

## **Scenario :-**

- Application Running on Physical/Virtual Machines
- Work load in your Datacentre.

## **Problem:-**

- Complex Management
- Scale up & scale down
- Cost
- Manual Process
- Time Consuming

## **Solution:-**

- **Cloud Setup –**

Pay-As-You-go, IAAS, Flexibility, Ease of Infra Management

- **AWS Service:-**

EC2 Instances

ELB

Autoscaling

S3

Route 53

- **Objective:-**

Flexible Infra

No Upfront Cost

Modernize Effectively

IAAC

# **Architecture of AWS Setup for Web Application:-**

EC2 Instances, ELB, Autoscaling, EFS/S3 for shared storage, IAM Role

**Users -> ELB -> Autoscaling Group -> Route 53**

Flow of Execution:-

1. Login to AWS Account
2. Create Key Pair
3. Create Security Groups
4. Launch Instances with user data (Bash Scripts)
5. Update IP to name mapping in route 53
6. Build Application from source code
7. Upload to S3 bucket
8. Download Artifact to Tomcat Ec2 instance
9. Setup ELB with HTTPS[Cert from Amazon Certificate Manager]
10. Build Autoscaling Group for Tomcat Instances.

## **Prerequisite to start the project:-**

Install Chocolatey in your local machine with powershell

<https://chocolatey.org/install#individual>

AWS Account

## 1. Login to AWS Account:-

- North Virginia Region

## 2. Create Key Pair:-

Goto Key pair > click create key pair >

Name : vprofile-key

Key format : .pem

Click Create key Pair.

### Key pair

A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.

Name

vprofile-key

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type [Info](#)

☒ RSA

☐ ED25519

Private key file format

☒ .pem

For use with OpenSSH

☐ .ppk

For use with PuTTY

Tags - *optional*

No tags associated with the resource.

Add new tag

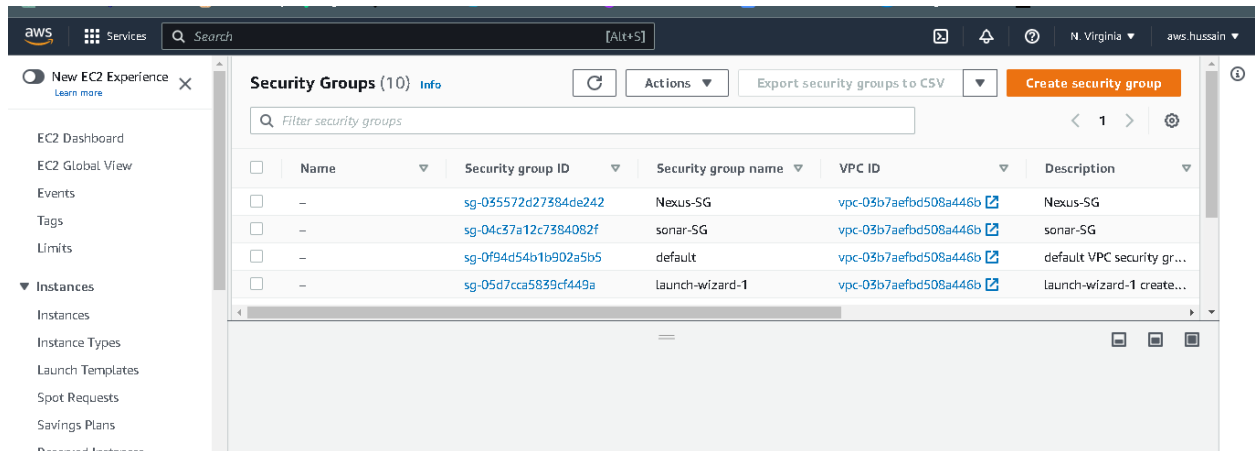
You can add up to 50 more tags.

Cancel

Create key pair

### 3. Create Security Groups:-

Go to Security group > create security group for ELB >



Click Create Security Group >

Name : vprofile-ELB-SG

EC2 > Security Groups > Create security group

## Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

**Basic details**

Security group name [Info](#)

Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)

Allow the Security group rules as follows:-

HTTP : 80 : Anywhere Ipv4

Custom TCp : 80 : anywhere Ipv6

HTTPS : 443 : Anywhere Ipv4

HTTPS : 443 : Anywhere Ipv6

Ssh : 80 : Anywhere from ipv4

**Inbound rules** [Info](#)

Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>	
HTTP	TCP	80	Anywh... <input type="text" value="0.0.0.0/0"/>		Delete
Custom TCP	TCP	80	Anywh... <input type="text" value="::/0"/>		Delete
HTTPS	TCP	443	Anywh... <input type="text" value="0.0.0.0/0"/>		Delete
HTTPS	TCP	443	Anywh... <input type="text" value="::/0"/>		Delete

[Add rule](#)

---

SSH TCP 22 Anywh...  Allow SSH from anywhere Delete

Next we are going to create security group for Tomcat App:-

Click Create Security group > Name : vprofile-app-sg

Allow these rules :-

Cusom TCP : 8080 : Allow from ELB SG (type ELB in search bar, you will get the SG id)

Ssh : 80 : Anywhere from ipv4

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

### Basic details

Security group name [Info](#)

Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)

### Inbound rules [Info](#)

Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>	
Custom TCP	TCP	8080	<div> <div>Security Groups</div> <div> vprofile-ELB-SG   sg-04c8452eced93acae </div> </div>		Delete
			elb		
SSH	TCP	22	Anywh...	Allow SSH from anywhere	Delete
			0.0.0.0/0		

Now Create a another security group for backend services like RabbitMQ, Memcached, 7 MySQL

Click New Security Group > Name : backend services

EC2 > Security Groups > Create security group

## Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

### Basic details

Security group name [Info](#)

Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)

In inbound Rules > Give these below rules

**Note :- MySQL Works on port 3306. Memcached works on port 11211. RabbitMQ works on 5672**

MySQL : 3306 : type app in search bar, you will get tomcat app SG, Then select it.

Custom TCP : 11211 : select tomcat app SG

Custom TCP : 5672 : select tomcat app SG

Ssh : 80 : Anywhere from ipv4

Inbound rules

Type	Protocol	Port range	Source	Description - optional
MYSQL/Aurora	TCP	3306	Custom	Allow tomcat to connect MySQL
Custom TCP	TCP	11211	Custom	Allow tomcat to connect Memcached
Custom TCP	TCP	5672	Custom	Allow tomcat to connect RabbitMQ

Add rule

SSH TCP 22 Anywh... 0.0.0.0/0 Allow SSH from anywhere

Click Create

Again select our backend security group >

Add another rule which is backend SG itself, so that our backend services will communicate internally with each other.

EC2 > Security Groups > sg-030b70f738b0d25fd - backend SG

### sg-030b70f738b0d25fd - backend SG

Actions

**Details**

Security group name backend SG	Security group ID sg-030b70f738b0d25fd	Description Security group for backend services	VPC ID vpc-03b7aefbd508a446b
Owner 911308114181	Inbound rules count 3 Permission entries	Outbound rules count 1 Permission entry	

Inbound rules | Outbound rules | Tags

## Edit Inbound Rules >

**Inbound rules** [Info](#)

Security group rule ID	Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>
sgr-03690fe56a4add57	Custom TCP ▼	TCP	11211	Custom ▼	Allow tomcat to connect Mi <span>Delete</span>
sgr-0121a75957399f750	MySQL/Aurora ▼	TCP	3306	Custom ▼	Allow tomcat to connect M <span>Delete</span>
sgr-075c66bd6d00dc98	Custom TCP ▼	TCP	5672	Custom ▼	Allow tomcat to connect R2 <span>Delete</span>
-	All traffic ▼	All	All	Custom ▼	<span>Delete</span>
-	SSH ▼	TCP	22	Anywh... ▼	Allow SSH from anywhere <span>Delete</span>

