

Q1. When to use Elastic IP over Public IP

Ans-We use elastic IP over public ip when we want ip doesn't change when we start or stop the instance.

For eg: if we are hosting a website on an Ec2 instance we will give that instance a elastic ip so that it doesn't get changed.

We use elastic Ip in the NAT server in a VPC.

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

Class A Network - 10.0.0.0 - 10.255.255.255

Class B Network - 172.16.0.0 - 172.31.255.255

Class C Network - 192.168.0.0 - 192.168.255.255

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

- 1. The owner of the *requester VPC* sends a request to the owner of the *accepter VPC* to create the VPC peering connection. The accepter VPC can be owned by you, or another AWS account, and cannot have a CIDR block that overlaps with the requestor VPC's CIDR block.**
- 2. The owner of the accepter VPC accepts the VPC peering connection request to activate the VPC peering connection.**
- 3. To enable the flow of traffic between the VPCs using private IP addresses, the owner of each VPC in the VPC 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 (the peer VPC).**
- 4. If required, update the security group rules that are associated with your instance to ensure that traffic to and from the peer VPC is not restricted.**
- 5. Both the VPC should have different CIDR range otherwise there will be an ambiguity in the route table and Network access control lists.**

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 IPs in the subnet.

No. of subnets = $20 - 16 = 4 = 2^4 = 16$ subnets.

Ip in each subnet= $32-20=12=2^4$ 12Ip in a particular subnet.

Q5. Differentiate between NACL and Security Groups.

NACL has Rule number priority whereas Security Group doesn't have.

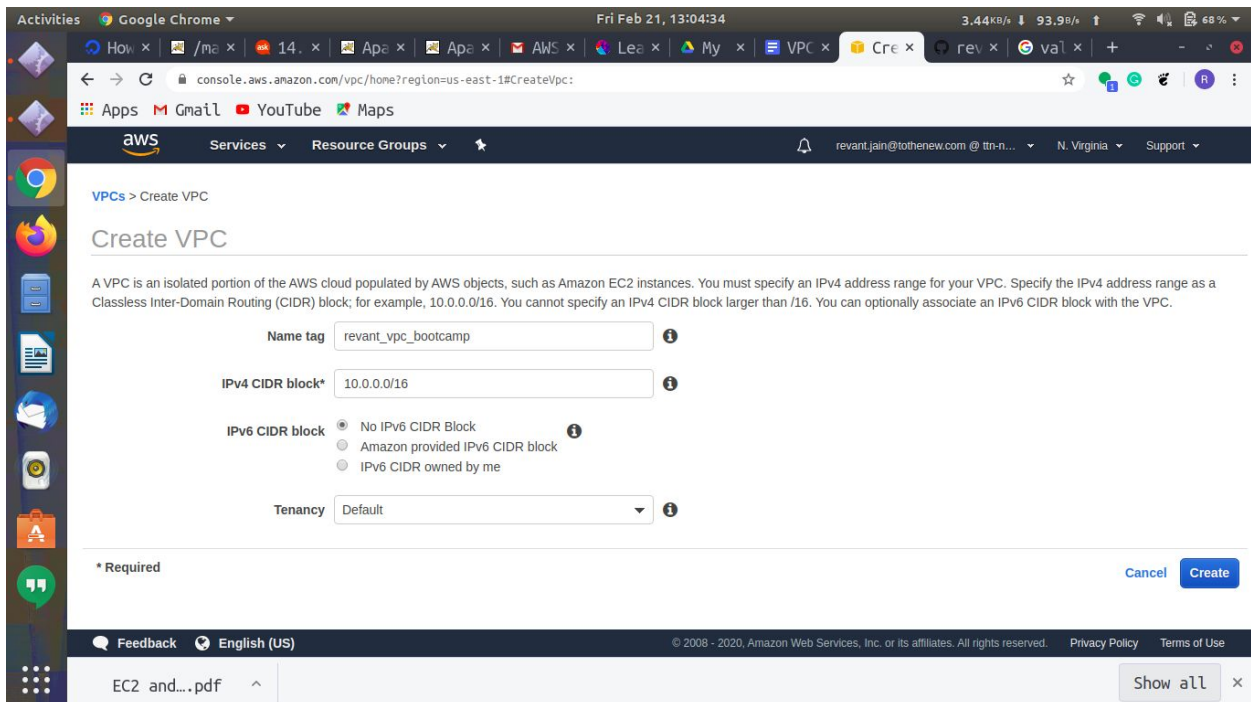
In NACL we can allow and deny both and in Security group we can only allow.

