VPC Session

Q1.When to use Elastic IP over Public IP

If we want to host our application in such a manner that even after stopping and restarting our instance, our application is accessed by the same ip as it was accessed before then Elastic IP is used. It can be associated and deassociated with our instances. The elastic IP is reserved for our use only (it is a public IP but it is removed from the public IP pool and is available in the assigned user's pool).

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

Class A : 10.0.0.0 – 10.0.255.255z

Class B : 172.16.0.0 – 172.13.255.255

Class C : 192.168.0.0 – 192.168.255.255

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

To enable flow of traffic b/w multiple VPC's the owner of each VPC must manually set the route in the route table of the VPC that points to the IP address range of other VPC.

If required, update the security group rules of instances so that traffic to and from the peer VPC is not restricted.

If both VPCs are in the same region, you can reference a security group from the peer VPC as a source or

destination for ingress or egress rules in your security group rules.

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.

10.0.0.0/16:

00001010.00000000.00000000.00000000 (In /16, first 2 octets are fixed).

00001010.00000000.00000000.00000000 (In /20, extra 4 bits are borrowed from hosts)

* These extra 4 bits are subnetting bits.

So, total number of subnets = 2^4 (16)

And, total IP'S in each subnet = 2^12 (4096)

Q5. Differentiate between NACL and Security Groups.

Security Groups are stateful while NACL are stateless:

If we allow inbound rule for HTTP at port 8080 is security group, the outbound rule of the same will be allowed automatically. But, in NACL, we have to add the rule explicitly.

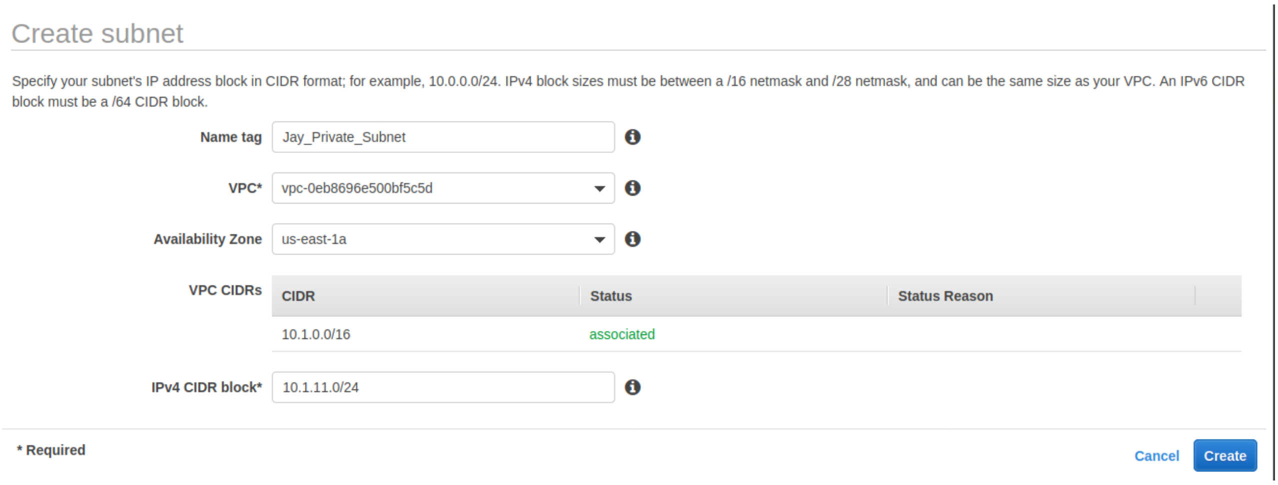
Security groups are for instances, while nacl are for subnets.

SG’s are first layer of defence, and NACL’S are second layer of defence.

