

# SBA9

## SPRINGBOOT APPLICATION IN AWS

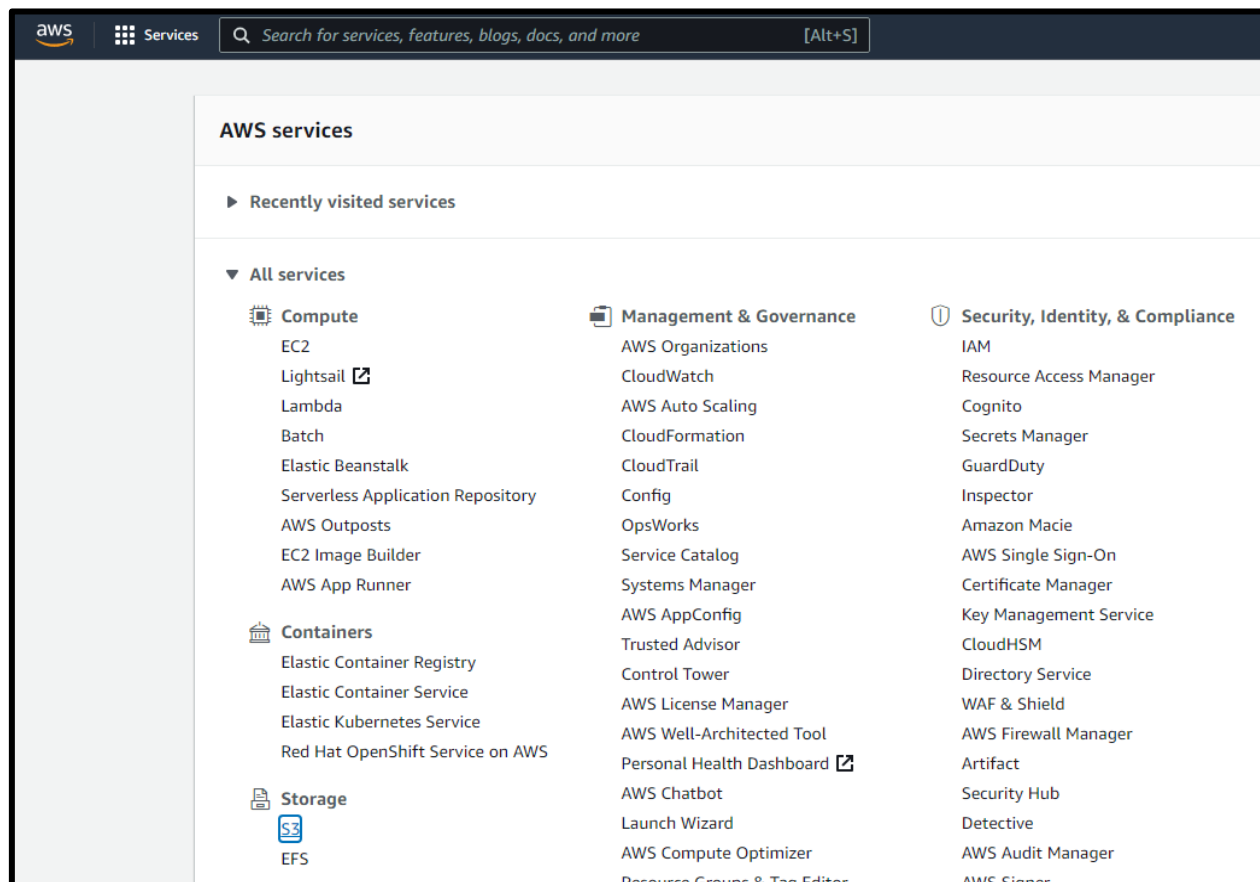
### 1. CREATE AWS ACCOUNT

#### 1.1 GO TO THE AWS WEB PAGE (I.E.: <https://aws.amazon.com/premiumsupport/knowledge-center/create-and-activate-aws-account/>) AND

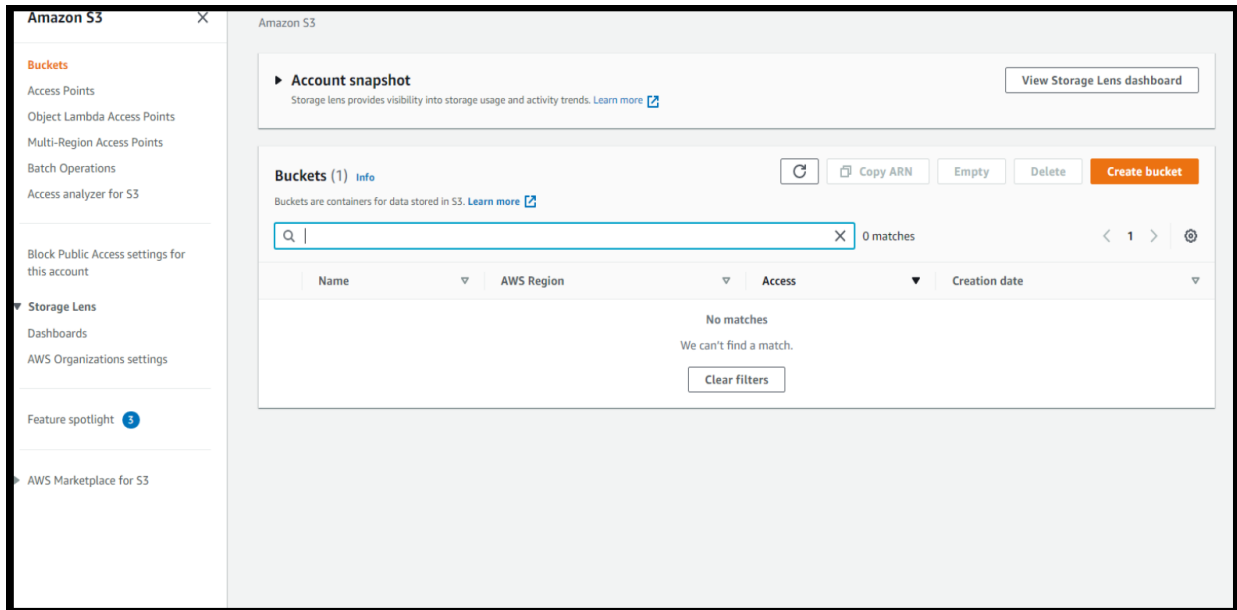
- ADD BASIC DETAILS AND
- ADD CARD INFO
- PAY THE FEE FOR THE ACC.
- AFTER ACC. CREATION GO TO THE HOME PAGE OF AWS

