Build Instructions
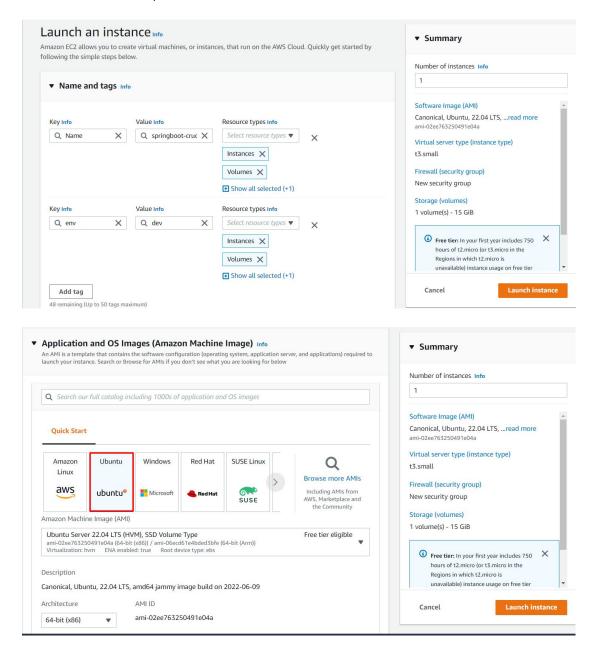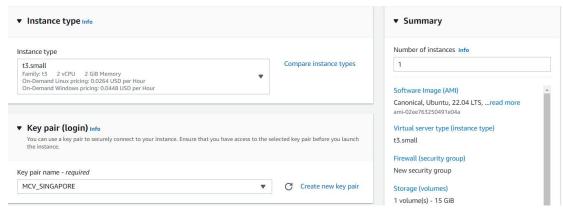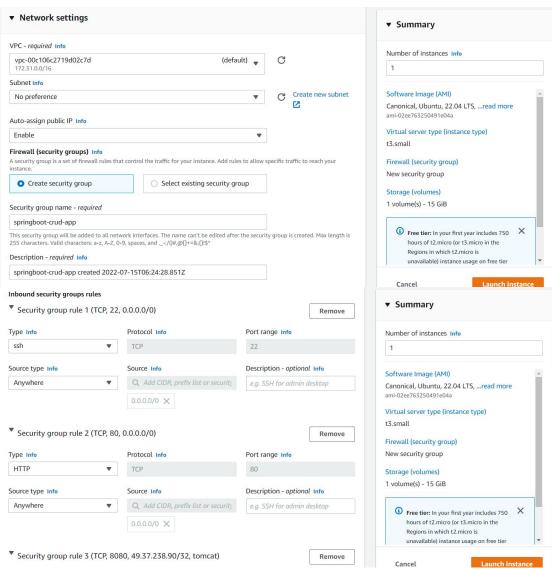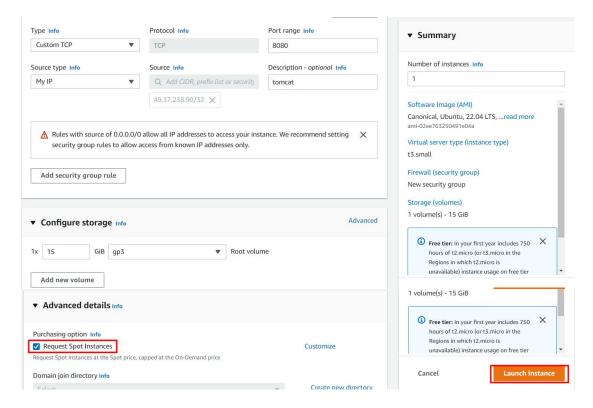
1. Login to AWS Console > EC2
2. Launch a t3.micro Spot instance with an Ubuntu AMI - Ubuntu 22.04 LTS

▼ Instance type Info

Instance type

t3.small
Family: t3   2 vCPU   2 GiB Memory
On-Demand Linux pricing: 0.0264 USD per Hour
On-Demand Windows pricing: 0.0448 USD per Hour

Compare instance types

▼ Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

MCV_SINGAPORE

Create new key pair

▼ Network settings

VPC - required Info

vpc-00c106c2719d02c7d   (default)
172.31.0.0/16

Subnet Info

No preference

Create new subnet

Auto-assign public IP Info

Enable

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

Security group name - required

springboot-crud-app

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - required Info

springboot-crud-app created 2022-07-15T06:24:28.851Z

Inbound security groups rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)   Remove

