

Name: Anthea Gamjya

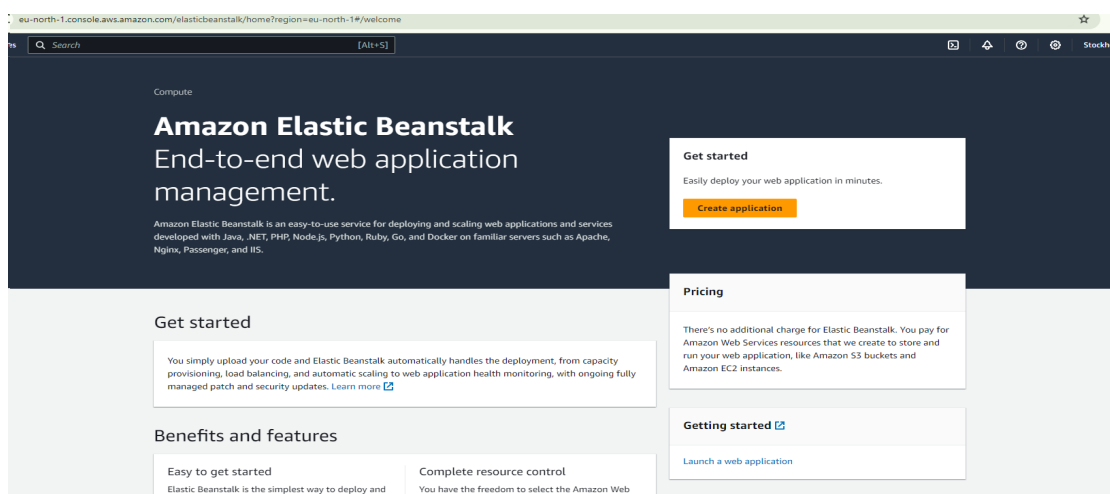
Roll no: A022

Date of submission: 30/1/24

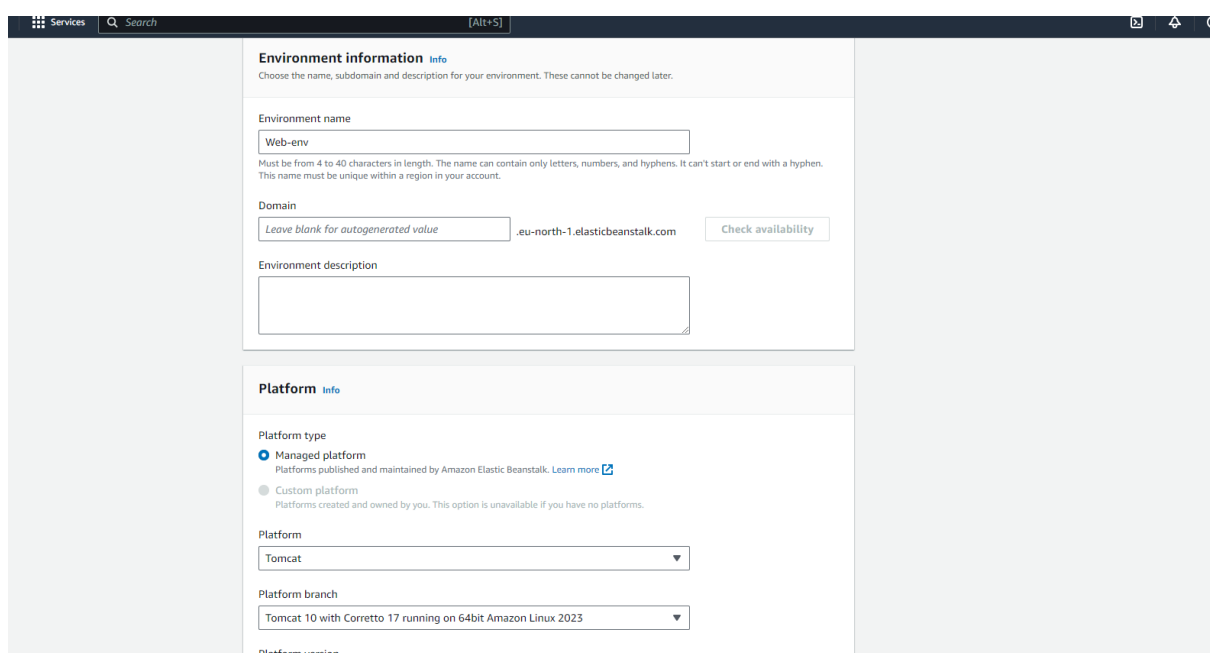
## Practical 2: Implementation of PAAS using AWS