NACL acts as a firewall for a particular subnet whereas Security group acts as a firewall for a particular EC2 instance.

NACL are stateless which means whenever we allow a particular port in inbound it will not be automatically applied in outbound. Whereas Security group is stateful.

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 proxy pass to Tomcat from Nginx



The screenshot shows the AWS Management Console interface for creating a new VPC. The browser address bar indicates the URL is `console.aws.amazon.com/vpc/home?region=us-east-1#CreateVpc:`. The page title is "Create VPC". Below the title, there is a descriptive paragraph about VPCs. The form contains the following fields and options:

- Name tag:** A text input field containing "revant_vpc_bootcamp".
- IPv4 CIDR block*:** A text input field containing "10.0.0.0/16".
- IPv6 CIDR block:** A section with three radio button options: "No IPv6 CIDR Block" (selected), "Amazon provided IPv6 CIDR block", and "IPv6 CIDR owned by me".
- Tenancy:** A dropdown menu set to "Default".

At the bottom right of the form, there are "Cancel" and "Create" buttons. The footer of the console shows "Feedback", "English (US)", and copyright information for Amazon Web Services, Inc.

Create a public subnet

The screenshot shows the AWS Management Console 'Create subnet' page. The browser address bar shows the URL: `console.aws.amazon.com/vpc/home?region=us-east-1#CreateSubnet:`. The page title is 'Subnets > Create subnet'. Below the title, there is a heading 'Create subnet' and a descriptive paragraph: '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.'

The form contains the following fields:

- Name tag:** `revant_publicsubnet`
- VPC*:** `vpc-01d1840e02a773da9`
- Availability Zone:** `us-east-1a`
- VPC CIDRs:** A table with columns 'CIDR', 'Status', and 'Status Reason'. It contains one row: `10.0.0.0/16` with status `associated`.
- IPv4 CIDR block*:** `10.0.0.0/20`

At the bottom of the form, there is a 'Feedback' link, 'English (US)' language selector, and copyright information: '© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.' There are also links for 'Privacy Policy' and 'Terms of Use'. A 'Show all' button is visible in the bottom right corner.

Create a private subnet

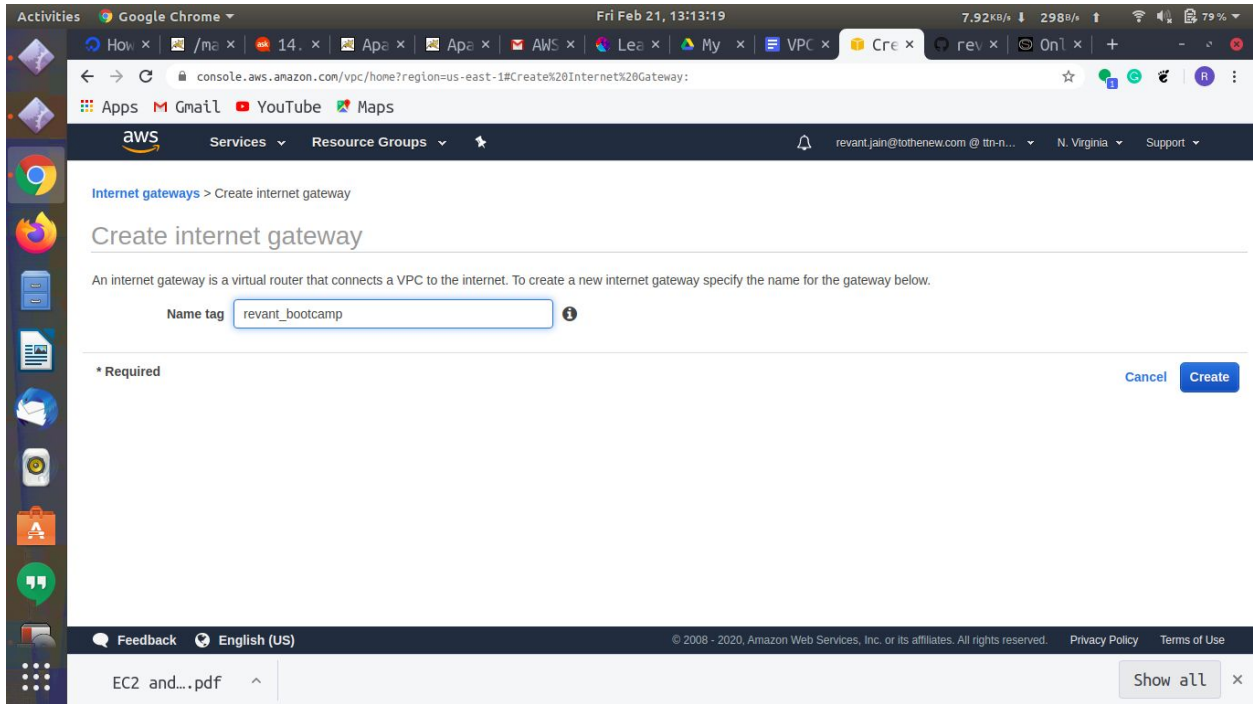
The screenshot shows the AWS Management Console 'Create subnet' page. The browser address bar shows the URL: `console.aws.amazon.com/vpc/home?region=us-east-1#CreateSubnet:`. The page title is 'Subnets > Create subnet'. Below the title, there is a heading 'Create subnet' and a descriptive paragraph: '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.'

