VPC

Q1. When to use Elastic IP over Public IP

Elastic IP is used when you are working on long time project and configuration of IP sometimes consumes more time and you don't want your IP to change.

Q2. Valid IP Ranges for LAN, Implication of using Public IP ranges for Private Network.

Valid IP ranges of LAN:

- **192.168.0.0 - 192.168.255.255** (65,536 IP addresses)
- **172.16.0.0 - 172.31.255.255** (1,048,576 IP addresses)
- **10.0.0.0 - 10.255.255.255** (16,777,216 IP addresses)

It is public global addresses that are used in the Internet. A public IP address is an IP address that is used to access the Internet. Public (global) IP addresses are routed on the Internet, unlike private addresses.

The presence of a public IP address on your private network will allow you to organize your own server (VPN, FTP, WEB, etc.), remote access to your computer, video surveillance cameras, and access them from anywhere in the global network.

Q3. List down the things to keep in mind while VPC peering.

- Choosing the proper VPC configuration for your organization's needs
- Choosing a CIDR block for your VPC implementation
- Isolating your VPC environments
- Creating your disaster recovery plan
- Traffic control and security
- Keep your data close
- Determining the NAT instance type
- IAM for your AWS VPC infrastructure

Q4. CIDR of a VPC is 10.0.0.0/16, if the subnet mask is /20 calculate the number of subnets that could be created from the VPC. Also find the number of IP in subnet.

No. of subnets created = 2pow4=16

No. of IPs in a subnet = 2pow12=4096-2(reserved)=4094

Q5. Differentiate between NACL and Security Groups.

Security Group	NACL (Network Access Control List)
It supports only **allow** rules, and by default, all the rules are denied. You cannot deny the rule for establishing a connection.	It supports both **allow and deny** rules, and by default, all the rules are denied. You need to add the rule which you can either allow or deny it.
It is a **stateful** means that any changes made in the inbound rule will be automatically reflected in the outbound rule. For example, If you are allowing an incoming port 80, then you also have to add the outbound rule explicitly.	It is a **stateless** means that any changes made in the inbound rule will not reflect the outbound rule, i.e., you need to add the outbound rule separately. For example, if you add an inbound rule port number 80, then you also have to explicitly add the outbound rule.
It is associated with an EC2 instance.	It is associated with a subnet.
All the rules are evaluated before deciding whether to allow the traffic.	Rules are evaluated in order, starting from the lowest number.

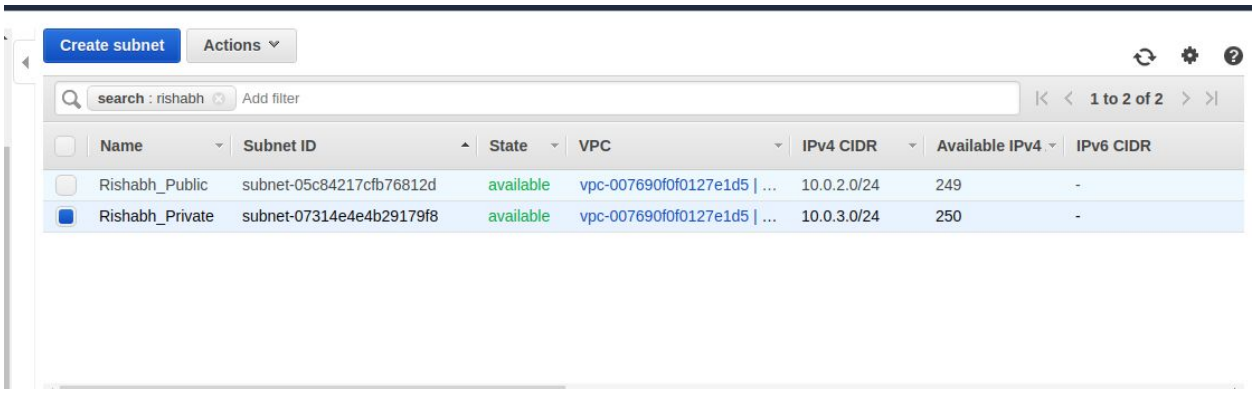
Security Group is applied to an instance only when you specify a security group while launching an instance.	NACL has applied automatically to all the instances which are associated with an instance.
It is the first layer of defense.	It is the second layer of defense.

