National University of Computer
and Emerging Sciences

CS4075-Cloud Computing

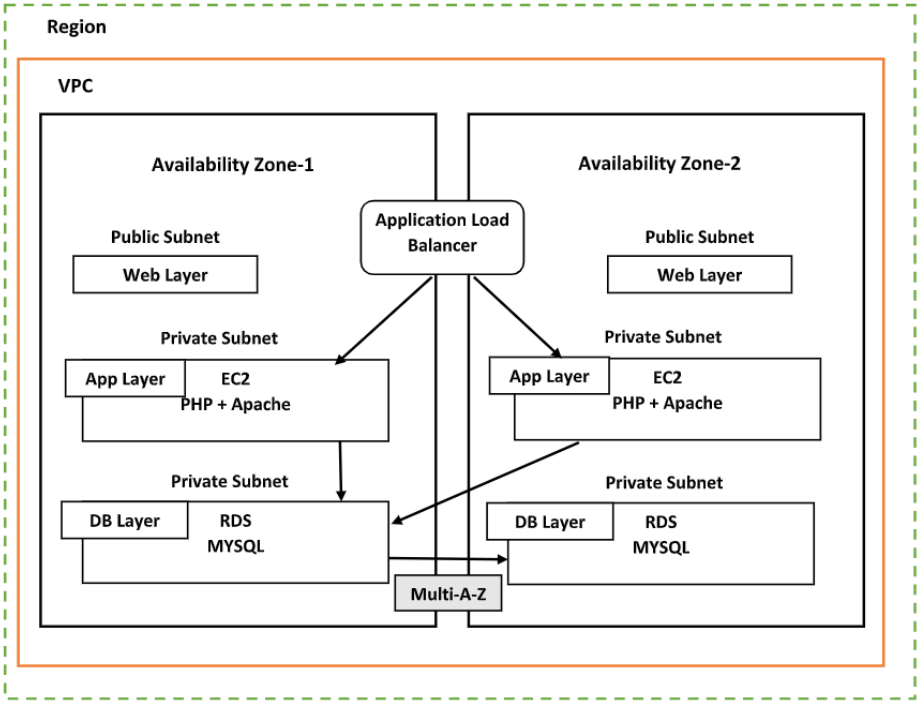
Three-tier architecture- Manual

Submitted By:

Shaheer Sarfraz

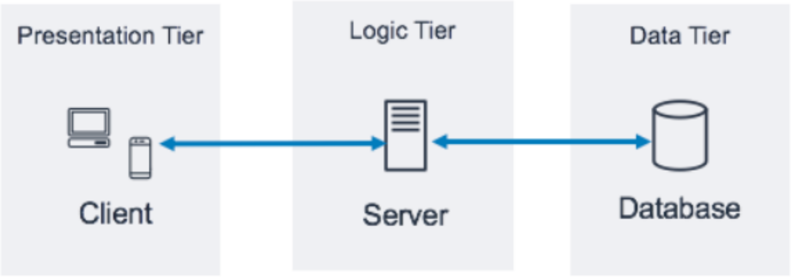
Question:

Deploy an application on a three tier architecture.



Problem Understanding:

The three-tier architecture is the most popular implementation of a multi-tier architecture and consists of a single presentation tier, logic tier, and data tier. This architecture is used in a client-server application such as a web application that has the frontend, the backend and the database.



What we are solving ?

Modularity:

The essence of having a three-tier architecture is to modularize our application so that each part can be managed independently.

Scalability:

Each tier of the architecture can scale horizontally to support the traffic and request demand coming to it.

High Availability:

we can design our infrastructure to be highly available by hosting our application in different locations known as the availability zones.

Fault Tolerance

We want our infrastructure to comfortably adapt to any unexpected change both to traffic and fault.

Security:

We want to design an infrastructure that is highly secured and protected from the prying eyes of hackers.

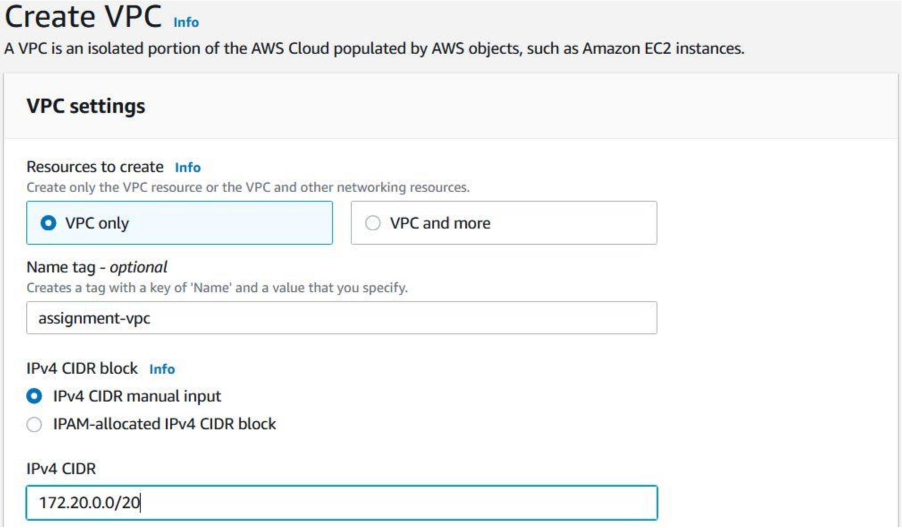
AWS Services:

- Elastic Compute Cloud (EC2)
- Auto Scaling Group
- Virtual Private Cloud (VPC)
- Elastic Load Balancer (ELB)
- Security Groups
- Internet Gateway.

