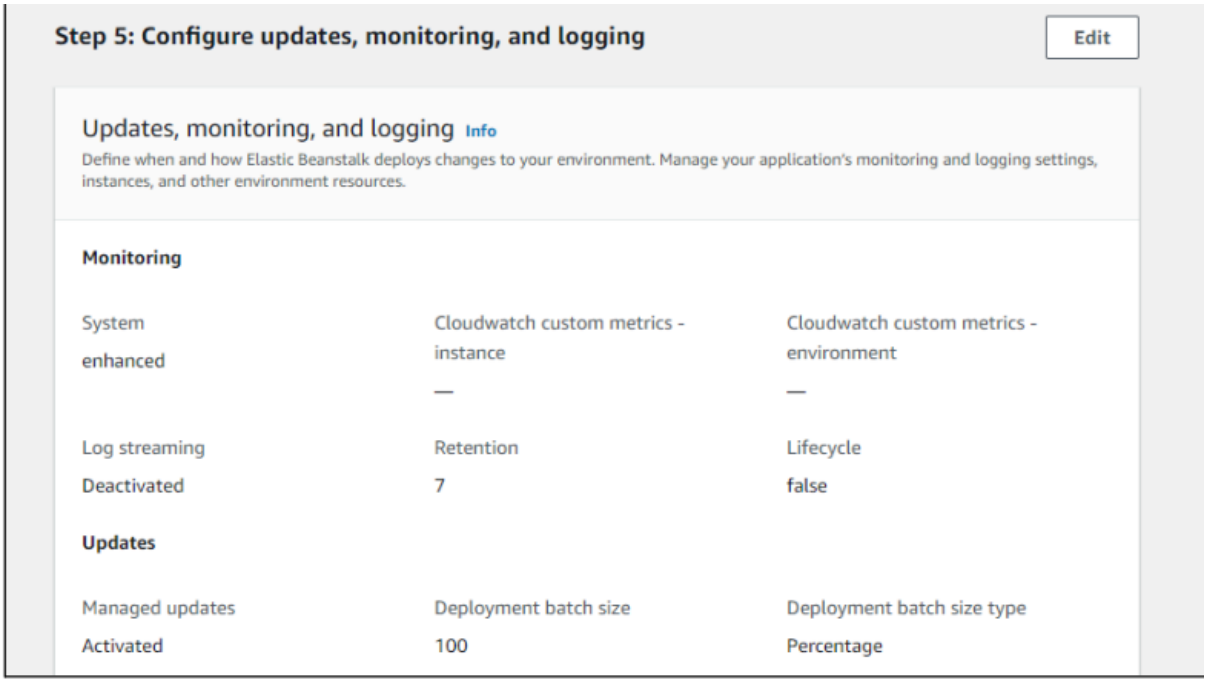
Configure VPC settings, and subnets for your environment's EC2 instances and load balancer. Set up an Amazon RDS database that's integrated with your environment.

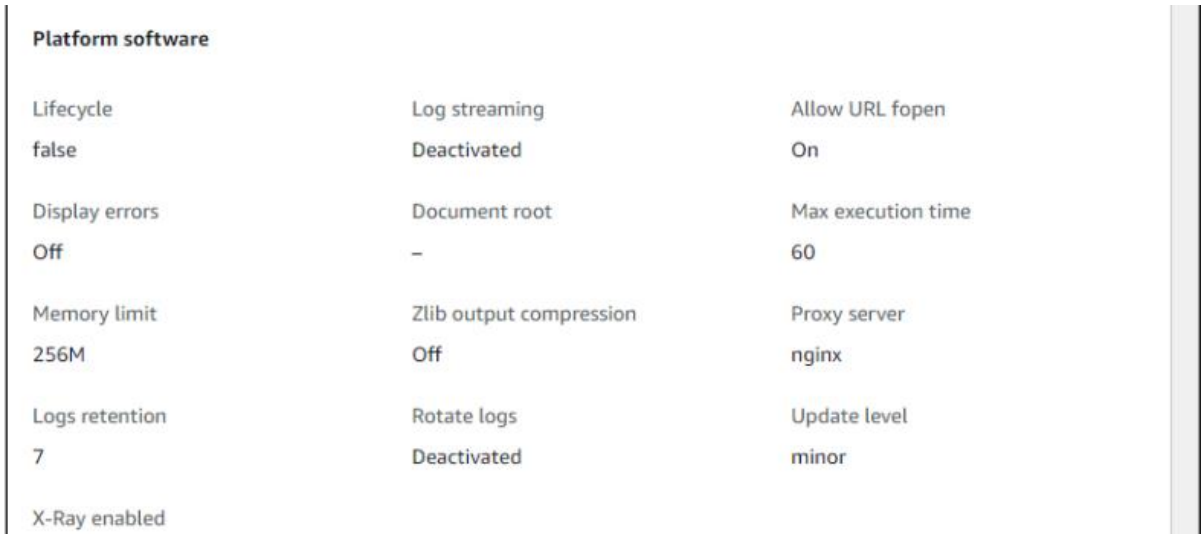
Network

VPC
vpc-0bf7d7d872a737f13

Public IP address
false

Instance subnets
subnet-035fe38d8d742329e,subnet-0a7c9c6dedec1325d


Step 5: Configure updates, monitoring, and logging
Edit
Updates, monitoring, and logging Info
Define when and how Elastic Beanstalk deploys changes to your environment. Manage your application's monitoring and logging settings, instances, and other environment resources.
Monitoring
System
enhanced
Cloudwatch custom metrics - instance
—
Cloudwatch custom metrics - environment
—
Log streaming
Deactivated
Retention
7
Lifecycle
false
Updates
Managed updates
Activated
Deployment batch size
100
Deployment batch size type
Percentage