Q6. Implement a 2-tier vpc with following requirements:

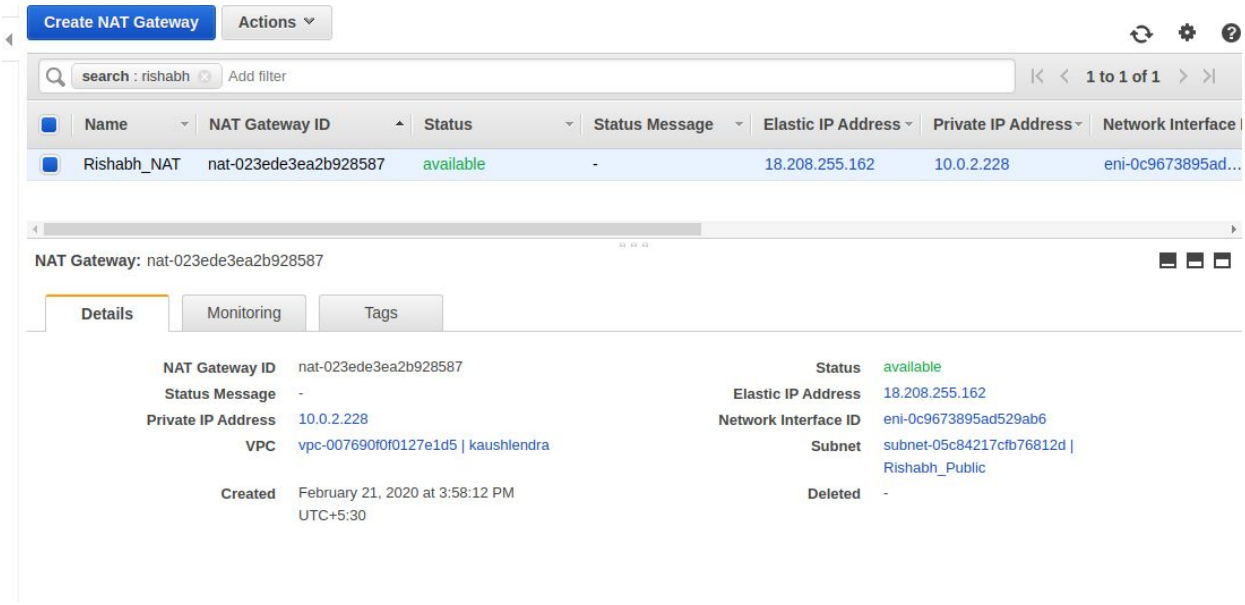
1. Create a private subnet, attach NAT, and host an application server(Tomcat)