Architecture Deployment:

Step 1: VPC

Create Virtual Private Cloud



Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.
● VPC only ○ VPC and more

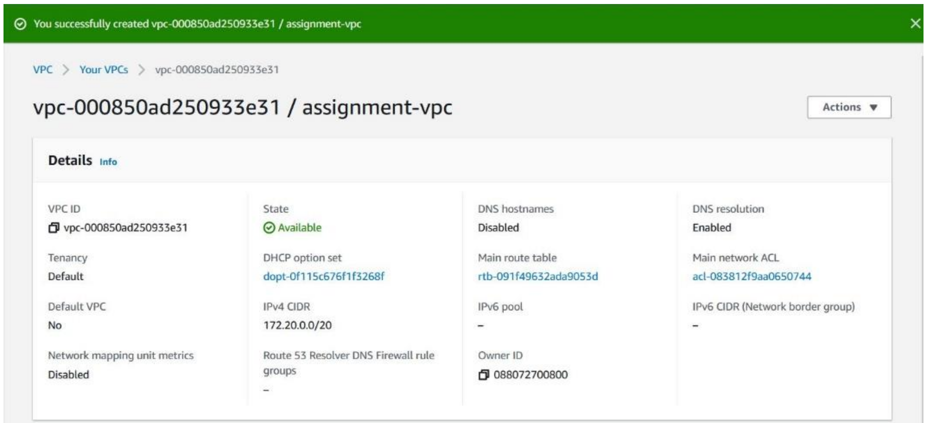
Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.
assignment-vpc

IPv4 CIDR block Info
● IPv4 CIDR manual input
○ IPAM-allocated IPv4 CIDR block

IPv4 CIDR
172.20.0.0/20

Fig:1.1

Fig:1.1 shows assigning IPv4 CIDR and Name tag for our VPC .



You successfully created vpc-000850ad250933e31 / assignment-vpc

VPC > Your VPCs > vpc-000850ad250933e31

vpc-000850ad250933e31 / assignment-vpc

Details Info

VPC ID
vpc-000850ad250933e31

State
Available

DNS hostnames
Disabled

DNS resolution
Enabled

Tenancy
Default

DHCP option set
dopt-0f115c676f1f3268f

Main route table
rtb-091f49632ada9053d

Main network ACL
acl-083812f9aa0650744

Default VPC
No

IPv4 CIDR
172.20.0.0/20

IPv6 pool
–

IPv6 CIDR (Network border group)
–

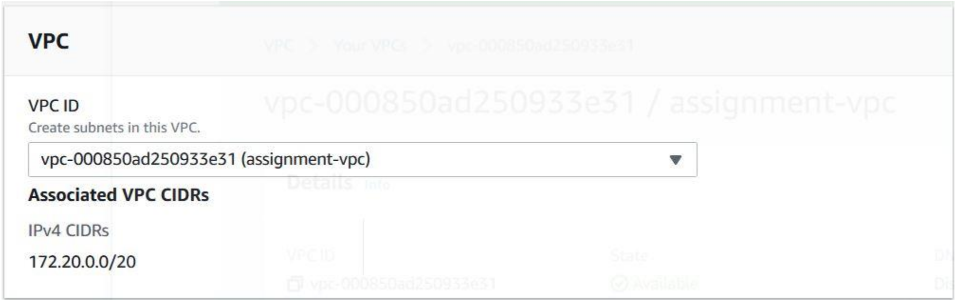
Network mapping unit metrics
Disabled

Route 53 Resolver DNS Firewall rule groups
–

Owner ID
088072700800

Fig:1.2

Step 2: Subnets



VPC

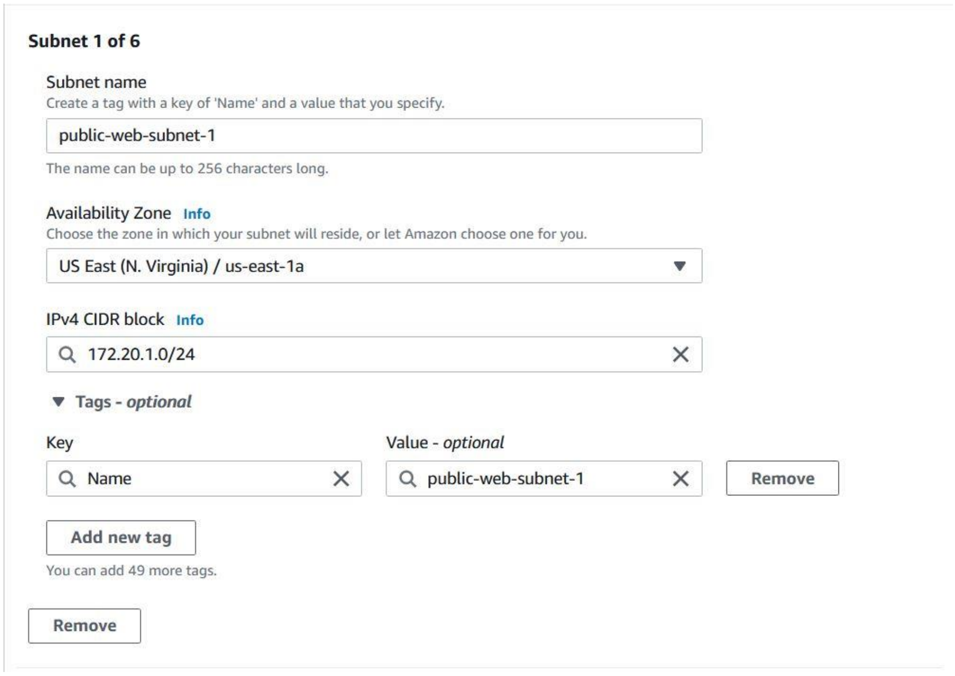
VPC ID
Create subnets in this VPC.
vpc-000850ad250933e31 (assignment-vpc) ▼

Associated VPC CIDRs

IPv4 CIDRs
172.20.0.0/20

Fig:2.1

For creating subnets we need to assign our VPC which is shown in fig:2.1.