Security Groups

vprofile-app-SG | sg-0474be92fca6a0471

default | sg-0f94d54b1b902a5b5

launch-wizard-1 | sg-05d7cca5839cf449a

eks\_rf-SG | sg-0d4ddb6f6ee190d10d

backend SG | sg-030b70f738b0d25fd

vprofile-ELB-SG | sg-04c8452eced93acae

Horizon-SG | sg-08f9e3e515506c69

Q

bac X

0.0.0.0 X

*select*



## 4. Launch Instances with user data (Bash Scripts):-

Now Launch Instance as mentioned below :-

Launch CentOS Instance for MySQL

Launch CentOS Instance for MySQL

Launch an instance for Database-> Name : vprofile-db

EC2 > Instances > Launch an instance

### Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

#### Name and tags [Info](#)

Name

[Add additional tags](#)

Choose AMI CentOS 7

### Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

✕ ▾

Quickstart AMIs (0)  
Commonly used AMIs

My AMIs (0)  
Created by me

**AWS Marketplace AMIs (1264)**  
AWS & trusted third-party AMIs


Community AMIs (500)  
Published by anyone

**Refine results**  
  
Categories  
Infrastructure  
Software (1042)  
DevOps (864)  
Business  
Applications (98)  
Industries (18)  
Machine Learning (10)  
IoT (7)

centos (1264 results) showing 1 - 50  

< 1 ... > ⚙

Sort By: Relevance ▾

 **CentOS 7 (x86\_64) - with Updates HVM**  
By [Amazon Web Services](#) | Ver CentOS-7.2009-20220825.1  
★★★★☆ 2 AWS reviews [🔗](#)

This is the Official CentOS 7 x86\_64 HVM image that has been built with a minimal profile, suitable for use in HVM instance types only. The image contains just enough packages to run within AWS, bring up an SSH Server and allow users to login. Please note that this is the default CentOS-7 image...

Select

Select instance type : t2 micro

Select Key pair : vprofile-key

▼ Instance type [Info](#)

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory

Free tier eligible ▼

[Compare instance types](#)

The AMI vendor recommends using a t2.micro instance (or larger) for the best experience with this product.

▼ 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*

vprofile-key

▼

[Create new key pair](#)

Select Existing Security Group : backend SG

▼ Network settings Info

Edit

Network Info

vpc-03b7aefbd508a446b

Subnet Info

No preference (Default subnet in any availability zone)

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 groups Info

Select security groups ▼

backend SG sg-030b70f738b0d25fd ✕  
VPC: vpc-03b7aefbd508a446b

Compare security group rules

Click on Advanced details > Go to User Data

► Advanced details Info

Paste the MySQL user data from the given link :

<https://github.com/Hussain147/webapp-on-aws/blob/main/userdata/mysql.sh>

#### User data - *optional* [Info](#)

Enter user data in the field.

```
#!/bin/bash
DATABASE_PASS='admin123'
sudo yum update -y
sudo yum install epel-release -y
sudo yum install git zip unzip -y
sudo yum install mariadb-server -y

# starting & enabling mariadb-server
sudo systemctl start mariadb
sudo systemctl enable mariadb
cd /tmp/
git clone -b vp-rem https://github.com/devopshydclub/vprofile-repo.git
#restore the dump file for the application
sudo mysqladmin -u root password "$DATABASE_PASS"
```

☐ User data has already been base64 encoded

Then Click Launch Instance

Do SSH to the launched instance >

```
ssh -i vprofile-key.pem centos@ipv4 public address
```

```
Hussain@DESKTOP-572PBGQ MINGW64 ~/OneDrive/Desktop
$ ssh -i vprofile-key.pem centos@34.200.242.2
[centos@ip-172-31-0-93 ~]$
```

Now, check the status of MySQL whether it is active or not:-

```
systemctl status mariadb
```

```
[centos@ip-172-31-0-93 ~]$ systemctl status mariadb
● mariadb.service - MariaDB database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2023-02-28 11:21:54 UTC; 2h 5min ago
     Process: 16809 ExecStartPost=/usr/libexec/mariadb-wait-ready $MAINPID (code=exited, status=0/SUCCESS)
     Process: 16774 ExecStartPre=/usr/libexec/mariadb-prepare-db-dir %n (code=exited, status=0/SUCCESS)
    Main PID: 16808 (mysqld_safe)
      CGroup: /system.slice/mariadb.service
              └─16808 /bin/sh /usr/bin/mysqld_safe --basedir=/usr
                  └─16973 /usr/libexec/mysqld --basedir=/usr --datadir=/var/lib/mysq...

Feb 28 11:21:52 ip-172-31-0-93.ec2.internal systemd[1]: Starting MariaDB data...
Feb 28 11:21:52 ip-172-31-0-93.ec2.internal mariadb-prepare-db-dir[16774]: Da...
Feb 28 11:21:53 ip-172-31-0-93.ec2.internal mysqld_safe[16808]: 230228 11:21:...
Feb 28 11:21:53 ip-172-31-0-93.ec2.internal mysqld_safe[16808]: 230228 11:21:...
Feb 28 11:21:54 ip-172-31-0-93.ec2.internal systemd[1]: Started MariaDB datab...
Hint: Some lines were ellipsized, use -l to show in full.
[centos@ip-172-31-0-93 ~]$ |
```

Validate the Database ->

MySQL -u root -p

It will ask password -> Password : admin

show databases;

```
[centos@ip-172-31-0-93 ~]$ mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 6
Server version: 5.5.68-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| accounts |
| mysql |
| performance_schema |
| test |
+-----+
5 rows in set (0.00 sec)
```

Now Go to AWS EC2 console > launch another instance for Memcached with CentOS

## Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

### Name and tags [Info](#)

Name

[Add additional tags](#)

▼ **Application and OS Images (Amazon Machine Image)** [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below.

**AMI from catalog**


Recents

Quick Start

Amazon Machine Image (AMI)

CentOS-7-2111-20220825\_1.x86\_64-d9a3032a-921c-4c6d-b150-

Verified provider

  
[Browse more AMIs](#)

Instance Type : t2 micro

Key Pair : vprofile-key

▼ **Instance type** [Info](#)

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory

Free tier eligible ▼

[Compare instance types](#)


The AMI vendor recommends using a t2.micro instance (or larger) for the best experience with this product.

▼ **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*

▼

 [Create new key pair](#)

## Security Group: backend SG

▼ Network settings Info

Edit

Network Info

vpc-03b7aefbd508a446b

Subnet Info

No preference (Default subnet in any availability zone)

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 groups Info

Select security groups

backend SG sg-030b70f738b0d25fd X

VPC: vpc-03b7aefbd508a446b

Compare security group rules

Paste the **Memcached** user data from the given link :

<https://github.com/Hussain147/webapp-on-aws/blob/main/userdata/memcache.sh>

### User data - optional Info

Enter user data in the field.

```
#!/bin/bash
sudo yum install epel-release -y
sudo yum install memcached -y
sudo systemctl start memcached
sudo systemctl enable memcached
sudo systemctl status memcached
sudo memcached -p 11211 -U 11111 -u memcached -d|
```

☐ User data has already been base64 encoded

**Click Launch Instance**

Now, do ssh :-

```
ssh -I vprofile-key.pem centos@ipv4 pub address
```

```
Hussain@DESKTOP-572PBGQ MINGW64 ~/OneDrive/Desktop
$ ssh -i vprofile-key.pem centos@54.90.43.43
```

Wait for sometime to start our memcached service(it takes 2-5 minutes to start)

Now, Check the status of memcached:-

```
systemctl status memcached
```

```
[root@ip-172-31-54-65 ~]# systemctl status memcached
● memcached.service - Memcached
   Loaded: loaded (/usr/lib/systemd/system/memcached.service; disabled; vendor preset: disabled)
   Active: active (running) since Tue 2023-02-28 13:45:27 UTC; 5s ago
     Main PID: 1388 (memcached)
    CGroup: /system.slice/memcached.service
            └─1388 /usr/bin/memcached -u memcached -p 11211 -m 64 -c 1024

Feb 28 13:45:27 ip-172-31-54-65.ec2.internal systemd[1]: Started Memcached.
```