Platform software
Lifecycle
false
Log streaming
Deactivated
Allow URL fopen
On
Display errors
Off
Document root
–
Max execution time
60
Memory limit
256M
Zlib output compression
Off
Proxy server
nginx
Logs retention
7
Rotate logs
Deactivated
Update level
minor
X-Ray enabled

Trusted entity type

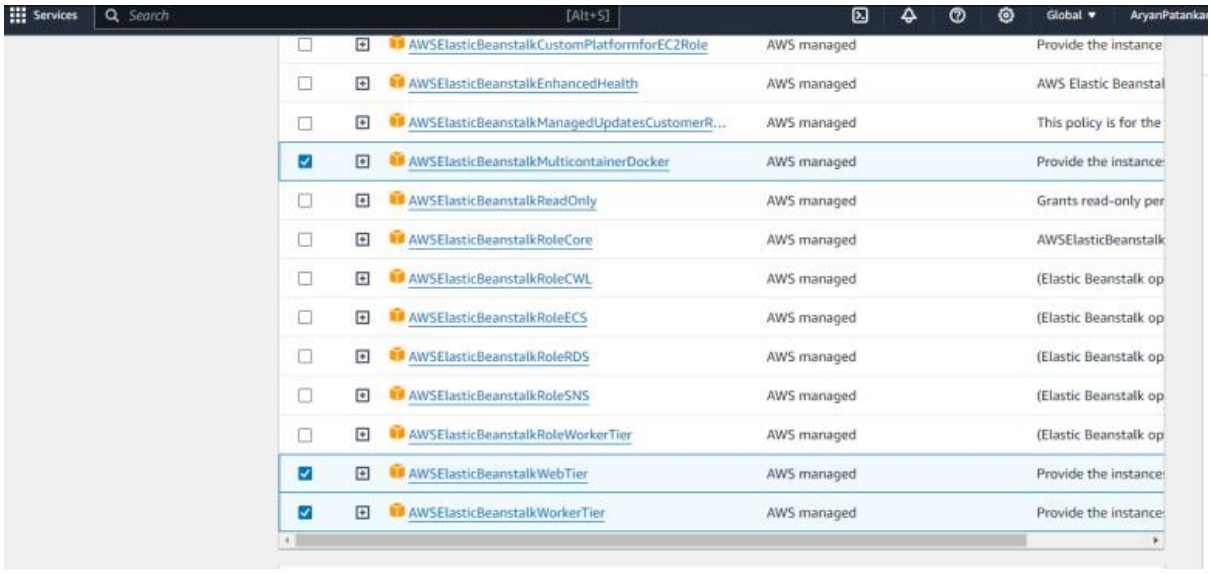
- **AWS service**
  Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- **AWS account**
  Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- **Web identity**
  Allows users federated by the specified external web 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.