Subnet 1 of 6

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
public-web-subnet-1
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (N. Virginia) / us-east-1a ▼

IPv4 CIDR block Info
172.20.1.0/24

▼ Tags - *optional*

Key	Value - *optional*	
Name	public-web-subnet-1	Remove

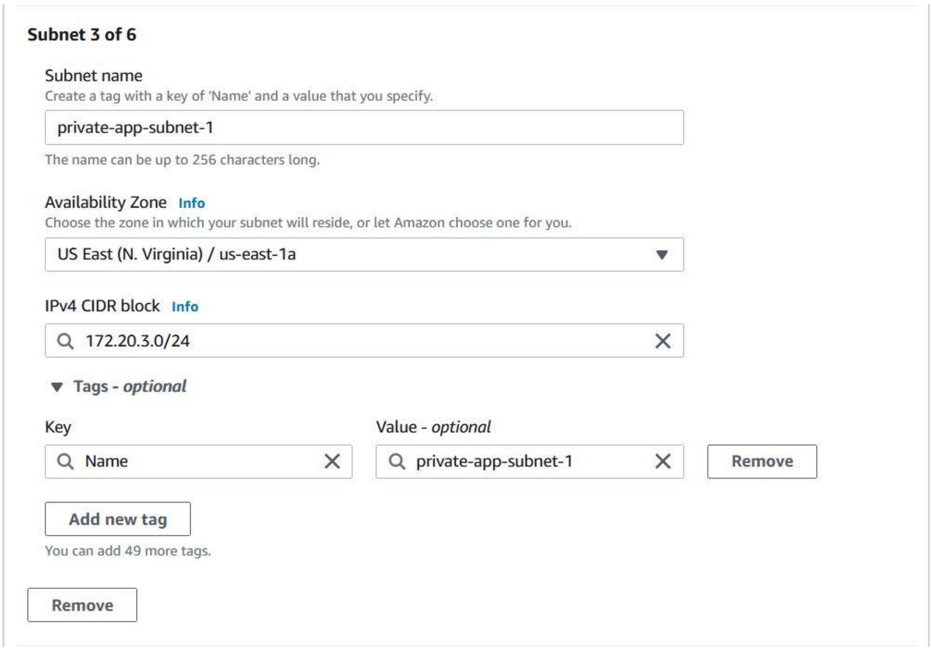
Add new tag
You can add 49 more tags.

Remove

Fig:2.2

Now creating subnet for web tier, setting availability zone and IPv4 which would be different for web subnet 1 and subnet 2 .

Now Creating Subnets for private app tier which is shown in fig:2.3.



Subnet 3 of 6

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
private-app-subnet-1
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (N. Virginia) / us-east-1a

IPv4 CIDR block Info
172.20.3.0/24

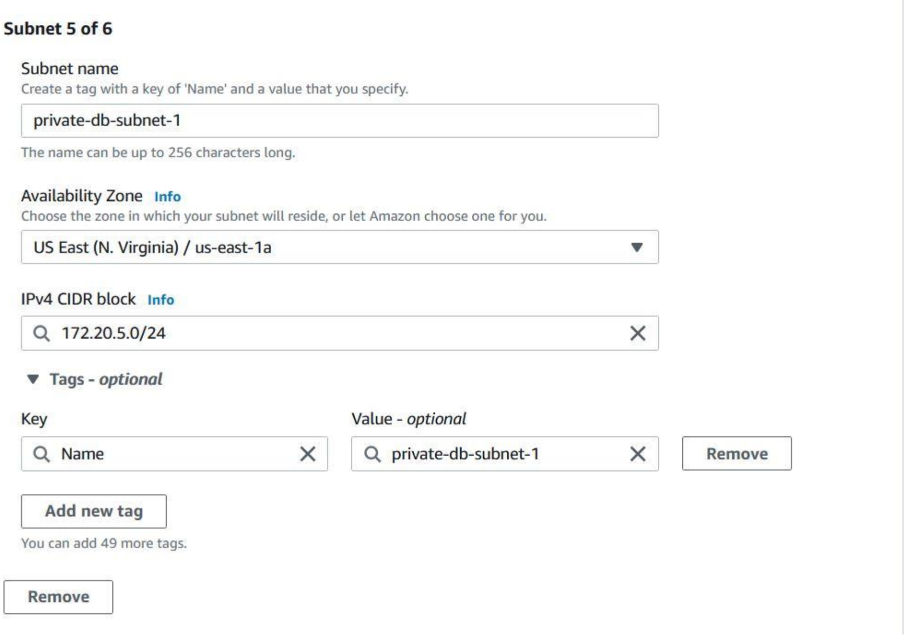
▼ Tags - *optional*

Key	Value - *optional*
Name	private-app-subnet-1

You can add 49 more tags.

Fig:2.3

Now Creating Subnets for private DB tier which is shown in fig:2.4.



