

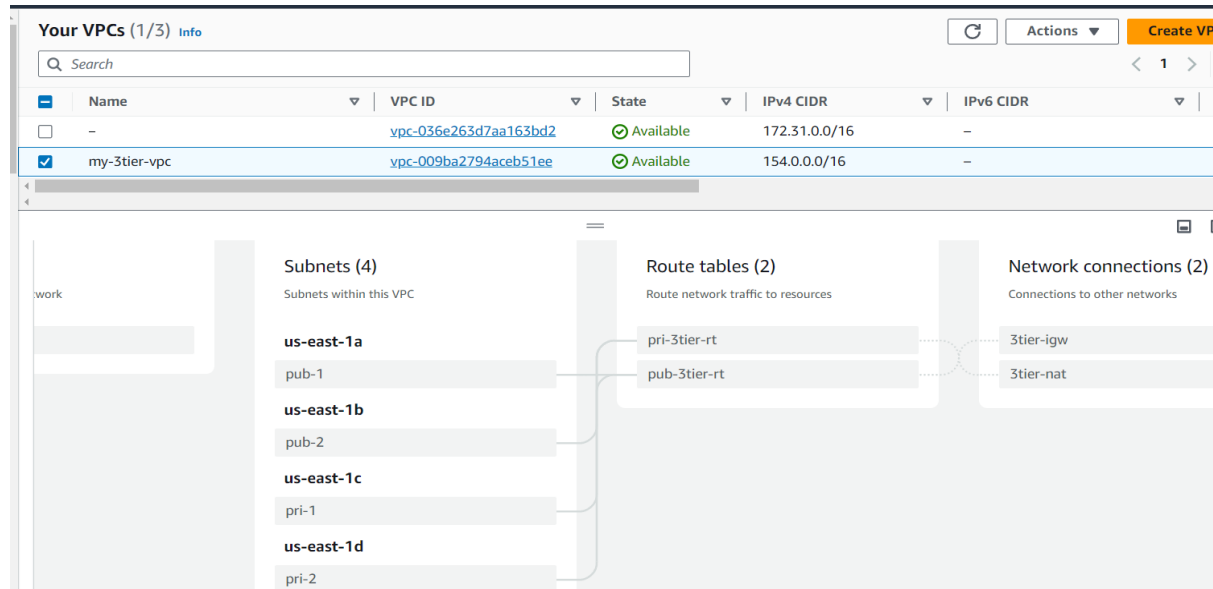
3-TIER-ARCHITECTURE USING AWS IMAGE

Create VPC

Name – my-3tier-vpc

Public subnet – 2, Private subnet -2

NAT gateway – both private subnets



Created private RDS

Create database (RDS service)

