**Design Document**

Configuration for this scenario includes   
  
**Region**   
us-east-1  
  
**Availability Zone**   
us-east-1a  
us-east-1b  
  
**Resources**

1. **Virtual Private Network**  
   IPv4 CIDR Block - 10.0.0.0/16

Enable DNS Hostnames - True

1. **Public Subnets**Subnet 1   
   IPv4 CIDR Block – 10.0.1.0/24  
    AZ – us-east-1a  
   Subnet 2   
   IPv4 CIDR Block – 10.0.3.0/24  
   AZ – us-east-1b
2. **Internet Gateway**Entity attached to a VPC will allow internet traffic flow to the public subnet
3. **Route Tables**Need to create a route table to route the outside world and map it to our internet gateway
4. **Route Tables Association**Public subnets need to be associated with route table to access internet
5. **Application Load Balancer**Facing the internet and managing EC2 instances behind it which also serves as a SSL termination proxy
6. **Bastion Hosts**To allow secure access to EC2 instances
7. **Private Subnets**Subnet3  
   IPv4 CIDR Block – 10.0.2.0/24  
    AZ – us-east-1a  
   Subnet4  
   IPv4 CIDR Block – 10.0.4.0/24  
    AZ – us-east-1b
8. **NAT Gateways**  
   Instances launched in the private subnet will be able to communicate with any services within VPC and go to the internet using NAT gateway
9. **Elastic IP**  
   NAT gateway cannot be launched without elastic IP address associated with it
10. **Route Table – Private Subnet**CIDR Block – 0.0.0.0/0  
    Associate with NAT Gateway
11. **Route Table Association**Private subnet needs to be associated with route table
12. **DB Instance**PostgreSQL version 10.14 in private subnet
13. **S3 Bucket**For database backups and logs
14. **CloudWatch**Basic monitoring for all applications, collect and store logs.