The form contains the following fields:

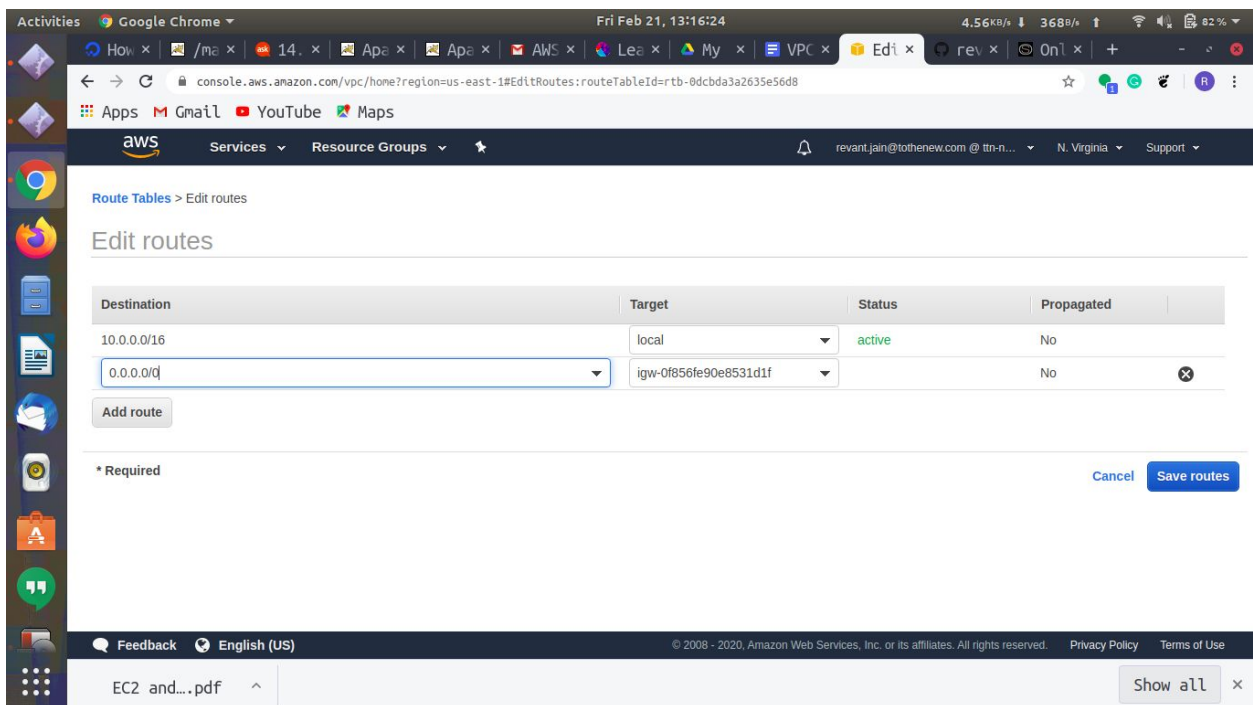
- Name tag:** `Revant_privatesubnet`
- VPC*:** `vpc-01d1840e02a773da9`
- Availability Zone:** `us-east-1b`
- VPC CIDRs:** A table with columns 'CIDR', 'Status', and 'Status Reason'. It contains one row: `10.0.0.0/16` with status `associated`.
- IPv4 CIDR block*:** `10.0.16.0/20`

At the bottom of the form, there is a '* Required' label, a 'Cancel' button, and a 'Create' button. There is also a 'Feedback' link, 'English (US)' language selector, and copyright information: '© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.' There are also links for 'Privacy Policy' and 'Terms of Use'. A 'Show all' button is visible in the bottom right corner.

