

**TO  
THE  
NEW**™



**VPC**

Trainee Name : Chhavi Sharma

Newers ID : 4023

Mentor Name : Nishith Kulshrestha

College : UPES

## 1. When to use Elastic IP over Public IP

Ans.

Public **IP addresses** are dynamic - i.e. if you stop/start your instance you get reassigned a new public IP. Elastic **IPs** get allocated to your account, and stay the same - it's up to you to attach them to an instance or not. You could say they are static public **IP addresses**. Elastic IP addresses also have the advantage of being dynamically re-mappable. So, rather than being assigned to a particular EC2 instance for the life of the instance, they can be assigned to different EC2 instances as necessary - for example to switch between instances while an upgrade is being performed, or to direct traffic to a second instance if the first instance fails.

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

Ans.

1. Class A : 10.0. 0.0 – 10.255. 255.255.
2. Class B : 172.16. 0.0 – 172.31. 255.255.
3. Class C : 192.168. 0.0 – 192.168. 255.255.

We can use a public IP-Address-Range in our private network. There is no law against this. But we have to take precautions to avoid any routing-trouble when a machine with an IP-Address that actually belongs to a public range wants to access the internet.

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

Ans.

1. To enable flow of traffic between the VPCs using private IP addresses, the owner of each VPC in the peering connection must manually add a route to one or more of their VPC route tables that points to the IP address range of the other VPC(i.e. The peer VPC).
2. The owner of the requester VPC sends a request to the owner of the acceptor VPC to create a VPC peering connection. The acceptor VPC can be owned by you , or another AWS account, and cannot have a CIDR block that overlaps with the requestor VPCs CIDR block.
3. You have a quota on the number of active and pending VPC peering connections that you can have per VPC.
4. You cannot have more than one VPC peering connection between the same two VPCs at the same time.

4. 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.

Ans.

Number of Subnets :

$$20 - 16 = 4$$

Therefore,  $2^4 = 16$  subnets.

Now, The number of IPs in each subnet is

$$32 - 20 = 12$$

Therefore,  $2^{12} = 4096$  IPs

5. Differentiate between NACL and Security Groups.

Ans.

Sno.	NACL	Security Groups
1.	Stateless	Stateful
2.	Operates at subnet level	Operates at instance level
3.	Supports allow and deny rules	Supports only allow rules
4.	Rules are evaluated until matched(in the order of the rule number specified)	All the rules are evaluated when deciding whether to allow traffic.
5.	Applied to all instances within the subnet.	Applied to a particular instance during launch configuration

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

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

Ans.

## 1. Create a 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

Chhavi-private-subnet

VPC\*

vpc-0dc75714b5d93c571

Availability Zone

us-east-1b

VPC CIDRs

CIDR	Status	Status Reason
10.0.0.0/16	associated	

IPv4 CIDR block\*

10.0.10.0/24

\* Required

Cancel

Create

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

by VPC:

Select a VPC

ual Private  
id

VPCs

ets

e Tables

net Gateways

ss Only Internet  
ways

Options, Sate

Create subnet

Actions

search : chhavi

Add filter

1 to 2 of 2

	Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CII
<input checked="" type="checkbox"/>	Chhavi-priv...	subnet-0182c77e3da188274	available	vpc-0dc75714b5d93c571 ...	10.0.10.0/24	251	-
<input type="checkbox"/>	Chhavi-publ...	subnet-03213c9074d4817b6	available	vpc-0dc75714b5d93c571 ...	10.0.12.0/24	251	-

Copied the pem file from the local machine to public instance .

```
chhavi@chhavi:~$ sudo scp -i "/home/chhavi/Downloads/chhavi-ec2-assessment.pem" /home/chhavi/Downloads/chhavi-ec2-assessment.pem ubuntu@54.226.26.147:/home/ubuntu/
chhavi-ec2-assessment.pem
100% 1696 2.2KB/s 00:00
chhavi@chhavi:~$
```

ssh into the private instance from public instance and install tomcat9

```
ubuntu@ip-10-0-12-241:~$ sudo ssh -i /home/ubuntu/chhavi-ec2-assessment.pem ubuntu@10.0.10.214
The authenticity of host '10.0.10.214 (10.0.10.214)' can't be established.
ECDSA key fingerprint is SHA256:7yenJsY0HRv//4GtxYkWTOb5fAuh/CxG312yEL6CiM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.10.214' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-1057-aws x86_64)
```