### 2. CREATE A STORAGE SPACE

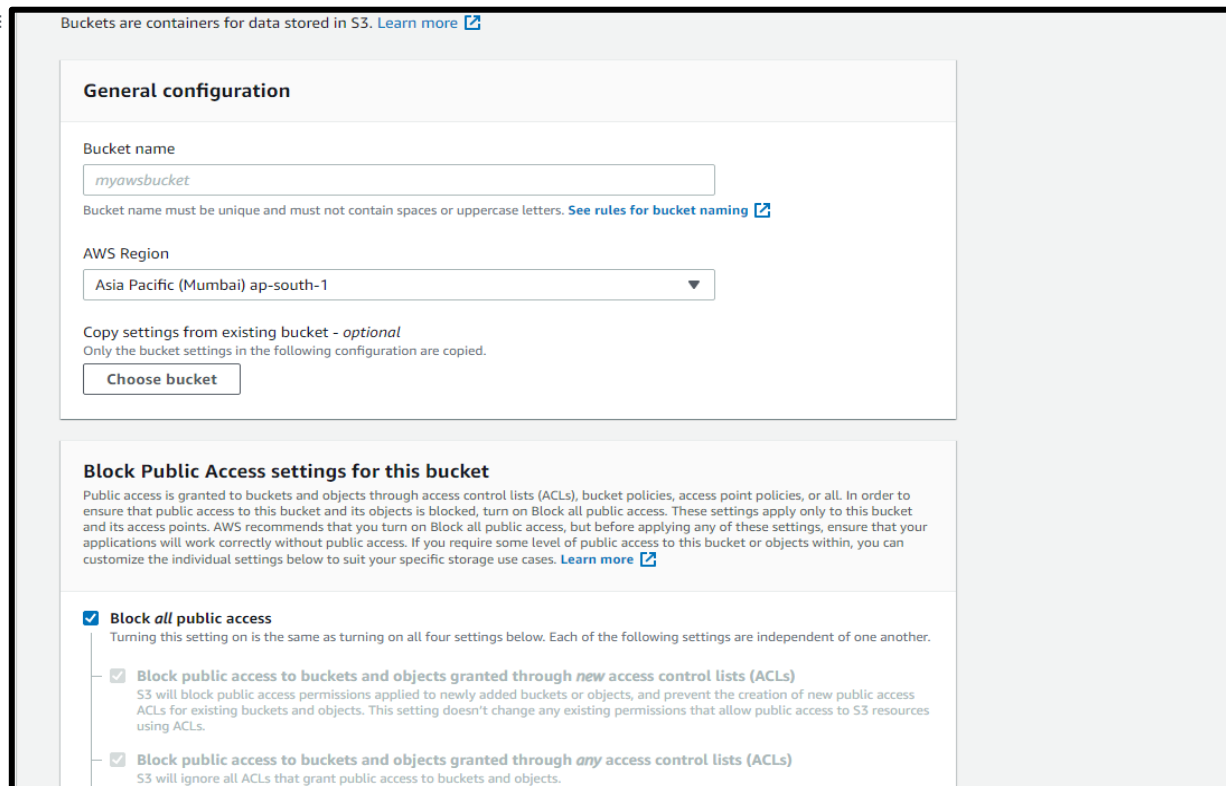
#### 2.1 SELECT S3 (ALL SERVICES -> STORAGE -> S3)



## 2.2 CREATE A BUCKET




## 2.3. ADD GENERAL INFO THEN UNTICK TICK THE BLOCK ALL PUBLIC ACCESS (☒ → ☐)



## 2.4. THEN TICK ☒ “TURNING OFF BLOCK ALL PUBLIC ACCESS .....”.

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.

**Turning off block all public access might result in this bucket and the objects within becoming public**  
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☒ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

## 2.5. FINALLY CLICK CREATE BUCKET BUTTON

Amazon S3

► **Account snapshot** View Storage Lens dashboard  
Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

**Buckets (2)** [Info](#) Refresh Copy ARN Empty Delete Create bucket

Buckets are containers for data stored in S3. [Learn more](#)

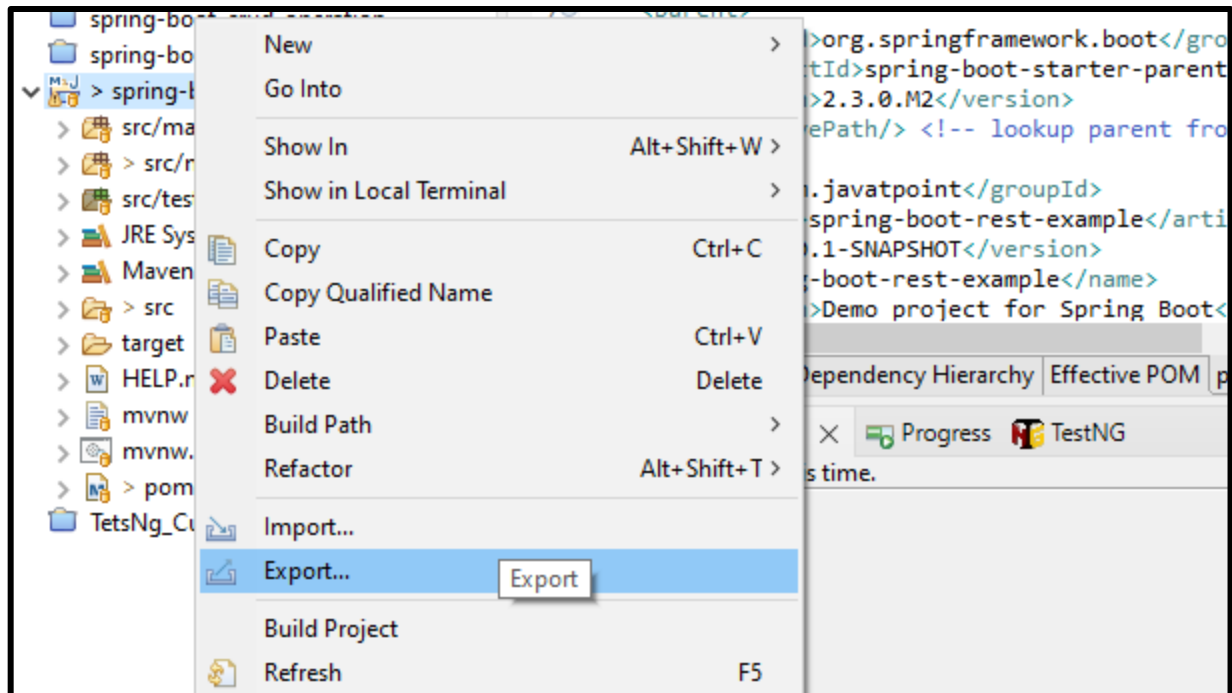
Find buckets by name

	Name ▼	AWS Region ▼	Access ▼	Creation date ▼
<input type="radio"/>	t4est1222	Asia Pacific (Mumbai) ap-south-1	Objects can be public	November 26, 2021, 10:53:33 (UTC+05:30)

