

Application (MERN stack) deployed in HA, secure environment

1. Created VPC with CIDR 172.0.0.0/16
2. Two private subnets and public subnets were created in two availability Zone
3. Created public route table , associated with public subnets where traffic going to destination 0.0.0.0/0 (all traffic) is targeted to **Internet Gateway**
4. Created private route table, pointing to private subnet
5. Created one EC2 instance in public subnet – AZ 1A to host **frontend application (in React.JS)** & installed Node JS which comes with NPM(Node Package Manager)
6. Created two more EC2 instances in public subnet – AZ 1b to host

* **frontend application (in React.JS) to make it high available** & installed Node JS which comes with NPM(Node Package Manager)
* **back end application in Express framework** and install **Node** there as well

1. Created Elastic IP for backend application
2. Have EIP of backend application coded in frontend application , so that it can invoke backend API
3. Created Document DB (MongoDB engine 4.0) cluster in private subnet
4. IAM role is created for backend application to access Document DB, **enhancing security**
5. Back end application is coded to access Document DB URI using mongoose package and also certificate is installed to access document DB securely from application program
6. All these application endpoints and database endpoint are having security group in front. So traffic coming from internet has to meet SG to access application/DB
7. Created **Application load balancer(ALB1)** in two AZs, mapping two front end application server as target
8. Also created route 53 ALIAS record to map ALB

Thus [www.myapp.com](http://www.myapp.com) (not actual name, actual application is shutdown to not incur server cost) **is able to securely communicate with DB (hosted in private subnet) in high availability environment.**