2. Create a public subnet, and host a web server(Nginx), also proxypass to Tomcat from Nginx

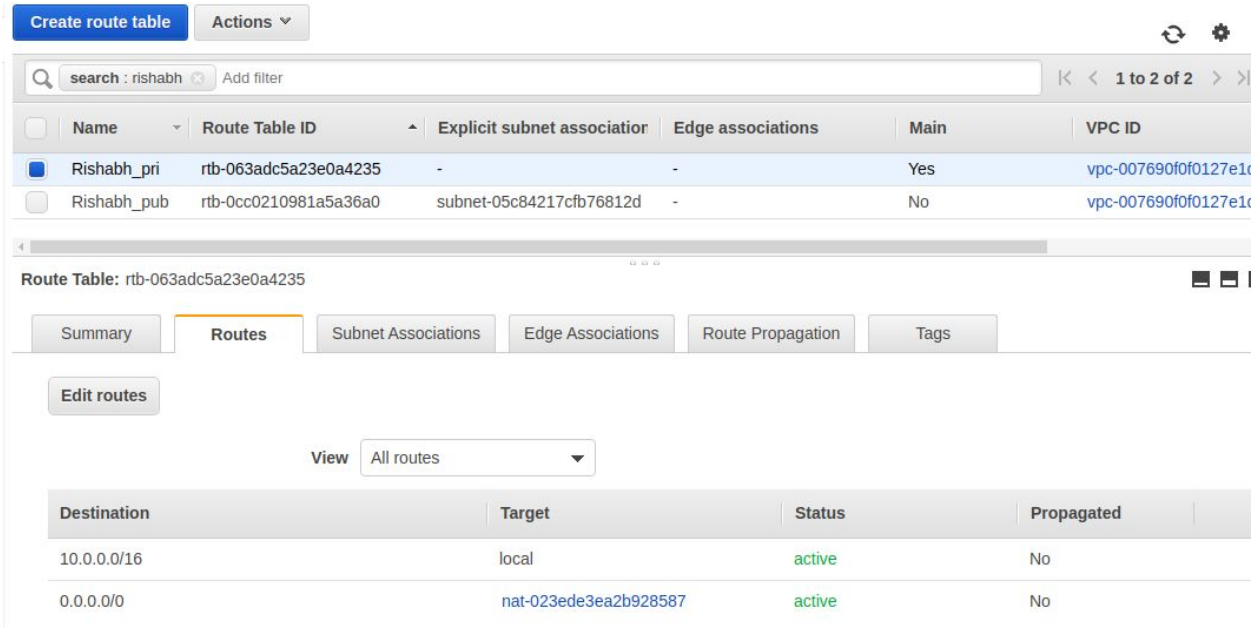
Created two subnets in a VPC