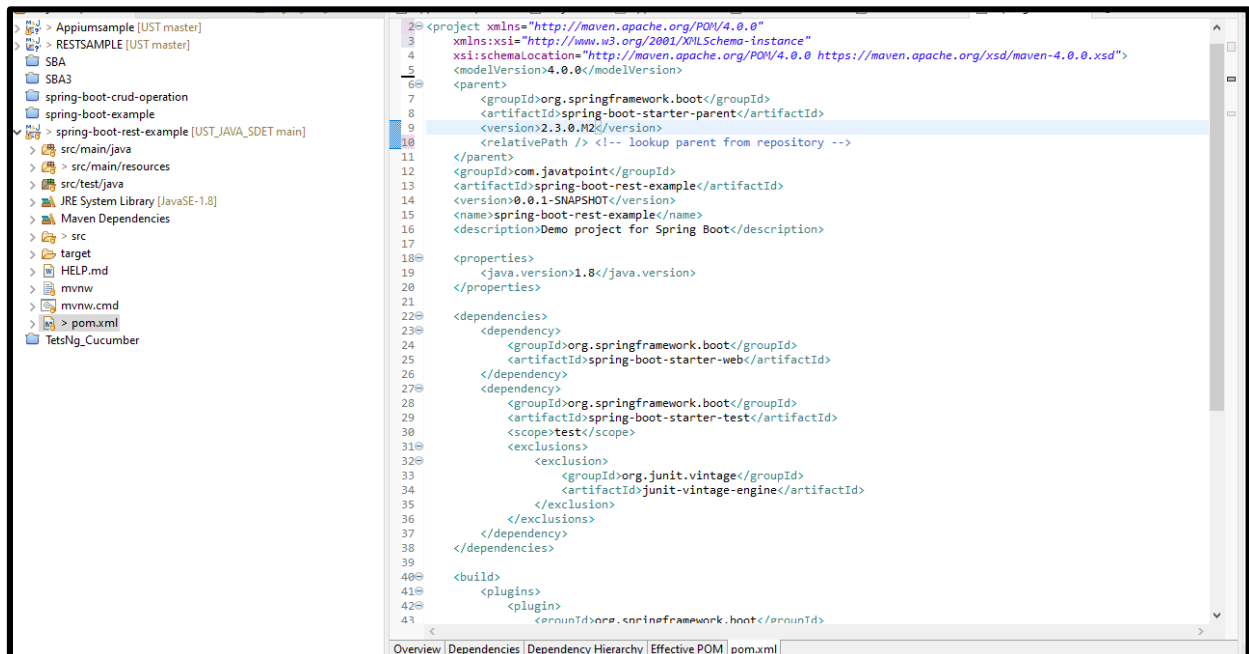
## 3. WE NEED TO CREATE WAR OR JAR FILE FOR OUR JAVA SPRINTBOOT PROJECT

### 3.1 GO TO YOUR JAVA PROJECT IN ECLIPSE THEN

- ONE WAY TO MAKE JAR OR WAR FILE
  - RIGHT CLICK ON THE PROJECT U WILL SEE AN EXPORT OPTION



- CLICK ON THE EXPORT IT WILL SHOW MANY TYPES OF FILE FORMAT IF YOU WANT TO EXPORT THE FILE IN JAR FORMAT CHOOSE JAVA → JAR OTHERWISE, CHOOSE WAR IN WEB → WAR.
- ANOTHER WAY TO MAKE JAR OR WAR IS THAT IN YOUR PROJECT THERE IS A POM FILE, OPEN IT IN ECLIPSE.



- IN HERE

- ADD A TAG I.E, <PACKAGING>
- INSIDE THIS TAG ADD WHICH TYPE OF FILE FORMAT WE WANT, PUT IT THERE.
- I.E, IF WE WANTED A WAR FILE THEN  

```
<packaging>war</packaging>
```