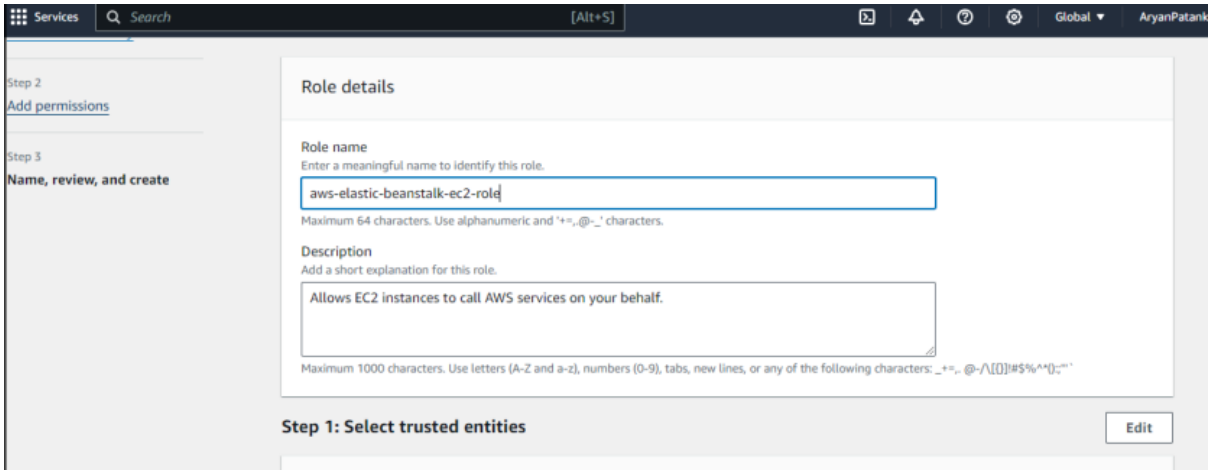
Use case

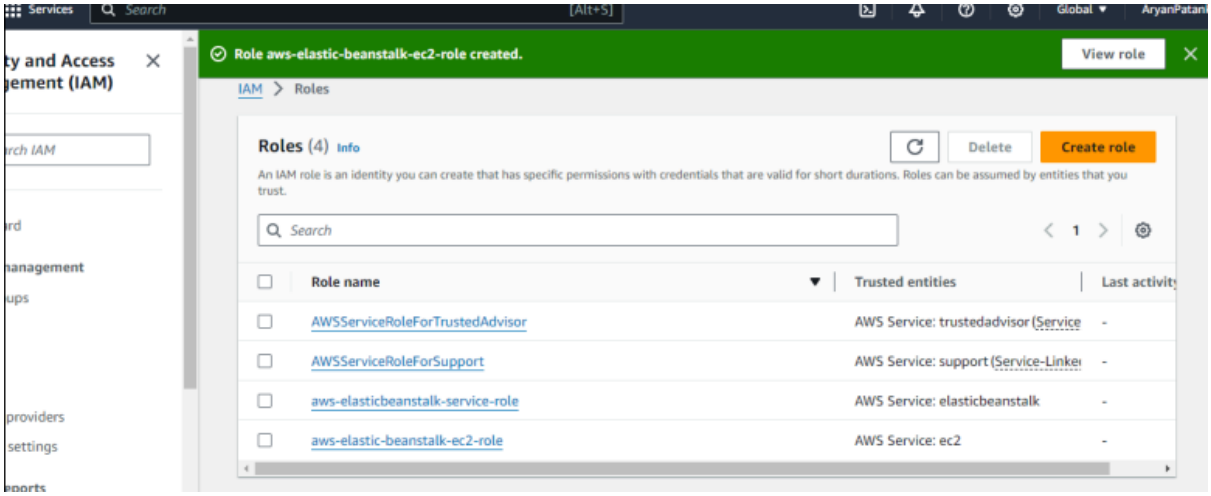
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