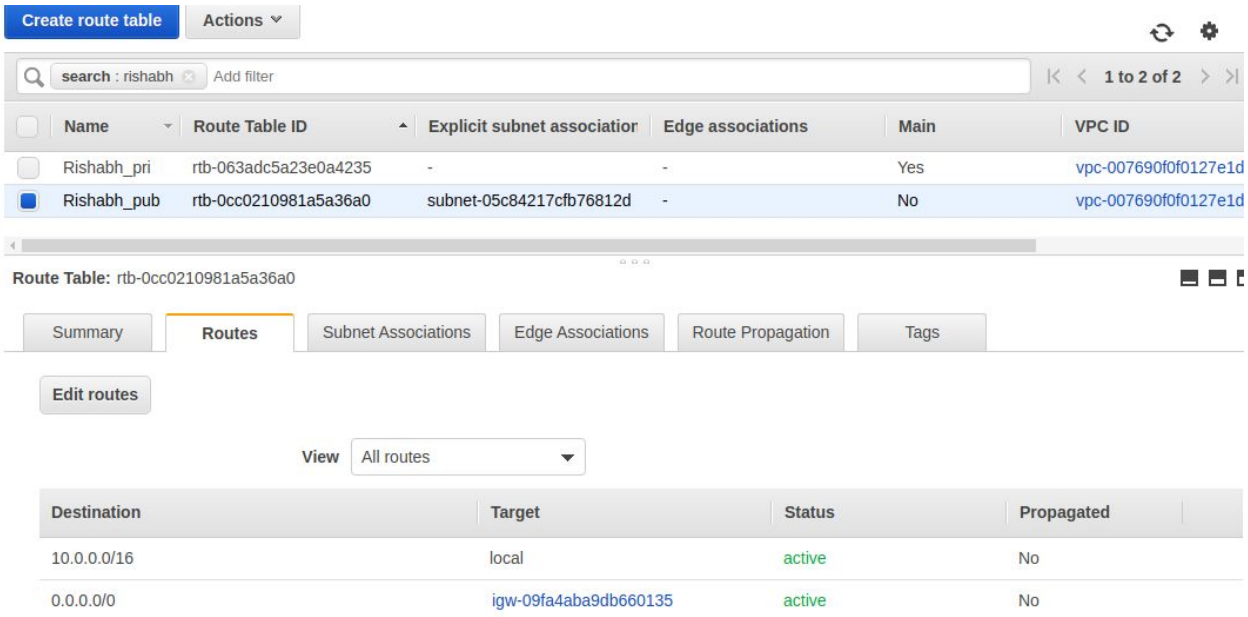
Created a NAT gateway



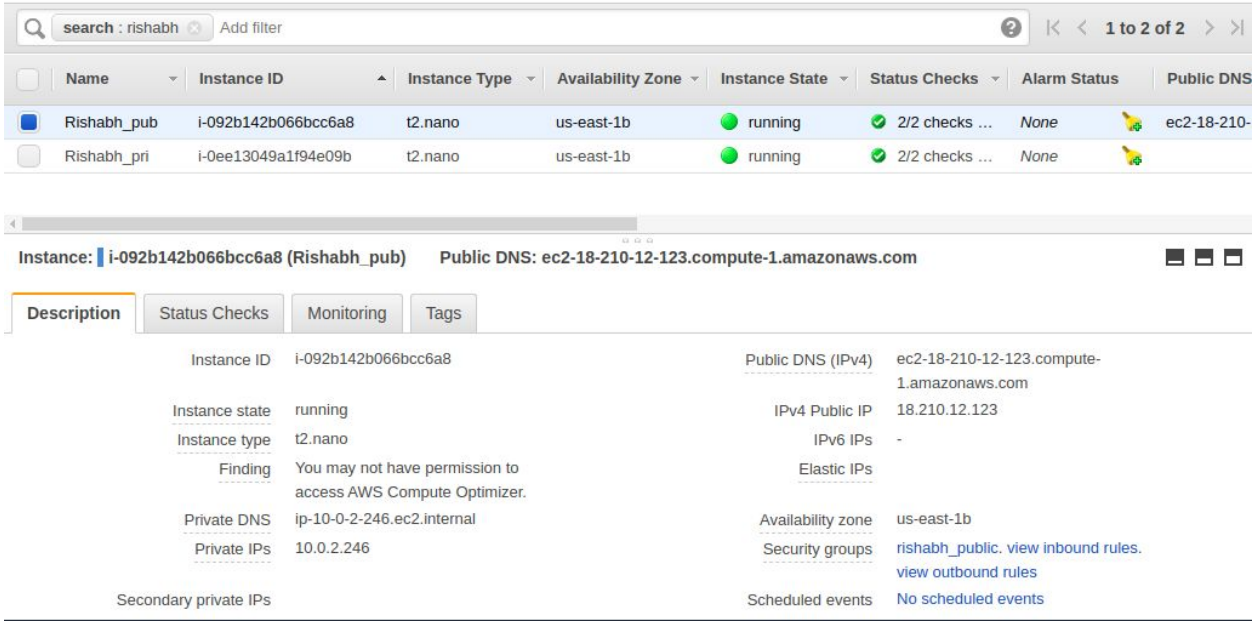
Attached the NAT gateway to private subnet