 OR NEED A JAR THEN  

```
<packaging>jar</packaging>
```

 LIKE THIS,

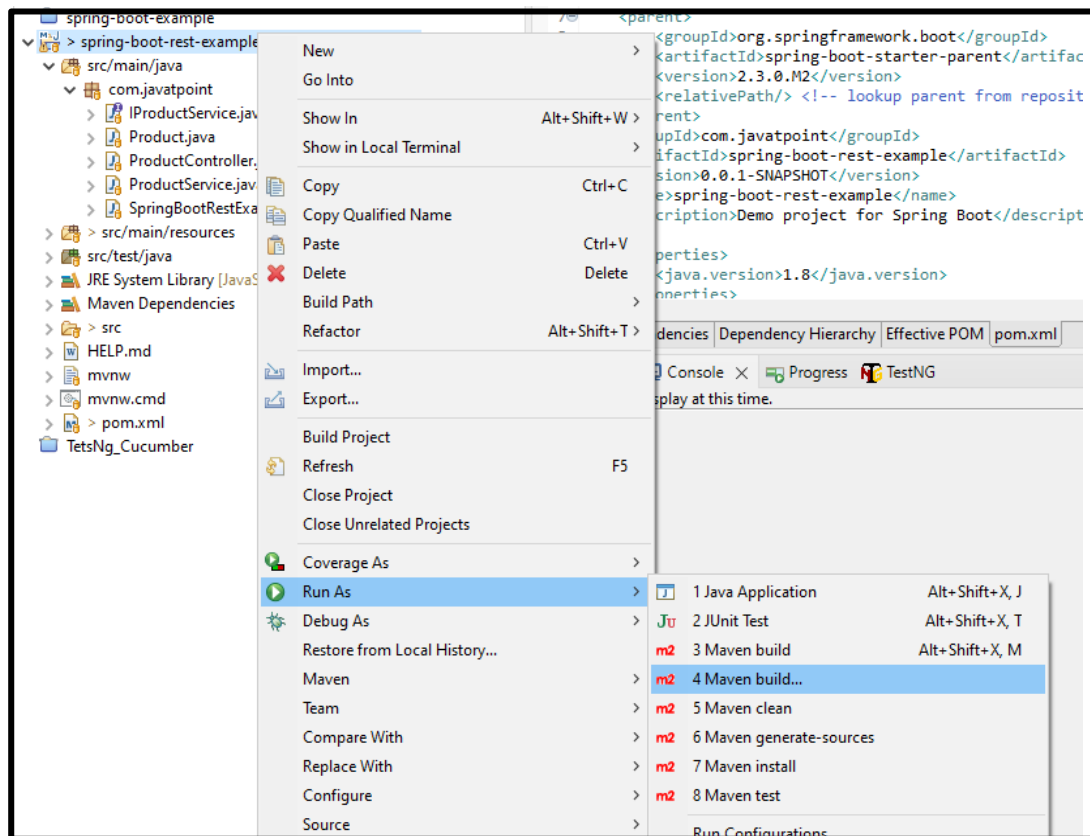
```

1 <?xml version="1.0" encoding="UTF-8"?>
2 <project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
3   xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 https://maven.apache.org/xsd/maven-4.0.0.xsd">
4   <modelVersion>4.0.0</modelVersion>
5   <packaging>jar</packaging>
6
7   <parent>
8     <groupId>org.springframework.boot</groupId>
9     <artifactId>spring-boot-starter-parent</artifactId>
10    <version>2.3.0.M2</version>

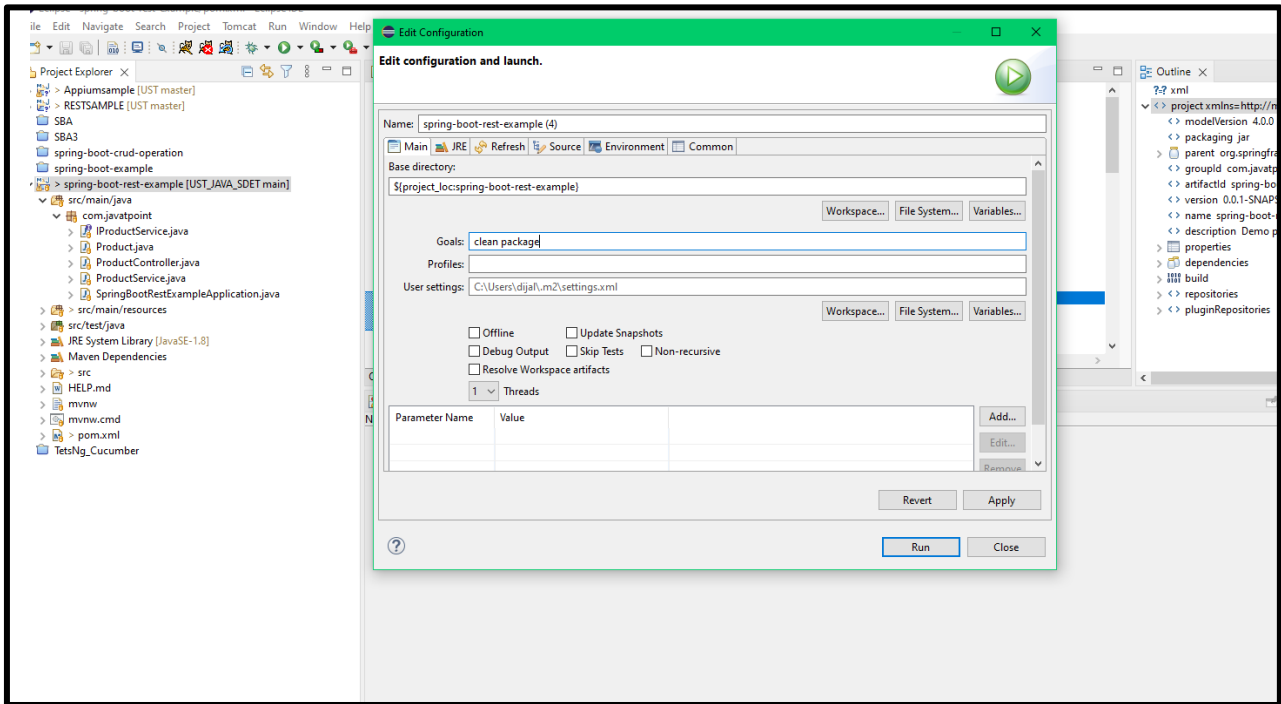
```

- AFTER THAT RIGHT CLICK ON THIS SPRINGBOOT PRJCT.