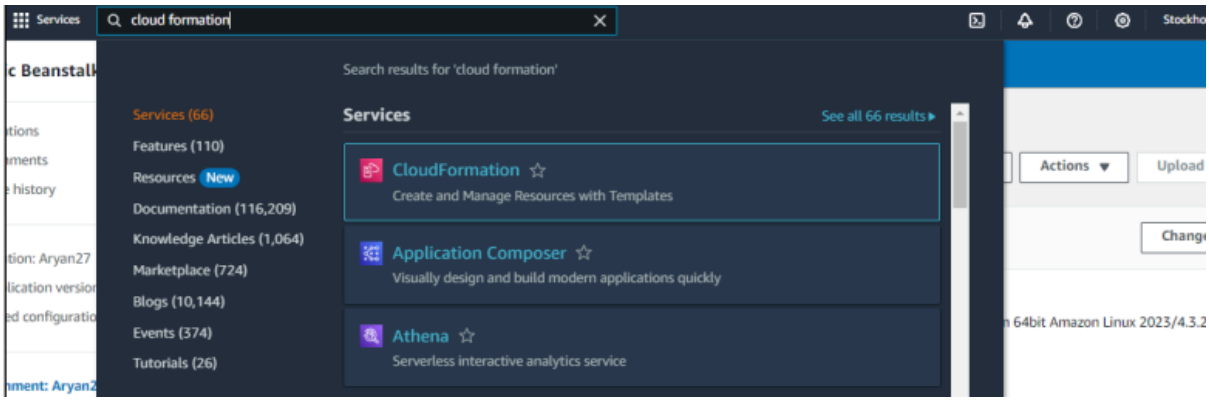
Service or use case

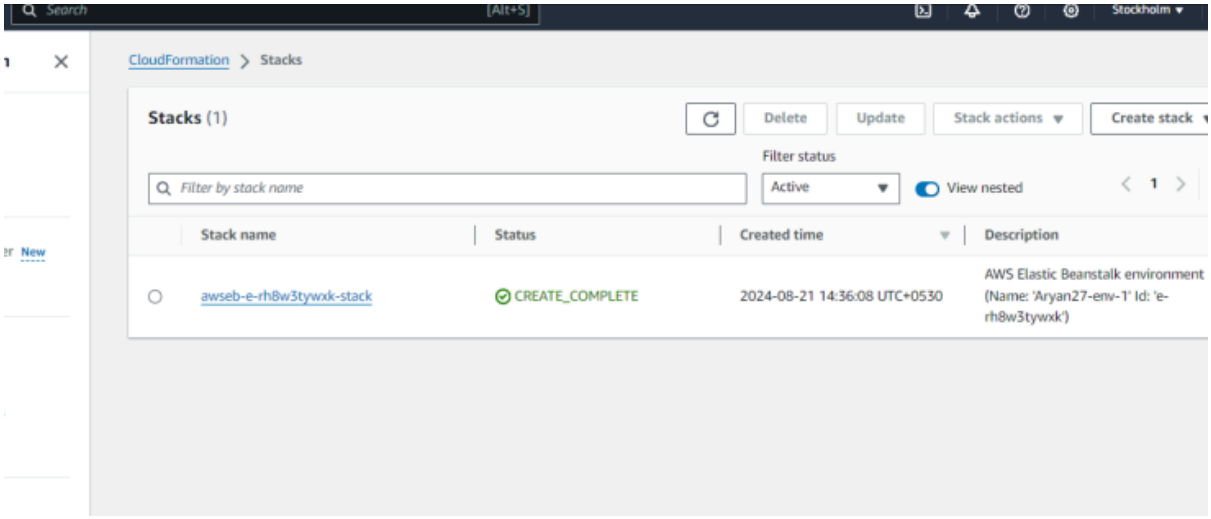
EC2

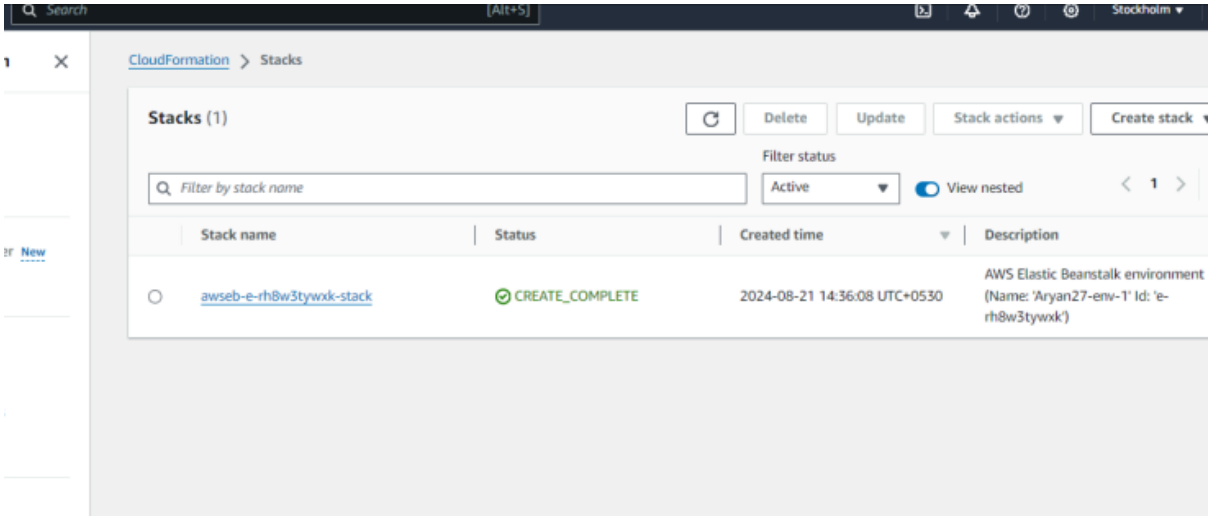


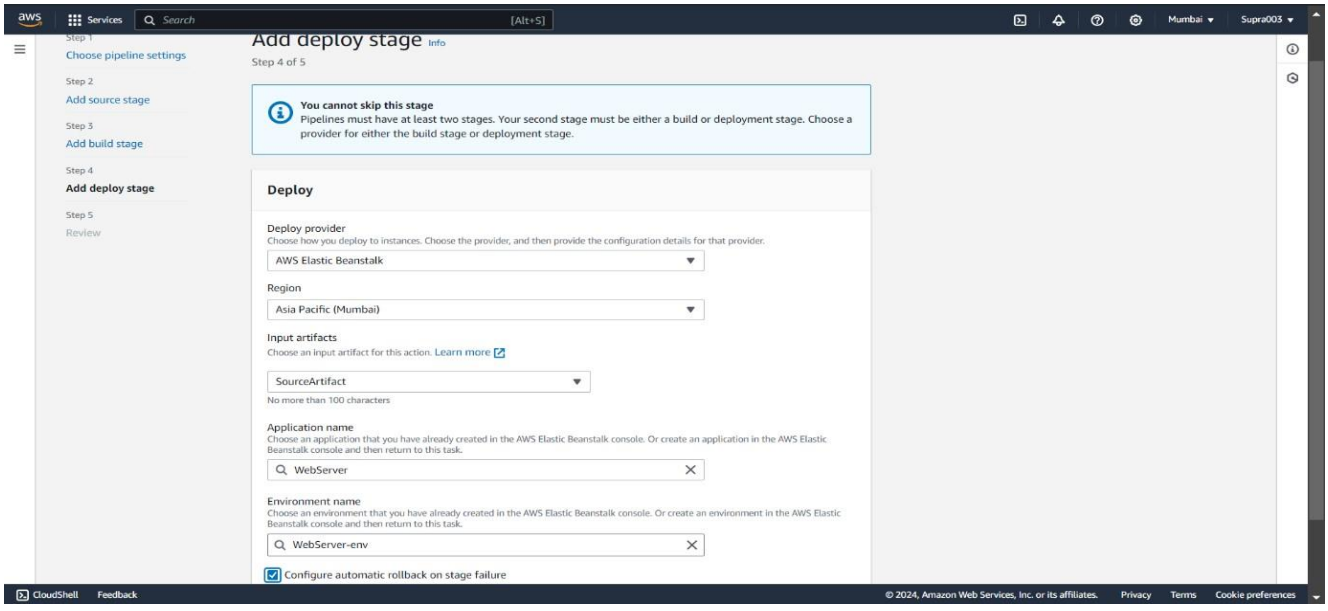

Services
Search
[Alt+S]
Global
AryanPatank
Step 2
Add permissions
Step 3
Name, review, and create
Role details
Role name
Enter a meaningful name to identify this role.
aws-elastic-beanstalk-ec2-role
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.
Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=,. @-/\[{}]!#$%^*();:"'`
Step 1: Select trusted entities
Edit