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

1.Made a public subnet and private subnet



Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag: Jay_Private_Subnet

VPC*: vpc-0eb8696e500bf5c5d

Availability Zone: us-east-1a

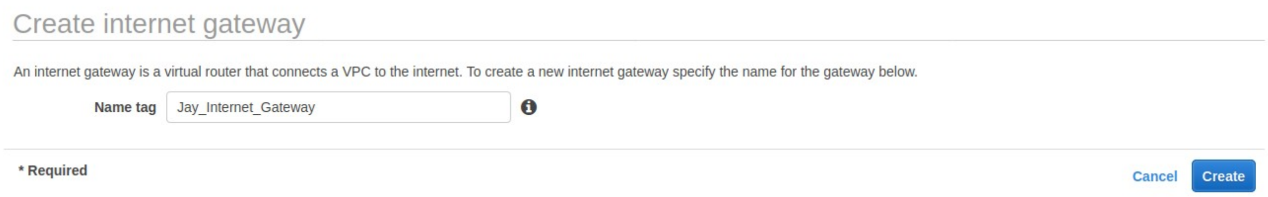
VPC CIDRs:

CIDR	Status	Status Reason
10.1.0.0/16	associated	

IPv4 CIDR block*: 10.1.11.0/24

* Required

2. Made a IGW



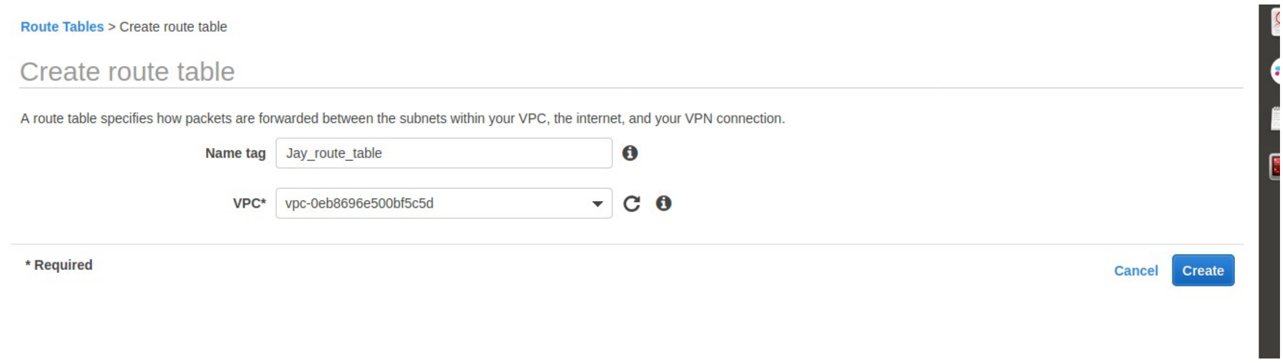
Create internet gateway

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Name tag: Jay_Internet_Gateway

* Required

3. route table for public subnet



Route Tables > Create route table

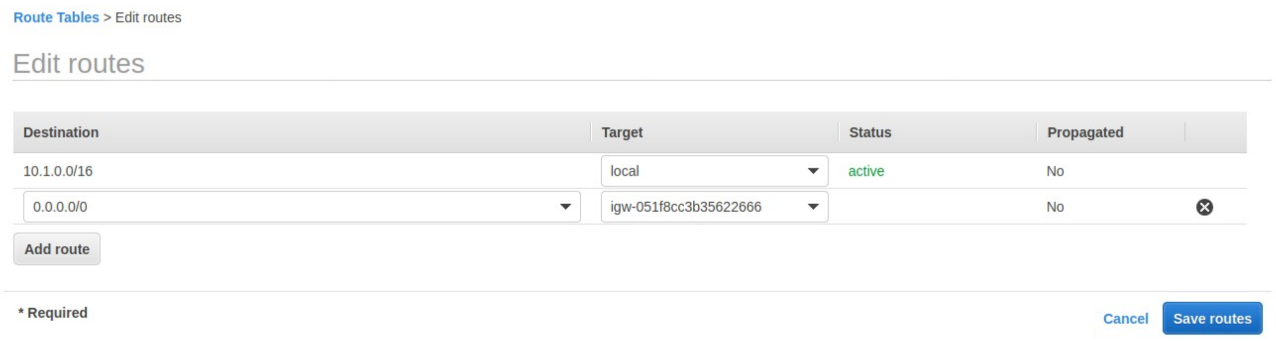
Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Name tag: Jay_route_table

