Make VPC

* 4 subnets (1 public, 3 private)
* Enable in subnet settings public ip addresses
* Make it highly available (use 2 availability zones, the final private subnet can be the only one in a different subnet)
* Allocate an Elastic IP
* Create a nat gateway
* Create an internet gateway and attach it to your VPC
* Make route tables for your public and private subnets and attach an internet gateway and nat gateway to them respectively
* Make security groups for Bastion Host, web server, app server, and database
* Make sure to go back to security groups after making them and adding security groups to link them together, for example in the app server security group adding a rule for the database security group after creating the database security group.

Create Bastion Host

* EC2 instance
  + Amazon linux 2 ami
  + T2.micro
  + Use your vpc and public subnet
  + Use Security Group for Bastion Host made in VPC Setup

Create Web Server

* EC2 instance
  + Amazon linux 2 ami
  + T2.micro
  + Use your vpc and public subnet
  + In user data
    - #!/bin/bash
    - sudo yum update -y
    - sudo amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
    - Sudo yum install -y httpd
    - Use sudo systemctl start httpd to start up the webserver
    - Use sudo systemctl enable httpd to do it on reboot
  + Use Security Group for Web Server made in VPC Setup

Create App Server

* EC2 instance
  + Amazon linux 2 ami
  + T2.micro
  + Use your vpc and public subnet
  + Type into user data
    - #!/bin/bash
    - sudo yum install -y mariadb-server
    - Sudo service mariadb start
  + Use Security Group for App Server made in VPC Setup

Create DB instance

* Create a subnet group
* Make a database instance
  + Standard create
  + mariadb
  + Free Tier
  + Disable automated backups
  + Disable encryption
  + User = root
  + Password = test
  + Initial database = mydb

Upload ssh keys to Bastion Host

* Windows users
  + Go to your command prompt and type out
    - Pscp -scp -P 22 -i ’.\Downloads\labsuser.ppk’ -l user ec2-user ‘.\Downloads\labsuser.pem’ ec2-user@bastion-host-public-ip:/home/ec2-user
    - Replace labsuser.ppk and labsuser.pem with what you named your keys
    - Replace bastion-host-public-ip with your bastion host public ip address
* Mac and Linux Users
  + Go to your terminal and type out
    - Chmod 400 labuser.pem
    - Scp -i ’.\Downloads\labsuser.pem’ -l user ec2-user ’.\Downloads\labsuser.pem’ ec2-user@bastion-host-public-ip:/home/ec2-user
    - Replace labsuser.ppk and labsuser.pem with what you named your keys
    - Replace bastion-host-public-ip with your bastion host public ip address

Test to make sure key was uploaded into Bastion Host

* Ssh into Bastion Host
* Type ls
* Labsuser.pem should show up

Connect to App Server

* From ssh inside of Bastion Host use the terminal
* Type out chmod 400 labsuser.pem to change file permissions
* Type out ssh -i my-key-pair.pem ec2-user@app-server-private-ip
* Replace my-key-pair with the name of your key
* Replace app-server-private-ip with your app server’s private ip address
* Test out pinging the web server by typing out ping and the private ip address
* Test out connecting to database by typing out mysql –user

=root -password=’test’ –host=database-server-endpoint

* Replace database-server-endpoint with the database server endpoint
* Type show databases; to see your database from the app server