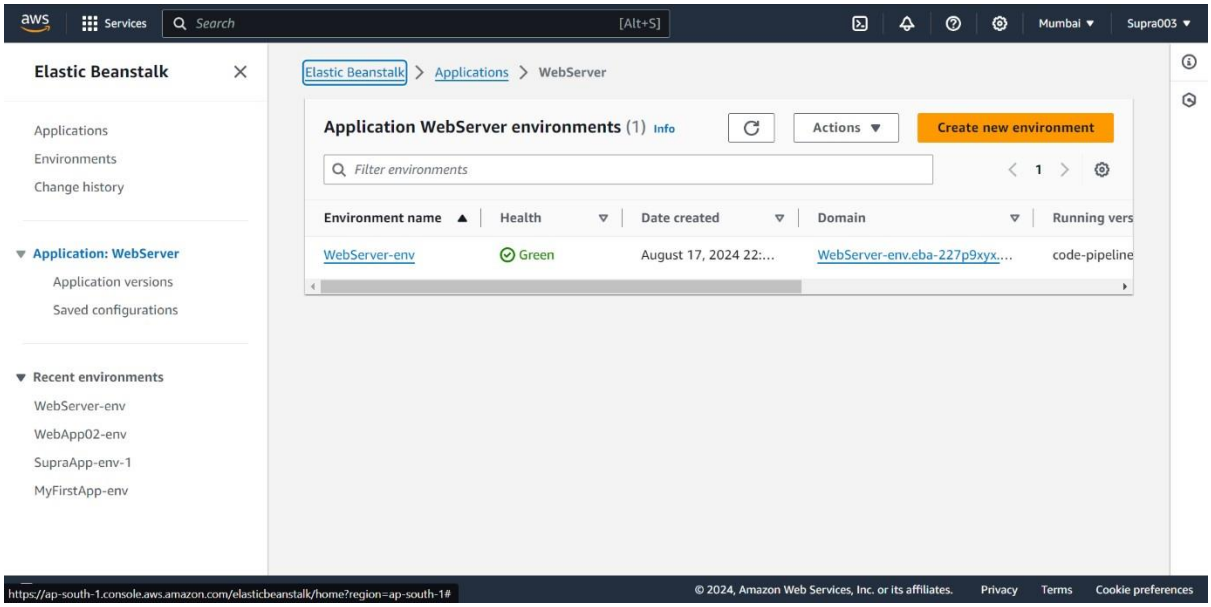

Role aws-elastic-beanstalk-ec2-role created.
View role
IAM > Roles
Roles (4) Info
Delete
Create role
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.
Search
Role name
Trusted entities
AWSServiceRoleForTrustedAdvisor
AWS Service: trustedadvisor (Service
AWSServiceRoleForSupport
AWS Service: support (Service-Linke
aws-elasticbeanstalk-service-role
AWS Service: elasticbeanstalk
aws-elastic-beanstalk-ec2-role
AWS Service: ec2

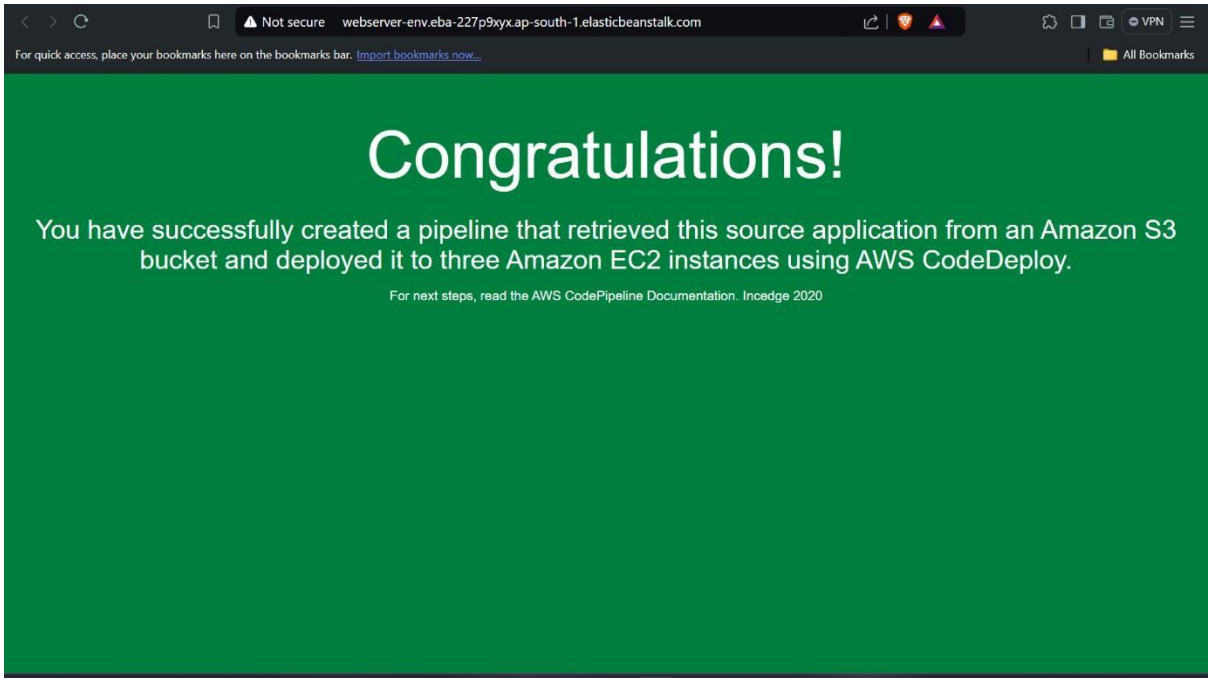

Services
cloud formation
Search results for 'cloud formation'
Services (66)
Features (110)
Resources New
Documentation (116,209)
Knowledge Articles (1,064)
Marketplace (724)
Blogs (10,144)
Events (374)
Tutorials (26)
Services
See all 66 results
CloudFormation
Create and Manage Resources with Templates
Application Composer
Visually design and build modern applications quickly
Athena
Serverless interactive analytics service
Actions
Upload