Standard create

Mariadb Engine version – mariadb10.11.6

Free tier

DB name – database-1

Username – admin

Password – 12345678

VPC – myvpc

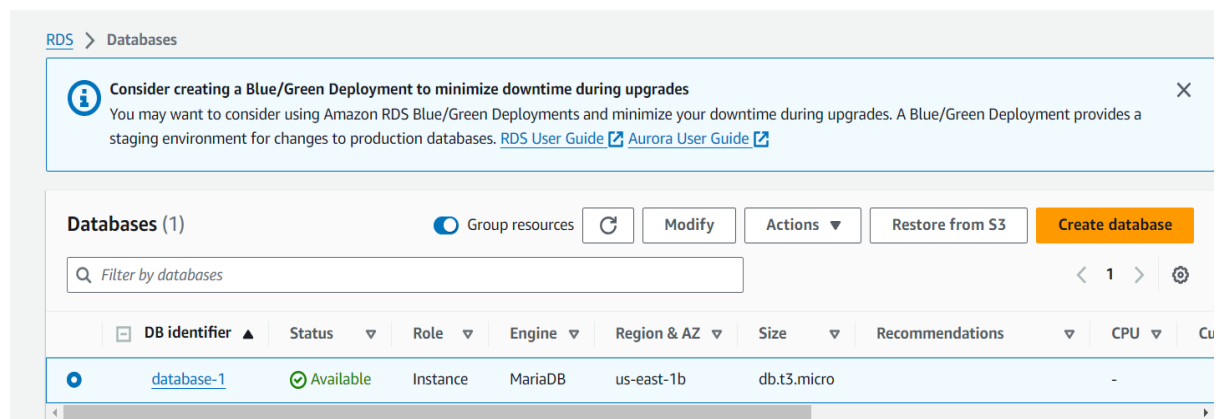
Public access – no

A.Z. – no preference

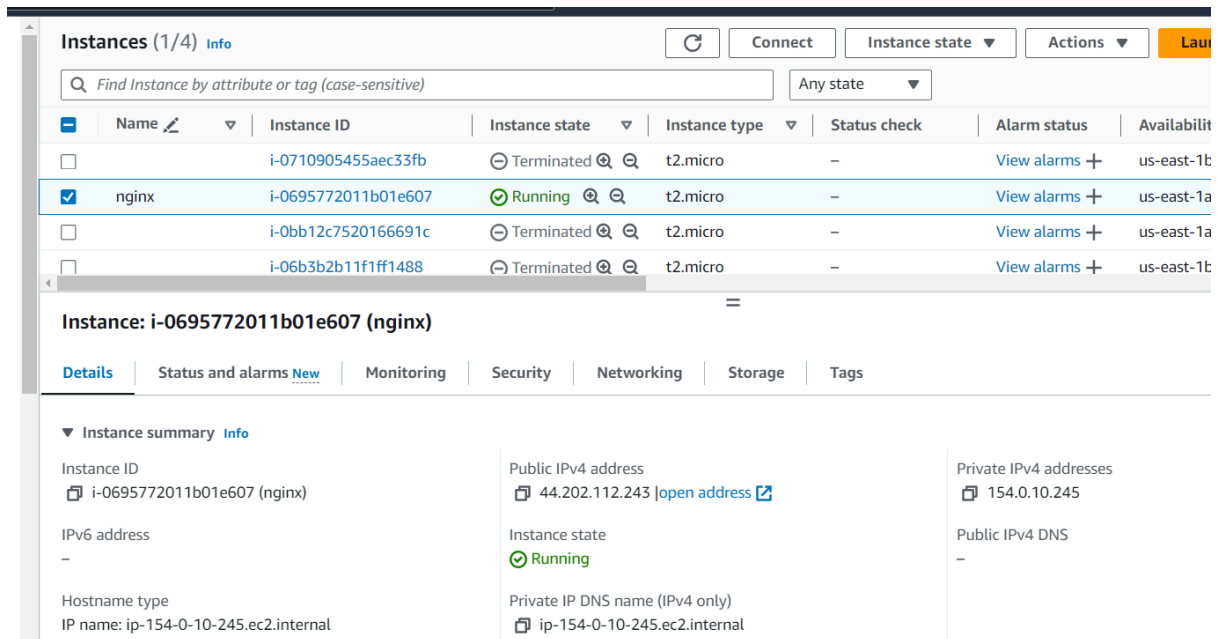
Create database

Edit security group of database

Add 3306 port in it and save



Launch 1 public instance for nginx
VPC – myvpc Subnet – 1pubsub
Auto-assign public IP – enable
Security group – add 80 port
User data
#!/bin/bash
sudo -i
yum install nginx -y
launch



Instances (1/4) Info

Find Instance by attribute or tag (case-sensitive) Any state

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability
	i-0710905455aec33fb	Terminated	t2.micro	–	View alarms +	us-east-1b
nginx	i-0695772011b01e607	Running	t2.micro	–	View alarms +	us-east-1a
	i-0bb12c7520166691c	Terminated	t2.micro	–	View alarms +	us-east-1a
	i-06b3b2b11f1ff1488	Terminated	t2.micro	–	View alarms +	us-east-1b

Instance: i-0695772011b01e607 (nginx)

Details Status and alarms New Monitoring Security Networking Storage Tags

Instance summary Info

Instance ID i-0695772011b01e607 (nginx)	Public IPv4 address 44.202.112.243 open address	Private IPv4 addresses 154.0.10.245
IPv6 address –	Instance state Running	Public IPv4 DNS –
Hostname type IP name: ip-154-0-10-245.ec2.internal	Private IP DNS name (IPv4 only) ip-154-0-10-245.ec2.internal	

launch 1 private instance for tomcat
VPC – myvpc
Subnet – 1prisub (2a)
Auto-assign public IP – disable
Security group add 8080 port
User data
#!/bin/bash
sudo -i
yum install java -y
yum install elinks -y
mkdir /opt/tomcat
curl -O https://dldcn.apache.org/tomcat/tomcat-8/v8.5.99/bin/apache-tomcat-8.5.99.tar.gz
tar -xvf apache-tomcat-8.5.99.tar.gz -C /opt/tomcat
cd /opt/tomcat/apache-tomcat-8.5.99/webapps
curl -O https://s3-us-west-2.amazonaws.com/studentapi-cit/student.war
cd ../lib
curl -O https://s3-us-west-2.amazonaws.com/studentapi-cit/mysql-connector.jar
launch instance

Instances (1/6) Info

Find Instance by attribute or tag (case-sensitive) Any state

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability
	i-0d86fa21228a15abf	Terminated	t2.micro	-	View alarms +	us-east-1c
tomcat	i-0f83f1788e5737c5b	Pending	t2.micro	-	View alarms +	us-east-1c
	i-0710905455aec33fb	Terminated	t2.micro	-	View alarms +	us-east-1b
nginx	i-0695772011b01e607	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a

Instance: i-0f83f1788e5737c5b (tomcat)