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

System information as of Mon Feb 24 14:50:18 UTC 2020

```
System load:  0.0          Processes:      86
Usage of /:   13.6% of 7.69GB Users logged in: 0
Memory usage: 15%         IP address for eth0: 10.0.10.214
Swap usage:   0%
```

```
0 packages can be updated.
0 updates are security updates.
```

```
Get:26 http://security.ubuntu.com/ubuntu bionic-security/universe Translation-en [218 kB]
Get:27 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64 Packages [6760 B]
Get:28 http://security.ubuntu.com/ubuntu bionic-security/multiverse Translation-en [2700 B]
Fetched 18.4 MB in 4s (4780 kB/s)
```

Reading package lists... Done

```
ubuntu@ip-10-0-10-214:~$ sudo apt-get install tomcat9
```

Reading package lists... Done

Building dependency tree

Reading state information... Done

The following additional packages will be installed:

```
ca-certificates-java default-jre-headless fontconfig-config fonts-dejavu-core java-common libapr1
libasound2 libasound2-data libavahi-client3 libavahi-common-data libavahi-common3 libcups2
libecjclipse-jdt-core-java libfontconfig1 libjpeg-turbo8 libjpeg8 liblcms2-2 libnspr4 libnss3
libpcsc-lite1 libtcnative-1 libtomcat9-java libx16 libxrender1 libxtst6 openjdk-11-jre-headless
tomcat9-common x11-common
```

Suggested packages:

```
default-jre libasound2-plugins alsa-utils cups-common liblcms2-utils pcsd libnss-mdns
fonts-dejavu-extra fonts-ipafont-gothic fonts-ipafont-mincho fonts-wqy-microhei | fonts-wqy-zenhei
fonts-indic tomcat9-admin tomcat9-docs tomcat9-examples tomcat9-user
```

The following NEW packages will be installed:

```
ca-certificates-java default-jre-headless fontconfig-config fonts-dejavu-core java-common libapr1
libasound2 libasound2-data libavahi-client3 libavahi-common-data libavahi-common3 libcups2
```

```
ubuntu@ip-10-0-10-214:/var/lib/tomcat9/conf$ curl localhost: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>CA
```

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

Ans.

Create a public subnet.

(Create a route table. Attach an internet gateway in the route table and associate it to the subnet)

Subnets > Create 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:

VPC\*:

Availability Zone:

VPC CIDRs

CIDR	Status	Status Reason
10.0.0.0/16	associated	

IPv4 CIDR block\*:

\* Required

Cancel Create

by VPC:

Select a VPC

Create subnet Actions

search : chhavi Add filter

1 to 2 of 2

	Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR
<input checked="" type="checkbox"/>	Chhavi-priv...	subnet-0182c77e3da188274	available	vpc-0dc75714b5d93c571 ...	10.0.10.0/24	251	-
<input type="checkbox"/>	Chhavi-publ...	subnet-03213c9074d4817b6	available	vpc-0dc75714b5d93c571 ...	10.0.12.0/24	251	-

In the user data write :

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

```
sudo apt-get update -y
```



```
sudo apt-get install nginx -y
```

When the instance is launched, ssh and check if nginx is running.

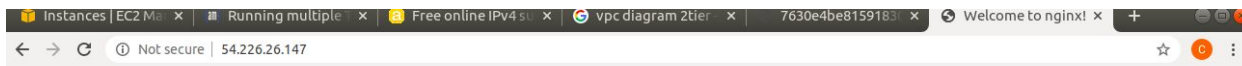
```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-12-241:~$ sudo service nginx status
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2020-02-24 12:05:11 UTC; 4s ago
     Docs: man:nginx(8)
    Main PID: 2373 (nginx)
      Tasks: 2 (limit: 1152)
   CGroup: /system.slice/nginx.service
           └─2373 nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
             └─2376 nginx: worker process

Feb 24 12:05:11 ip-10-0-12-241 systemd[1]: Starting A high performance web server and a reverse proxy server...
Feb 24 12:05:11 ip-10-0-12-241 systemd[1]: nginx.service: Failed to parse PID from file /run/nginx.pid: Invalid argument
Feb 24 12:05:11 ip-10-0-12-241 systemd[1]: Started A high performance web server and a reverse proxy server.
ubuntu@ip-10-0-12-241:~$
```



## Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to [nginx.org](http://nginx.org).  
Commercial support is available at [nginx.com](http://nginx.com).