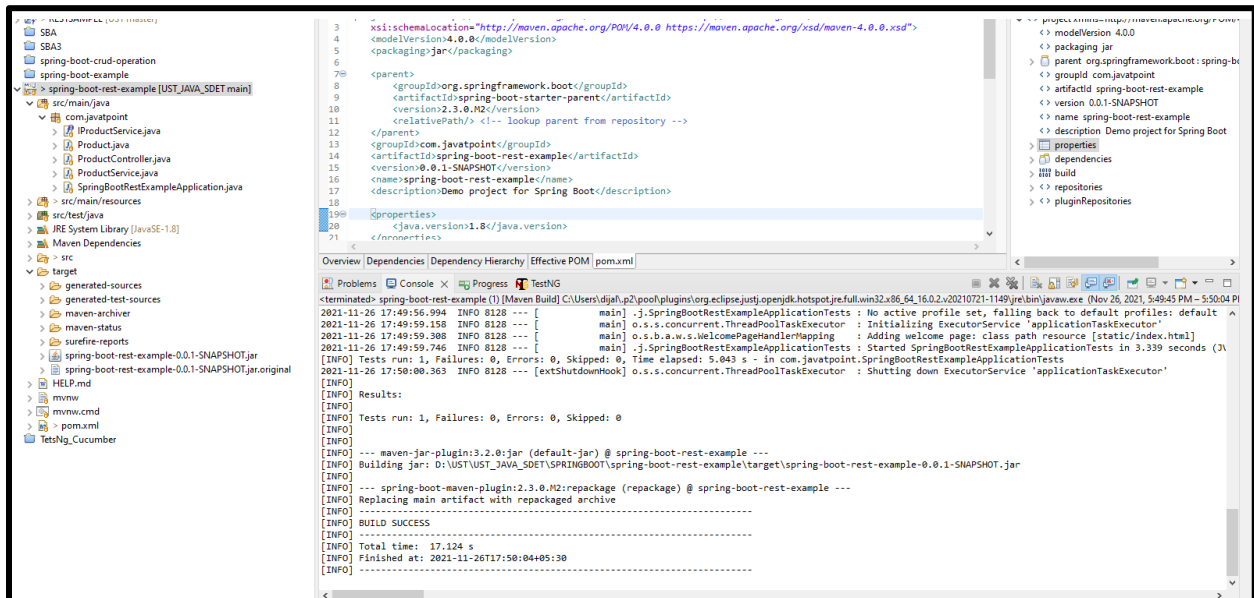
- RUN AS → MAVEN BUILD



- AFTER THAT, INSIDE IN THE CONFIGURATION SET GOAL AS →
- CLEAN PACKAGE



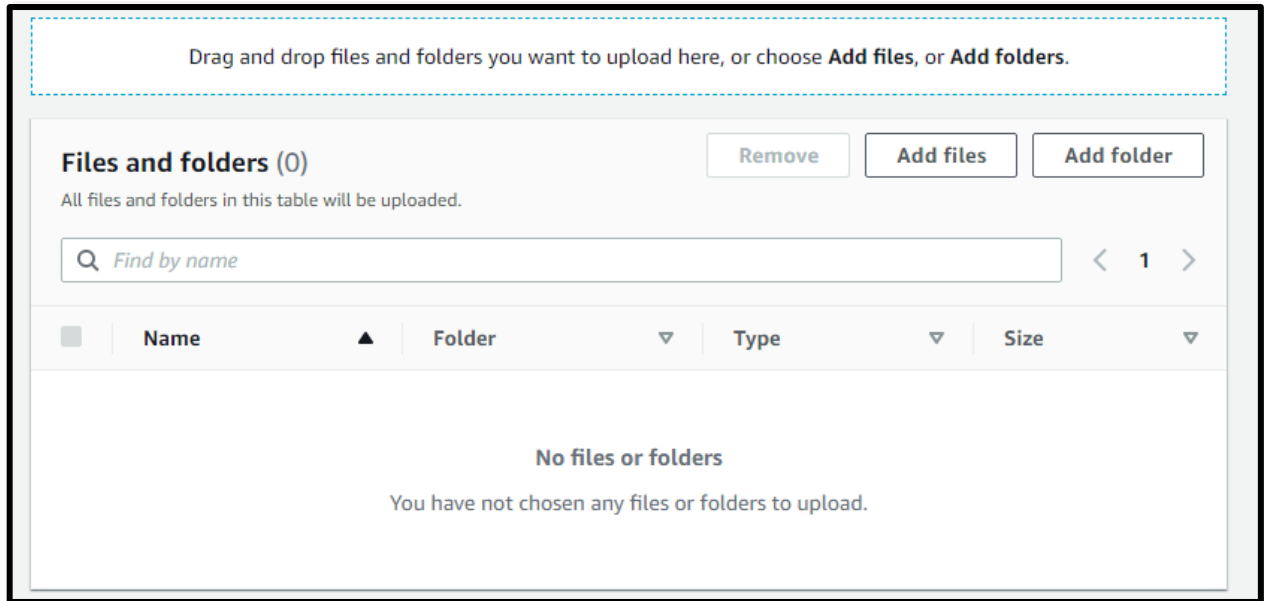
- RUN IT, AFTER IT BUILD SUCCESFULL, THEN REFRESH THE PROJECT AND U WILL SEE A FOLDER IN THE PROJECT TARGET.



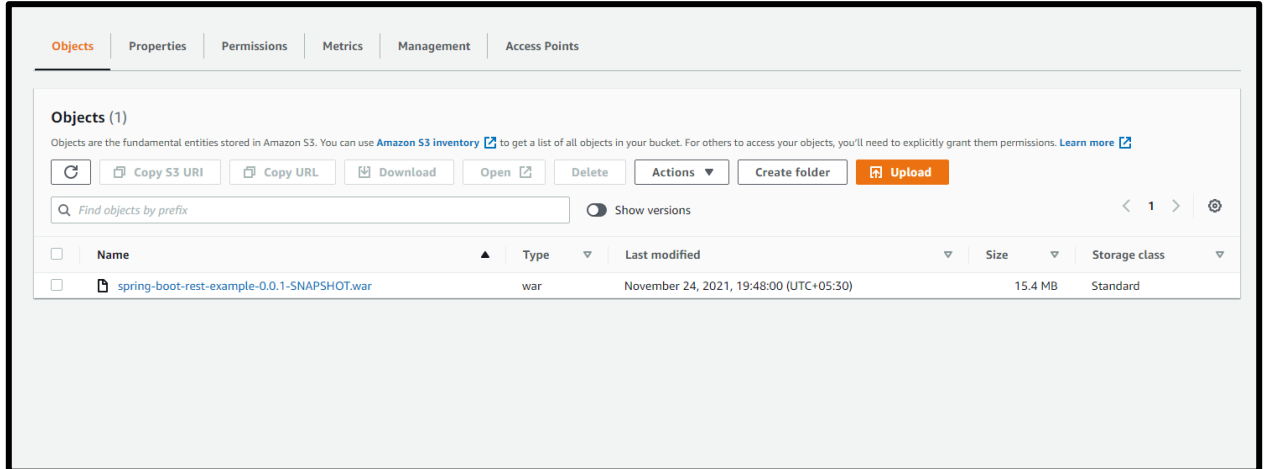
- INSIDE THIS TARGET FOLDER U WILL SEE A JAR FILE.

4. NEXT STEP GO TO THE AWS → S3 → OPEN THE BUCKET THAT U CREATED.

4.1 IN THAT BUCKET U WILL SEE UPLOAD FILES BUTTON.



4.2 CLICK ON THAT UPLOAD FILES AND CHOOSE THE FILE (JAR OR WAR) FROM THAT SPRINGBOOT PROJECT LOCATION AFTER THAT UPLOAD IT.