VPC*: vpc-0eb8696e500bf5c5d

* Required



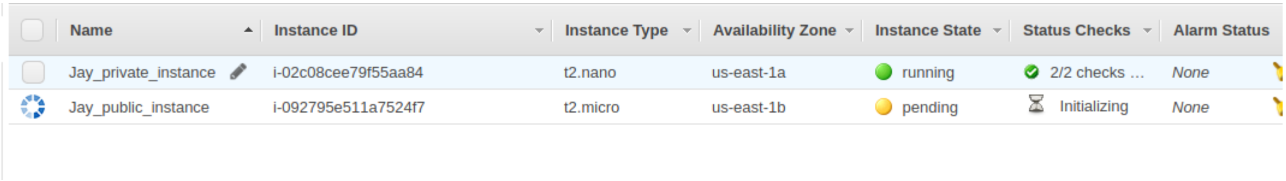
Route Tables > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.1.0.0/16	local	active	No
0.0.0.0/0	igw-051f8cc3b35622666		No

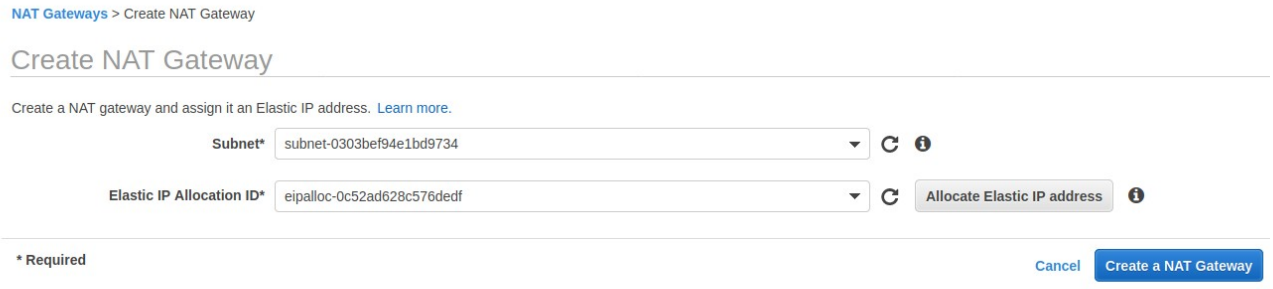
* Required

5. Made public and private instance



	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status
□	Jay_private_instance	i-02c08cee79f55aa84	t2.nano	us-east-1a	● running	✓ 2/2 checks ...	*None*
	Jay_public_instance	i-092795e511a7524f7	t2.micro	us-east-1b	● pending	⌛ Initializing	*None*

5. Made Nat Gateway for in public subnet



NAT Gateways > Create NAT Gateway

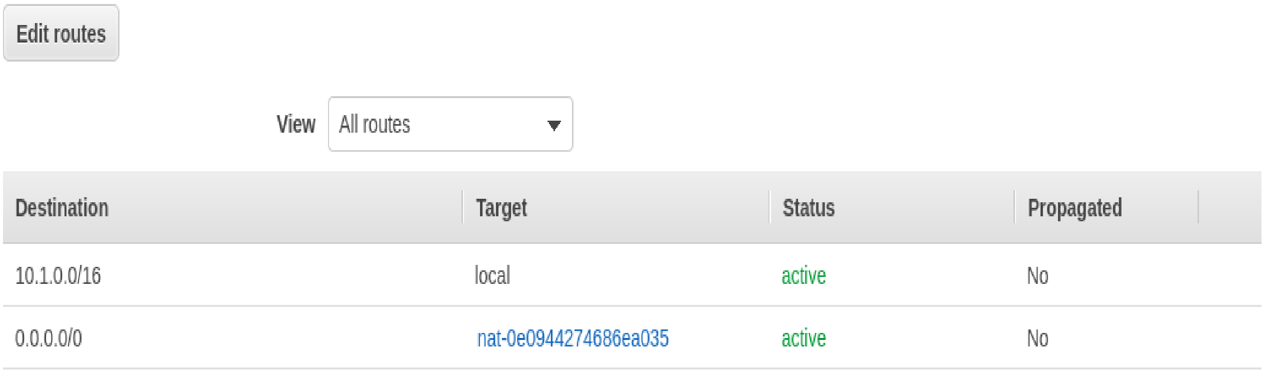
Create NAT Gateway

Create a NAT gateway and assign it an Elastic IP address. Learn more.