Check whether it is running on right port:

```
ss -tunpl | grep 11211
```

```
[root@ip-172-31-54-65 ~]# ss -tunpl | grep 11211
udp      UNCONN    0         0      *:11211      *:
users:(("memcached",pid=1388,fd=28))
udp      UNCONN    0         0      [::]:11211  [::]:*
users:(("memcached",pid=1388,fd=29))
tcp      LISTEN    0        128      *:11211      *:
users:(("memcached",pid=1388,fd=26))
tcp      LISTEN    0        128      [::]:11211  [::]:*
users:(("memcached",pid=1388,fd=27))
```

Now Go to AWS EC2 Console & launch another instance for RabbitMQ :

Name: vprofile-rmq01

OS; CentOS



## Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

### Name and tags [Info](#)

Name

[Add additional tags](#)

### ▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

[AMI from catalog](#)[Recents](#)[Quick Start](#)

Amazon Machine Image (AMI)

CentOS-7-2111-20220825\_1.x86\_64-  
d9a3032a-921c-4c6d-b150-

Verified provider



[Browse more](#)  
AMIs

Instance Type : t2 micro

Key Pair: vprofile-key

Security Group : backend SG

▼ Instance type [Info](#)

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory

Free tier eligible ▼

[Compare instance types](#)

The AMI vendor recommends using a t2.micro instance (or larger) for the best experience with this product.

▼ 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*

vprofile-key

▼

[Create new key pair](#)

▼ Network settings [Info](#)

Edit

Network [Info](#)

vpc-03b7aefbd508a446b

Subnet [Info](#)

No preference (Default subnet in any availability zone)

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 groups [Info](#)

Select security groups ▼

backend SG sg-030b70f738b0d25fd ✕

VPC: vpc-03b7aefbd508a446b

[Compare security group rules](#)

Paste the **RabbitMQ** user data from the given link :

<https://github.com/Hussain147/webapp-on-aws/blob/main/userdata/rabbitmq.sh>

#### User data - optional [Info](#)

Enter user data in the field.

```
#!/bin/bash
sudo yum install epel-release -y
sudo yum update -y
sudo yum install wget -y
cd /tmp/
wget http://packages.erlang-solutions.com/erlang-solutions-2.0-1.noarch.rpm
sudo rpm -Uvh erlang-solutions-2.0-1.noarch.rpm
sudo yum -y install erlang socat
curl -s https://packagecloud.io/install/repositories/rabbitmq/rabbitmq-
server/script.rpm.sh | sudo bash
sudo yum install rabbitmq-server -y
sudo systemctl start rabbitmq-server
sudo systemctl enable rabbitmq-server
sudo systemctl status rabbitmq-server
sudo sh -c 'echo "[{rabbit, [{loopback_users, []}}].\" >
/etc/rabbitmq/rabbitmq.config'
sudo rabbitmqctl add_user test test
sudo rabbitmqctl set_user_tags test administrator
sudo systemctl restart rabbitmq-server]
```

**Click Launch Instance**

Connect with ssh:

```
ssh -i vprofile-key.pem centos@ipv4 pub address
```

```
systemctl status rabbitmq-server
```

```
[root@ip-172-31-56-24 ~]# systemctl status rabbitmq-server
● rabbitmq-server.service - RabbitMQ broker
   Loaded: loaded (/usr/lib/systemd/system/rabbitmq-server.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2023-02-28 14:05:33 UTC; 1s ago
     Process: 17640 ExecStop=/usr/sbin/rabbitmqctl shutdown (code=exited, status=0/SUCCESS)
    Main PID: 17676 (beam.smp)
      CGroup: /system.slice/rabbitmq-server.service
              └─17676 /usr/lib64/erlang/erts-12.3.2.1/bin/beam.smp -W w -MBas ageffcbf -MHas ag...
                 └─17691 erl_child_setup 32768
                    └─17714 /usr/lib64/erlang/erts-12.3.2.1/bin/epmd -daemon
                       └─17731 inet_gethost 4
                          └─17732 inet_gethost 4
```

Now, Launch another server for Tomcat Application:

Go to AWS EC2 Console > Launch instance:

Name: vprofile-app01

OS: Ubuntu Server 18.04 LTS

Name

vprofile-app01

Add additional tags

▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Q Search our full catalog including 1000s of application and OS images

Recents

Quick Start

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

⋮

>

Q

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 18.04 LTS (HVM), SSD Volume Type

ami-0263e4deb427da90e (64-bit (x86)) / ami-0e5599794d252b611 (64-bit (Arm))

Virtualization: hvm   ENA enabled: true   Root device type: ebs

Free tier eligible ▼

Instance Type: t2 micro

Key Pair: vprofile-key

Security Group: vprofile-app-SG

▼ Instance type Info

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory  
On-Demand Windows pricing: 0.0162 USD per Hour  
On-Demand SUSE pricing: 0.0116 USD per Hour  
On-Demand RHEL pricing: 0.0716 USD per Hour  
On-Demand Linux pricing: 0.0116 USD per Hour

Free tier eligible

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

vprofile-key

Create new key pair

▼ Network settings Info Edit

Network Info

vpc-03b7aefbd508a446b

Subnet Info

No preference (Default subnet in any availability zone)

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 groups Info

Select security groups

vprofile-app-SG sg-0474be92fca6a0471 X  
VPC: vpc-03b7aefbd508a446b

Compare security group rules

Paste the **Tomcat** user data from the given link :

[https://github.com/Hussain147/webapp-on-aws/blob/main/userdata/tomcat\\_ubuntu.sh](https://github.com/Hussain147/webapp-on-aws/blob/main/userdata/tomcat_ubuntu.sh)

#### User data - optional Info

Enter user data in the field.

```
#!/bin/bash
sudo apt update
sudo apt upgrade -y
sudo apt install openjdk-8-jdk -y
sudo apt install tomcat8 tomcat8-admin tomcat8-docs tomcat8-common git
-y|
```

**Click Launch Instance**

## 5. Update IP to name mapping in route 53:-

Copy all the instances private ip's in a notepad like below

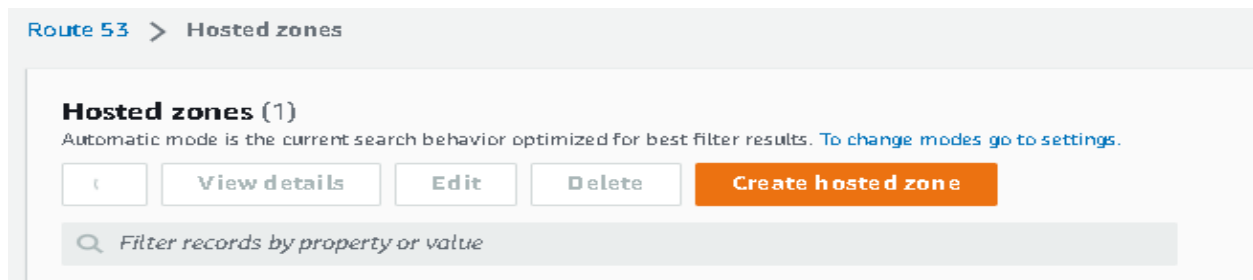
vprofile-db01:- Private Ip addr

vprofile-mc01 :- Private Ip addr

vprofile-rmq01 :- Private Ip addr

Now Goto Route 53 >

Click on Create Hosted Zone



Domain Name: vprofile.in

The screenshot shows the 'Create hosted zone' form in the AWS Route 53 console. The breadcrumb is 'Route 53 > Hosted zones > Create hosted zone'. The main heading is 'Create hosted zone' with an 'Info' link. Below this is the 'Hosted zone configuration' section, which includes a description: 'A hosted zone is a container that holds information about how you want to route traffic for a domain, such as example.com, and its subdomains.' The form has three main sections: 1. 'Domain name' with an 'Info' link, a text input field containing 'vprofile.in', and a list of valid characters. 2. 'Description - optional' with an 'Info' link, a text area containing 'The hosted zone is used for...', and a character count '0/256'. 3. 'Type' with an 'Info' link, showing two radio button options: 'Public hosted zone' (selected) and 'Private hosted zone'. Each option has a brief description of its routing behavior.