### For tomcat (without code)

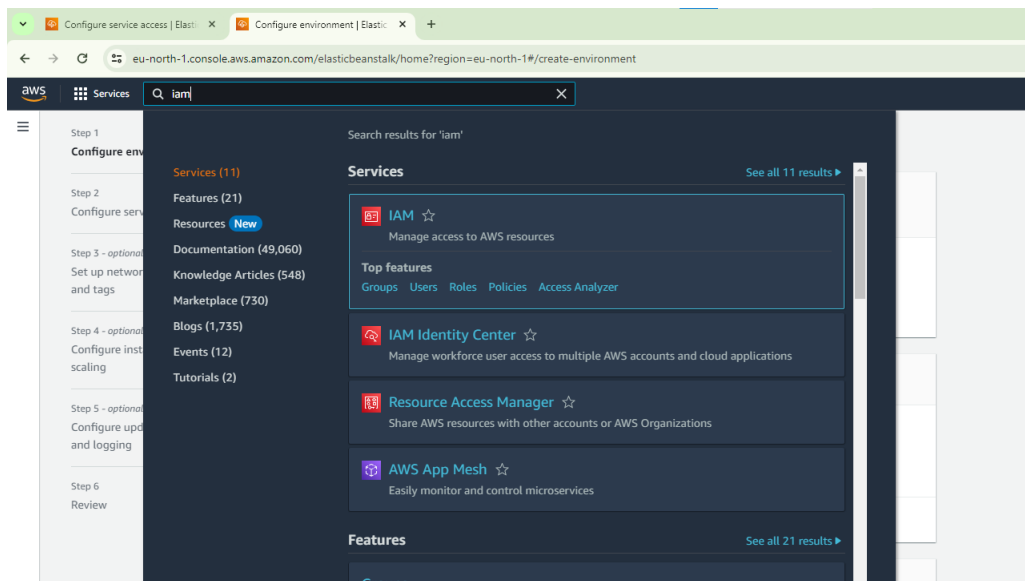
- 1) Login into your aws account
- 2) In services search elastic beanstalk
- 3) Create application