Subnet*: subnet-0303bef94e1bd9734

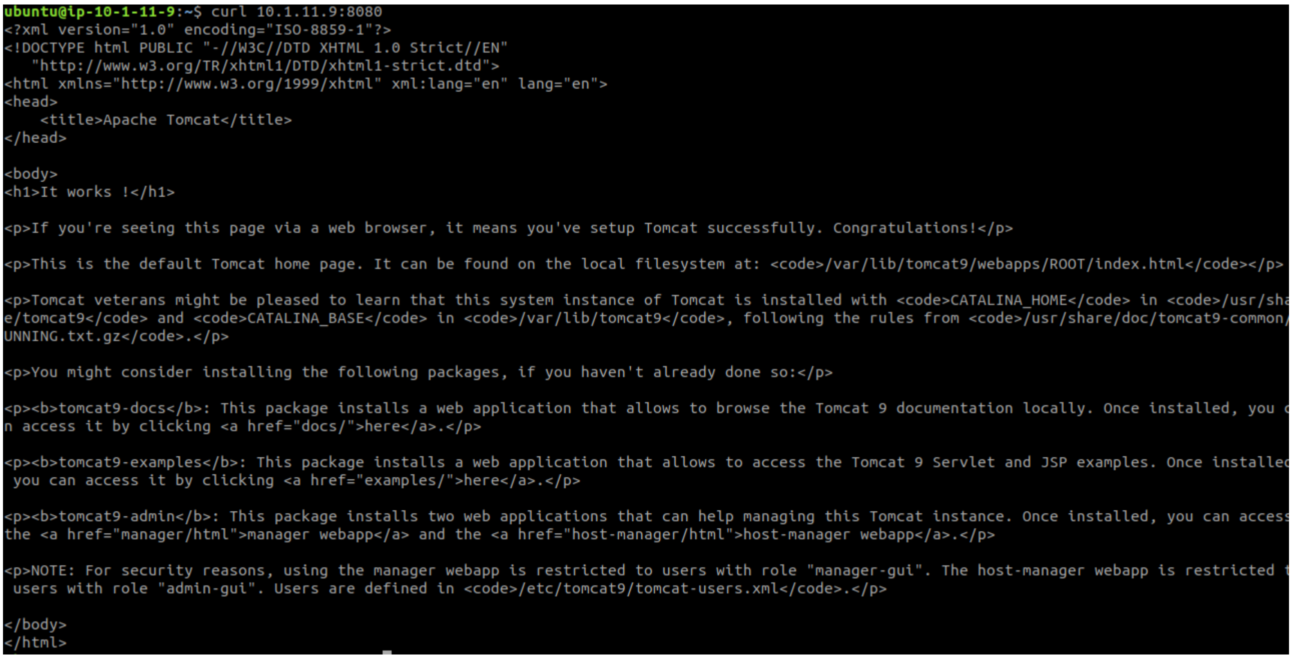
Elastic IP Allocation ID*: eipalloc-0c52ad628c576dedf