5. CREATE A EC2 INSTANCE

5.1 GOTO HOME PAGE OF AWS OR CLICK ON THE SERVICES.

5.2 CLICK ON THE COMPUTE → EC2

5.3 CLICK LAUNCH INSTANCE SELECT A MACHINE (IN HERE I SELECT "Ubuntu Server 20.0.4 ")

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### Step 1: Choose an Amazon Machine Image (AMI)

[Launch a database using RDS](#) [Cancel and Exit](#)

**Red Hat Enterprise Linux 8 (HVM), SSD Volume Type** - ami-06a0b4e3b7eb7a300 (64-bit x86) / ami-0cbe04a3ce796c98e (64-bit Arm)

Red Hat Enterprise Linux version 8 (HVM), EBS General Purpose (SSD) Volume Type

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Free tier eligible

**Select**

☒ 64-bit (x86)  
☐ 64-bit (Arm)

**SUSE Linux Enterprise Server 15 SP2 (HVM), SSD Volume Type** - ami-0b3ac3edf2397475 (64-bit x86) / ami-0ab71076ab9b53b0d (64-bit Arm)

SUSE Linux Enterprise Server 15 Service Pack 2 (HVM), EBS General Purpose (SSD) Volume Type. Amazon EC2 AMI Tools preinstalled; Apache 2.2, MySQL 5.5, PHP 5.3, and Ruby 1.8.7 available.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Free tier eligible

**Select**

☒ 64-bit (x86)  
☐ 64-bit (Arm)

**Ubuntu Server 20.04 LTS (HVM), SSD Volume Type** - ami-0567e0d2b4b2169ae (64-bit x86) / ami-08198662331cf1a51 (64-bit Arm)

Ubuntu Server 20.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Free tier eligible

**Select**

☒ 64-bit (x86)  
☐ 64-bit (Arm)

**Microsoft Windows Server 2019 Base** - ami-02d47a75baf6e320

Microsoft Windows 2019 Datacenter edition, [English]

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Free tier eligible

**Select**

64-bit (x86)

**Microsoft Windows Server 2019 Base with Containers** - ami-0b91d3e2e1746c4c7

Microsoft Windows 2019 Datacenter edition with Containers, [English]

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Free tier eligible

**Select**

64-bit (x86)

## 5.4 SELECT FREE TIER TYPE AND GOTO NEXT.

### Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: **All instance families** **Current generation** [Show/Hide Columns](#)

Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, ~, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input type="checkbox"/>	t2	t2.2xlarge	8	32	EBS only	-	Moderate	Yes

## 5.5 GOTO 6TH STEP AND CHANGE THE TYPE OF PROTOCOL AND SOURCE LIKE THAT IN THE BELOW IMAGE.THEN GOTO THE 7TH STEP CLICK ON LAUNCH.

### Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group  
☐ Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range	Source	Description
All traffic	All	0 - 65535	Anywhere 0.0.0.0, ::0	e.g. SSH for Admin Desktop

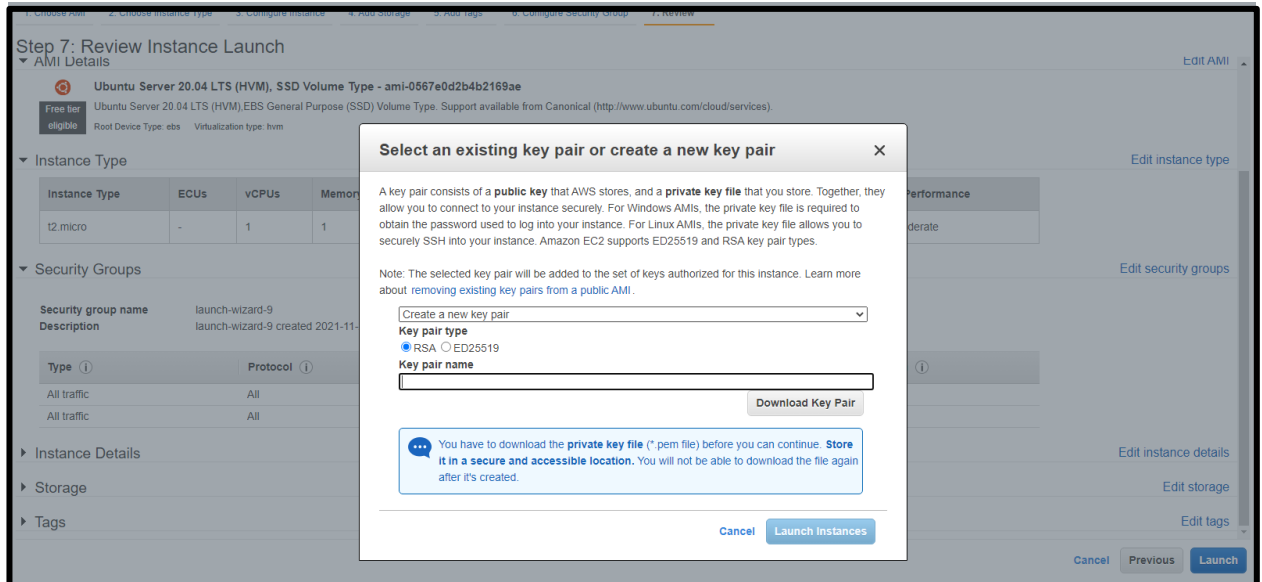
[Add Rule](#)

**Warning**

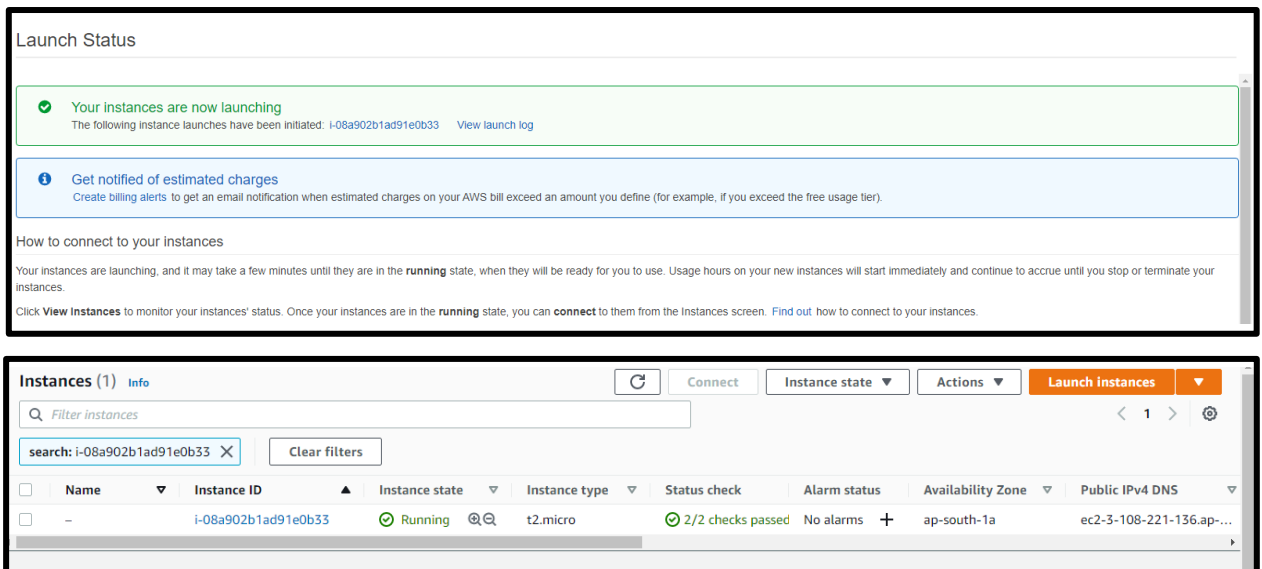
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.