- 4) Create environment
- 5) Enter name
- 6) Select platform -> Tomcat

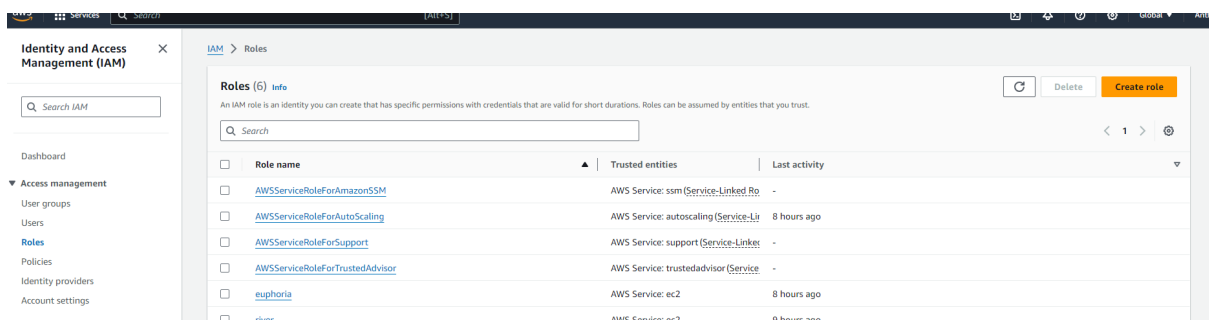


## 7) Duplicate the web page and from services select IAM

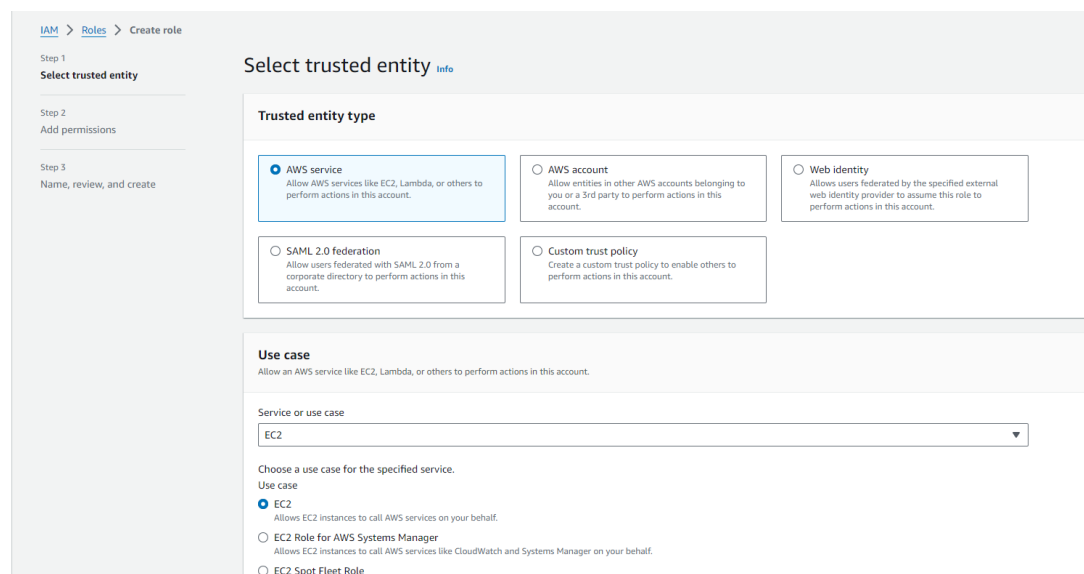


## 8) Click of Roles

## 9) Create Role
















## 10) In the select entrusted entity > use case > select EC2



11) In add permissions search> beanstalk

12) Select the 3 -> docker,webTier,workerTier

<input type="checkbox"/>	 <a href="#">AWSElasticBeanstalkCustomPlatformforEC2Role</a>	AWS managed
<input type="checkbox"/>	 <a href="#">AWSElasticBeanstalkEnhancedHealth</a>	AWS managed
<input type="checkbox"/>	 <a href="#">AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy</a>	AWS managed
<input checked="" type="checkbox"/>	 <a href="#">AWSElasticBeanstalkMulticontainerDocker</a>	AWS managed
<input type="checkbox"/>	 <a href="#">AWSElasticBeanstalkReadOnly</a>	AWS managed
<input type="checkbox"/>	 <a href="#">AWSElasticBeanstalkRoleCore</a>	AWS managed
<input type="checkbox"/>	 <a href="#">AWSElasticBeanstalkRoleCWL</a>	AWS managed
<input type="checkbox"/>	 <a href="#">AWSElasticBeanstalkRoleECS</a>	AWS managed
<input type="checkbox"/>	 <a href="#">AWSElasticBeanstalkRoleRDS</a>	AWS managed
<input type="checkbox"/>	 <a href="#">AWSElasticBeanstalkRoleSNS</a>	AWS managed
<input type="checkbox"/>	 <a href="#">AWSElasticBeanstalkRoleWorkerTier</a>	AWS managed
<input checked="" type="checkbox"/>	 <a href="#">AWSElasticBeanstalkWebTier</a>	AWS managed
<input checked="" type="checkbox"/>	 <a href="#">AWSElasticBeanstalkWorkerTier</a>	AWS managed