Create an internet gateway and attach it to Vpc.



Put entry of igw in the route table of public subnet,



Create a NAT gateway

The screenshot shows the AWS Management Console interface for creating a NAT gateway. The browser address bar indicates the URL: `console.aws.amazon.com/vpc/home?region=us-east-1#CreateNatGateway:`. The page title is "Create NAT Gateway". Below the title, there is a sub-header "NAT Gateways > Create NAT Gateway". The main content area contains a form with two dropdown menus: "Subnet*" set to "subnet-0faca81a74feca1e8" and "Elastic IP Allocation ID*" set to "eipalloc-0f08bdb5995481eea". A button labeled "Allocate Elastic IP address" is next to the second dropdown. Below the form, it states "Elastic IP address (52.87.9.178) allocated." At the bottom right, there are "Cancel" and "Create a NAT Gateway" buttons. The footer includes "Feedback", "English (US)", and copyright information for 2008-2020 Amazon Web Services.

Activities Google Chrome Fri Feb 21, 13:20:46 6.18KB/s 5.00KB/s 86%

console.aws.amazon.com/vpc/home?region=us-east-1#CreateNatGateway:

Apps Gmail YouTube Maps

aws Services Resource Groups

revant.jain@tothenew.com @ ttn-n... N. Virginia Support

NAT Gateways > Create NAT Gateway

Create NAT Gateway

Create a NAT gateway and assign it an Elastic IP address. [Learn more.](#)

Subnet* subnet-0faca81a74feca1e8

Elastic IP Allocation ID* eipalloc-0f08bdb5995481eea

Allocate Elastic IP address

Elastic IP address (52.87.9.178) allocated.

* Required

Cancel Create a NAT Gateway

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

EC2 and...pdf Show all

The screenshot shows the AWS Management Console interface for editing routes. The browser address bar indicates the URL: `console.aws.amazon.com/vpc/home?region=us-east-1#EditRoutes:routeTableId=rtb-0bf3d9551dfa5b632`. The page title is "Edit routes". Below the title, there is a sub-header "Route Tables > Edit routes". The main content area contains a table with columns: "Destination", "Target", "Status", and "Propagated". The table has two rows: one for "10.0.0.0/16" with target "local" and status "active", and another for "0.0.0.0/0" with target "nat-06a2c8c8bf199df07" and status "No". Below the table, there is an "Add route" button. At the bottom right, there are "Cancel" and "Save routes" buttons. The footer includes "Feedback", "English (US)", and copyright information for 2008-2020 Amazon Web Services.

Activities Google Chrome Fri Feb 21, 13:24:25 4.52KB/s 391B/s 89%

console.aws.amazon.com/vpc/home?region=us-east-1#EditRoutes:routeTableId=rtb-0bf3d9551dfa5b632

Apps Gmail YouTube Maps

aws Services Resource Groups

revant.jain@tothenew.com @ ttn-n... N. Virginia Support

Route Tables > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	nat-06a2c8c8bf199df07	No	No