*Thank you for using nginx.*

Create a NAT gateway in the public subnet and attach it to the private subnet route table.

(NAT gateway uses an elastic IP)

NAT Gateways > Create NAT Gateway

### Create NAT Gateway

✓

**Your NAT gateway has been created.**

Note: In order to use your NAT gateway, ensure that you [edit your route tables](#) to include a route with the following NAT gateway.  
[Find out more.](#)

NAT Gateway ID    nat-0c8b83df27fcd3981

[Edit route tables](#) [Close](#)

## PROXY PASS

In the public instance create a virtual host. In the server block write the following.

Proxy pass to the tomcat running in the private subnet.

```
server{
    listen 80;
    server_name bootcamp.com;
    location /{
        proxy_pass http://10.0.10.214:8080
    }
}
~
~
```

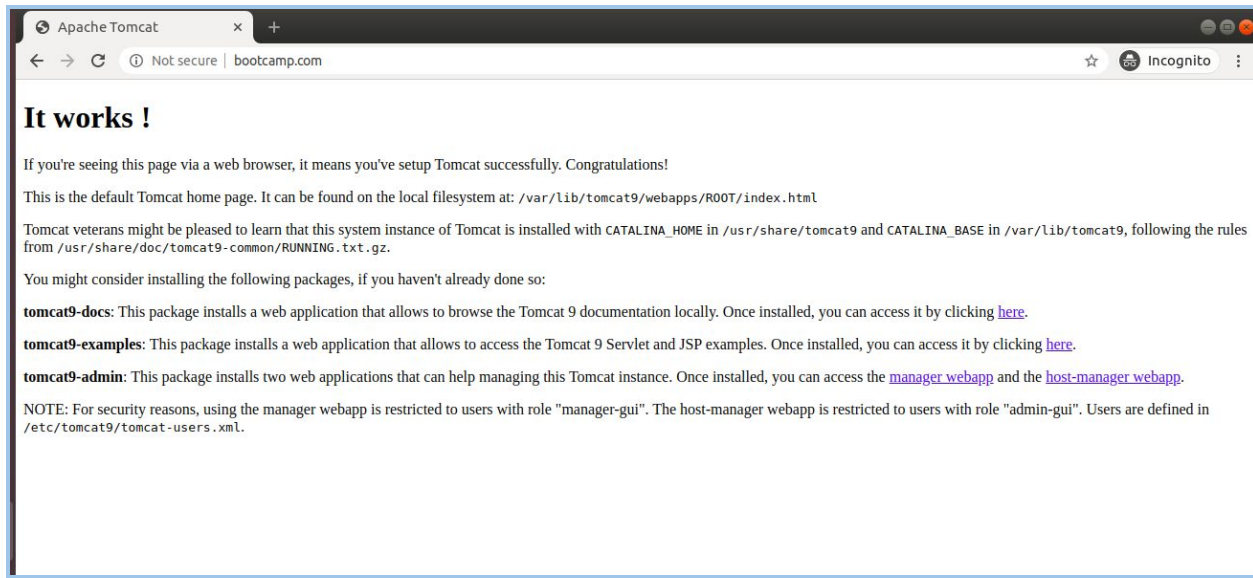
Create an entry for the public IP and associated server name in the /etc/hosts file.

```
chhavi@chhavi: /var/lib/tomcat9/conf x ubuntu@ip-10-0-12-241: /etc/nginx/sites-enabled
127.0.0.1      localhost abc.com xyz.com www.abc.com
127.0.1.1      chhavi
54.226.26.147  bootcamp.com

# 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
~
~
~
~
```

Hit bootcamp.com in the browser. You'll be proxy passed to Tomcat.