13) Enter the dets for Role

## 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 alphanumeric and '+=, @-\_' characters.

### Step 1: Select trusted entities

#### Trust policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": [  
7         "sts:AssumeRole"  
8       ],  
9       "Principal": {  
10        "Service": [  
11          "ec2.amazonaws.com"  
12        ]  
13    }  
14  ]  
15 }
```

14) Role is created

15) Go back to the original web page(not the duplicated ) > refresh and select the role which we created just now

### 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.

app

**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.

app

16) Next

17) Select the default vpc address

**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-097e5a4365f5c8ba5 | (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](#)

18) Select the cidr which is similar to vpc address

Filter instance subnets

	Availability Zone	Subnet	CIDR	Name
<input type="checkbox"/>	eu-north-1b	subnet-02c5b89cd...	172.31.32.0/20	
<input checked="" type="checkbox"/>	eu-north-1c	subnet-0980fd2da...	172.31.0.0/20	
<input type="checkbox"/>	eu-north-1a	subnet-0c6aa5382...	172.31.16.0/20	

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 (3)

Filter database subnets

	Availability Zone	Subnet	CIDR	Name
<input type="checkbox"/>	eu-north-1b	subnet-02c5b89cd...	172.31.32.0/20	
<input checked="" type="checkbox"/>	eu-north-1c	subnet-0980fd2da...	172.31.0.0/20	
<input type="checkbox"/>	eu-north-1a	subnet-0c6aa5382...	172.31.16.0/20	

☐ Enable database

19) Keep the default options for configure

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

Amazon CloudWatch monitoring

The time interval between when metrics are reported from the EC2 instances

Monitoring interval

5 minute

Instance metadata service (IMDS)

20)