Subnet 5 of 6

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
private-db-subnet-1
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (N. Virginia) / us-east-1a

IPv4 CIDR block Info
172.20.5.0/24

▼ Tags - *optional*

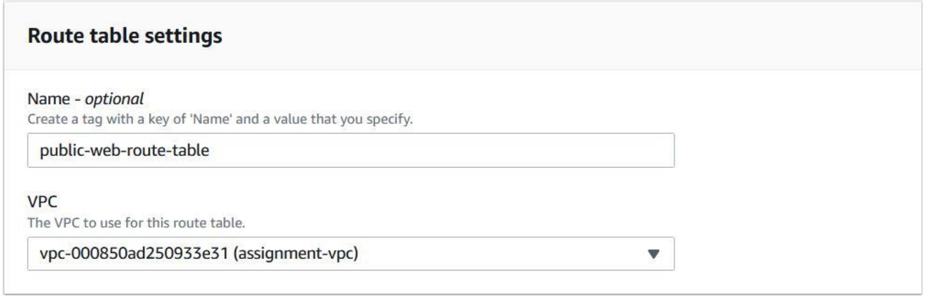
Key	Value - *optional*
Name	private-db-subnet-1

You can add 49 more tags.

Fig:2.4

Step 3:Route Table

Now we will create Route tables to which we can attach our subnets.

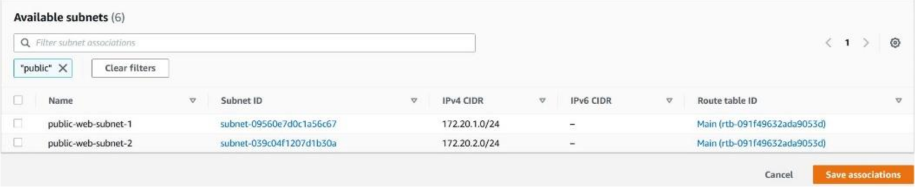


Route table settings

Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.
public-web-route-table

VPC
The VPC to use for this route table.
vpc-000850ad250933e31 (assignment-vpc)

Fig:3.1

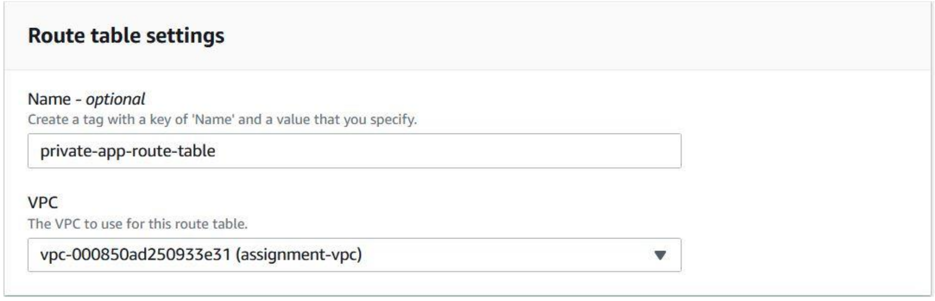


Available subnets (6)

□	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
□	public-web-subnet-1	subnet-09560e7d0c1a56c67	172.20.1.0/24	–	Main (rtb-091f49632ada9053d)
□	public-web-subnet-2	subnet-039c04f1207d1b30a	172.20.2.0/24	–	Main (rtb-091f49632ada9053d)

Fig:3.2

Attaching public-web-subnets to our public-web-route-table shown in fig:3.2.

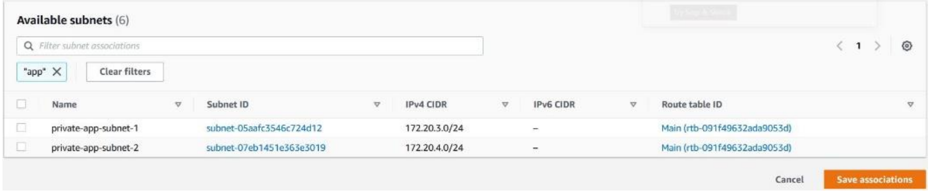


Route table settings

Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.
private-app-route-table

VPC
The VPC to use for this route table.
vpc-000850ad250933e31 (assignment-vpc)

Fig:3.3

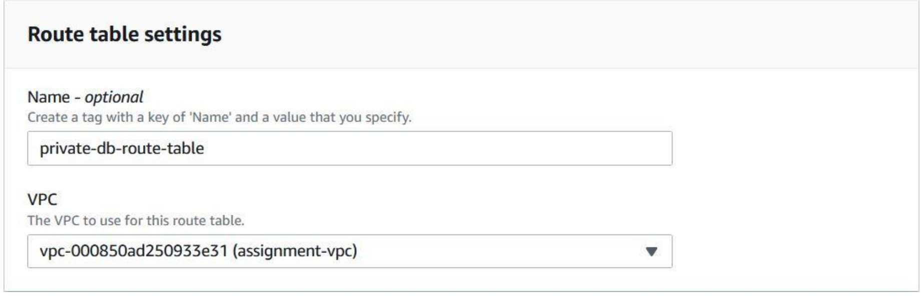


Available subnets (6)

□	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
□	private-app-subnet-1	subnet-05aafc3546c724d12	172.20.3.0/24	–	Main (rtb-091f49632ada9053d)
□	private-app-subnet-2	subnet-07eb1451e363e3019	172.20.4.0/24	–	Main (rtb-091f49632ada9053d)

Fig:3.4

Attaching private-app-subnets to our private-app-route-table shown in fig:3.4.