Add route

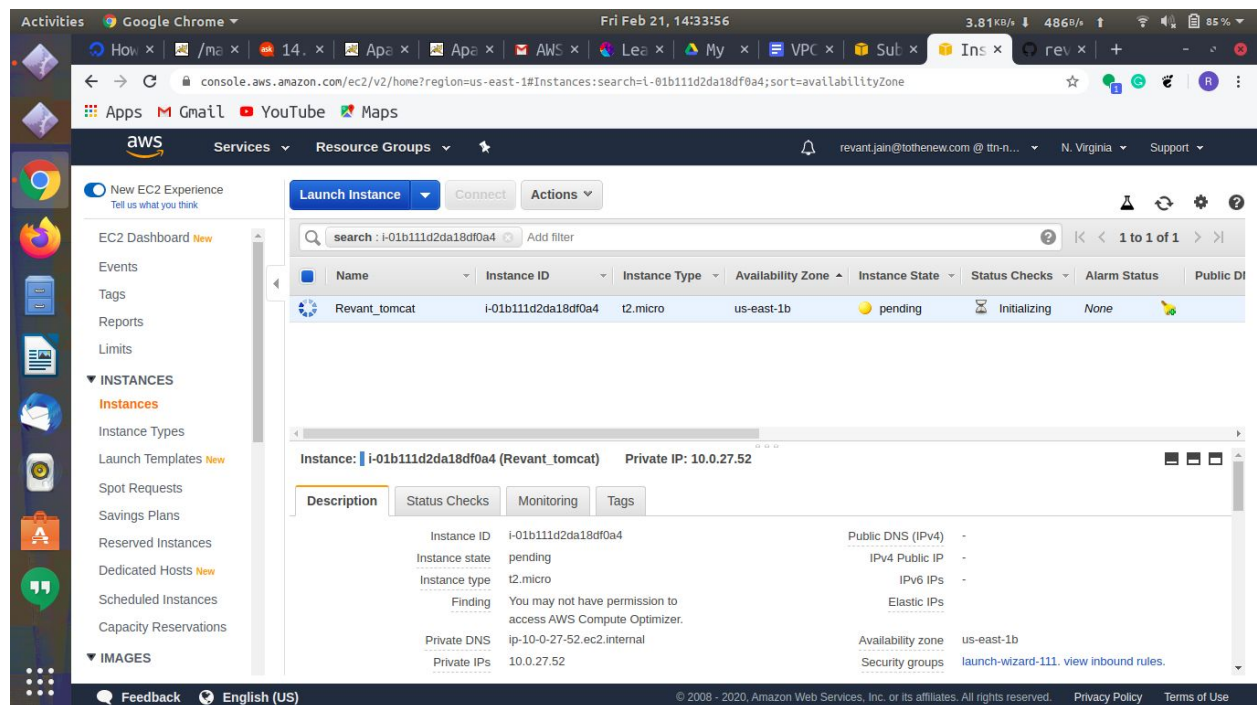
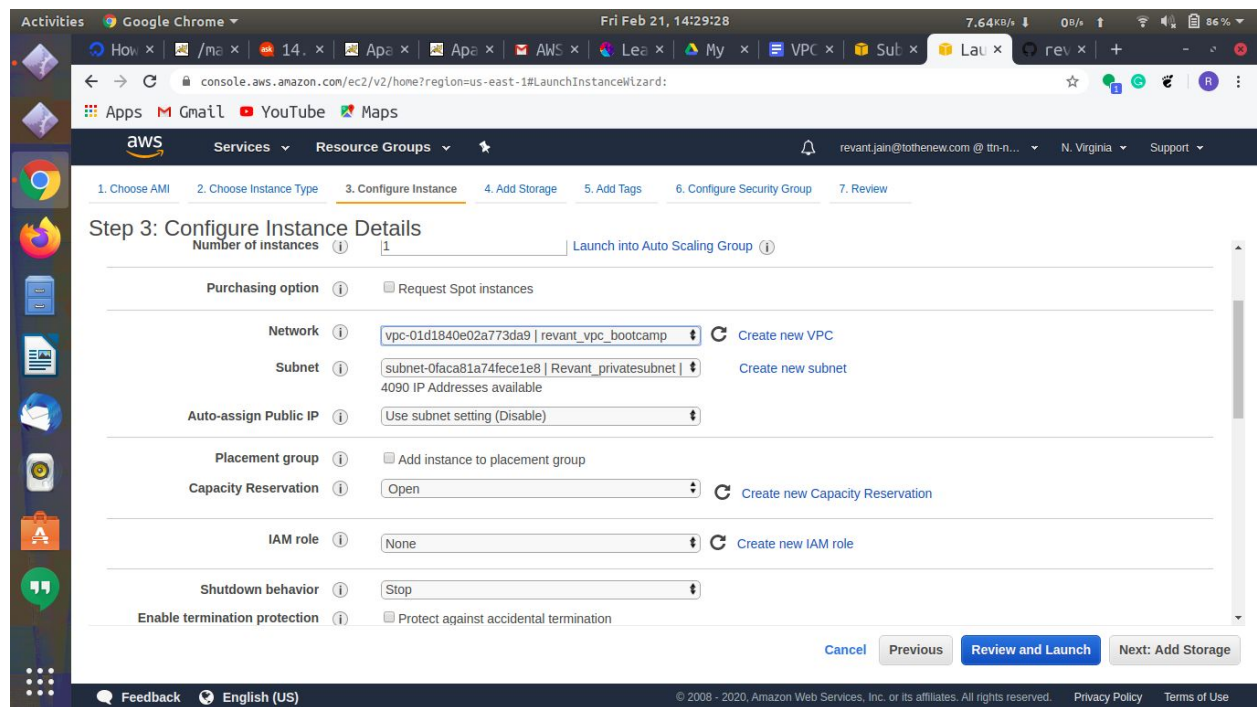
* Required