Click **Create Hosted Zone**

## Now, Click create Record

Route 53 > Hosted zones > vprofile.in

Public vprofile.in Info Delete zone Test record Configure query logging

► Hosted zone details Edit hosted zone

Records (2) DNSSEC signing Hosted zone tags (0)

**Records (2)** Info Automatic mode is the current search behavior optimized for best filter results. [To change modes go to settings.](#)

Filter records by property or value Type Routing policy Alias < 1 > ⚙

<input type="checkbox"/>	Record name ▼	Type ▼	Routin... ▼	Differ... ▼	Value/Route traffic to ▼
<input type="checkbox"/>	vprofile.in	NS	Simple	-	ns-652.awsdns-17.net. ns-1312.awsdns-36.org. ns-1932.awsdns-49.co.uk. ns-13.awsdns-01.com.
<input type="checkbox"/>	vprofile.in	SOA	Simple	-	ns-652.awsdns-17.net. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400

Record Name: - db01

Value :- <db01 private ip>

Create record Info

Quick create record Switch to wizard

▼ Record 1 Delete

Record name Info db01 .vprofile.in Record type Info A – Routes traffic to an IPv4 address and some AWS resources

Keep blank to create a record for the root domain.

☒ Alias

Value Info 172.31.0.93

Enter multiple values on separate lines.

Click Create Record

Record Name: - mc01

Value :- <mc01 private ip>

Quick create record

Switch to wizard

▼ Record 1

Delete

Record name

Info

mc01

.vprofile.in

Record type

Info

A – Routes traffic to an IPv4 address and some AWS resources

Keep blank to create a record for the root domain.

☐ Alias

Value

Info

172.31.54.65

Enter multiple values on separate lines.

TTL (seconds)

Info

300

1m

1h

1d

Routing policy

Info

Simple routing

Recommended values: 60 to 172800 (two days)

Click Create Record

-----

Record Name: - rmq01

Value :- <rmq01 private ip>

Quick create record

Switch to wizard

▼ Record 1

Delete

Record name

Info

rmq01

.vprofile.in

Record type

Info

A – Routes traffic to an IPv4 address and some AWS resources

Keep blank to create a record for the root domain.

☐ Alias

Value

Info

172.31.56.24

Enter multiple values on separate lines.

TTL (seconds)

Info

300

1m

1h

1d

Routing policy

Info

Simple routing

Recommended values: 60 to 172800 (two days)

Click Create Record



## 6. Build Application from source code:-

Now come to local machine > open powershell with administration > install jdk 8 & maven

**Note :- you need to install chocolatey in powershell before installing the jdk8 & maven**

```
choco install jdk8 -y
```

```
choco install mvn -y
```

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> choco install jdk8 -y
Chocolatey v0.12.1
Installing the following packages:
jdk8
By installing, you accept licenses for the packages.
jdk8 v8.0.211 already installed.
Use --force to reinstall, specify a version to install, or try upgrade.

Chocolatey installed 0/1 packages.
See the log for details (C:\ProgramData\chocolatey\logs\chocolatey.log).

Warnings:
- jdk8 - jdk8 v8.0.211 already installed.
Use --force to reinstall, specify a version to install, or try upgrade.

PS C:\WINDOWS\system32> choco install maven -y
Chocolatey v0.12.1
Installing the following packages:
maven
By installing, you accept licenses for the packages.
maven v3.8.5 already installed.
Use --force to reinstall, specify a version to install, or try upgrade.

Chocolatey installed 0/1 packages.
See the log for details (C:\ProgramData\chocolatey\logs\chocolatey.log).

Warnings:
- maven - maven v3.8.5 already installed.
Use --force to reinstall, specify a version to install, or try upgrade.
```

Now go to src > main > resources

You will have application.properties file

Edit the properties file as given in screenshots below

vi application.properties

```
jdbc.url=jdbc:mysql://db01.vprofile.in:3306/accounts?useUnicode=true&characterEncoding=UTF-8&zeroDateTimeBehavior=convertToNull
memcached.active.host=mc01.vprofile.in
rabbitmq.address=rmq01.vprofile.in
```

```

#JDBC Configuration for Database Connection
jdbc.driverClassName=com.mysql.jdbc.Driver
jdbc.url=jdbc:mysql://db01.vprofile.in:3306/accounts?useUnicode=true&characterEncoding=UTF-8&zeroDateTimeBehavior=convertToNull
jdbc.username=admin
jdbc.password=admin123

#Memcached Configuration For Active and StandBy Host
#For Active Host
memcached.active.host=mc01.vprofile.in
memcached.active.port=11211
#For StandBy Host
memcached.standBy.host=127.0.0.2
memcached.standBy.port=11211

#RabbitMq Configuration
rabbitmq.address=rmq01.vprofile.in
rabbitmq.port=5672
rabbitmq.username=test
rabbitmq.password=test

#Elasticsearch Configuration
elasticsearch.host=192.168.1.85
elasticsearch.port=9300
elasticsearch.cluster=vprofile
elasticsearch.node=vprofilenode
~

```

Save and exit

Now come to our project directory where we see src directory

Type **mvn install** to build our artifact

mvn install (this will take couple of minutes to build an artifact)

```

Hussain@DESKTOP-572PBGQ MINGW64 ~/OneDrive/Desktop/Institute/Projects/Web App Setup With AWS Project/webapp-on-aws (main)
$ cd ../../../../

Hussain@DESKTOP-572PBGQ MINGW64 ~/OneDrive/Desktop/Institute/Projects/Web App Setup With AWS Project/webapp-on-aws (main)
$ ls
Jenkinsfile  'Web App Setup With AWS Project.docx'  pom.xml  userdata/
README.md    ansible/                                src/

Hussain@DESKTOP-572PBGQ MINGW64 ~/OneDrive/Desktop/Institute/Projects/Web App Setup With AWS Project/webapp-on-aws (main)
$ mvn install

```

Type ls > you will get Target directory

```

Hussain@DESKTOP-572PBGQ MINGW64 ~/OneDrive/Desktop/Institute/Projects/Web App Setup With AWS Project/webapp-on-aws (main)
$ ls
Jenkinsfile  'Web App Setup With AWS Project.docx'  pom.xml  target/
README.md    ansible/                                src/      userdata/

```

Goto Target Directory >type ls > You will get vprofile-v2.war(It is built by us using maven)

```

Hussain@DESKTOP-572PBGQ MINGW64 ~/OneDrive/Desktop/Institute/Projects/Web App Setup With AWS Project/webapp-on-aws (main)
$ cd target

Hussain@DESKTOP-572PBGQ MINGW64 ~/OneDrive/Desktop/Institute/Projects/Web App Setup With AWS Project/webapp-on-aws/target (main)
$ ls
classes/ generated-sources/ generated-test-sources/ jacoco.exec maven-archiver/ maven-status/ site/ surefire-reports/ test-classes/ vprofile-v2/ vprofile-v2.war

```

## 7. Upload to S3 bucket:-

Now, we need to send this artifact(vprofile-v2.war) to the S3 bucket by using AWSCLI

**Note:-** You need to install awscli in local machine & configured

```
Hussain@DESKTOP-572PBGQ MINGW64 ~/OneDrive/Desktop/Institute/Projects/Web App Setup With AWS Project/webapp-on-aws/target (main)
$ aws configure
AWS Access Key ID [*****ONHT]:
AWS Secret Access Key [*****wLNI]:
Default region name [us-east-1]:
Default output format [None]: |
```

**Create a S3 bucket:-**

```
aws s3 mb s3://my-vprofile-artifact
```

**Note:-** You need to take unique bucket name(S3 bucket name should be different)