6. Route table for private subnet



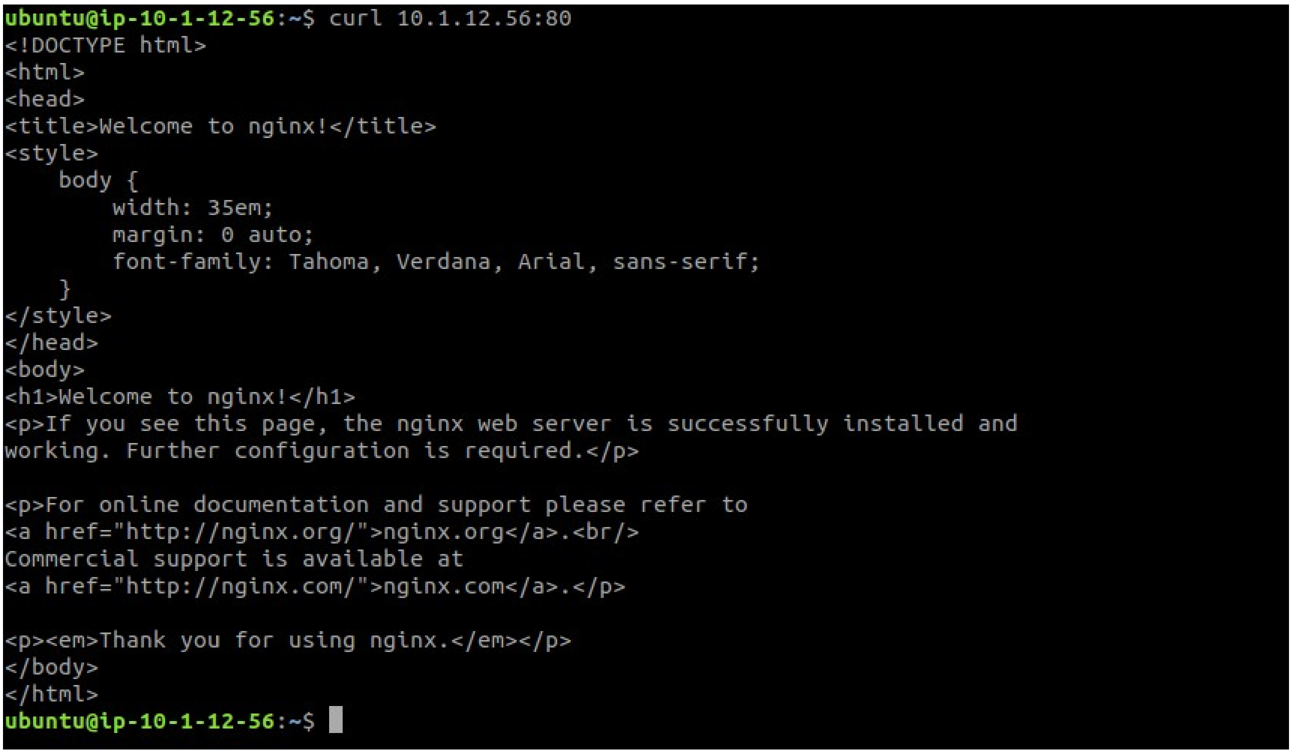
Destination	Target	Status	Propagated
10.1.0.0/16	local	active	No
0.0.0.0/0	nat-0e0944274686ea035	active	No

7. bastion host in private instance and installed tomcat on private instance.



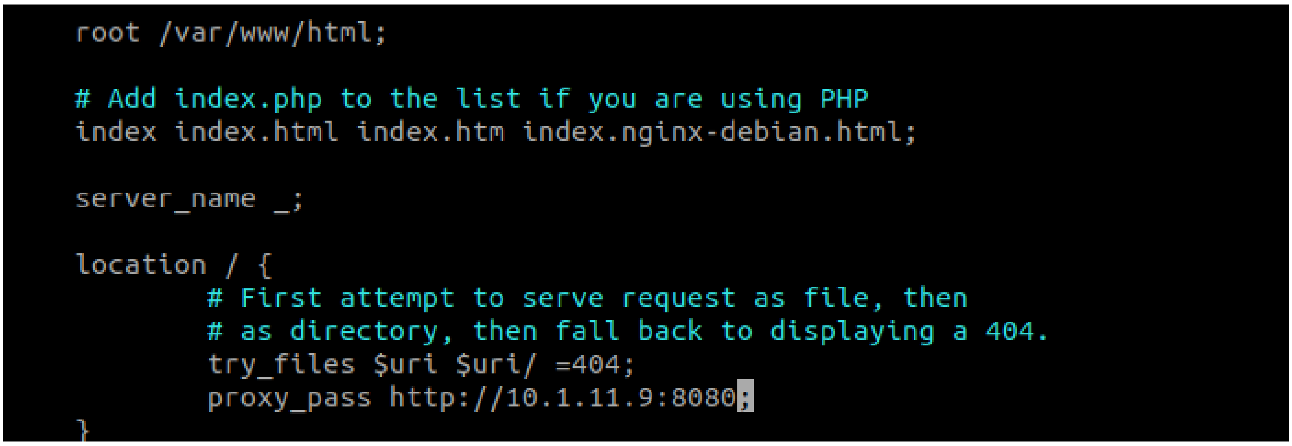
```
ubuntu@ip-10-1-11-9:~$ curl 10.1.11.9:8080
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
   "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
    <title>Apache Tomcat</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/sha
e/tomcat9</code> and <code>CATALINA_BASE</code> in <code>/var/lib/tomcat9</code>, following the rules from <code>/usr/share/doc/tomcat9-common/
UNNING.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 installed, you c
n 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. Once installed
 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, you can access
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 is restricted t
 users with role "admin-gui". Users are defined in <code>/etc/tomcat9/tomcat-users.xml</code>.</p>

</body>
</html>
```