Details Status and alarms New Monitoring Security Networking Storage Tags

Instance summary Info

Instance ID i-0f83f1788e5737c5b (tomcat)	Public IPv4 address -	Private IPv4 addresses 154.0.179.95
IPv6 address -	Instance state Pending	Public IPv4 DNS -
Hostname type IP name: ip-154-0-179-95.ec2.internal	Private IP DNS name (IPv4 only) ip-154-0-179-95.ec2.internal	

launch 2 private instance for mariadb
VPC – myvpc
Subnet – 2prisub (2b)
Auto-assign public IP – disable
Security group add – 3306 port
User data
#!/bin/bash
sudo -i
yum install mariadb105-server -y
systemctl start mariadb
systemctl enable mariadb
launch instance

Instances (1/7) Info

Find Instance by attribute or tag (case-sensitive) Any state

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability
database	i-068b5d4acb00174	Running	t2.micro	Initializing	View alarms +	us-east-1d
	i-0d86fa21228a15abf	Terminated	t2.micro	-	View alarms +	us-east-1c
tomcat	i-0f83f1788e5737c5b	Running	t2.micro	Initializing	View alarms +	us-east-1c
	i-0710905455aec33fb	Terminated	t2.micro	-	View alarms +	us-east-1b

Instance: i-068b5d4acb00174 (database)

Details Status and alarms New Monitoring Security Networking Storage Tags

Instance summary Info

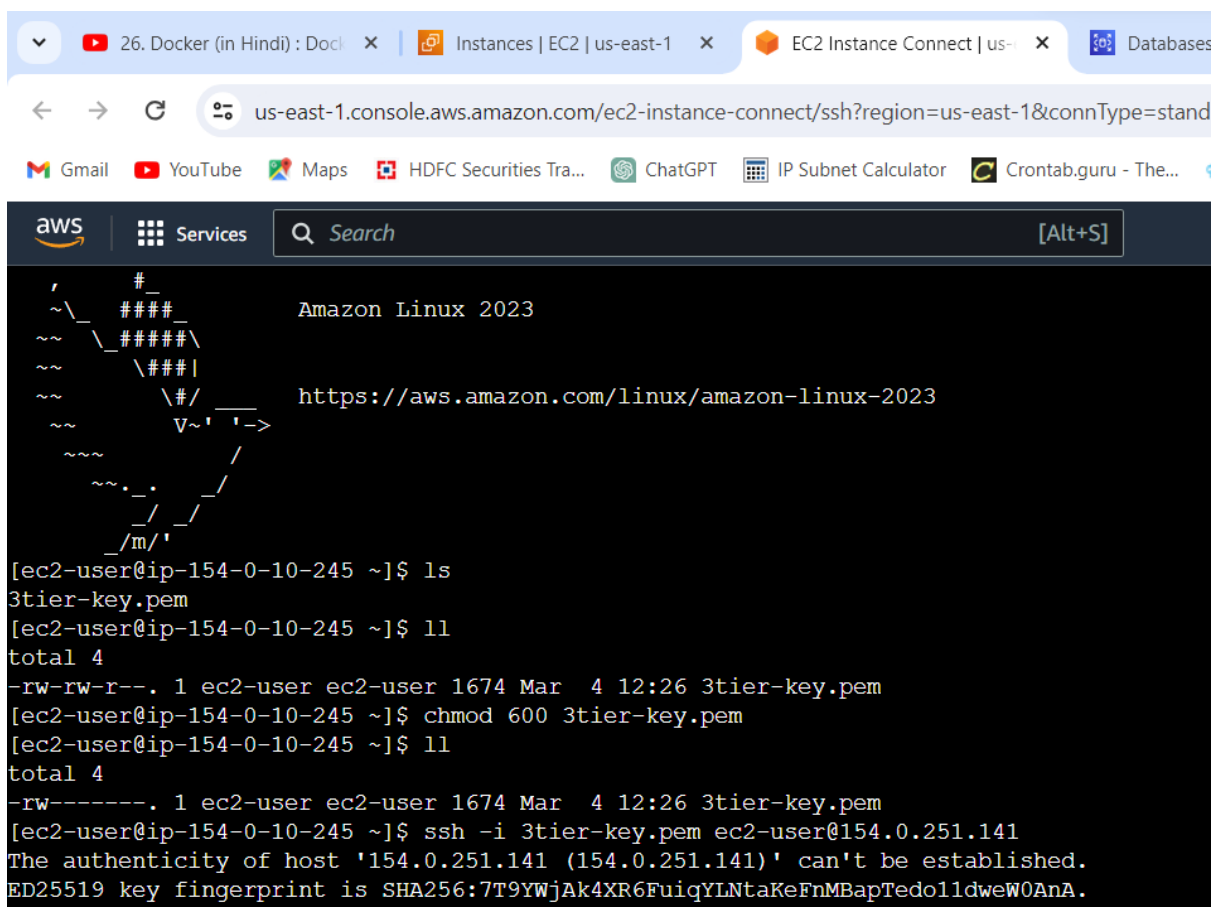
Instance ID i-068b5d4acb00174 (database)	Public IPv4 address -	Private IPv4 addresses 154.0.251.141
IPv6 address -	Instance state Running	Public IPv4 DNS -
Hostname type IP name: ip-154-0-251-141.ec2.internal	Private IP DNS name (IPv4 only) ip-154-0-251-141.ec2.internal	