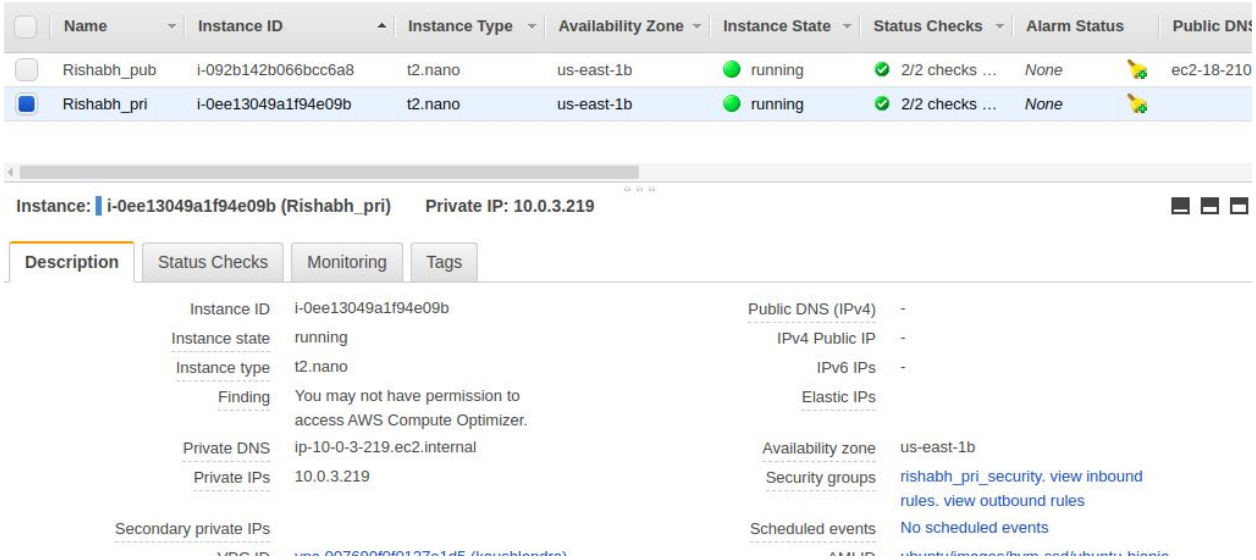
Attached the IGW to public subnet



Public Instance



Private Instance



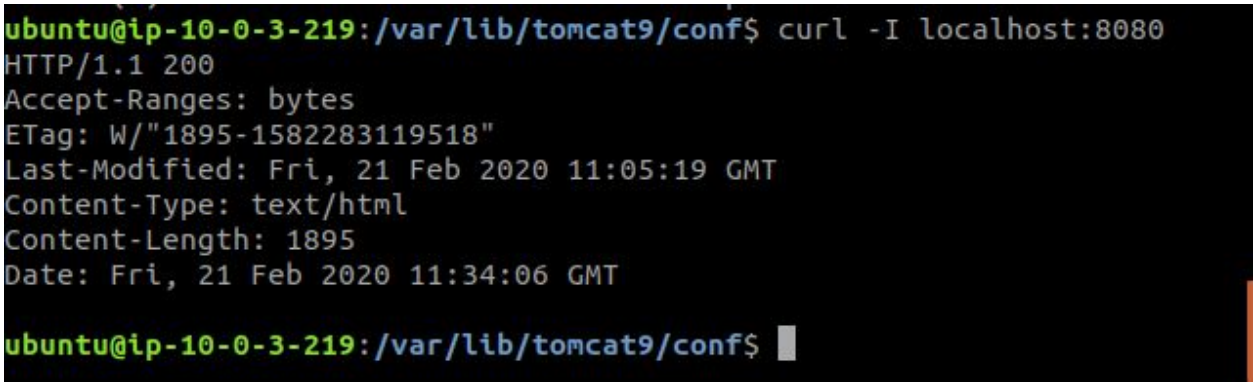
Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS
Rishabh_pub	i-092b142b066bcc6a8	t2.nano	us-east-1b	running	2/2 checks ...	None	ec2-18-210
Rishabh_pri	i-0ee13049a1f94e09b	t2.nano	us-east-1b	running	2/2 checks ...	None	

Instance: i-0ee13049a1f94e09b (Rishabh_pri) Private IP: 10.0.3.219

Description | Status Checks | Monitoring | Tags

Instance ID	i-0ee13049a1f94e09b	Public DNS (IPv4)	-
Instance state	running	IPv4 Public IP	-
Instance type	t2.nano	IPv6 IPs	-
Finding	You may not have permission to access AWS Compute Optimizer.	Elastic IPs	
Private DNS	ip-10-0-3-219.ec2.internal	Availability zone	us-east-1b
Private IPs	10.0.3.219	Security groups	rishabh_pri_security. view inbound rules. view outbound rules
Secondary private IPs		Scheduled events	No scheduled events