9. Installed nginx on public instance



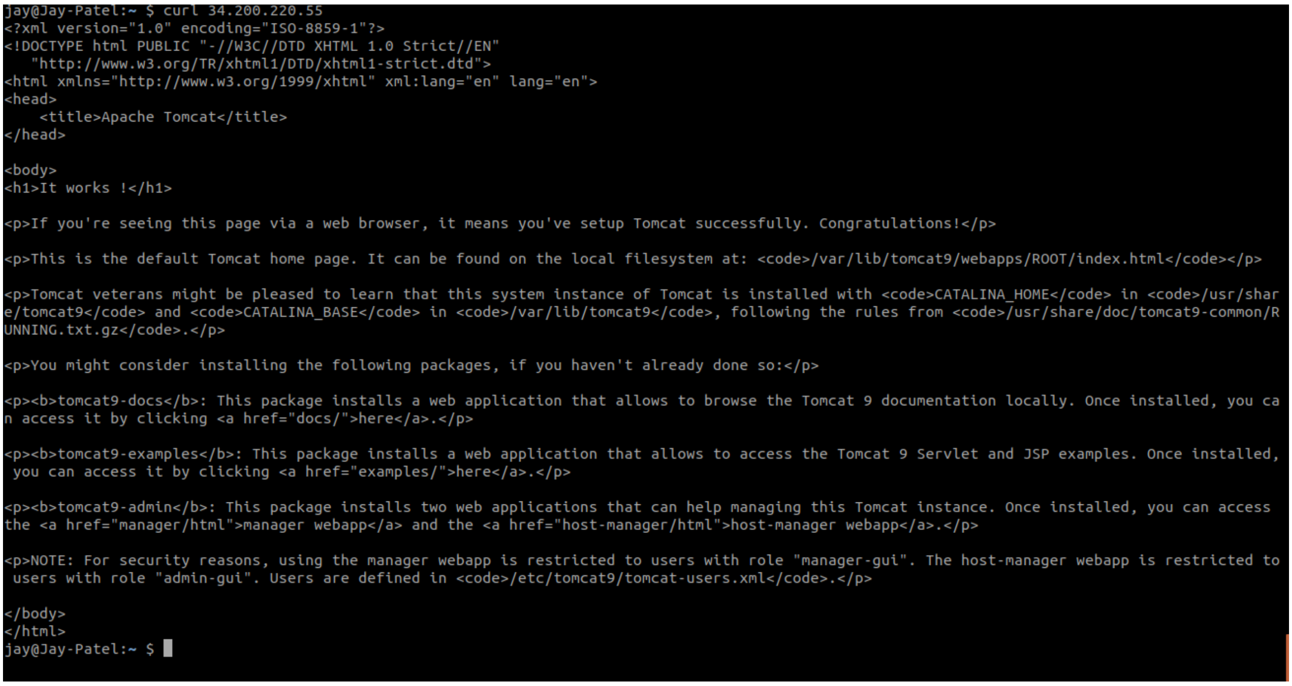
```
ubuntu@ip-10-1-12-56:~$ curl 10.1.12.56:80
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
    body {
        width: 35em;
        margin: 0 auto;
        font-family: Tahoma, Verdana, Arial, sans-serif;
    }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
ubuntu@ip-10-1-12-56:~$
```