## Configure updates, monitoring, and logging - *optional* [Info](#)

### ▼ 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

##### CloudWatch Custom Metrics - Instance

Choose metrics ▼

##### CloudWatch Custom Metrics - Environment

Choose metrics ▼

#### 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 ▼

## 21) Review the dets

## Review [Info](#)

### Step 1: Configure environment [Edit](#)

#### Environment information

Environment tier	Application name
Web server environment	web
Environment name	Application code
Web-env	Sample application
Platform	
arn:aws:elasticbeanstalk:eu-north-1::platform/Tomcat 10 with Corretto 17 running on 64bit Amazon Linux 2023/5.1.3	

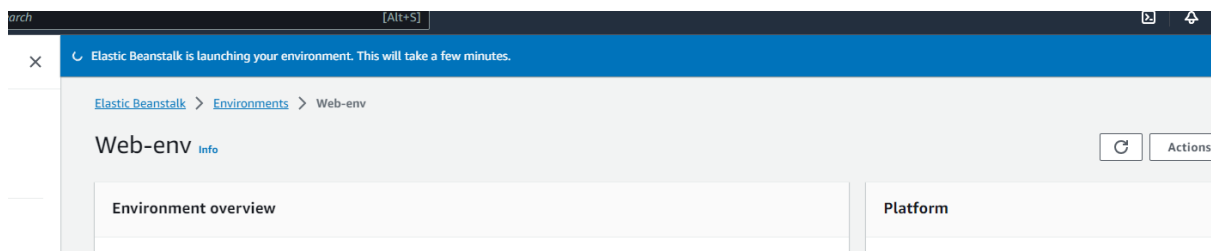
### Step 2: Configure service access [Edit](#)

#### Service access [Info](#)

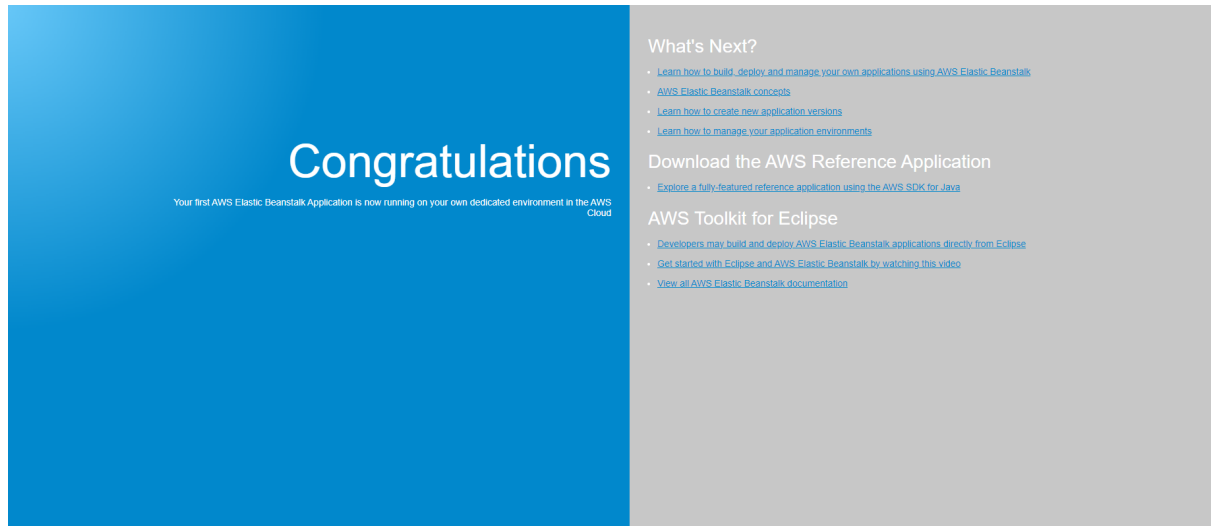
Configure the service role and EC2 instance profile that Elastic Beanstalk uses to manage your environment. Choose an EC2 key pair to securely log in to your EC2 instances.

Service role	EC2 instance profile
arn:aws:iam::339713188308:role/app	app

## 22) Create > elastic beanstalk is launching the environment

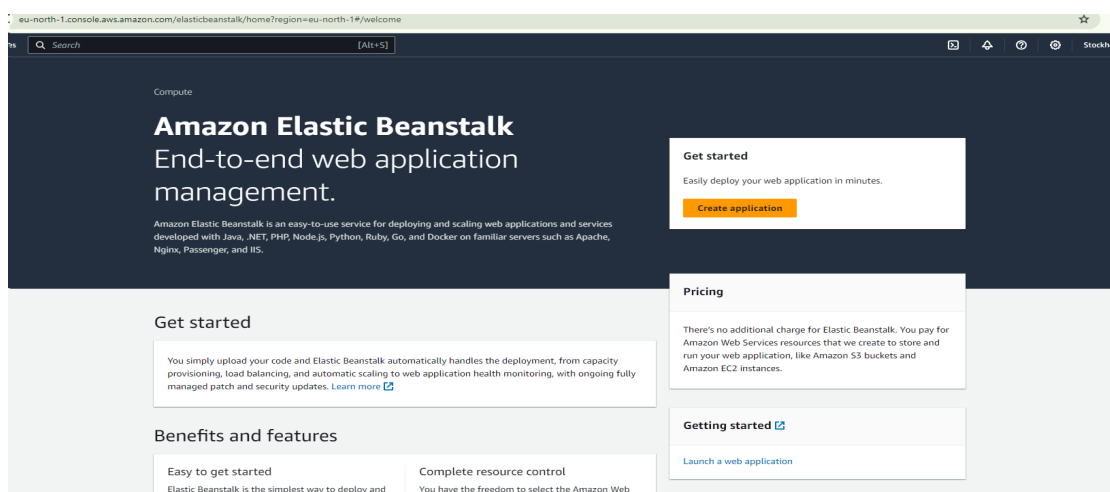


## 23) Tomcat cat application is running



## For tomcat (with code)

- 1) Login into your aws account
- 2) In services search elastic beanstalk
- 3) Create application



- 4) Create environment
- 5) Enter name
- 6) Select platform -> Tomcat

## 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

tomcatcode

Maximum length of 100 characters.

**Application >app code> upload your code >**

**Write a version label -> local file ->choose file (calender.war from github)**

Platform branch

Choose a platform branch

Platform version

Choose a platform version

## 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.

an

Source code origin. Maximum size 500 MB

☒ **Local file**

Upload application

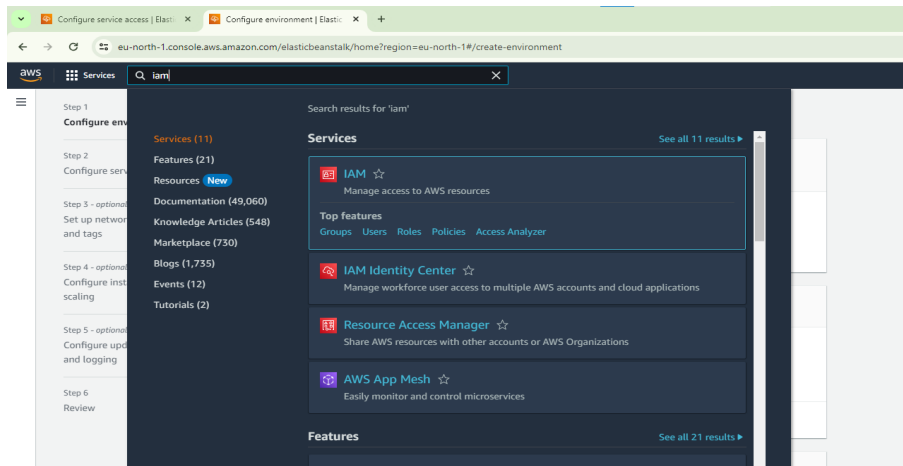
