**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
2. **Internet Gateway**Entity attached to the VPC will allow internet traffic flow to the public subnet
3. **Application Load Balancer**Facing the internet and managing EC2 instances behind it which also serves as a SSL termination proxy
4. **In the 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  
   Route Table  
   Associated with Internet Gateway

|  |  |
| --- | --- |
| Destination | Target |
| 10.0.0.0/16 | Local |
| 0.0.0.0/0 | Igw |

Route Table AssociationAssociation between a route table and a subnet, internet gateway or NAT gateway  
  
Bastion HostsTo allow secure access to EC2 instances

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

Elastic IP  
NAT gateway cannot be launched without elastic IP address associated with it

1. **In the Private Subnets:**Subnet 3IPv4 CIDR Block – 10.0.2.0/24  
    AZ – us-east-1a  
     
   Subnet4  
   IPv4 CIDR Block – 10.0.4.0/24  
    AZ – us-east-1b  
     
   Route TableAssociate with NAT Gateway

|  |  |
| --- | --- |
| Destination | Target |
| 10.0.0.0/16 | local |
| 0.0.0.0/0 | ngw |

Route Table AssociationInstances in private subnet needs to be associated with route table  
  
EC2 Instances  
OS – Amazon Linux 2  
Type – t3.small  
Application – JIRA – Version 8.13.1 LTS  
  
DB Instance  
Engine – PostgreSQL – Version 10.14  
Class – db.t3.small  
Storage – General Purpose (SSD) – 20 GiB  
Multi AZ – Yes  
Automatic Backups – Yes  
Backup Retention Period – 7 days  
Backup Window – Start Time – 02:00 IST – Duration – 1 Hour  
Encryption – Yes  
Performance Insights – Yes  
Deletion Protection – Yes

1. **S3 Bucket**Storing database backups and logs centrally  
   Implement WORM  
   Using encryption keys
2. **AWS KMS**

Create and manage keys

1. **AWS RDS**Scalable relational database with high availability, security and low cost
2. **AWS Systems Manager**View operational data for group of resources  
   Parameter Store – Managing secrets centrally for databasePatch Manager – Managing patching centrally for instances
3. **CloudWatch**Monitor JIRA instances  
   Capturing access logs for ALB  
   Monitor resources, collect and store logs