**5.6 AFTER LAUNCH IT WILL SHOW A WINDOW FOR SELECT SECURITY KEY-PAIR, IF YOU DON'T HAVE IT CLICK ON THE DROP DOWN AND SELECT CREATE A NEW KEY-PAIR.THEN SAVE IT INTO YOUR DESIRED LOCATION.AND CLICK ON LAUNCH INSTANCE.**



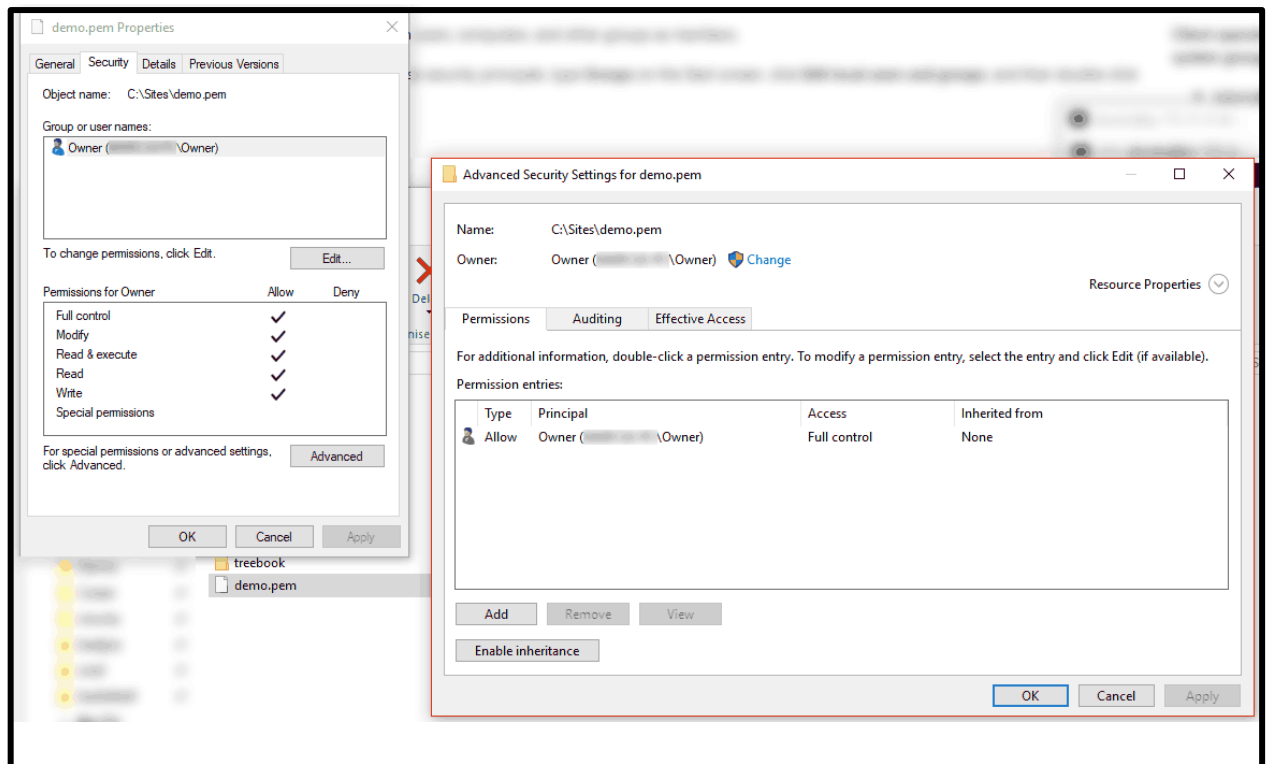
**5.7 CLICK ON THE INSTANCE (AS YOU CAN SEE THE STATUS OF YOUR INSTANCE IS NOW RUNNING)**



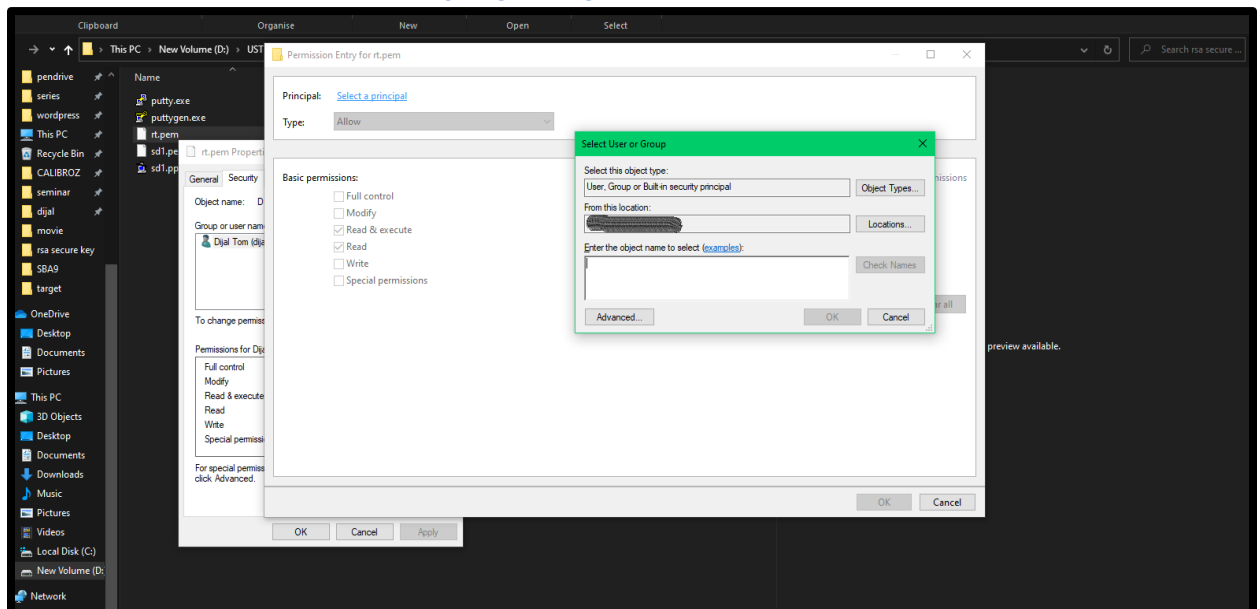
**5.8 DOWNLOAD PuTTY FOR CONNECTING TO THE SERVER OR USE YOUR OWN CMD FOR CONNECTING THE SEREVR.**

- IF YOU USE PUTTY THEN →DOWNLOAD IT FROM THIS LINK AND CHECK HOW TO USE IT.(<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>)
- IF YOU USE CMD

- GOTO THE SECURITY FILE LOCATION THAT YOU DOWNLOADED FROM THE AWS.
- RIGHT CLICK ON THE (. PEM) FILE AND GOTO THE PROPERTIES AND SELECT ADVANCED.