Cancel Save routes

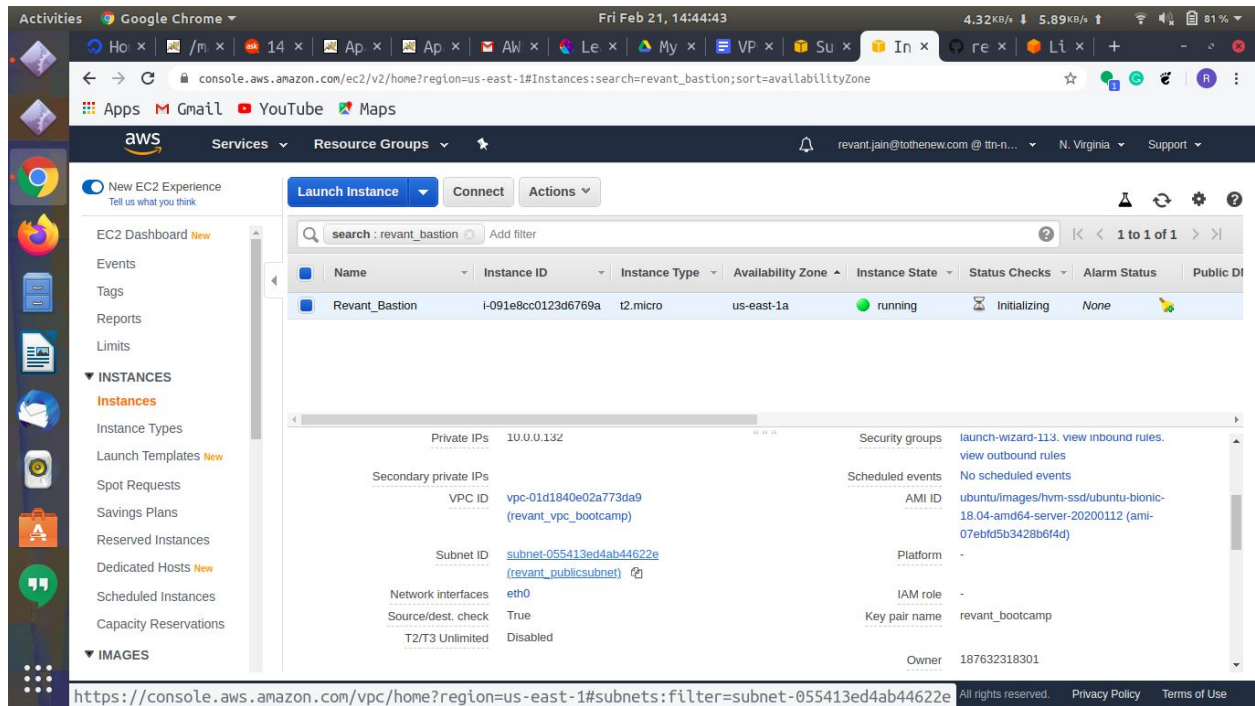
Feedback English (US) © 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