Now, open cmd
cd Downloads/

```
scp -i private-key-of-nginx private-key-of-mariadb ec2-user@publicIPofnginx:/home/ec2-user/  
(private key of mariadb will get copied to nginx instance)
```

```
C:\Users\91866\Downloads>scp -i 3tier-key.pem 3tier-key.pem ec2-user@44.202.112.243:/home/ec2-user/
The authenticity of host '44.202.112.243 (44.202.112.243)' can't be established.
ED25519 key fingerprint is SHA256:FNYponeEt98oLOkmjaDUUMNZU2ThMIWVL4F09Qt4jh0.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])?
Warning: Permanently added '44.202.112.243' (ED25519) to the list of known hosts.
3tier-key.pem 100% 1674 1.9KB/s 00:00
C:\Users\91866\Downloads>
```

```
Connect to nginx instance
ls (private key will be present)
chmod 600 private-key-of-mariadb
```





```
ssh -i key ec2-user@privatePofmaridbinstance
yes
(you will login in mariadb instance)
```

```
total 4
-rw-----. 1 ec2-user ec2-user 1674 Mar  4 12:26 3tier-key.pem
[ec2-user@ip-154-0-10-245 ~]$ ssh -i 3tier-key.pem ec2-user@154.0.251.141
The authenticity of host '154.0.251.141 (154.0.251.141)' can't be established.
ED25519 key fingerprint is SHA256:7T9YWjAk4XR6FuiqYLNtaKeFnMBapTedolldweW0AnA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '154.0.251.141' (ED25519) to the list of known hosts.

      #_
    ~\  #####_      Amazon Linux 2023
    ~~ \_#####\
    ~~   \###|
    ~~     \#/      https://aws.amazon.com/linux/amazon-linux-2023
    ~~       V~' '->
    ~~~
    ~~~_._
    ~~~/_/_/_/_/_/_
    ~~~/_/m/'

[ec2-user@ip-154-0-251-141 ~]$ sudo -i
```

```
aws   Services  [Alt+S]
```

```
[root@ip-154-0-251-141 ~]# mysql -h database-1.c14oiegg0gzy.us-east-1.rds.amazonaws.com -u admin -p12345678
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 24
Server version: 10.11.7-MariaDB-log managed by https://aws.amazon.com/rds/

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 |
| innodb |
| mysql |
| performance_schema |
| sys |
+-----+
5 rows in set (0.002 sec)

MariaDB [(none)]> create database studentapp;
Query OK, 1 row affected (0.004 sec)
```



```

maxTotal="500" maxIdle="30" maxWaitMillis="1000"
username="admin" password="12345678" driverClassName="com.mysql.jdbc.Driver"
url="jdbc:mysql://endpoint:3306/studentapp?useUnicode=yes&characterEncoding=utf8"/>
(change endpoint to RDS endpoint)
:wq

```

```

6 The ASF licenses this file to You under the Apache License, Version 2.0
7 (the "License"); you may not use this file except in compliance with
8 the License. You may obtain a copy of the License at
9
10 http://www.apache.org/licenses/LICENSE-2.0
11
12 Unless required by applicable law or agreed to in writing, software
13 distributed under the License is distributed on an "AS IS" BASIS,
14 WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
15 See the License for the specific language governing permissions and
16 limitations under the License.
17
18 <!-- The contents of this file will be loaded for each web application -->
19 <Context>
20 <Resource name="jdbc/TestDB" auth="Container" type="javax.sql.DataSource"
21 maxTotal="500" maxIdle="30" maxWaitMillis="1000"
22 username="admin" password="12345678" driverClassName="com.mysql.jdbc.Driver"
23 url="jdbc:mysql://database-1.c14oiegg0gzy.us-east-1.rds.amazonaws.com:3306/studentapp?useUnicode=yes&characterEncoding=utf8"/>
24
25 <!-- Default set of monitored resources. If one of these changes, the -->
26 <!-- web application will be reloaded. -->
27 <WatchedResource>WEB-INF/web.xml</WatchedResource>
28 <WatchedResource>${catalina.base}/conf/web.xml</WatchedResource>
29
30 </Context>