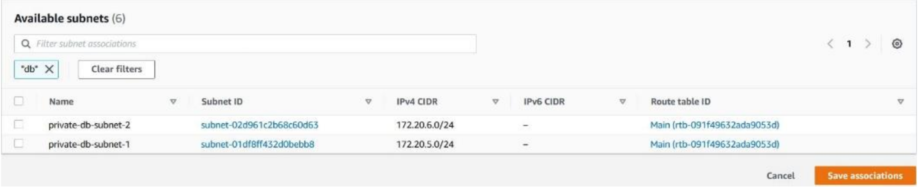


Route table settings

Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.
private-db-route-table

VPC
The VPC to use for this route table.
vpc-000850ad250933e31 (assignment-vpc)

Fig:3.5



Available subnets (6)

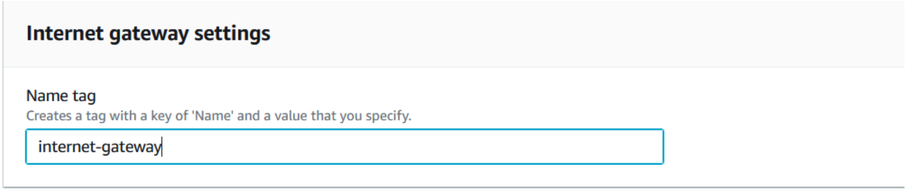
☐	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
☐	private-db-subnet-2	subnet-02d961c2b68c60d63	172.20.6.0/24	–	Main (rtb-091f49632ada9053d)
☐	private-db-subnet-1	subnet-01df8ff432d0bebb8	172.20.5.0/24	–	Main (rtb-091f49632ada9053d)

Fig:3.6

Attaching private-db-subnets to our private-db-route-table shown in fig:3.6.

Step 4: Internet Gateway

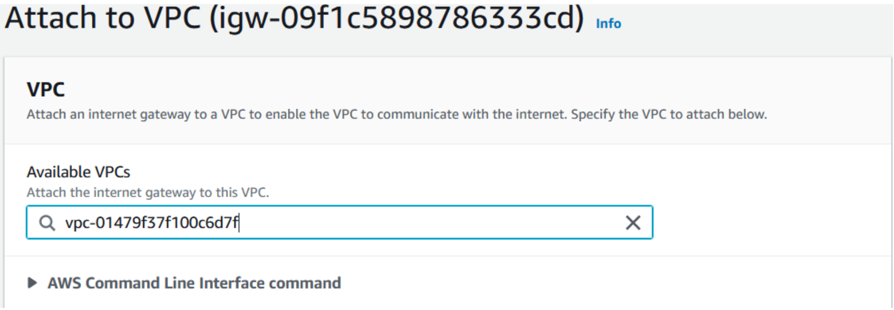
Creating Internet gateway which would be attached to our VPC.



Internet gateway settings

Name tag
Creates a tag with a key of 'Name' and a value that you specify.
internet-gateway

Fig:4.1



Attach to VPC (igw-09f1c5898786333cd) Info

VPC
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

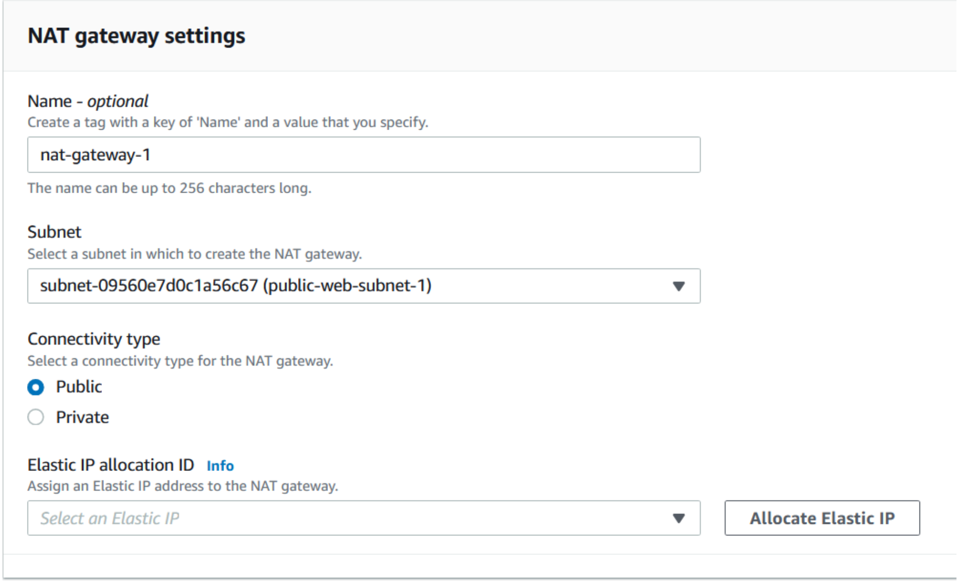
Available VPCs
Attach the internet gateway to this VPC.
vpc-01479f37f100c6d7f

▶ AWS Command Line Interface command

Fig:4.2

Step 5: NAT Gateway

Creating NAT gateway for our private subnets.



NAT gateway settings

Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.
nat-gateway-1
The name can be up to 256 characters long.

Subnet
Select a subnet in which to create the NAT gateway.
subnet-09560e7d0c1a56c67 (public-web-subnet-1)

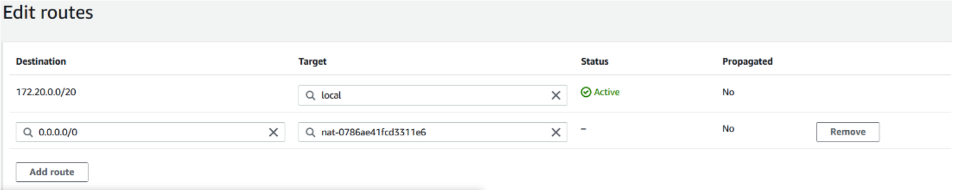
Connectivity type
Select a connectivity type for the NAT gateway.
● Public
○ Private

Elastic IP allocation ID Info
Assign an Elastic IP address to the NAT gateway.
Select an Elastic IP

Fig:5.1

Step 6:Setting Routes

Now we will set routes for public and private tiers.