Choose file

☒ File name: **Calendar.war**  
File must be less than 500MB max file size

☐ Public S3 URL



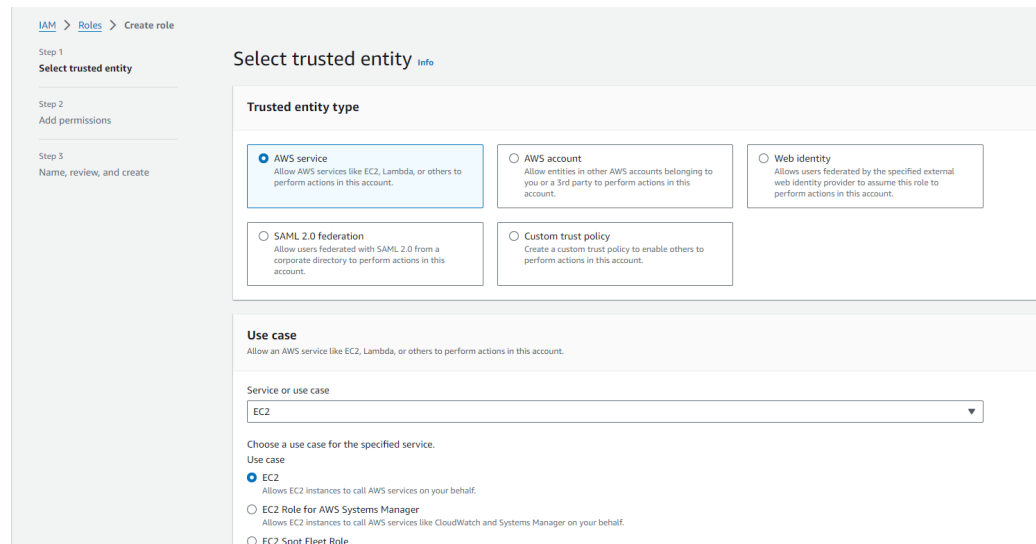
## 7) Duplicate the web page and from services select IAM



## 8) Click of Roles

## 9) Create Role

## 10) In the select entrusted entity > use case > select EC2



## 11) In add permissions search> beanstalk

## 12) Select the 3 -> docker,webTier,workerTier

<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">AWSElasticBeanstalkCustomPlatformforEC2Role</a>	AWS managed
<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">AWSElasticBeanstalkEnhancedHealth</a>	AWS managed
<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy</a>	AWS managed
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">AWSElasticBeanstalkMulticontainerDocker</a>	AWS managed
<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">AWSElasticBeanstalkReadOnly</a>	AWS managed
<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">AWSElasticBeanstalkRoleCore</a>	AWS managed
<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">AWSElasticBeanstalkRoleCWL</a>	AWS managed
<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">AWSElasticBeanstalkRoleECS</a>	AWS managed
<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">AWSElasticBeanstalkRoleRDS</a>	AWS managed
<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">AWSElasticBeanstalkRoleSNS</a>	AWS managed
<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">AWSElasticBeanstalkRoleWorkerTier</a>	AWS managed
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">AWSElasticBeanstalkWebTier</a>	AWS managed
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">AWSElasticBeanstalkWorkerTier</a>	AWS managed

- 13) Enter the details for Role
- 14) Role is created
- 15) Go back to the original web page(not the duplicated ) > refresh and select the role which we created just now