```
Hussain@DESKTOP-572PBGQ MINGW64 ~/OneDrive/Desktop/Institute/Projects/Web App Setup With AWS Project/webapp-on-aws/target (main)
$ aws s3 mb s3://my-vprofile-artifact
make_bucket: my-vprofile-artifact
```

Now Copy our artifact to our S3 bucket & validate :-

```
aws s3 cp vprofile-v2.war s3://my-vprofile-artifact/vprofile-v2.war
```

```
aws s3 ls s3://my-vprofile-artifact/
```

```
Hussain@DESKTOP-572PBGQ MINGW64 ~/OneDrive/Desktop/Institute/Projects/Web App Setup With AWS Project/webapp-on-aws/target (main)
$ aws s3 cp vprofile-v2.war s3://my-vprofile-artifact/vprofile-v2.war
upload: .\vprofile-v2.war to s3://my-vprofile-artifact/vprofile-v2.war

Hussain@DESKTOP-572PBGQ MINGW64 ~/OneDrive/Desktop/Institute/Projects/Web App Setup With AWS Project/webapp-on-aws/target (main)
$ aws s3 ls s3://my-vprofile-artifact/
2023-02-28 20:23:27 48450938 vprofile-v2.war
```

Now we need to create a Role to store our artifact to the tomcat server

Go to IAM > Role > Create Role :

Select AWS Service >

Use Case: EC2

## Select trusted entity [Info](#)

### Trusted entity type

<input checked="" type="radio"/> <b>AWS service</b> Allow AWS services like EC2, Lambda, or others to perform actions in this account.	<input type="radio"/> <b>AWS account</b> Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.	<input type="radio"/> <b>Web identity</b> Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
<input type="radio"/> <b>SAML 2.0 federation</b> Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.	<input type="radio"/> <b>Custom trust policy</b> 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.

#### Common use cases


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

## Add permissions > s3fullaccess

### Add permissions [Info](#)

**Permissions policies** (Selected 1/816) [Info](#)  
Choose one or more policies to attach to your new role.

1 match

<input checked="" type="checkbox"/>	Policy name <a href="#">Info</a>	Type	Description
<input checked="" type="checkbox"/>	 AmazonS3FullAccess	AWS ...	Provides full access to all buckets via the AWS Management Console.

Role Name: vprofile-artifact-storage-role

## Name, review, and create

### Role details

Role name

Enter a meaningful name to identify this role.

vprofile-artifact-storage-role

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

Click **Create Role**


Now go to EC2 > select app01 server > Actions > Security > Modify IAM Role >

Select our Role (vprofile-artifact-storage-role)

EC2 > Instances > i-0be730ceabe5f2d44 > Modify IAM role

**Modify IAM role** [Info](#)  
Attach an IAM role to your instance.



Instance ID

 i-0be730ceabe5f2d44 (vprofile-app01)

IAM role

Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

vprofile-artifact-storage-role ▼

 [Create new IAM role](#) 

Cancel

**Update IAM role**

Click **Update IAM Role**

## 8. Download Artifact to Tomcat Ec2 instance:-

Now connect app01 server with ssh >

```
Hussain@DESKTOP-572PBGQ MINGW64 ~/OneDrive/Desktop
$ ssh -i vprofile-key.pem ubuntu@34.203.33.172
```

Now go to /var/lib/tomcat8/webapps

Stop the tomcat server: - systemctl stop tomcat

Remove ROOT directory :- rm -rf ROOT

```
root@ip-172-31-62-187:/var# ls
backups  cache  crash  lib  local  lock  log  mail  opt  run  snap  spool  tmp
root@ip-172-31-62-187:/var# clear
root@ip-172-31-62-187:/var# ls
backups  cache  crash  lib  local  lock  log  mail  opt  run  snap  spool  tmp
root@ip-172-31-62-187:/var# cd lib
root@ip-172-31-62-187:/var/lib# ls
AccountsService  dpkg          man-db          python          ucf
amazon            git           misc            shim-signed     unattended-upgrades
appport          grub          mlocate         snapd           update-manager
apt              initramfs-tools  os-prober      sudo            update-notifier
cloud            landscape     pam             systemd         ureadahead
command-not-found  logrotate    plymouth        tomcat8         usbutils
dbus             lxcfs        polkit-1        ubuntu-advantage  vim
dhcp            lxd          private         ubuntu-release-upgrader
root@ip-172-31-62-187:/var/lib# cd tomcat8
root@ip-172-31-62-187:/var/lib/tomcat8# ls
conf  lib  logs  policy  webapps  work
root@ip-172-31-62-187:/var/lib/tomcat8# cd webapps
root@ip-172-31-62-187:/var/lib/tomcat8/webapps# ls
ROOT
root@ip-172-31-62-187:/var/lib/tomcat8/webapps# systemctl stop tomcat8
root@ip-172-31-62-187:/var/lib/tomcat8/webapps# ls
ROOT
root@ip-172-31-62-187:/var/lib/tomcat8/webapps# rm -rf ROOT
root@ip-172-31-62-187:/var/lib/tomcat8/webapps# ls
```

Now Install AWSCLI , (No need to Configure)

```
root@ip-172-31-62-187:/var/lib/tomcat8/webapps# apt install awscli -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
```

aws s3 ls s3://my-vprofile-artifact

**Download the artifact from S3 to our tomcat server in /tmp directory**

`aws s3 cp s3://my-vprofile-artifact/vprofile-v2.war /tmp/vprofile-v2.war`

```
root@ip-172-31-62-187:~# aws s3 ls s3://my-vprofile-artifact
2023-02-28 14:53:27    48450938 vprofile-v2.war
root@ip-172-31-62-187:~# aws s3 cp s3://my-vprofile-artifact/vprofile-v2.war /tmp/vprofile-v2.war
download: s3://my-vprofile-artifact/vprofile-v2.war to ../tmp/vprofile-v2.war
root@ip-172-31-62-187:~# |
```

**Now copy the artifact to /var/lib/tomcat8/ROOT.war**

```
root@ip-172-31-62-187:/tmp# cp vprofile-v2.war /var/lib/tomcat8/webapps/ROOT.war
```

**Start Tomcat8 :- systemctl start tomcat8**

```
root@ip-172-31-62-187:/tmp# systemctl start tomcat8
```

**Now go to the path as given below:-**

`cd /var/lib/tomcat8/webapps/ROOT/WEB-INF/classes`

`ls`

`cat application.properties`

```

root@ip-172-31-62-187:/var/lib/tomcat8/webapps/ROOT/WEB-INF/classes# ls
application.properties  com  db_backup.sql  logback.xml  validation.properties
root@ip-172-31-62-187:/var/lib/tomcat8/webapps/ROOT/WEB-INF/classes# cat application.properties
#JDBC Configuration for Database Connection
jdbc.driverClassName=com.mysql.jdbc.Driver
jdbc.url=jdbc:mysql://db01.vprofile.in:3306/accounts?useUnicode=true&characterEncoding=UTF-8&zeroDateTimeBehavior=convertToNull
jdbc.username=admin
jdbc.password=admin123

#Memcached Configuration For Active and StandBy Host
#For Active Host
memcached.active.host=mc01.vprofile.in
memcached.active.port=11211
#For StandBy Host
memcached.standBy.host=127.0.0.2
memcached.standBy.port=11211

#RabbitMq Configuration
rabbitmq.address=rmq01.vprofile.in
rabbitmq.port=5672
rabbitmq.username=test
rabbitmq.password=test

#Elasticsearch Configuration
elasticsearch.host =192.168.1.85
elasticsearch.port =9300
elasticsearch.cluster=vprofile
elasticsearch.node=vprofilenode
root@ip-172-31-62-187:/var/lib/tomcat8/webapps/ROOT/WEB-INF/classes# |

```

Then type vi /etc/hosts > add the private IP's of backend servers(db01, mc01, rmq01)

```

127.0.0.1 localhost
172.31.0.93 db01.vprofile.in
172.31.54.65 mc01.vprofile.in
172.31.56.24 rmq01.vprofile.in