Search
[Alt+S]
Stockholm
CloudFormation
Stacks
Stacks (1)
Delete
Update
Stack actions
Create stack
Filter status
Filter by stack name
Active
View nested
1
Stack name
Status
Created time
Description
awseb-e-rh8w3tywxk-stack
CREATE_COMPLETE
2024-08-21 14:36:08 UTC+0530
AWS Elastic Beanstalk environment (Name: 'Aryan27-env-1' Id: 'e-rh8w3tywxk')
New

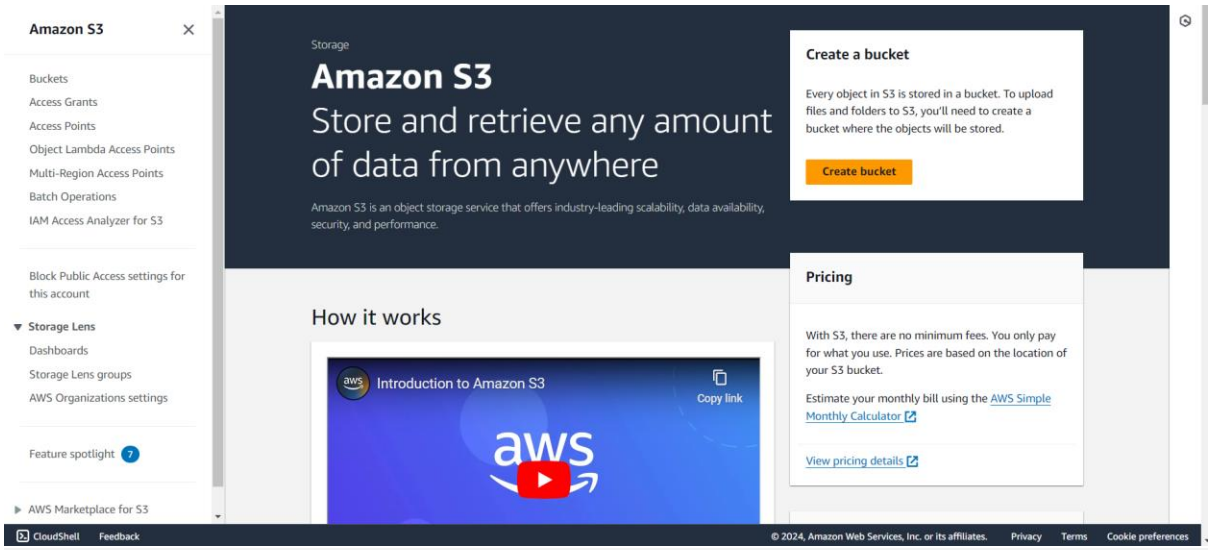

Search
[Alt+S]
Stockholm
CloudFormation
Stacks
Stacks (1)
Delete
Update
Stack actions
Create stack
Filter status
Filter by stack name
Active
View nested
1
Stack name
Status
Created time
Description
awseb-e-rh8w3tywxk-stack
CREATE_COMPLETE
2024-08-21 14:36:08 UTC+0530
AWS Elastic Beanstalk environment (Name: 'Aryan27-env-1' Id: 'e-rh8w3tywxk')
New


aws
Services
Search
[Alt+S]
Mumbai
Supra003
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
Asia Pacific (Mumbai)
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.
WebServer
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.
WebServer-env
Configure automatic rollback on stage failure
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
Mumbai
Supra003
Elastic Beanstalk
Applications
Environments
Change history
Application: WebServer
Application versions
Saved configurations
Recent environments
WebServer-env
WebApp02-env
SupraApp-env-1
MyFirstApp-env
Elastic Beanstalk > Applications > WebServer
Application WebServer environments (1) Info
Actions
Create new environment
Filter environments
1
Environment name
Health
Date created
Domain
Running vers
WebServer-env
Green
August 17, 2024 22:...
WebServer-env.eba-227p9xyx....
code-pipeline
https://ap-south-1.console.aws.amazon.com/elasticbeanstalk/home?region=ap-south-1#
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Not secure
webserver-env.eba-227p9xyx.ap-south-1.elasticbeanstalk.com
VPN
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
All Bookmarks
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. Incedge 2020