Type Info

ssh

Protocol Info

TCP

Port range Info

22

Source type Info

Anywhere

Source Info

Add CIDR, prefix list or security

0.0.0.0/0 ✕

Description - optional Info

e.g. SSH for admin desktop

▼ Security group rule 2 (TCP, 80, 0.0.0.0/0)   Remove

Type Info

HTTP

Protocol Info

TCP

Port range Info

80

Source type Info

Anywhere

Source Info

Add CIDR, prefix list or security

0.0.0.0/0 ✕

Description - optional Info

e.g. SSH for admin desktop

▼ Security group rule 3 (TCP, 8080, 49.37.238.90/32, tomcat)   Remove

▼ Summary

Number of instances Info

1

Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-02ee763250491e04a

Virtual server type (instance type)
t3.small

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 15 GiB

▼ Summary

Number of instances Info

1

Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-02ee763250491e04a

Virtual server type (instance type)
t3.small

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 15 GiB

ⓘ **Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier ✕

Cancel   Launch instance

▼ Summary

Number of instances Info

1

Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-02ee763250491e04a

Virtual server type (instance type)
t3.small

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 15 GiB

ⓘ **Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier ✕

Cancel   Launch instance

Type **Info**
Custom TCP ▼

Protocol **Info**
TCP

Port range **Info**
8080

Source type **Info**
My IP ▼

Source **Info**
🔍 Add CIDR, prefix list or security
49.37.238.90/32 ✕

Description - *optional* **Info**
tomcat

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. ✕

Add security group rule

▼ **Configure storage** Info   Advanced

1x 15 GiB gp3 ▼   Root volume

Add new volume

▼ **Advanced details** Info

Purchasing option **Info**
☑ Request Spot Instances   Customize
Request Spot Instances at the Spot price, capped at the On-Demand price

Domain join directory **Info**
Select   Create new directory

▼ Summary

Number of instances **Info**
1

Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-02ee763250491e04a

Virtual server type (instance type)
t3.small

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 15 GiB

ⓘ **Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier ✕

1 volume(s) - 15 GiB

ⓘ **Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier ✕

Cancel   Launch instance

3. Add an entry to the ssh client config file so that it is easy to connect

nano ~/.ssh/config

Host springbootapp-aws
    HostName 18.136.119.50
    User ubuntu
    Port 22
    IdentityFile "G:\My Drive\vault\aws\MCV_SINGAPORE.pem"
    ServerAliveInterval 240

4. Connect to the instance

ssh springbootapp-aws

sudo apt update
sudo apt upgrade -y

sudo reboot
sudo apt install mysql-server -y

Root Password: KcFmlj32nxiE7gAnQYxS
DB Name: employee_db
DB User: springcrudapp
DB Pass: 9EN6derDK5SCWDF
---

sudo mysql
---

mysql> ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password by 'KcFmlj32nxiE7gAnQYxS';
Query OK, 0 rows affected (0.01 sec)

mysql> create database employee_db;
Query OK, 1 row affected (0.01 sec)

mysql> create user 'springcrudapp'@'localhost' identified by '9EN6derDK5SCWDF';
Query OK, 0 rows affected (0.04 sec)

mysql> grant all on employee_db.* to 'springcrudapp'@'localhost';
Query OK, 0 rows affected (0.01 sec)

mysql> \q
Bye

sudo mysql_secure_installation

```
ubuntu@ip-172-31-18-131:~$ sudo mysql_secure_installation

Securing the MySQL server deployment.

Enter password for user root:
The 'validate_password' component is installed on the server.
The subsequent steps will run with the existing configuration
of the component.
Using existing password for root.

Estimated strength of the password: 50
Change the password for root ? ((Press y|Y for Yes, any other key for No) : n

 ... skipping.
By default, a MySQL installation has an anonymous user,
allowing anyone to log into MySQL without having to have
a user account created for them. This is intended only for
testing, and to make the installation go a bit smoother.
You should remove them before moving into a production
environment.

Remove anonymous users? (Press y|Y for Yes, any other key for No) : y
Success.


Normally, root should only be allowed to connect from
'localhost'. This ensures that someone cannot guess at
the root password from the network.

Disallow root login remotely? (Press y|Y for Yes, any other key for No) : y
Success.

By default, MySQL comes with a database named 'test' that
anyone can access. This is also intended only for testing,
and should be removed before moving into a production
environment.

Remove test database and access to it? (Press y|Y for Yes, any other key for No) : y
 - Dropping test database...
Success.

 - Removing privileges on test database...
Success.

Reloading the privilege tables will ensure that all changes
made so far will take effect immediately.

Reload privilege tables now? (Press y|Y for Yes, any other key for No) : y
Success.

All done!
ubuntu@ip-172-31-18-131:~$
```

git clone https://github.com/melvincv/springboot-crud-webapp.git
cd springboot-crud-webapp

sudo apt install openjdk-11-jdk maven -y

Check status of Mysql, java and maven

sudo systemctl status mysql.service
● mysql.service - MySQL Community Server
   Loaded: loaded (/lib/systemd/system/mysql.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2022-07-15 06:45:44 UTC; 8min ago

sudo systemctl is-enabled mysql.service
enabled

java -version

mvn --version

mvn spring-boot:run

http://18.136.119.50:8080/

mvn clean package

cd target/
java -jar springboot-thymeleaf-crud-web-app-0.0.1-SNAPSHOT.jar

http://18.136.119.50:8080/