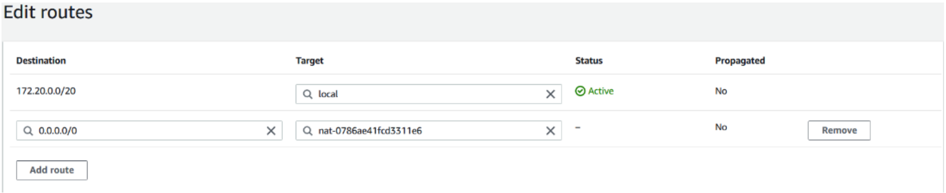


Edit routes

Destination	Target	Status	Propagated	
172.20.0.0/20	local	Active	No	
0.0.0.0/0	nat-0786ae41fcd3311e6	-	No	Remove

Fig:6.1

Setting NAT for App tier shown in fig:6.1.

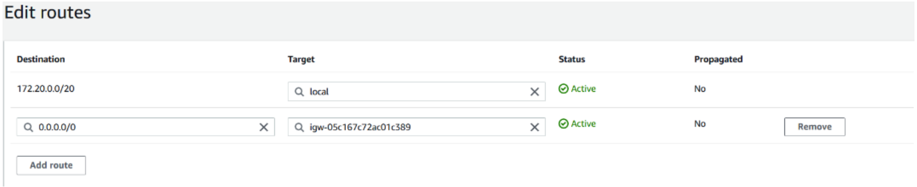


Edit routes

Destination	Target	Status	Propagated	
172.20.0.0/20	local	Active	No	
0.0.0.0/0	nat-0786ae41fcd3311e6	-	No	Remove

Fig:6.2

Setting NAT for DB tier shown in fig:6.2.



Edit routes

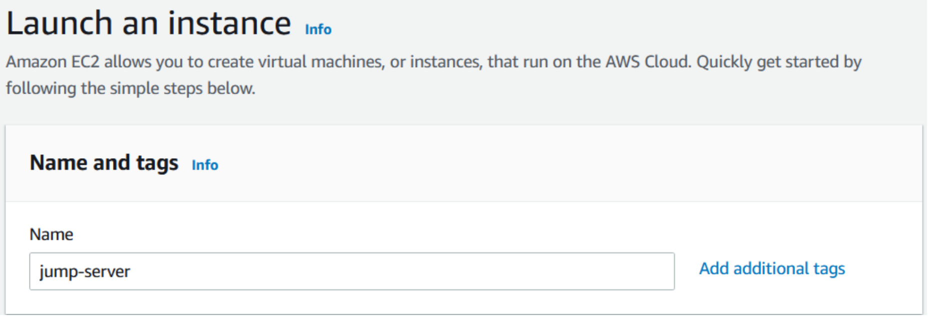
Destination	Target	Status	Propagated	
172.20.0.0/20	local	Active	No	
0.0.0.0/0	igw-05c167c72ac01c389	Active	No	Remove

Fig:6.3

Setting Internet Gateway for Web layer shown in fig:6.3.

Step:7 Launch Instances

Setting jump server instance for our architecture



Launch an instance

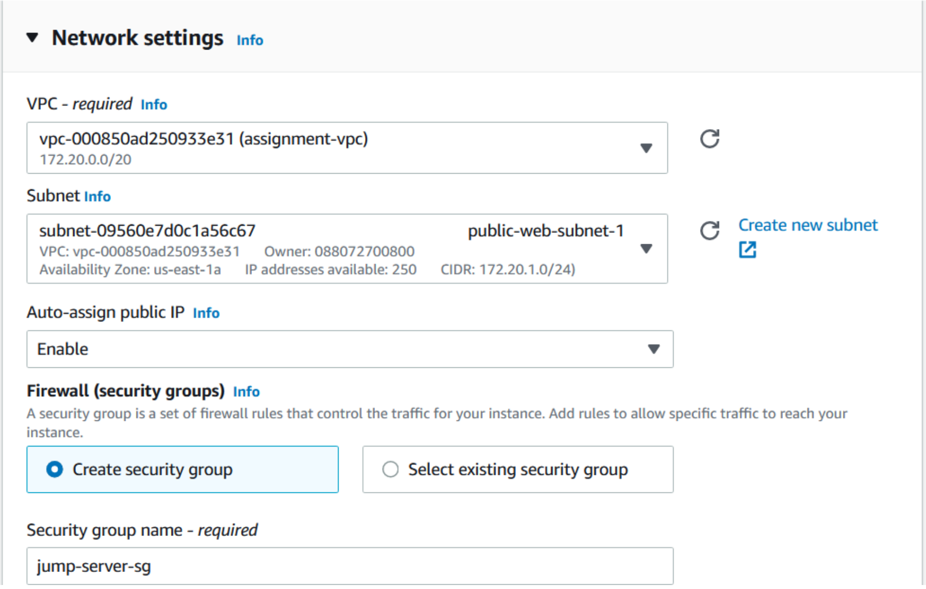
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Name: jump-server

Fig:7.1

Now selecting our VPC, subnet and security group



Network settings

VPC - *required*: vpc-000850ad250933e31 (assignment-vpc) 172.20.0.0/20

Subnet: subnet-09560e7d0c1a56c67 public-web-subnet-1
VPC: vpc-000850ad250933e31 Owner: 088072700800
Availability Zone: us-east-1a IP addresses available: 250 CIDR: 172.20.1.0/24)

Auto-assign public IP: Enable

Firewall (security groups)