- THEN DISABLE INHERITANCE > 'CONVERT INHERITED PERMISSIONS INTO EXPLICIT PERMISSION ON THIS OBJECT' > REMOVE ALL USERS AND CLICK ON THE ADD > SELECT PRINCIPAL

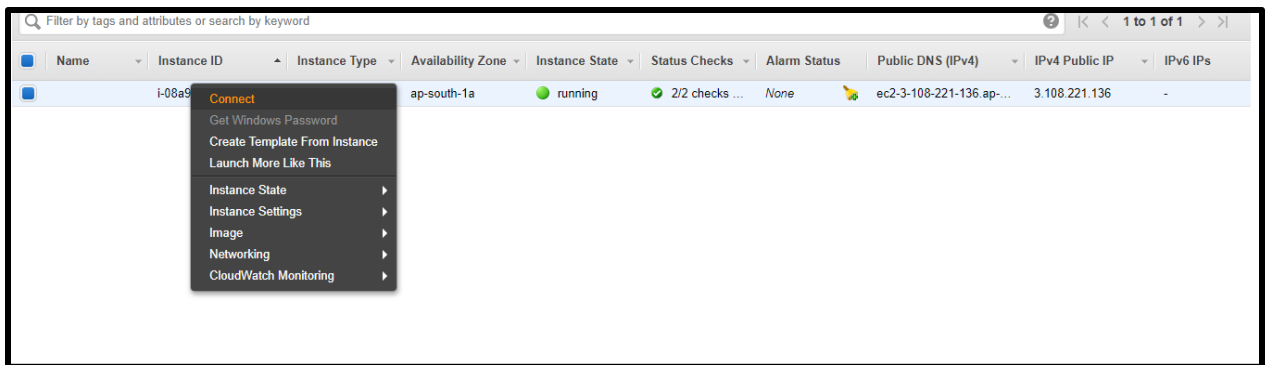


- ENTER THE CURRENT USERNAME AND > CHECK NAMES > OK>  
CLICK ON "ALLOW | EVERYONE | FULL CONTROL" >OK > OK > OK (OK UNTIL ALL WINDOWS ARE CLOSED).

## 6. CONNECTING TO THE SERVER

### 6.1 COPY THE SSH COMMAND FROM

- #### 6.1.1 GOTO THE CURRENT EC2 INSTANCE THAT YOU CREATED AND RIGHT CLICK ON THE INSTANCE→ SELECT CONNECT



- #### 6.1.2 THEN COPY THE SSH COMMAND

Eg:

```
ssh -i "rt.pem" ubuntu@ec2-3-108-221-136.ap-south-1.compute.amazonaws.com
```

- ### 6.2 THEN GOTO YOUR KEY FILE (.PEM) SAVED LOCATION AND OPEN THE CMD IN THERE.

- #### 6.2.1 PASTE THE SSH COMMAND THERE AND IT WILL POP UP A MESSAGE AND TYPE YES THEN IT WILL LOOK LIKE IN THE BELOW IMAGE.

```
ubuntu@ip-172-31-32-87: ~
Microsoft Windows [Version 10.0.19043.1348]
(c) Microsoft Corporation. All rights reserved.

D:\UST\rsa secure key>ssh -i "rt.pem" ubuntu@ec2-3-108-221-136.ap-south-1.compute.amazonaws.com
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.11.0-1020-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Fri Nov 26 13:53:54 UTC 2021

System load:  0.0          Processes:    98
Usage of /:   17.9% of 7.69GB   Users logged in:  0
Memory usage: 20%          IPv4 address for eth0: 172.31.32.87
Swap usage:   0%

1 update can be applied immediately.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Fri Nov 26 13:17:18 2021 from 103.199.144.97
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-32-87:~$
```

## 7. TYPE THE FOLLOWING COMMAND

7.1.1 `sudo apt update`

7.1.2 `sudo apt-get install default-jre -y`

## 7.2 CHECK THE JAVA VERSION

7.2.1 `java -version`

```
done.
ubuntu@ip-172-31-32-87:~$ java -version
openjdk version "11.0.11" 2021-04-20
OpenJDK Runtime Environment (build 11.0.11+9-Ubuntu-0ubuntu2.20.04)
OpenJDK 64-Bit Server VM (build 11.0.11+9-Ubuntu-0ubuntu2.20.04, mixed mode, sharing)
ubuntu@ip-172-31-32-87:~$
```

## 7.3 COPY THE OBJECT URL FROM S3

7.3.1 OPEN YOUR AWS → GOTO YOUR BUCKET → AND CLICK ON THAT BUCKET → CLICK ON THAT (WAR OR JAR) FILE → COPY THE OBJECT URL

EG: <https://yourbucketname.s3.ap-south-1.amazonaws.com/spring-boot.war>

7.3.2 GOTO THAT CMD AFTER THE JAVA VERSION COMMAND TYPE

- `wget https://yourbucketname.s3.ap-south-1.amazonaws.com/spring-boot.war`
- `ls`

7.3.3 COPY THE FILE NAME FROM THE CMD THEN TYPE

- `java -jar filename`

## 7.4 AFTER IT WILL START THE SPRING-BOOT APPLICATION

7.4.1 THEN GOTO AWS AND GOTO THE CURRENT EC2 INSTANCE THAT YOU CREATED AND RIGHT CLICK ON THE INSTANCE → SELECT CONNECT → COPY THE PUBLIC DNS

## 8. OPEN ANY WEB-BROWSER

SUCH AS, (CHROME, EDGE....ETC)

9. PASTE THE URL AND ADD THE PORT NUMBER (THAT U GAVE IN SPRING-BOOT APPLICATION) IN THE URL

EG.