Curl on private instance



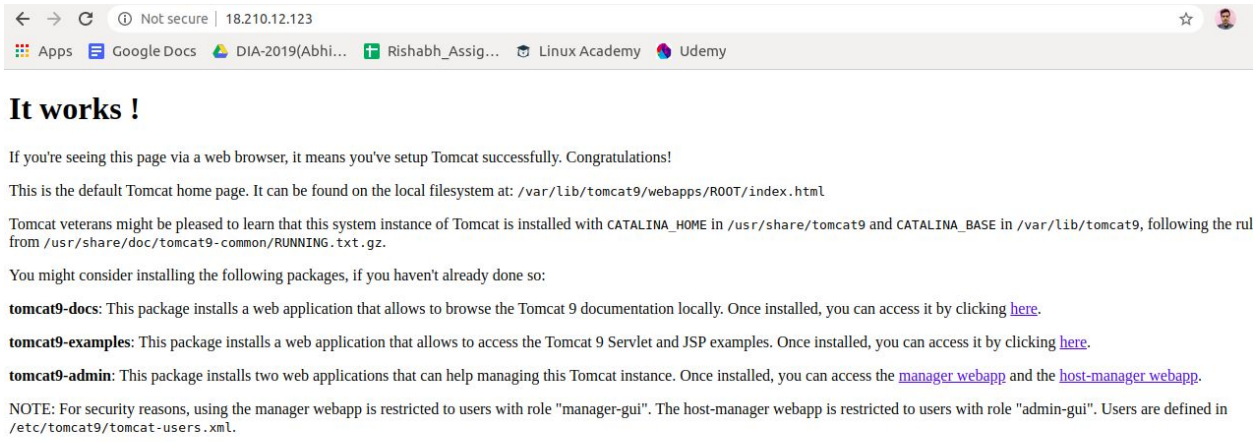
```
ubuntu@ip-10-0-3-219:/var/lib/tomcat9/conf$ curl -I localhost:8080
HTTP/1.1 200
Accept-Ranges: bytes
ETag: W/"1895-1582283119518"
Last-Modified: Fri, 21 Feb 2020 11:05:19 GMT
Content-Type: text/html
Content-Length: 1895
Date: Fri, 21 Feb 2020 11:34:06 GMT

ubuntu@ip-10-0-3-219:/var/lib/tomcat9/conf$
```

Curl on public instance but response of private instance is shown

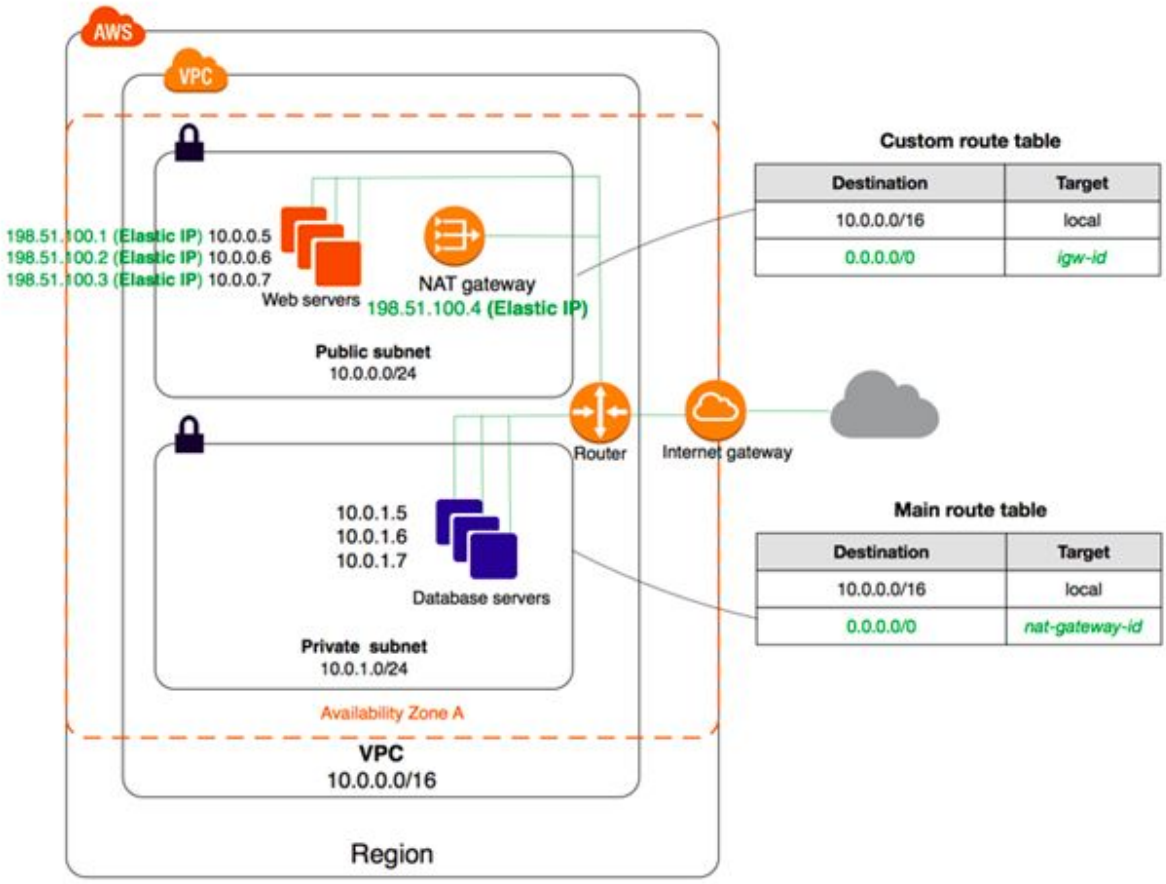
```
ubuntu@ip-10-0-2-246:/var/www/html$ curl -I localhost
HTTP/1.1 200
Server: nginx/1.14.0 (Ubuntu)
Date: Fri, 21 Feb 2020 11:33:38 GMT
Content-Type: text/html
Content-Length: 1895
Connection: keep-alive
Accept-Ranges: bytes
ETag: W/"1895-1582283119518"
Last-Modified: Fri, 21 Feb 2020 11:05:19 GMT

ubuntu@ip-10-0-2-246:/var/www/html$ curl localhost
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
   "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
    <title>Apache Tomcat</title>
</head>

<body>
<h1>It works !</h1>

<p>If you're seeing this page via a web browser, it means you've setup
 Tomcat successfully. Congratulations!</p>

<p>This is the default Tomcat home page. It can be found on the local
filesystem at: <code>/var/lib/tomcat9/webapps/ROOT/index.html</code></
p>

<p>Tomcat veterans might be pleased to learn that this system instance
 of Tomcat is installed with <code>CATALINA_HOME</code> in <code>/usr/
share/tomcat9</code> and <code>CATALINA_BASE</code> in <code>/var/lib/
tomcat9</code>, following the rules from <code>/usr/share/doc/tomcat9-
common/RUNNING.txt.gz</code>.</p>
```