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
~

```

Save & Exit

Now, type telnet db01.vprofile.in 3306 -> to confirm that our backend servers are connecting to tomcat server

```

root@ip-172-31-18-202:~# telnet db01.vprofile.in 3306
Trying 172.31.0.93...
Connected to db01.vprofile.in.
Escape character is '^['.
&
5.5.68-MariaDB
@+S@&;9CSYE,LzD%(8$mysql_native_password

```



## 9. Setup ELB with HTTP:-

Go to Load Balancer > Target Groups > Create Target Groups >

Target Group Name : vprofile-app-TG

Target Type: Instance

Protocol : HTTP

Port: 8080

Path : /login

### Create target group

Your load balancer routes requests to the targets in a target group using the target group settings that you specify.

Target group name	<input type="text" value="vprofile-app-TG"/>
Target type	<input checked="" type="radio"/> Instance <input type="radio"/> IP <input type="radio"/> Lambda function
Protocol	<input type="text" value="HTTP"/>
Port	<input type="text" value="8080"/>
VPC	<input type="text" value="vpc-03b7aefbd508a446b (172.31.0.0/16) (M)"/>

### Health check settings

Protocol	<input type="text" value="HTTP"/>
Path	<input type="text" value="/login"/>

### ▼ Advanced health check settings

Port	<input type="radio"/> traffic port <input checked="" type="radio"/> override <input type="text" value="8080"/>
Healthy threshold	<input type="text" value="3"/>
Unhealthy threshold	<input type="text" value="2"/>

Click **Create**

Now, Select our Target Group: vprofile-app-TG >

**New features for target groups are available only in the new experience**  
We are replacing this older experience for target groups with a new one. We will add new features and make improvements only to the new experience. To switch between the old and new experiences, use the New EC2 Experience toggle at the top of the left navigation pane.

**Create target group** **Actions** Filter by tags and attributes 1 to 2 of 2

Name	Port	Protocol	Target type	Load Balancer	VPC ID	Monitoring
vprofile-app-TG	8080	HTTP	instance		vpc-03b7aefbd508a446b	

**Actions**

- Edit health check
- Register and deregister instance / ip targets**
- Edit attributes
- Delete

Select the Target Group > Register Instances > Register Instances > Select our Tomcat App Instance > Add > Save Changes

**Register and deregister targets**

To deregister instances, select one or more registered instances and then click Remove.

**Remove**

Instance	Name	Port	State	Security groups	Zone
i-0be730ceabe5f2b44	vprofile-app01	8080	running	vprofile-app-SG	us-east-1e

**Instances**

To register additional instances, select one or more running instances, specify a port, and then click Add. The default port is the port specified for the target group. If the instance is already registered on the specified port, you must specify a different port.

**Add to registered** on port

**Search Instances**

Instance	Name	State	Security group	Zone	Subnet ID	Subnet CIDR
i-067effb2a48a...	vprofile-db	running	backend SG	us-east-1b	subnet-0c6d196eccc76f2f	172.31.0.0/20
i-09306ce4a87...	vprofile-mc01	running	backend SG	us-east-1e	subnet-0a409b757d057e008	172.31.48.0/20
i-0be730ceabe...	vprofile-app01	running	vprofile-app-SG	us-east-1e	subnet-0a409b757d057e008	172.31.48.0/20

Now Go to Load Balancer > Create Load Balancer > Select Application Load Balancer > Create

Name: vprofile-app-ELB

Scheme : Internet Facing

Ip type: ipv4

1. Configure Load Balancer

2. Configure Security Settings

3. Configure Security Groups

4. Configure Routing

5. Register Targets

6. Review

Step 1: Configure Load Balancer

Basic Configuration

To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and select a network. The default configuration HTTP traffic on port 80.

Name ⓘ

Scheme ⓘ

IP address type ⓘ

vprofile-app-ELB

internet-facing

internal

ipv4

Listener: HTTP : 80

Listeners

A listener is a process that checks for connection requests, using the protocol and port that you configured.

Load Balancer Protocol	Load Balancer Port
<div>HTTP</div>	<div>80</div>
<div>Add listener</div>	

Select ELB Security Group

Step 3: Configure Security Groups

A security group is a set of firewall rules that control the traffic to your load balancer. On this page, you can add rules to allow specific traffic to reach your load b existing one.

Assign a security group

Create a new security group

Select an existing security group

Security Group ID	Name	Description
<input type="checkbox"/> sg-030b70f738b0d25fd	backend-SG	Security group for backend services
<input type="checkbox"/> sg-0f94d54b1b902a5b5	default	default VPC security group
<input type="checkbox"/> sg-0a37054458e17e3b8	docker-SG	docker-SG
<input type="checkbox"/> sg-0d4ddb6ee190d10d	eks_tf-SG	eks_tf-SG
<input type="checkbox"/> sg-089e3e515506c699	Horizon-SG	Horizon-SG
<input type="checkbox"/> sg-05d7cca5839cf449a	launch-wizard-1	launch-wizard-1 created 2023-02-07T06:44:53.467Z
<input type="checkbox"/> sg-0474be92fca6a0471	vprofile-app-SG	Allowing TomcatApp from ELB
<input checked="" type="checkbox"/> sg-04c8452eced93acae	vprofile-ELB-SG	Security group for Vprofile prod ELB

Select our Target Group : vprofile-app-TG

1. Configure Load Balancer 2. Configure Security Settings 3. Configure Security Groups 4. Configure Routing 5. Register Targets 6. Review

## Step 4: Configure Routing

Your load balancer routes requests to the targets in this target group using the protocol and port that you specify here. It also performs health checks on the apply to all of the listeners configured on this load balancer. You can edit or add listeners after the load balancer is created.

### Target group

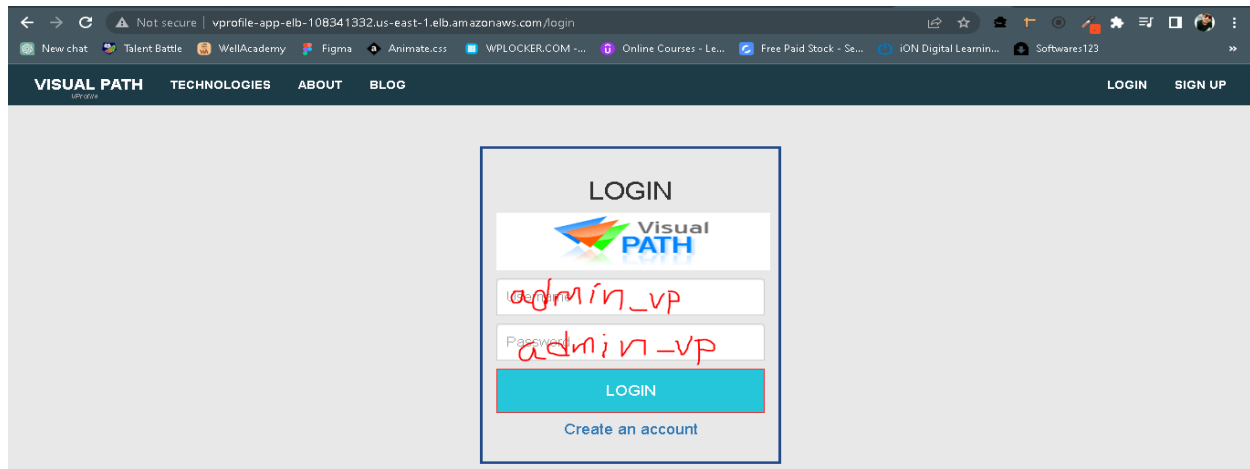
Target group	Existing target group
Name	vprofile-app-TG
Target type	<input checked="" type="radio"/> Instance <input type="radio"/> IP <input type="radio"/> Lambda function
Protocol	HTTP
Port	8080
Protocol version	<input checked="" type="radio"/> HTTP1 Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2. <input type="radio"/> HTTP2 Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.

Click **Register Targets** > Click **Review** > **Next** > Click on **Create**

Then Copy the DNS Name & paste it in the URL address