```

```

cd ../bin
./catalina start

```

```

catalina-storeconfig.jar el-api.jar jsp-api.jar tomcat-coyote.jar tomcat-i18n-fr.jar tomcat-i18n-zh-CN.jar
[root@ip-154-0-179-95 lib]# cd ../conf/
[root@ip-154-0-179-95 conf]# vim context.xml
[root@ip-154-0-179-95 conf]# cd ../bin/
[root@ip-154-0-179-95 bin]# ls
bootstrap.jar catalina.sh commons-daemon-native.tar.gz configtest.sh digest.sh shutdown.bat startup.sh
catalina-tasks.xml ciphers.bat commons-daemon.jar daemon.sh setclasspath.bat shutdown.sh tomcat-juli.jar
catalina.bat ciphers.sh configtest.bat digest.bat setclasspath.sh startup.bat tomcat-native.tar.gz
[root@ip-154-0-179-95 bin]# ./catalina.sh start
Using CATALINA_BASE: /opt/tomcat/apache-tomcat-8.5.99
Using CATALINA_HOME: /opt/tomcat/apache-tomcat-8.5.99
Using CATALINA_TMPDIR: /opt/tomcat/apache-tomcat-8.5.99/temp
Using JRE_HOME: /usr
Using CLASSPATH: /opt/tomcat/apache-tomcat-8.5.99/bin/bootstrap.jar:/opt/tomcat/apache-tomcat-8.5.99/bin/tomcat-juli.jar
Using CATALINA_OPTS:
Tomcat started.
[root@ip-154-0-179-95 bin]#

```

elinks (used to check studentapp page in CLI mode)
 enter private ip of tomcat:8080/student/
 (student app page will appear)

Student ID	StudentName	Student Addr	Student Age	Student Qualification	Student Percentage	Student Year Passed	Edit	Delete
1	Rinki	Pune	23	BE	9.05	2022	edit	delete

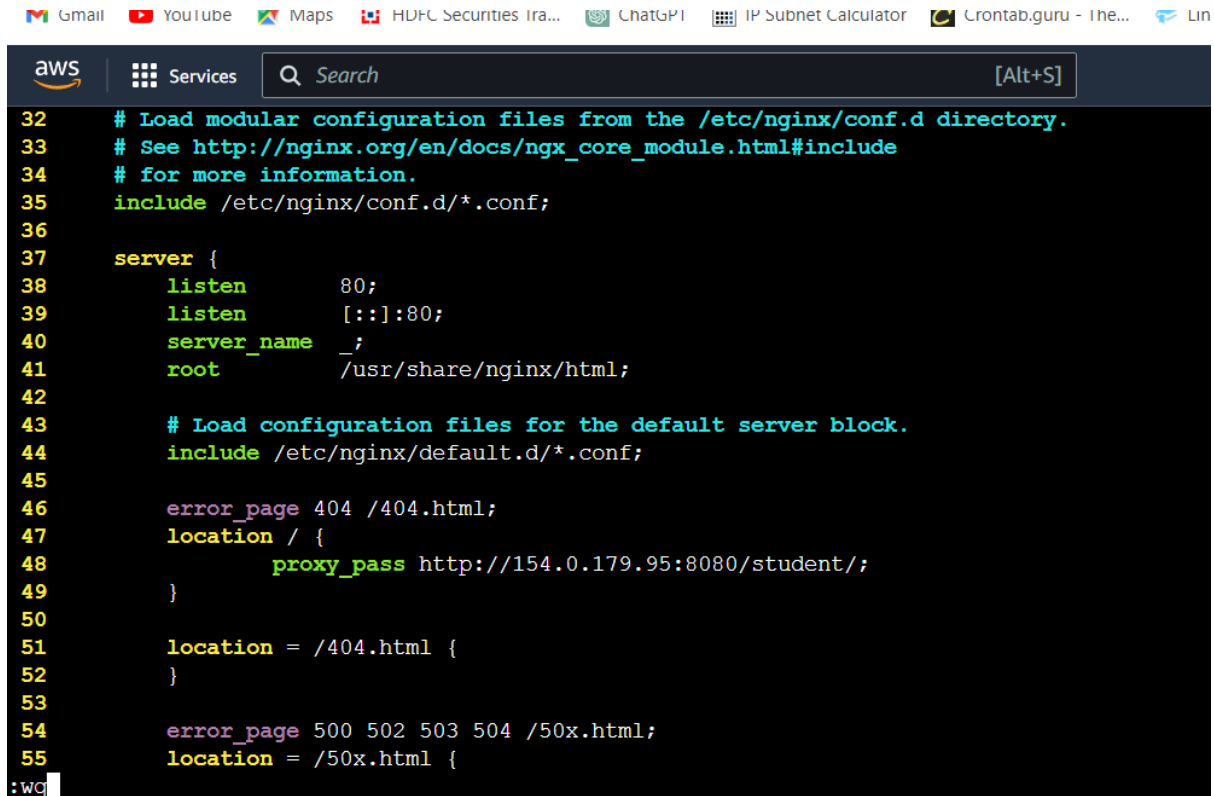
```

Enter data & save (it will work)
exit
exit (now in nginx instance)
sudo -i
vim /etc/nginx/nginx.conf
:set nu

```

(enter below data in line 47 in between error and location)