On doing a curl from local system to public subnet, we get the response of tomcat from private subnet

```
rishabh@rishabh:~ $ curl 18.210.12.123
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
   "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
    <title>Apache Tomcat</title>
</head>

<body>
<h1>It works !</h1>

<p>If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!</p>

<p>This is the default Tomcat home page. It can be found on the local filesystem at: <code>/var/lib/tomcat9/webapps/ROOT/index.h

<p>Tomcat veterans might be pleased to learn that this system instance of Tomcat is installed with <code>CATALINA_HOME</code> in
are/tomcat9</code> and <code>CATALINA_BASE</code> in <code>/var/lib/tomcat9</code>, following the rules from <code>/usr/share/do
on/RUNNING.txt.gz</code>.</p>

<p>You might consider installing the following packages, if you haven't already done so:</p>

<p><b>tomcat9-docs</b>: This package installs a web application that allows to browse the Tomcat 9 documentation locally. Once i
can access it by clicking <a href="docs/">here</a>.</p>

<p><b>tomcat9-examples</b>: This package installs a web application that allows to access the Tomcat 9 Servlet and JSP examples.
d, you can access it by clicking <a href="examples/">here</a>.</p>

<p><b>tomcat9-admin</b>: This package installs two web applications that can help managing this Tomcat instance. Once installed,
s the <a href="manager/html">manager webapp</a> and the <a href="host-manager/html">host-manager webapp</a>.</p>

<p>NOTE: For security reasons, using the manager webapp is restricted to users with role "manager-gui". The host-manager webapp
to users with role "admin-gui". Users are defined in <code>/etc/tomcat9/tomcat-users.xml</code>.</p>

</body>
</html>
```



After Implementing this on AWS, create an architecture diagram for this use case.



Note: For hosting Nginx in public subnet, use Elastic IP.