Select Mumbai region

Step 1: Create VPC (MyVPC) - 10.0.0.0/16

Step 2: Create two subnets

subnet1 - 10.0.1.0/24 - WebSN

subnet2 - 10.0.2.0/24 - DbSN

Step 3: Enable public IP to subnet1

Step 4: Create Internet Gateway attach to VPC -- MyIGW

Step 5: Create Route table -- InternetRT

Step 6: Attach Route table to subnet1

Step 7: Attach Route table to Internet Gateway

Now, subnet1 is public.

++++++++++++

Now, Let’s launch webserver in public subnet.

Services ---Ec2 ---- Launch instance -- Step3 Network: MyVPC

Subnet: 10.0.1.0/24

Additional Details -- User Data

#!/bin/bash

sudo su

yum update -y

yum install httpd -y

cd /var/www/html

echo "MyGoogle" > index.html

service httpd start

chkconfig httpd on

Next -- Next -- Name Tag: WebServer ---> Next -- Security Group : WebSG33 , Description: WebSG33

ADD RULE

Type Source

SSH Anywhere

HTTP Anywhere

Review and launch --- Launch -- Download keypair --> ( webKP33.pem ) Launch-- View Instance

+++++++++++++++++++++

Let’s Launch Database Server in Private Subnet.

Services ---Ec2 ---- Launch instance -- Step3 Network: MyVPC

Subnet: 10.0.2.0/24

Name Tag: DbServer -- ---> Next -- Security Group: DbSG33, Description: DbSG33

Change Type from SSH to MYSQL/Aurora

Type Source

MYSQL/Aurora Custom 10.0.1.0/24

(MySQL Port is open to entire subnet)

Review and launch -- Launch --> Create new keypair --> (dbKP33.pem ) launch instances --- View instances

++++++++++++++++

Now, web server can pull data from database server.

++++++++++++++++++++++++++++++++++++++++++++++++++

DBA wants to create some files. Wants to perform maintenance activity.

Can he connect?

As DB Server is not having public IP and it is not having internet connectivity, DBA cannot connect.

For this, we need to create Bastion server/ Jump server in public subnet

It is nothing but normal EC2 Machine

Services -- EC2 -- Launch -- Amazon Linux ---> select VPC , Select subnet

Name: BastionServer

Security Group: BastionSG33

Description: BastionSG33

(SSH port -- should be open to myself)

Type Source

SSH My IP

Review and launch –- launch -- Create new keypair ---Bastion33.pem

View Instances

+++++++++++++++

Now, Only I can connect to Bastion server through SSH

From the Bastion server, I should able to jump into Dbserver.

That means, DbServer SSH port should be open to Bastion server.

Goto Dbserver security group - DbSG30 ( new tab )

Select DbSG -- Inbound --Edit

Add Rule

Type Source

SSH Custom 10.0.1.66/32 (Private IP of bastion server)

Save.

Now, Let’s test can we connect to DB server

In EC2 Dashboard -- select bastion server -- connect

copy user@public\_ip

Open putty

Host Name - user@public\_ip

Provide PPK file -- Connect!

$ sudo su

# yum update -y

From bastion-- we need to jump to dbserver

Now, to connect to DBserver, we need to enter the details to DBserver in Bastion server.

Select DbServer --- connect

Copy the entire ssh command.

As we are connecting from linux to linux .pem file is enough.

Enter the ssh command in putty.

eg:

# ssh -i "DbKP7.pem" ec2-user@10.0.2.106

Note: To connect the .pem file need to be present in present working directory.

Now, we need to copy abc.pem file in bastion server.

It is there in our windows machine.

We use WINSCP to transfer the file from windows to linux

In google search for "WinSCP"

winscp.net

download and run.

Open WINSCP

We will connet to bastion server using Winscp

host name: user@ipaddress

advanced ---Authentication --- private key file - select the ppk file -- open -- ok - login

Now, drag and drop the pem file to bastion server.

In Putty

# ls ( We should able to see the file )

Now connect to Dbserver by running the SSH command

# ssh -i "DbKP7.pem" ec2-user@10.0.2.106

You are now connected to DBserver!!!

Now, In DB server, lets execute the following commands

$ sudo su

#

Now I want to upgrade the latest version of MYSQL database

Command to upgrade MYSQL database

# yum install mysql -y

not successful.

We cannot install, As we are not having internet connection to private subnet.

TO get internet connection, we create NAT server. (Network Address Translator)

The purpose of NAT is to provide internet to private subnet.

We need to create NAT in public subnet.

In VPC Dashboard

NAT Gateways --> Create NAT Gateway ( myNAT )

subnet: 10.0.1.0/24 (WebSN)

Create new EIP (allocate elastic ip) ---> Create a NAT Gateway -- Close

NAT needs 2 min appox to get created.

Name it as NAT

++++++++++++++

**What is Elastic IP?**

It is similar to Static IP

When we stop and start the EC2 Machines, public IP will change.

If you stop and start the machine, you want the same public IP, then we create Elastic IP

Elastic IP is nothing but static public IP

**Why do we need Elastic IP to NAT?**

If in case NAT is down, entire private subnet will not get internet.

Then we restart the NAT again, then it acquires new public IP

When NAT acquire new public IP, there could be connection issue.

So, we need Elastic IP to NAT

++++++++++++++++

NAT is a closed box. It does not have any ports concept.

No one, can connect to NAT.

We cannot connect NAT to private Subnet.

So, we create RouteTable.

One end of RouteTable , I connect to NAT.

Another end of RouteTable, I Connect to private subnet.

Instead of creating new RouteTable, we can use default RouteTable which was created, when we created VPC

Let’s change the name of default RouteTable to NatRT

Select NatRT -- Subnet Associations -- Edit subnet Associations -- select private subnet-- save

Select NatRT -- Routes -- Edit Routes --Add Route -- Target: NAT Gateway ( Select NAT )

Destination- 0.0.0.0/0 -- Save routes -- close

Now, let’s test are we able to get internet to our DBServer.

Run the same command in putty again

# yum install mysql -y

It Works!!

Deletion process

-------------------------

Step 1: Delete NAT

Step 2: Delete EC2 Machines

Step 3: Delete VPC

Step 4: Release Elastic IPs (Select Elastic IP from dashboard -- Actions -- Release Address)