10. Proxy pass to tomcat on nginx

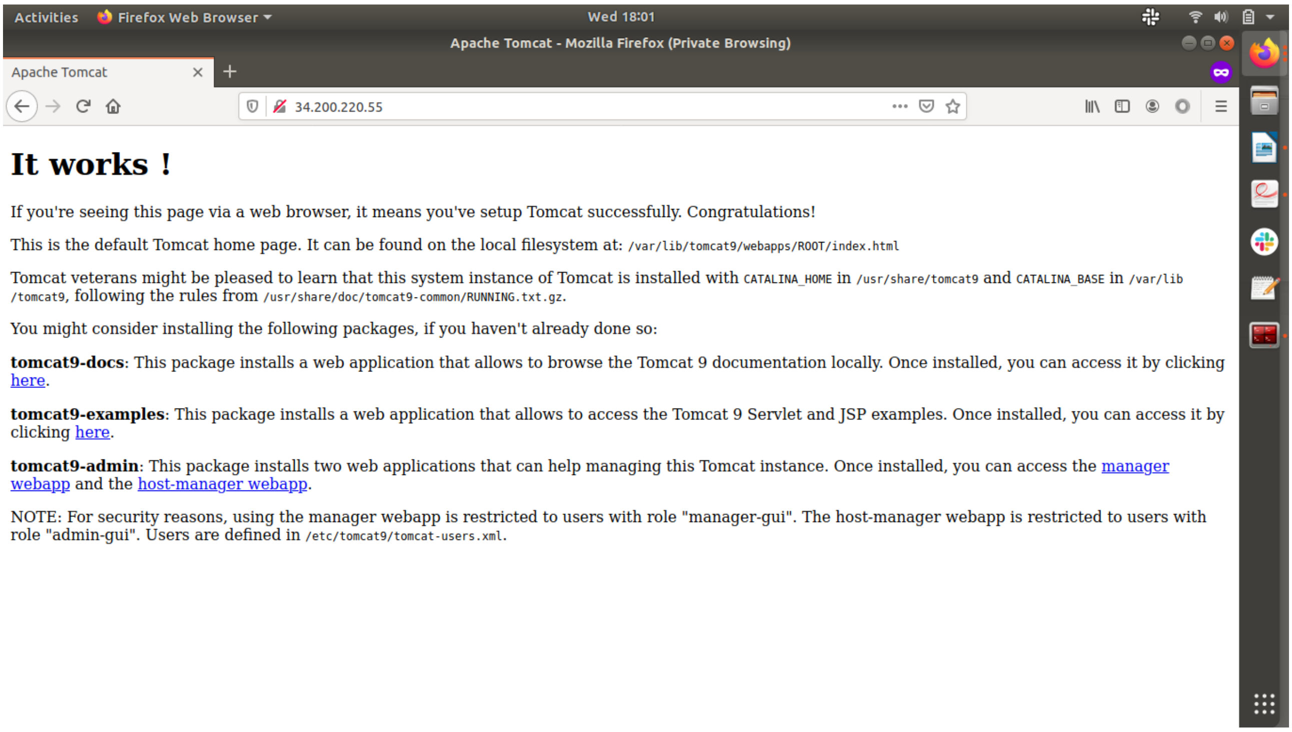


```
        root /var/www/html;

        # Add index.php to the list if you are using PHP
        index index.html index.htm index.nginx-debian.html;

        server_name _;

        location / {
                # First attempt to serve request as file, then
                # as directory, then fall back to displaying a 404.
                try_files $uri $uri/ =404;
                proxy_pass http://10.1.11.9:8080;
        }
```

11. curl on my local machine on public instance and show tomcat9 homepage



```
jay@Jay-Patel:~ $ curl 34.200.220.55
<?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/shar
e/tomcat9</code> and <code>CATALINA_BASE</code> in <code>/var/lib/tomcat9</code>, following the rules from <code>/usr/share/doc/tomcat9-common/R
UNNING.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 installed, you ca
n 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. Once installed,
 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, you can access
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 is restricted to
 users with role "admin-gui". Users are defined in <code>/etc/tomcat9/tomcat-users.xml</code>.</p>

</body>
</html>
jay@Jay-Patel:~ $ 
```



It works !

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

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

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

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

tomcat9-docs: This package installs a web application that allows to browse the Tomcat 9 documentation locally. Once installed, you can access it by clicking here.

tomcat9-examples: This package installs a web application that allows to access the Tomcat 9 Servlet and JSP examples. Once installed, you can access it by clicking here.

tomcat9-admin: This package installs two web applications that can help managing this Tomcat instance. Once installed, you can access the manager webapp and the host-manager webapp.

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

After Implementing this on AWS, create an architecture diagram for this use case.
Note: For hosting Nginx in public subnet, use Elastic IP.