Username: admin\_vp

Password: admin\_vp



Click > Login

Once you successfully logged in, check for backend servers are working are not.


Click on All Users – If it opens a new webpage then our memcache is working

Click on RabbitMq – If it opens a new webpage then our rabbitmq is working

VisualPath  
UP! Workspace

StreamMy Activity

admin\_vp



**admin\_vp** admin\_vp@visualpath.co.in ✓

#DevOps #Continuous Integration #Continuous Delivery #AutomationAll UsersRabbitMqElasticsearch

PostsPhotos 42Contacts 42

admin\_vp 42 minutes ago

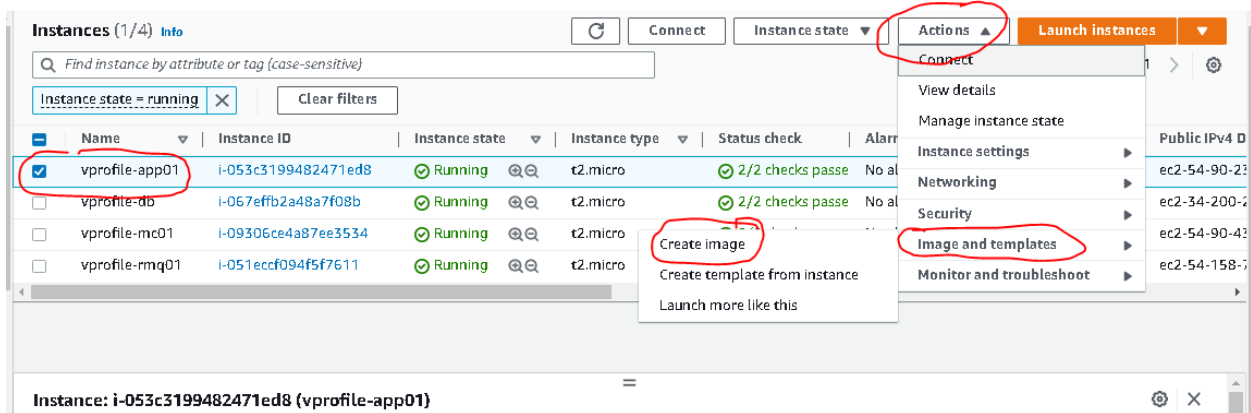
"The Key to DevOps Success."

The Key to DevOps Success" Collaboration". Collaboration is essential to DevOps,yet how to do it is often unclear with many teams falling back on ineffective conference calls, instant messaging, documents, and SharePoint sites. In this keynote,we will share a vision for a next generation DevOps where collaboration, continuous documentation, and knowledge capture are combined with automation toolchains to enable rapid innovation and deployment.

PublicLikeReshareComment

## 10. Build Autoscaling Group for Tomcat Instances:-

Go to EC2 > select our app01 server > Actions > Image and templates > Create Image



Name : vprofile-app-image

EC2 > Instances > i-053c3199482471ed8 > Create image

### Create image Info

An image (also referred to as an AMI) defines the programs and settings that are applied when you launch an EC2 instance. You can create an image from the configuration of an existing instance.

Instance ID  
i-053c3199482471ed8 (vprofile-app01)

Image name  
vprofile-app-image  
Maximum 127 characters. Can't be modified after creation.

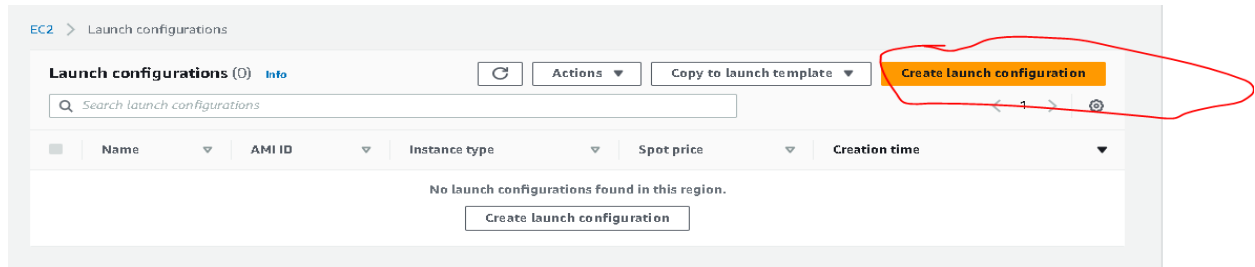
Image description - *optional*  
vprofile-app-image  
Maximum 255 characters

No reboot  
☐ Enable

Instance volumes

Click create

Then Go to Launch Configurations > Create Launch Configuration



Name : vprofile-app-LC

AMI : select our image (vprofile-app-image)

Instance Type : t2 micro (it is free tier)

IAM Instance Profile : select our Role (vprofile-artifact-storage-role)

Monitoring : enable to get the logs in cloudwatch

Security Group : select the **app-SG**

**Security groups** [Info](#)

Assign a security group

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

**Security groups** Copy to new View rules

	Security group ID	Name	VPC ID	Description
<input type="checkbox"/>	sg-04c8452eced93acae	vprofile-ELB-SG	vpc-03b7aefbd508a446b	Security group for Vprofile prod ELB
<input checked="" type="checkbox"/>	sg-0474be92fca6a0471	vprofile-app-SG	vpc-03b7aefbd508a446b	Allowing TomcatApp from ELB
<input type="checkbox"/>	sg-0f94d54b1b902a5b5	default	vpc-03b7aefbd508a446b	default VPC security group
<input type="checkbox"/>	sg-05d7cca5839cf449a	launch-wizard-1	vpc-03b7aefbd508a446b	launch-wizard-1 created 2023-02-07T06:44:53.467Z
<input type="checkbox"/>	sg-0d4ddbf6ee190d10d	eks_tf-SG	vpc-03b7aefbd508a446b	eks_tf-SG
<input type="checkbox"/>	sg-0a37054458e17e3b8	docker-SG	vpc-03b7aefbd508a446b	docker-SG

Keypair : vprofile-key > click **create Launch Configuration**

**Key pair (login)** [Info](#)

Key pair options

Existing key pair

☒ I acknowledge that I have access to the selected private key file (vprofile-key.pem), and that without this file, I won't be able to log into my instance.

Cancel Create launch configuration

Now go to Autoscaling Groups > click on create Autoscaling Group

## Amazon EC2 Auto Scaling

helps maintain the availability of your applications

Auto Scaling groups are collections of Amazon EC2 instances that enable automatic scaling and fleet management features. These features help you maintain the health and availability of your applications.

### Create Auto Scaling group

Get started with EC2 Auto Scaling by creating an Auto Scaling group.

[Create Auto Scaling group](#)

Name : vprofile-ASG

Click on **Switch to launch configuration**

Launch Configuration : vprofile-app-LC



EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1

Choose launch template or configuration

Step 2

Choose instance launch options

Step 3 - optional

Configure advanced options

Step 4 - optional

Configure group size and scaling policies

Step 5 - optional

Add notifications

Step 6 - optional

Add tags

Step 7

Review

Choose launch template or configuration [Info](#)

Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group. If you currently use launch configurations, you might consider migrating to launch templates.

Name

Auto Scaling group name

Enter a name to identify the group.

vprofile-ASG

Must be unique to this account in the current Region and no more than 255 characters.

Launch configuration [Info](#)

[Switch to launch template](#)

⚠

Instead of using launch configurations to create your EC2 Auto Scaling groups, we recommend that you use launch templates and make use of the Auto Scaling guidance option. For more information on migrating launch configurations and using launch templates, [see the documentation](#) [↗](#)

Launch configuration

Choose a launch configuration that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.

vprofile-app-LC

▼

G

[Create a launch configuration](#) [↗](#)

Click Next

Select the VPC(in my case I'm using default VPC) & select all the Availabilty Zones

## Network [Info](#)

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.

### VPC

Choose the VPC that defines the virtual network for your Auto Scaling group.

vpc-03b7aefbd508a446b  
172.31.0.0/16 Default



[Create a VPC](#)

### Availability Zones and subnets

Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.

Select Availability Zones and subnets



us-east-1a | subnet-0941d0011e50e389e X  
172.31.32.0/20 Default

us-east-1b | subnet-0c6d196eccc76f2f X  
172.31.0.0/20 Default

us-east-1c | subnet-0c94cb08a5c953824 X  
172.31.80.0/20 Default

us-east-1d | subnet-094c337d133541420 X  
172.31.16.0/20 Default

us-east-1e | subnet-0a409b757d057e008 X  
172.31.48.0/20 Default

Click **Next**

Select our existing Load Balancer

Select vprofile-app-TG

## Load balancing - *optional* [Info](#)

Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you define.

☐ No load balancer  