Using s3 bucket



General configuration

AWS Region

US East (N. Virginia) us-east-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

hutiypa

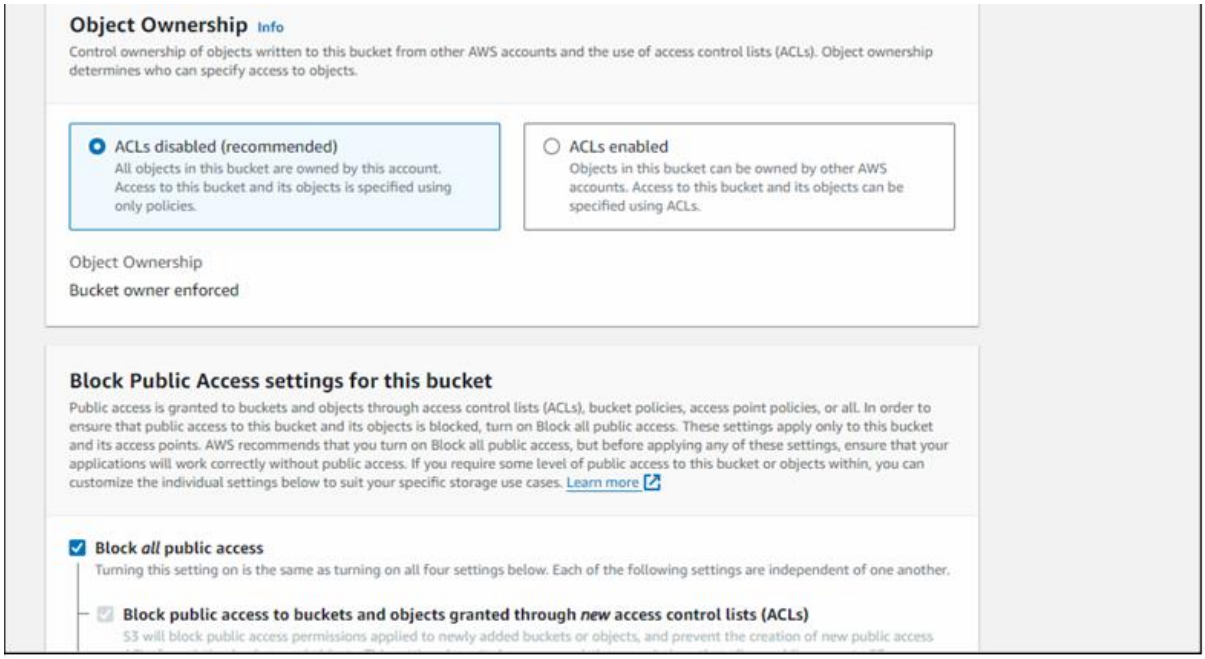
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

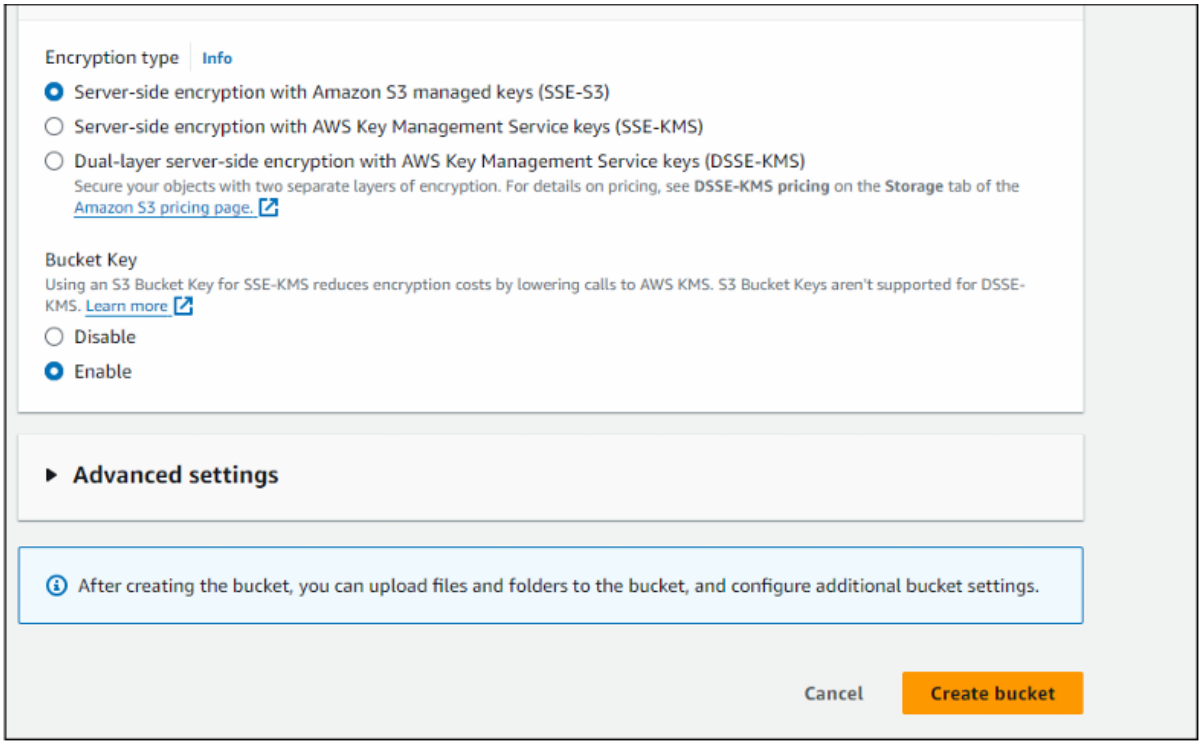
Copy settings from existing bucket - *optional*