EC2 and...pdf Show all

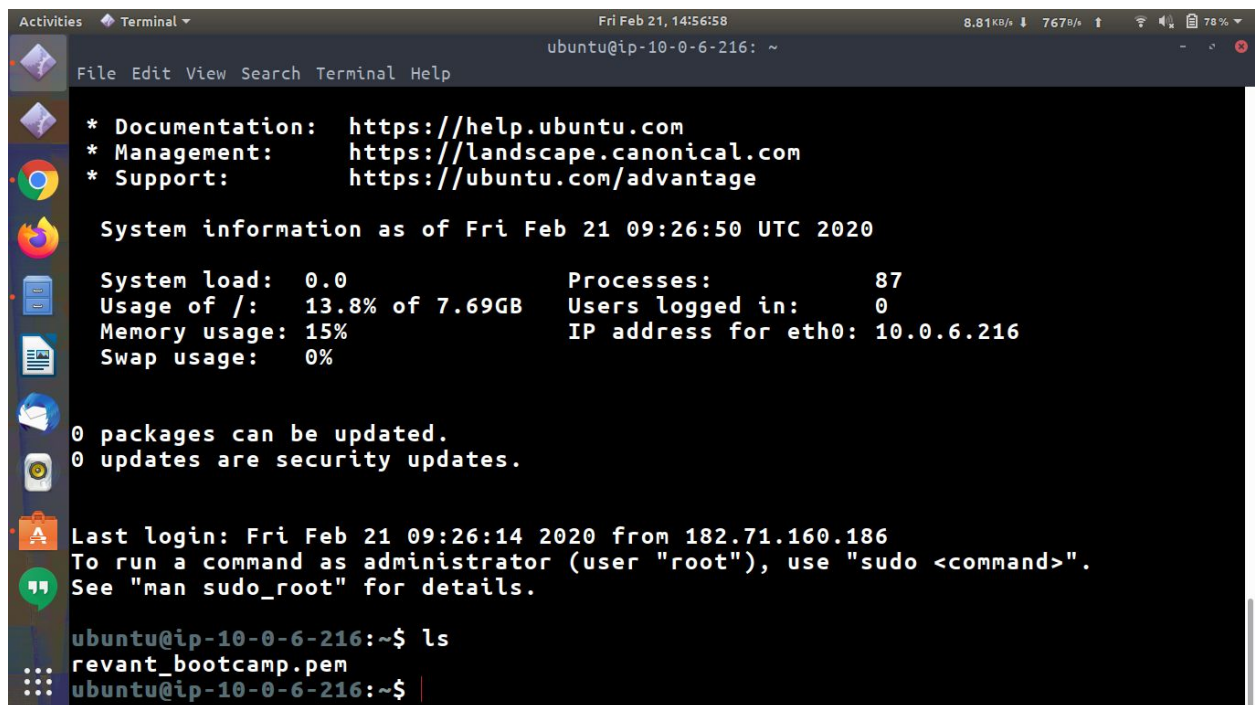
Make an Ec2 instance in private subnet and install tomcat in it.



Now we will create a bastion hosts in public subnet



Login into Bastion hosts.



Login into tomcat server

```
Activities Terminal Fri Feb 21, 14:58:27 4.68KB/s 298B/s 78%
ubuntu@ip-10-0-27-52: ~
File Edit View Search Terminal Help

System information as of Fri Feb 21 09:28:10 UTC 2020

System load: 0.0          Processes: 86
Usage of /: 13.6% of 7.69GB Users logged in: 0
Memory usage: 14%        IP address for eth0: 10.0.27.52
Swap usage: 0%

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

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-10-0-27-52:~$
```

Install tomcat

```
Activities Terminal Fri Feb 21, 15:20:00 7.82KB/s 1.22KB/s 72%
ubuntu@ip-10-0-27-52: /tmp
File Edit View Search Terminal Help

Processing triggers for ureadahead (0.100.0-21) ...
Processing triggers for libc-bin (2.27-3ubuntu1) ...
Processing triggers for systemd (237-3ubuntu10.33) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...

Processing triggers for ca-certificates (20180409) ...
Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...

done.
done.
ubuntu@ip-10-0-27-52:~$ sudo useradd -s /bin/false -g tomcat -d /opt/tomcat tomcat
useradd: group 'tomcat' does not exist
ubuntu@ip-10-0-27-52:~$ sudo groupadd tomcat
ubuntu@ip-10-0-27-52:~$ sudo useradd -s /bin/false -g tomcat -d /opt/tomcat tomcat
ubuntu@ip-10-0-27-52:~$ cd /tmp
ubuntu@ip-10-0-27-52:/tmp$ curl -O http://mirrors.estointernet.in/apache/tomcat/tomcat-9/v9.0.31/bin/apache-tomcat-9.0.31.tar.gz
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           %             %             Dload  Upload  Total   Spent    Left   Speed
 86 10.5M    86 9309k    0     0  960k      0  0:00:11  0:00:09  0:00:02 1098k
```



```
Activities Terminal Fri Feb 21, 15:46:56 9.48KB/s 93.9B/s 65%
ubuntu@ip-10-0-27-52: /opt/tomcat

File Edit View Search Terminal Help

ubuntu@ip-10-0-27-52:/opt/tomcat$ sudo chgrp -R tomcat /opt/tomcat
ubuntu@ip-10-0-27-52:/opt/tomcat$ sudo chmod -R g+r conf
ubuntu@ip-10-0-27-52:/opt/tomcat$ sudo chmod g+x conf
ubuntu@ip-10-0-27-52:/opt/tomcat$ sudo chown -R tomcat webapps/ work/ temp/ logs
/
ubuntu@ip-10-0-27-52:/opt/tomcat$ sudo update-java-alternatives -l
java-1.11.0-openjdk-amd64 1111 /usr/lib/jvm/java-1.11.0-openjdk-amd64
ubuntu@ip-10-0-27-52:/opt/tomcat$ sudo nano /etc/systemd/system/tomcat.service
ubuntu@ip-10-0-27-52:/opt/tomcat$ sudo systemctl daemon-reload
ubuntu@ip-10-0-27-52:/opt/tomcat$ sudo systemctl start tomcat
ubuntu@ip-10-0-27-52:/opt/tomcat$ sudo systemctl status tomcat
● tomcat.service - Apache Tomcat Web Application Container
   Loaded: loaded (/etc/systemd/system/tomcat.service; disabled; vendor preset:
   Active: active (running) since Fri 2020-02-21 10:16:48 UTC; 6s ago
   Process: 17862 ExecStart=/opt/tomcat/bin/startup.sh (code=exited, status=0/SUC
   Main PID: 17879 (java)
   Tasks: 30 (limit: 1152)
   CGroup: /system.slice/tomcat.service
           └─17879 /usr/lib/jvm/java-1.11.0-openjdk-amd64/bin/java -Djava.util.l

Feb 21 10:16:48 ip-10-0-27-52 systemd[1]: Starting Apache Tomcat Web Application
Feb 21 10:16:48 ip-10-0-27-52 startup.sh[17862]: Tomcat started.
Feb 21 10:16:48 ip-10-0-27-52 systemd[1]: Started Apache Tomcat Web Application
lines 1-12/12 (END)
```