- 16) Select the default vpc address

**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-097e5a4365f5c8ba5 | (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](#)

- 17) Select the cidr which is similar to vpc address

Filter instance subnets

	Availability Zone	Subnet ▲	CIDR	Name
<input type="checkbox"/>	eu-north-1b	subnet-02c5b89cd...	172.31.32.0/20	
<input checked="" type="checkbox"/>	eu-north-1c	subnet-0980fd2da...	172.31.0.0/20	
<input type="checkbox"/>	eu-north-1a	subnet-0c6aa5382...	172.31.16.0/20	

**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 (3)**

Filter database subnets

	Availability Zone	Subnet ▲	CIDR	Name
<input type="checkbox"/>	eu-north-1b	subnet-02c5b89cd...	172.31.32.0/20	
<input checked="" type="checkbox"/>	eu-north-1c	subnet-0980fd2da...	172.31.0.0/20	
<input type="checkbox"/>	eu-north-1a	subnet-0c6aa5382...	172.31.16.0/20	

☒ Enable database

- 18) Keep the default options for configure

## 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

#### Amazon CloudWatch monitoring

The time interval between when metrics are reported from the EC2 instances

Monitoring interval

5 minute ▼

Instance metadata service (IMDS)

19)

## Configure updates, monitoring, and logging - *optional* [Info](#)

### ▼ 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

CloudWatch Custom Metrics - Instance

Choose metrics ▼

CloudWatch Custom Metrics - Environment

Choose metrics ▼

#### 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 ▼

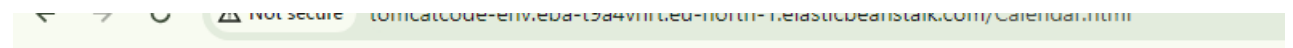
20) Review the details

21) Create > elastic beanstalk is launching the environment

22) Launched

23) Select domain

24) Calendar will be launched



## GWT Calendar

Click on day to get date popup. Example Datepicker. Built with the tomcat war builder.

<http://code.google.com/p/gwt-examples/>

< January >				< 2024 >		
Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			