Design a solution for a multi-tier web application that will be deployed in a custom VPC.

1. Create a custom VPC with CIDR block 10.0.0.0/16 with:
   * 2 Public subnets in two different AZs US-east-1a and us-east-1B in US-east-1 region. Use 10.0.10.0/24 and 10.0.20.0/24 ranges for these two subnets.
   * 2 Private Subnets in the same AZs as above. Use 10.0.100.0/24 and 10. 0.200.0/24. Create a separate route tables for the private subnets.
2. Launch two EBS-backed EC2 instances, one in each of the two private subnets above (10.0.100.0/24 and 10.0.200.0/24).
   * The instances will serve as the web and application tiers.
   * Ensure that the EBS volumes of these instances are encrypted at rest.
   * The instances will have the following user data script run at launch time.
   * Launch a NAT gateway in each of the two availability zones above to allow the two instances to access the internet for updates. Adjust the private subnets route table(s) to route the update traffic through the NAT Gateway.
   * The security group assigned to the instances should use the name webSG and must allow ports ssh (22), http (80) and https (443) in the inbound direction.

# The bash script to use for this project requirements

# #!bin/bash

# yum update -y

# yum install httpd -y # installs apache (httpd) service

# systemctl start httpd # starts httpd service

# systemctl enable httpd # enable httpd to auto-start at system boot

# echo " This is server \*1\* in AWS Region US-EAST-1 in AZ US-EAST-1B " > /var/www/html/index.html

#!bin/bash

yum update -y

yum install httpd -y

systemctl start httpd

systemctl enable httpd

echo " This is server \*1\* in AWS Region US-EAST-1 in AZ US-EAST-1A " > /var/www/html/index.html

1. create a target group with the name webTG and add the two application instances to it.
   * The target group will use the port 80 (HTTP) for traffic forwarding and health checks.
2. Launch an application load balancer that will load balance to these two instances using HTTP. The application load balancer must be enabled in the two public subnets you have configured in step 1.
   * Adjust the security group of the web/app instances to allow inbound traffic only from the application load balance security group as a source.
   * The ALB security group (ALBSG) must allow outbound http to the web/app security group (webSG)
   * The ALBSG must allow inbound traffic from the internet on port http.
3. Configure a target tracking auto scaling group that will ensure elasticity and cost effectiveness. The Auto Scaling group should monitor to the two instances and be able to add instances on-demand and replaced failed instances.
4. Launch a Multi AZ RDS database and ensure that its security group will only allow access from the web/app tier security group above.
5. Test to ensure thart you can get to the index.html message on the instances through the load balancer. If it works, congratulations on finishing this amazing project on AWS.