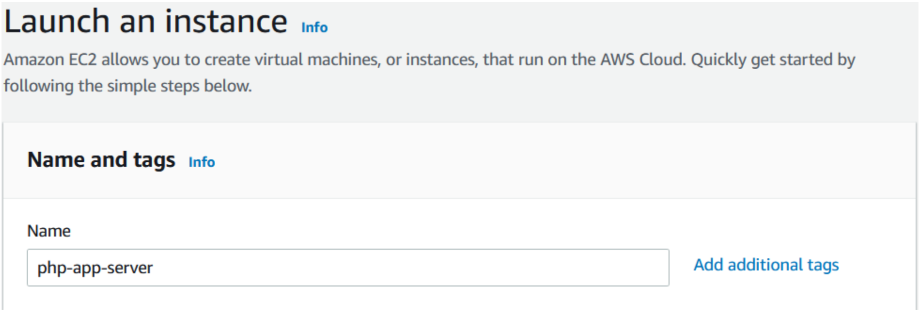
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

Security group name - *required*: jump-server-sg

Fig:7.2

Now creating php server instance



Launch an instance Info

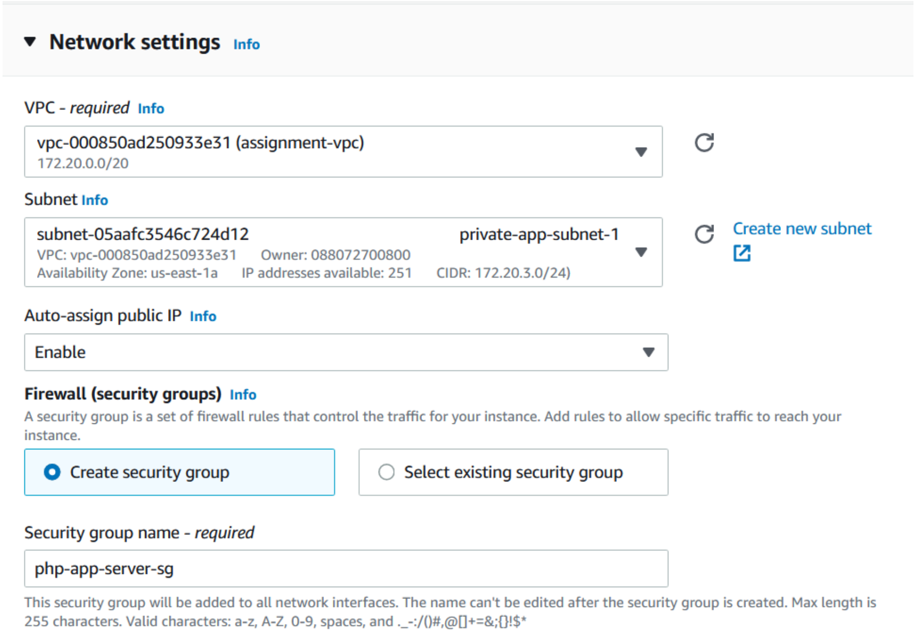
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name: php-app-server

Fig:7.3

Now selecting our VPC, subnet and security group.



▼ Network settings Info

VPC - *required* Info

vpc-000850ad250933e31 (assignment-vpc)
172.20.0.0/20

Subnet Info

subnet-05aafc3546c724d12 private-app-subnet-1
VPC: vpc-000850ad250933e31 Owner: 088072700800
Availability Zone: us-east-1a IP addresses available: 251 CIDR: 172.20.3.0/24)

Auto-assign public IP Info

Enable

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

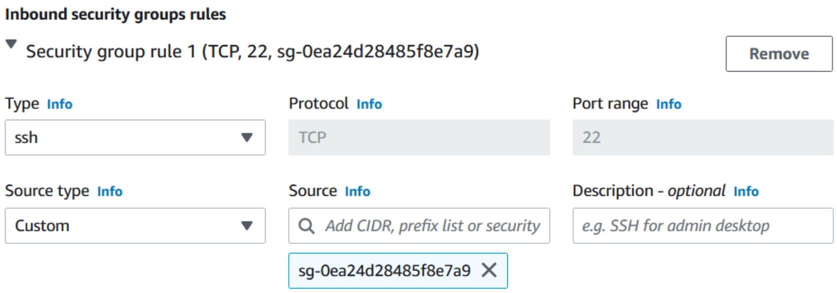
Security group name - *required*

php-app-server-sg

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Fig:7.4

For the inbound rule we will set custom and choose our jump server.



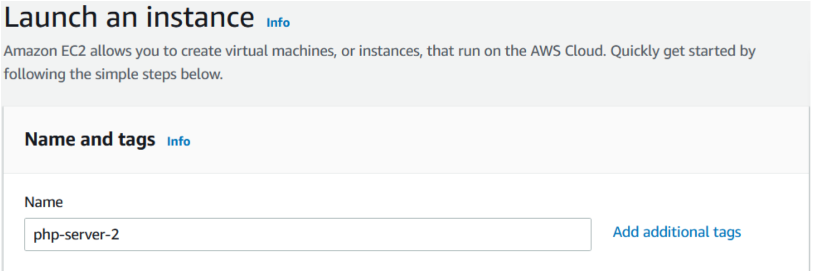
Inbound security groups rules

▼ Security group rule 1 (TCP, 22, sg-0ea24d28485f8e7a9)

Type Info	Protocol Info	Port range Info
ssh	TCP	22
Source type Info	Source Info	Description - *optional* Info
Custom	Add CIDR, prefix list or security sg-0ea24d28485f8e7a9 ✕	e.g. SSH for admin desktop