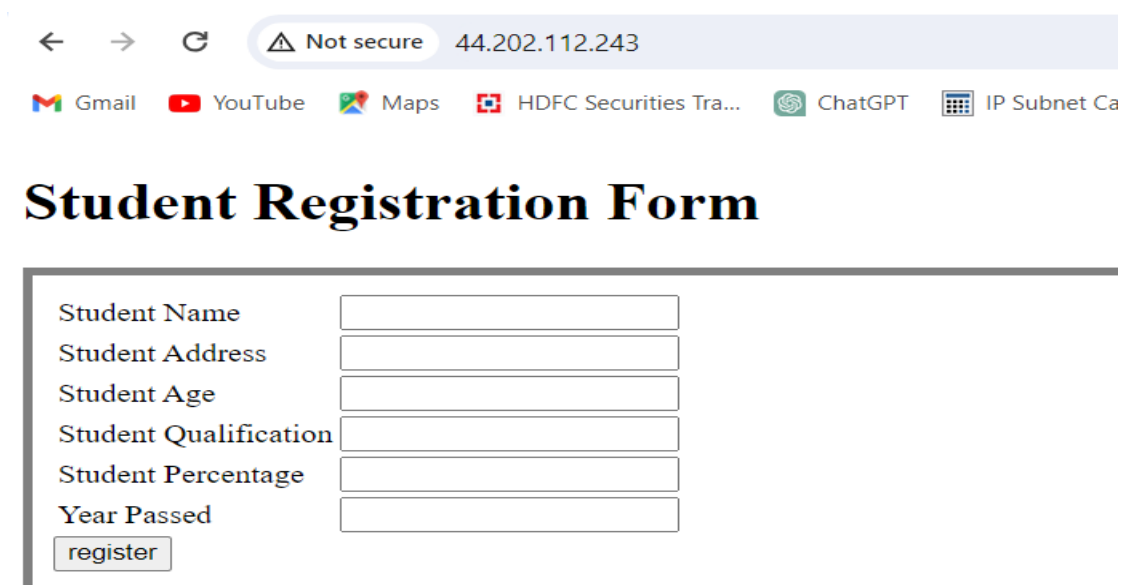
```
location / {  
proxy_pass http://privateIpofTomcat:8080/student/;  
}  
:wq
```



```
aws Services Search [Alt+S]  
32 # Load modular configuration files from the /etc/nginx/conf.d directory.  
33 # See http://nginx.org/en/docs/nginx_core_module.html#include  
34 # for more information.  
35 include /etc/nginx/conf.d/*.conf;  
36  
37 server {  
38     listen      80;  
39     listen      [::]:80;  
40     server_name _;  
41     root        /usr/share/nginx/html;  
42  
43     # Load configuration files for the default server block.  
44     include /etc/nginx/default.d/*.conf;  
45  
46     error_page 404 /404.html;  
47     location / {  
48         proxy_pass http://154.0.179.95:8080/student/;  
49     }  
50  
51     location = /404.html {  
52     }  
53  
54     error_page 500 502 503 504 /50x.html;  
55     location = /50x.html {  
:wq
```

systemctl restart nginx

Now, hit public IP of nginx on chrome same student app page will be shown, you can enter data, edit or delete it



← → ↻ ⚠ Not secure 44.202.112.243

Gmail YouTube Maps HDFC Securities Tra... ChatGPT IP Subnet Ca

Student Registration Form

Student Name	<input type="text"/>
Student Address	<input type="text"/>
Student Age	<input type="text"/>
Student Qualification	<input type="text"/>
Student Percentage	<input type="text"/>
Year Passed	<input type="text"/>

When you register data both tomcat inserted data & nginx inserted data will be shown to you

← → ↻ Not secure 44.202.112.243/viewStudents

[Gmail](#)
[YouTube](#)
[Maps](#)
[HDFC Securities Tra...](#)
[ChatGPT](#)
[IP Subnet Calculator](#)
[Crontab.guru - The...](#)
[Linux-Notes-Cloudb...](#)
[Netflix](#)
[Student/Parent Portal](#)
[AWS Policy Generator](#)
[Rinki Shrivastava | LL...](#)

[Register Student](#)

Students List

Student ID	StudentName	Student Addr	Student Age	Student Qualification	Student Percentage	Student Year Passed	Edit	Delete
1	Rinki	Pune	23	BE	9.05	2022	edit	delete
2	preeti	nashik	24	masters	67	2000	edit	delete

You can also stop the mariadb instance or remove the NAT connection for more security.
You can delete the previous created tomcat instance.