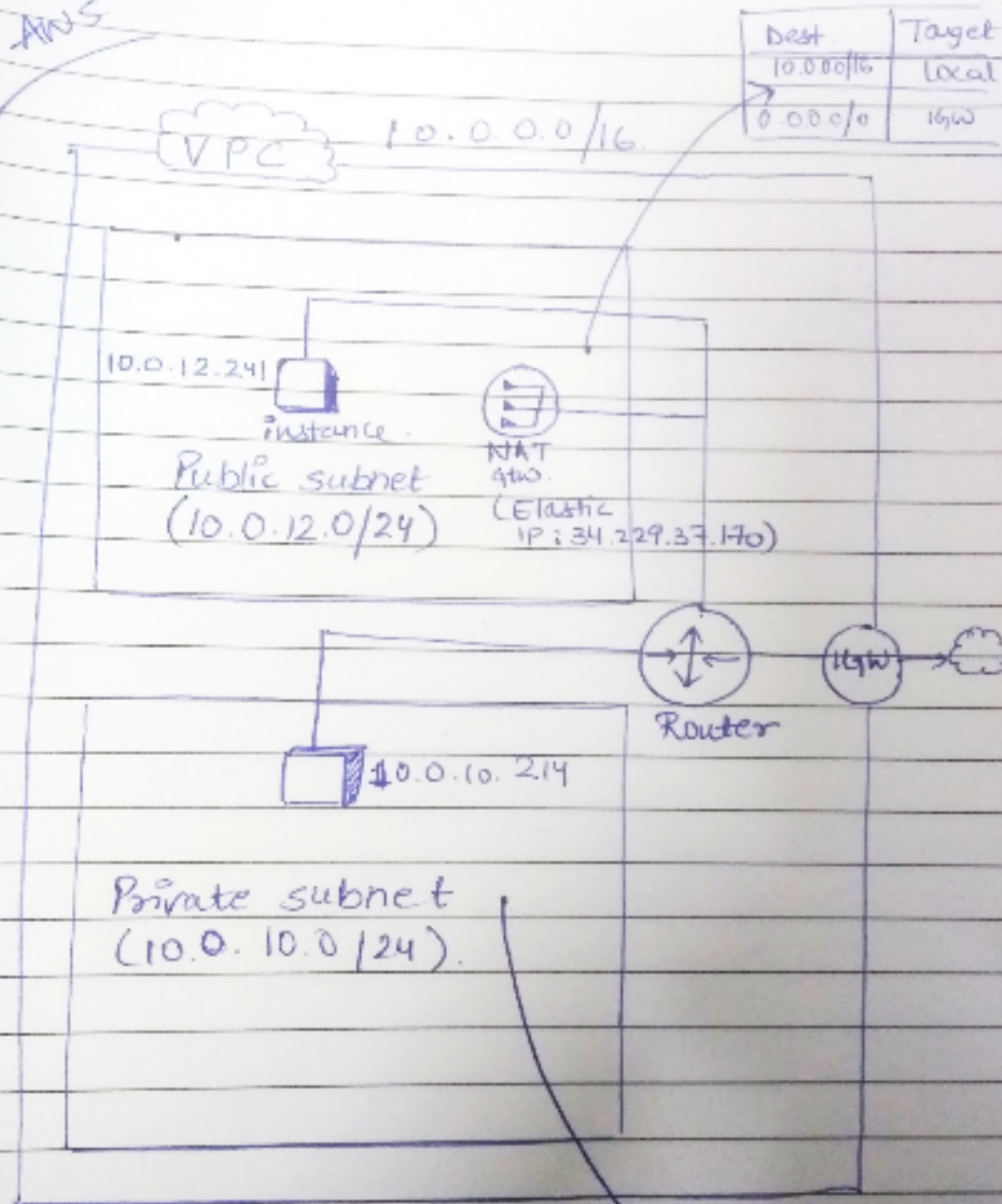




After Implementing this on AWS, create an architecture diagram for this use case.

Ans.

Ans



Dest	Target
10.0.0.0/16	local
0.0.0.0/0	igw

Dest	Target
10.0.0.0/16	local
0.0.0.0/0	NAT