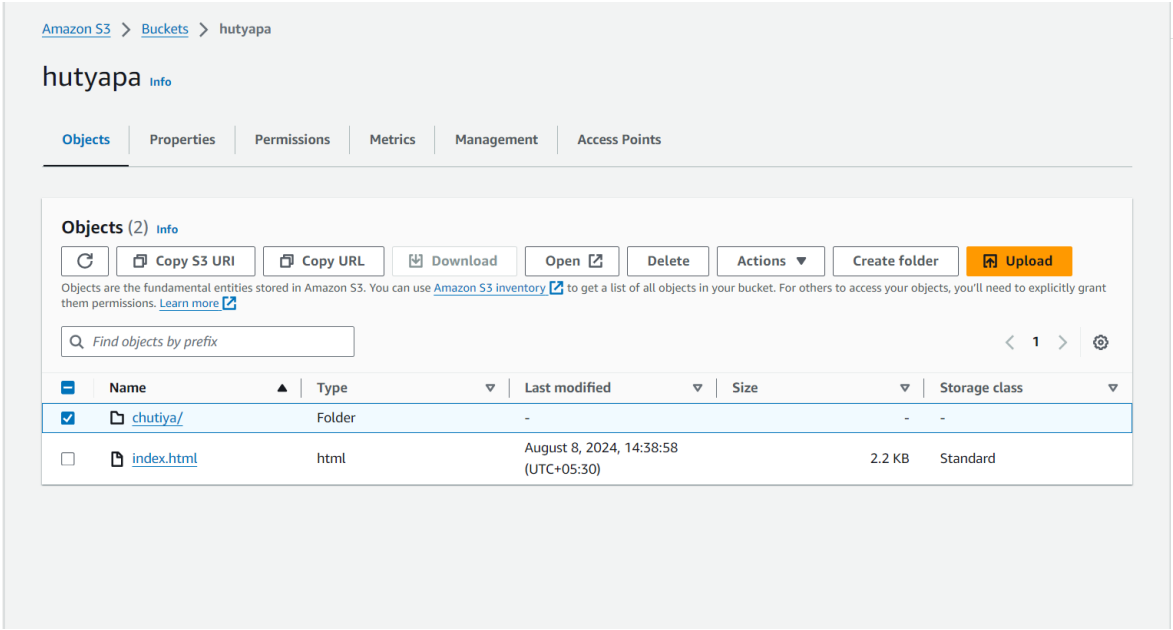
Only the bucket settings in the following configuration are copied.

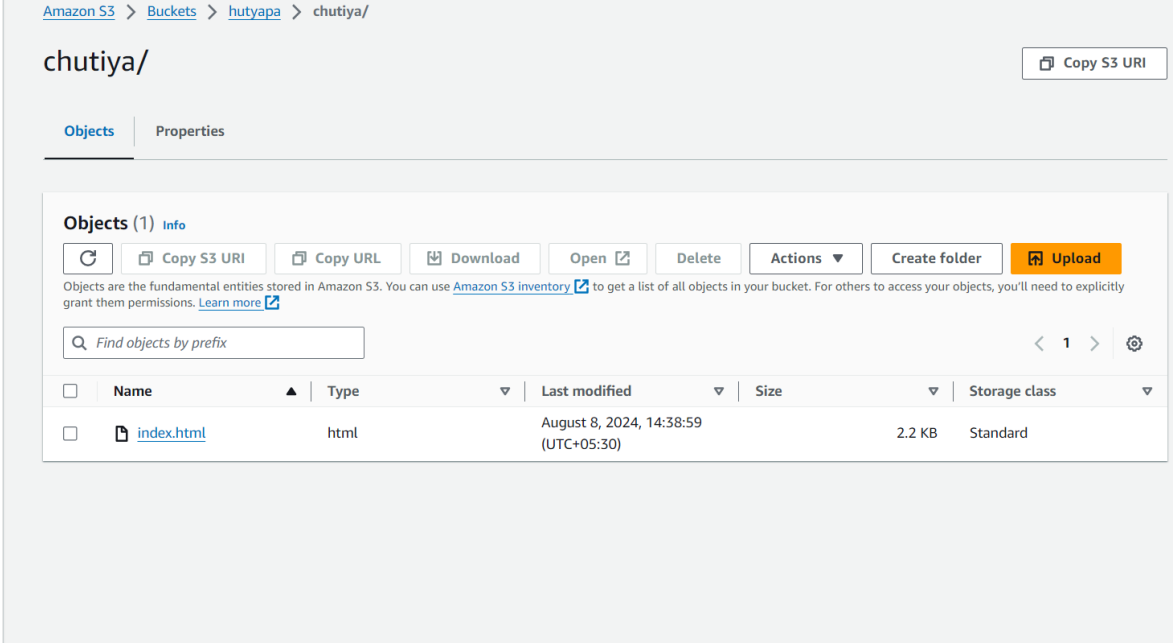
Choose bucket

Format: s3://bucket/prefix


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


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.
Cancel
Create bucket


Amazon S3 > Buckets > hutyapa
hutyapa Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (2) 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
Name
Type
Last modified
Size
Storage class
chutiya/
Folder
-
-
-
index.html
html
August 8, 2024, 14:38:58 (UTC+05:30)
2.2 KB
Standard


Amazon S3 > Buckets > hutyapa > chutiya/
chutiya/
Copy S3 URI
Objects
Properties
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
Name
Type
Last modified
Size
Storage class
index.html
html
August 8, 2024, 14:38:59 (UTC+05:30)
2.2 KB
Standard

About This Page

This is a simple and elegant web page designed with a modern and clean UI. The layout includes a header, a content area, and a footer, all styled to provide a pleasant user experience.

Learn More