Launch Nginx server in Public subnet

Activities Google Chrome Fri Feb 21, 15:52:08 6.32KB/s 94.0B/s 64%

console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:search=revant;sort=availabilityZone

aws Services Resource Groups

New EC2 Experience Tell us what you think

Launch Instance Connect Actions

search : revant Add filter 1 to 3 of 3

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public IP
Revant_nginx	i-041542145497950...	t2.micro	us-east-1a	pending	Initializing	None	
Revant_Bastion	i-0a82c4a9db25e2bf7	t2.micro	us-east-1a	running	2/2 checks ...	None	
Revant_tomcat	i-01b111d2da18df0a4	t2.micro	us-east-1b	running	2/2 checks ...	None	

Select an instance above

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

```
Activities Terminal Fri Feb 21, 15:54:19 14.2kB/s 188B/s 64%
ubuntu@ip-10-0-4-22: ~
File Edit View Search Terminal Help
Setting up libnginx-mod-http-image-filter (1.14.0-0ubuntu1.7) ...
Setting up nginx-core (1.14.0-0ubuntu1.7) ...
Setting up nginx (1.14.0-0ubuntu1.7) ...
Processing triggers for systemd (237-3ubuntu10.33) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for ufw (0.36-0ubuntu0.18.04.1) ...
Processing triggers for ureadahead (0.100.0-21) ...
Processing triggers for libc-bin (2.27-3ubuntu1) ...
ubuntu@ip-10-0-4-22:~$ service nginx restart
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to restart 'nginx.service'.
Authenticating as: Ubuntu (ubuntu)
Password:
ubuntu@ip-10-0-4-22:~$ 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 Fri 2020-02-21 10:23:44 UTC; 32s ago
     Docs: man:nginx(8)
    Main PID: 2416 (nginx)
      Tasks: 2 (limit: 1152)
    CGroup: /system.slice/nginx.service
            └─2416 nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
              └─2417 nginx: worker process

Feb 21 10:23:44 ip-10-0-4-22 systemd[1]: Starting A high performance web server and a reverse proxy server: nginx.
Feb 21 10:23:44 ip-10-0-4-22 systemd[1]: nginx.service: Failed to parse PID from file /run/nginx.pid: Invalid PID '0'.
Feb 21 10:23:44 ip-10-0-4-22 systemd[1]: Started A high performance web server and a reverse proxy server: nginx.
lines 1-13/13 (END)
```

```
Activities Terminal Fri Feb 21, 15:56:45 3.80kB/s 176B/s 62%
ubuntu@ip-10-0-4-22: /etc/nginx/sites-enabled
File Edit View Search Terminal Help
server {
    listen 80;
    server_name localhost;
    location / {
        proxy_pass http://10.0.27.52:8080;
    }
}

-- INSERT -- 7,2 All
```