Below are the steps to make nginx instance secure

Go to route53 service
Create hosted zone
Domain name – rinki.cloud
Type – public hosted zone
Create

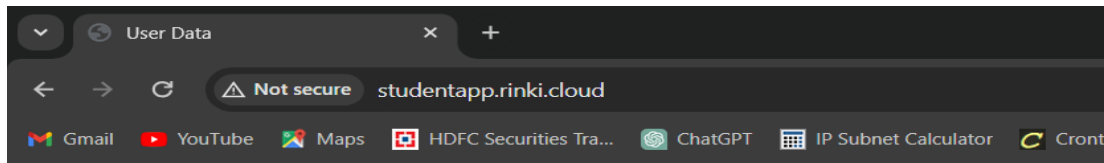
The screenshot shows the AWS Route 53 console for a public hosted zone named 'rinki.cloud'. The 'Hosted zone details' section is visible, showing the zone is in the 'Public' state. Below this, the 'Records (4)' tab is selected, displaying a table of DNS records:

Record	Type	Routing	Simple	Differ...	Alias	Value/Route traffic to	TTL (s...)	Health ...
rinki.cloud	NS	Simple	-	No	ns-1554.awsdns-02.co.uk, ns-91.awsdns-11.com, ns-1097.awsdns-09.org, ns-921.awsdns-51.net	172800	-	
rinki.cloud	SOA	Simple	-	No	ns-1554.awsdns-02.co.uk, a...	900	-	
_c5ecc3b...	CNAME	Simple	-	No	_52b9b09134b267d331e71...	300	-	
image.rin...	A	Simple	-	Yes	s3-website-us-east-1.amazo...	-	-	

Using domain name and not secure
Create record
Record name – studentapp
Value – public ip of nginx instance
Create

The screenshot shows the AWS Route 53 console with the 'Records (1/5)' tab selected. The 'Create record' button is highlighted. The 'Record name' field is set to 'studentapp' and the 'Record type' is set to 'A'. The 'Value' field is set to '44.202.112.243'. The 'TTL (seconds)' is set to '300' and the 'Routing policy' is set to 'Simple routing'. The 'Create record' button is highlighted in orange.

Hit the domain name “studentapp.rinki.cloud” on chrome tap
It will show the same student app page



Student Registration Form

Student Name	<input type="text"/>
Student Address	<input type="text"/>
Student Age	<input type="text"/>
Student Qualification	<input type="text"/>
Student Percentage	<input type="text"/>
Year Passed	<input type="text"/>
<input type="button" value="register"/>	

Now to make secure & with domain name

Go to ACM service

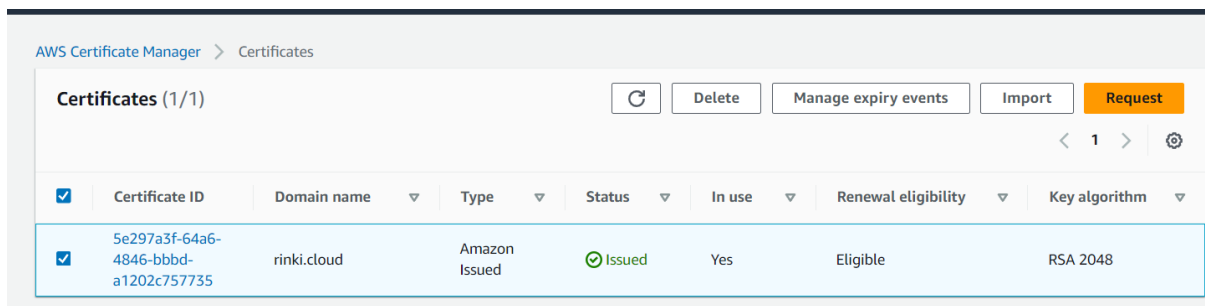
Request certificate

Request public certificate

Domain name – rinki.cloud

Request

When certificate gets issued use it



Go to cloudfront service

Origin domain – paste the public IP of nginx instance

ec2-44-202-112-243.compute-1.amazonaws.com

Protocol – HTTP only

Cache policy – CachingOptimized

Do not enable security protections

Alternate domain name (CNAME)

rinki.cloud

Custom SSL certificate

Select the certificate which you created in ACM service

Create distribution

Step for 3-tier-architecture created by using auto scaling group with load balancer –

Select tomcat instance – action – image & templates – create image

Create

Go to launch template

Create launch template

Name – tomcat-3tier-tmp

Select tomcat created image from My AMIs

Instance type – t2.micro

Key pair

Subnet – do not specify

Create security group

Tomcat-sg

Description – tomcat

Add – 8080 port

User data









```
#!/bin/bash
```

```
sudo -i
```

```
cd /opt/tomcat/apache-tomcat/bin
```

```
bash catalina.sh start
```

launch template

	lt-0fd6e726f79468026	tomcat-3tier-tmp	1	1	2024-03-04T14:08:36.000Z	arn:aws:iam::997825581095:user/rinki
tomcat-3tier-tmp (lt-0fd6e726f79468026)  						
<div><div>Version 1 (Default) ▼</div><div>Description -</div><div>Date created  2024-03-04T14:08:36.000Z</div><div>Created by  arn:aws:iam::997825581095:user/rinki</div></div>						
<div><div>Instance details</div><div>Storage</div><div>Resource tags</div><div>Network interfaces</div><div>Advanced details</div></div>						
AMI ID  ami-04ae349fecf833f81		Instance type  t2.micro		Availability Zone -		Key pair name  3tier-key

create auto scaling group

name – tomcat-asg

template – tomcat-temp (select created template)

VPC – my-3tier-vpc

A.Z. – both private sub A.Z.