Traffic to your Auto Scaling group will not be fronted by a load balancer.

☒ Attach to an existing load balancer  
Choose from your existing load balancers.

☐ Attach to a new load balancer  
Quickly create a basic load balancer to attach to your Auto Scaling group.

### Attach to an existing load balancer

Select the load balancers that you want to attach to your Auto Scaling group.

☒ Choose from your load balancer target groups  
This option allows you to attach Application, Network, or Gateway Load Balancers.

☐ Choose from Classic Load Balancers

#### Existing load balancer target groups

Only instance target groups that belong to the same VPC as your Auto Scaling group are available for selection.

Select target groups



vprofile-app-TG | HTTP X  
Application Load Balancer: vprofile-app-ELB

Enable **ELB & Monitoring**

### Health checks - *optional*

**Health check type** [Info](#)  
EC2 Auto Scaling automatically replaces instances that fail health checks. If you enabled load balancing, you can enable ELB health checks in addition to the EC2 health checks that are always enabled.

☒ EC2 ☒ ELB

**Health check grace period**  
The amount of time until EC2 Auto Scaling performs the first health check on new instances after they are put into service.

seconds

### Additional settings - *optional*

**Monitoring** [Info](#)  
☒ Enable group metrics collection within CloudWatch

**Default instance warmup** [Info](#)  
The amount of time that CloudWatch metrics for new instances do not contribute to the group's aggregated instance metrics, as their usage data is not reliable yet.

☐ Enable default instance warmup

Cancel

Skip to review

Previous

Next

Click **Next**

Select Desired Capacity : I choose 1

Minimum & maximum as per the requirement

### Group size - *optional*

[Info](#)

Specify the size of the Auto Scaling group by changing the desired capacity. You can also specify minimum and maximum capacity limits. Your desired capacity must be within the limit range.

**Desired capacity**

**Minimum capacity**

**Maximum capacity**

### Scaling policies - *optional*

Choose whether to use a scaling policy to dynamically resize your Auto Scaling group to meet changes in demand. [Info](#)



#### Target tracking scaling policy

Choose a desired outcome and leave it to the scaling policy to add and remove capacity as needed to achieve that outcome.



None

Scaling policy name

Target Tracking Policy

Metric type

Average CPU utilization ▼

Target value

50

Instances need

300

seconds warm up before including in metric

☐ Disable scale in to create only a scale-out policy

Click **Next**

Add Notification by creating SNS Topic

### Add notifications - *optional* [Info](#)

Send notifications to SNS topics whenever Amazon EC2 Auto Scaling launches or terminates the EC2 instances in your Auto Scaling group.

Add notification

Cancel

Skip to review

Previous

Next

Click **Next**

Give Some Tags as per your choice

### Add tags - *optional* [Info](#)

Add tags to help you search, filter, and track your Auto Scaling group across AWS. You can also choose to automatically add these tags to instances when they are launched.

**i** You can optionally choose to add tags to instances (and their attached EBS volumes) by specifying tags in your launch template. We recommend caution, however, because the tag values for instances from your launch template will be overridden if there are any duplicate keys specified for the Auto Scaling group. **X**

#### Tags (3)

Key	Value - optional	Tag new instances	
<input type="text" value="Name"/>	<input type="text" value="vprofile-app"/>	<input checked="" type="checkbox"/>	<input type="button" value="Remove"/>
<input type="text" value="Project"/>	<input type="text" value="vprofile-app-project"/>	<input checked="" type="checkbox"/>	<input type="button" value="Remove"/>
<input type="text" value="Owner"/>	<input type="text" value="Hussain"/>	<input checked="" type="checkbox"/>	<input type="button" value="Remove"/>
<input type="button" value="Add tag"/>			

47 remaining

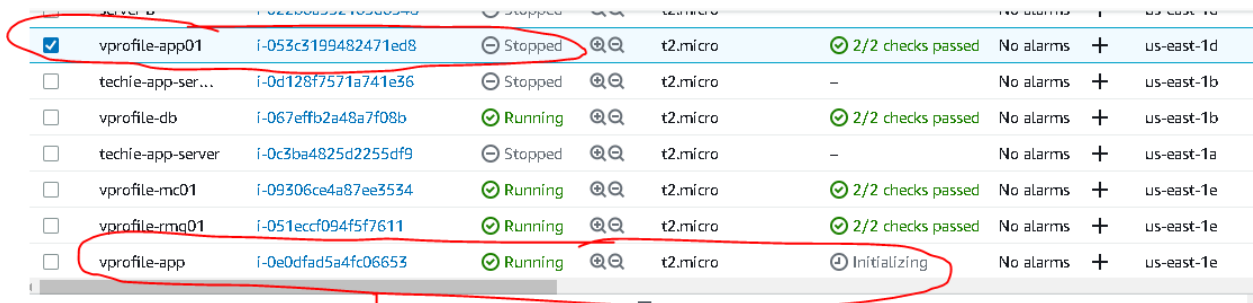
Click **Next**

Click **Create Auto Scaling Group** ->

**Now if your app01 get terminated or go down then your autoscaling group will scale up the instance with your application**

Instances (1/11) <a href="#">Info</a>		<input type="button" value="Refresh"/>	<input type="button" value="Connect"/>	<input type="button" value="Instance state"/>	<input type="button" value="Actions"/>	<input type="button" value="Launch instances"/>	<input type="button" value="Filter"/>
<input type="text" value="Find instance by attribute or tag (case-sensitive)"/>							
<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input checked="" type="checkbox"/>	vprofile-app01	i-053c3199482471ed8	<span>Running</span>	t2.micro	<span>2/2 checks passed</span>	No alarms	us-east-1d

I have stopped the app01 wantedly > see our ASG is launching app server automatically



<input checked="" type="checkbox"/>	vprofile-app01	i-053c3199482471ed8	Stopped	t2.micro	2/2 checks passed	No alarms	+	us-east-1d
<input type="checkbox"/>	techie-app-ser...	i-0d128f7571a741e36	Stopped	t2.micro	-	No alarms	+	us-east-1b
<input type="checkbox"/>	vprofile-db	i-067effb2a48a7f08b	Running	t2.micro	2/2 checks passed	No alarms	+	us-east-1b
<input type="checkbox"/>	techie-app-server	i-0c3ba4825d2255df9	Stopped	t2.micro	-	No alarms	+	us-east-1a
<input type="checkbox"/>	vprofile-mc01	i-09306ce4a87ee3534	Running	t2.micro	2/2 checks passed	No alarms	+	us-east-1e
<input type="checkbox"/>	vprofile-rmq01	i-051eccf094f5f7611	Running	t2.micro	2/2 checks passed	No alarms	+	us-east-1e
<input type="checkbox"/>	vprofile-app	i-0e0dfad5a4fc06653	Initializing	t2.micro	-	No alarms	+	us-east-1e

By ASG

**Note:** If you want to delete the entire project, then first delete autoscaling group > Launch Configurations > Target Groups > Load Balancer > Instances > Keypairs & Security Groups

If You don't delete autoscaling first, then it will go on launching new instances when you terminate the instance

**Congratulations**  
**you have successfully deployed the java**  
**application with ELB & Autoscaling..!**

**~~~THANK YOU~~~**