Fig:7.5

Create instance for php subnet 2



Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

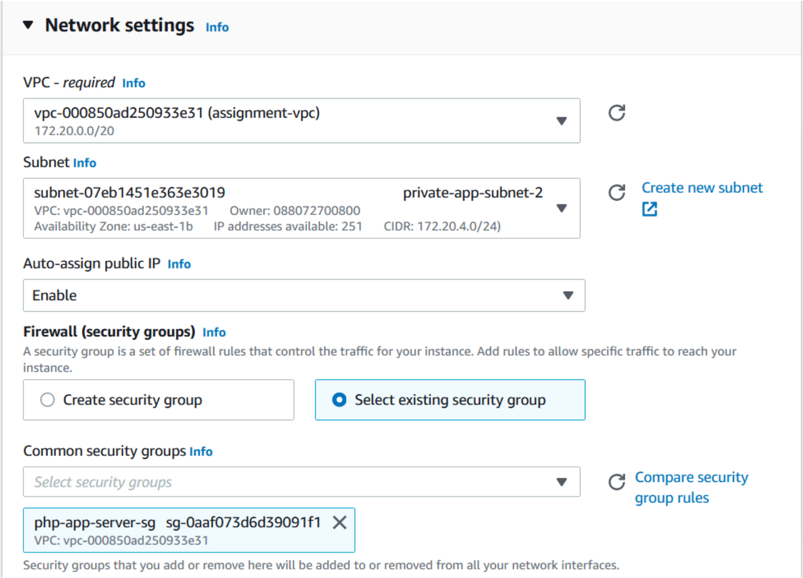
Name and tags Info

Name

php-server-2

Fig:7.6

We will choose the app subnet 2 and choose our existing security group which we made for php-server-1



Network settings Info

VPC - *required* Info

vpc-000850ad250933e31 (assignment-vpc)
172.20.0.0/20

Subnet Info

subnet-07eb1451e363e3019 private-app-subnet-2
VPC: vpc-000850ad250933e31 Owner: 088072700800
Availability Zone: us-east-1b IP addresses available: 251 CIDR: 172.20.4.0/24)

Auto-assign public IP Info

Enable

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

○ Create security group ● Select existing security group

Common security groups Info

Select security groups

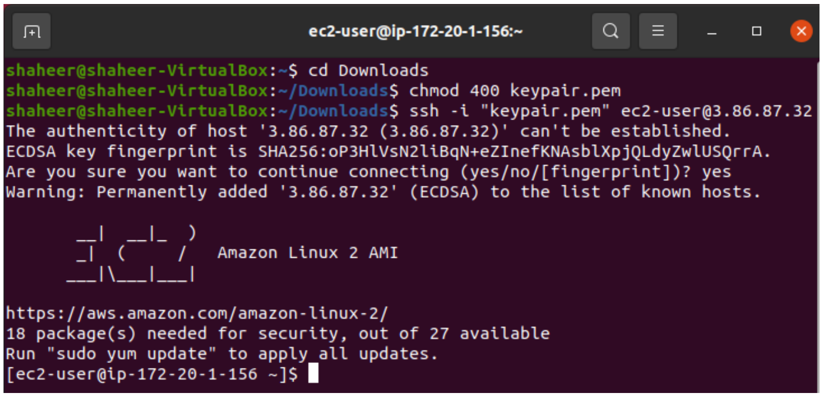
php-app-server-sg sg-0aaf073d6d39091f1
VPC: vpc-000850ad250933e31

Security groups that you add or remove here will be added to or removed from all your network interfaces.

Fig:7.7

Step:8 Connection with local machine

Now we will connect jump-server to our local machine and php-servers to jump-server

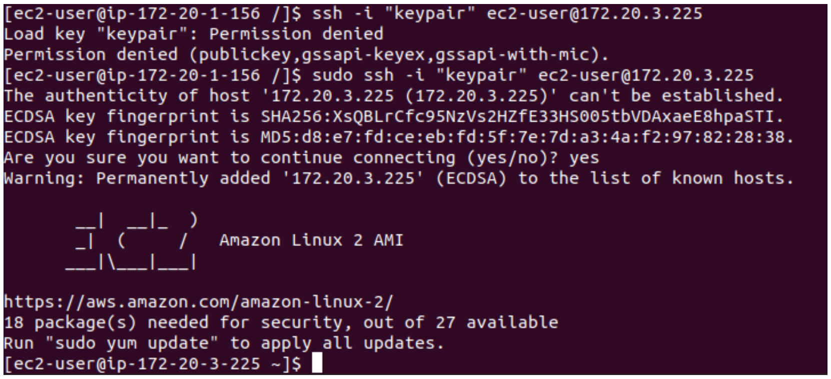


```
shaheer@shaheer-VirtualBox:~$ cd Downloads
shaheer@shaheer-VirtualBox:~/Downloads$ chmod 400 keypair.pem
shaheer@shaheer-VirtualBox:~/Downloads$ ssh -i "keypair.pem" ec2-user@3.86.87.32
The authenticity of host '3.86.87.32 (3.86.87.32)' can't be established.
ECDSA key fingerprint is SHA256:oP3HlVsN2liBqN+eZInefKNAsblXpjQLdyZwlUSQrrA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '3.86.87.32' (ECDSA) to the list of known hosts.

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
18 package(s) needed for security, out of 27 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-20-1-156 ~]$ 
```

Connecting jump-server to php-app-server.



```
[ec2-user@ip-172-20-1-156 /]$ ssh -i "keypair" ec2-user@172.20.3.225
Load key "keypair": Permission denied
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[ec2-user@ip-172-20-1-156 /]$ sudo ssh -i "keypair" ec2-user@172.20.3.225
The authenticity of host '172.20.3.225 (172.20.3.225)' can't be established.
ECDSA key fingerprint is SHA256:XsQBLrCfc95NzVs2HZfE33HS005tbVDAxaeE8hpaSTI.
ECDSA key fingerprint is MD5:d8:e7:fd:ce:eb:fd:5f:7e:7d:a3:4a:f2:97:82:28:38.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.20.3.225' (ECDSA) to the list of known hosts.

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
18 package(s) needed for security, out of 27 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-20-3-225 ~]$ 
```