Next

Attach to new load balancer

Application load balancer

Name – tomcat-alb

Internal

Port – 8080

Create a target group

Next

Desired capacity – 1

Minimum capacity – 1

Maximum capacity – 5

(you can set it as per you requirement)

Target tracking scaling policy

Cpu utilization

Target value – 30

Instance warmup – 60 sec

Next

Next

Tag – name – tomcat

Next

Create ASG

(here automatically 1 target group , 1 load balancer will get created & 1 instance will automatically get launched)

EC2 > Auto Scaling groups

Auto Scaling groups (1/1) Info

Launch configurations

Launch templates

Actions

Create Auto Scaling group

Search your Auto Scaling groups

< 1 >

<input checked="" type="checkbox"/>	Name	Launch template/configuration	Instances	Status	Desired capacity	Min
<input checked="" type="checkbox"/>	tomcat-asg	tomcat-3tier-tmp Version Default	1	-	1	1

Auto Scaling group: tomcat-asg

Edit

Group details

Auto Scaling group name tomcat-asg	Desired capacity 1	Desired capacity type Units (number of instances)	Amazon Resource Name (ARN) arn:aws:autoscaling:us-east-1:997825581095:autoScalingGroup:f4252feb-5abd-49db-b1ab-e7a85ba765b5:autoScalingGroupName/tomcat-asg
Date created Mon Mar 04 2024 19:46:08 GMT+0530 (India Standard Time)	Minimum capacity 1	Status -	
	Maximum capacity 5		

Load balancers (1/1)

Actions

Create load balancer

Filter load balancers

< 1 >

<input checked="" type="checkbox"/>	Name	DNS name	State	VPC ID	Availability Zones	Type
<input checked="" type="checkbox"/>	tomcat-alb	internal-tomcat-alb-4035...	Provisioning...	vpc-009ba2794aceb5...	2 Availability Zones	application

Load balancer: tomcat-alb

×

Details

Listeners and rules

Network mapping

Resource map - new

Security

Monitoring

Integrations

Attributes

Tags

Details

Load balancer type Application	Status Provisioning	VPC vpc-009ba2794aceb51ee	IP address type IPv4
Scheme Internal	Hosted zone Z35SXDOTRQ7X7K	Availability Zones subnet-0c35e5ea5c0745a96 us-east-1d (use1-az1)	Date created March 4, 2024, 19:46 (UTC+05:30)

EC2 > Target groups

Target groups (1/1) [Info](#)

[Refresh](#) [Actions](#) [Create target group](#)

<input checked="" type="checkbox"/>	Name	ARN	Port	Protocol	Target type	Load balancer
<input checked="" type="checkbox"/>	tomcat-tg	arn:aws:elasticloadbalancing:us-east-1:997825581095:targetgroup/tomcat-tg/8222e96269300534	8080	HTTP	Instance	tomcat-alb

Target group: tomcat-tg

[Details](#) [Targets](#) [Monitoring](#) [Health checks](#) [Attributes](#) [Tags](#)

Details

[arn:aws:elasticloadbalancing:us-east-1:997825581095:targetgroup/tomcat-tg/8222e96269300534](#)

Target type Instance	Protocol : Port HTTP: 8080	Protocol version HTTP1	VPC vpc-009ba2794aceb51ee
IP address type IPv4	Load balancer tomcat-alb		

Also 1 instance will get launched

Instances (1/4) [Info](#)

[Any state](#)

[Refresh](#) [Connect](#) [Instance state](#) [Actions](#) [Launch](#)

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability
<input type="checkbox"/>	tomcat	i-0f83f1788e5737c5b	Running	t2.micro	2/2 checks passed	View alarms	us-east-1c
<input checked="" type="checkbox"/>		i-03b0a5d4be77c6400	Running	t2.micro	Initializing	View alarms	us-east-1c
<input type="checkbox"/>	nginx	i-0695772011b01e607	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a
<input type="checkbox"/>	database	i-068b5d4acbbe00174	Running	t2.micro	2/2 checks passed	View alarms	us-east-1d

Instance: i-03b0a5d4be77c6400

[Details](#) [Status and alarms](#) [Monitoring](#) [Security](#) [Networking](#) [Storage](#) [Tags](#)

Instance summary

Instance ID i-03b0a5d4be77c6400	Public IPv4 address -	Private IPv4 addresses 154.0.151.97
IPv6 address -	Instance state Running	Public IPv4 DNS -
Hostname type IP name: ip-154-0-151-97.ec2.internal	Private IP DNS name (IPv4 only) ip-154-0-151-97.ec2.internal	