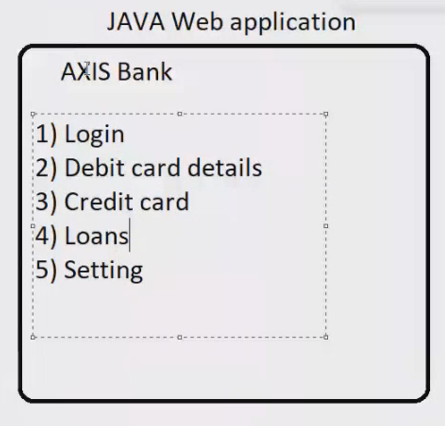
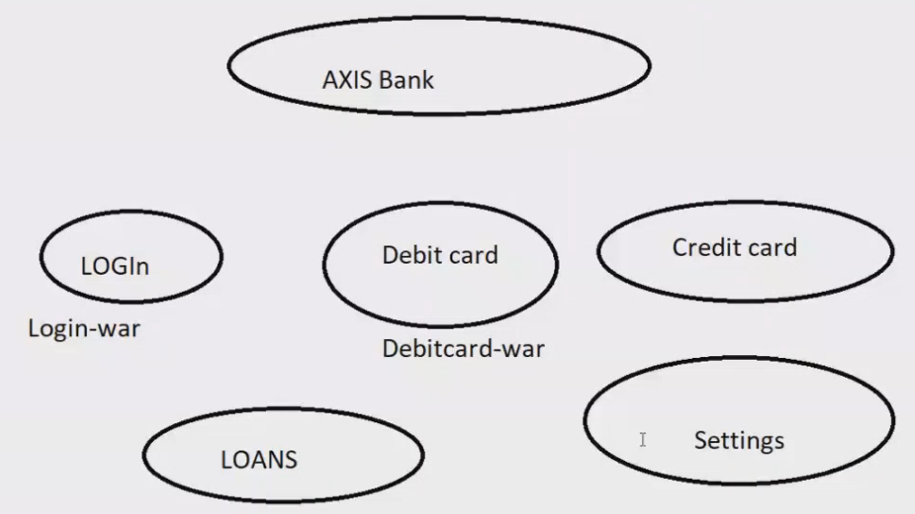
**AWS Architecture**

**CURRENTLY WE ARE USING MICRO-SERVICES ARCHITECTURE;**

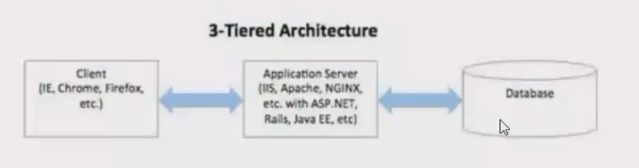
* **MONOLITH**
* **MICRO-SERVICES**

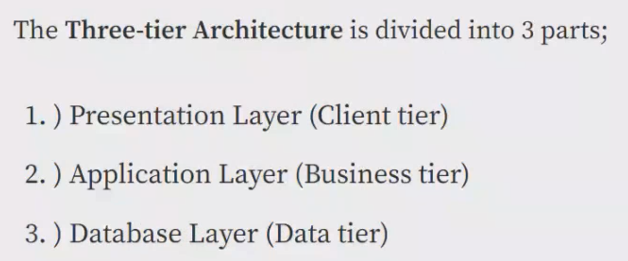
**MONOLITH Architecture: All are in one package if any parameter get disturbed so the entire page content we can’t be accessible.**

****

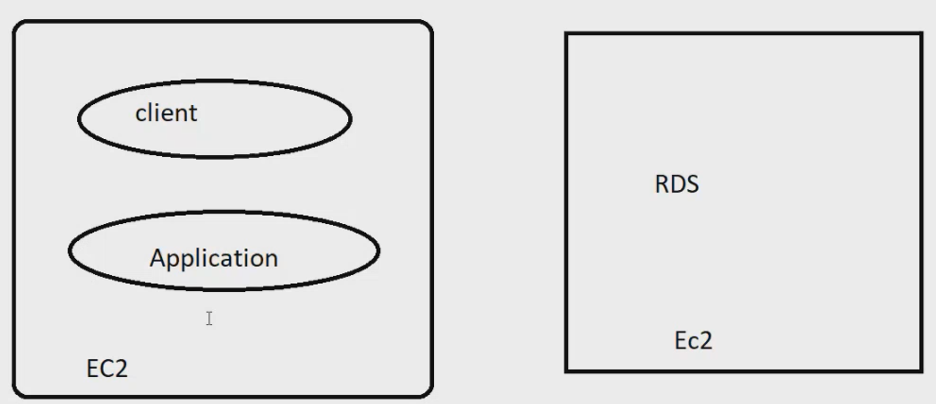
**MICRO-SERVICES : For all parameter we have dedicated package if any issue we can solve without disturbing the entire page. **

**3-Tier Architecture:**

****

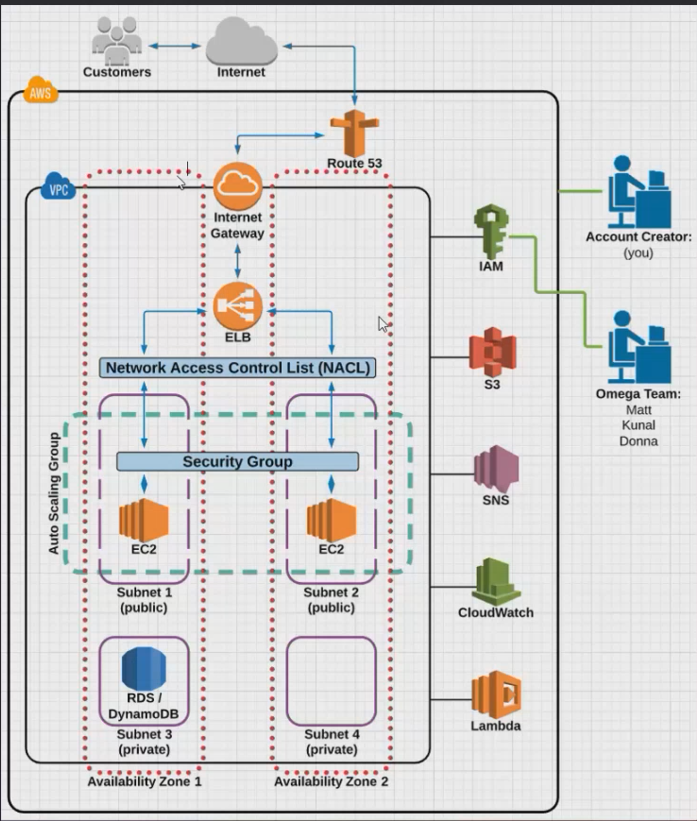
****

**\*\*We can also separate our tier’s like below diagram;**

****

**Data-base can be in the same server or different server**

**AWS - Architecture:**

****

**\*\* “IT IS HIGHLY AVAILABLE Architecture BECAUSE IF ANY ONE ZONE HAVING ANY ISSUES THEN IT CAN BE MANAGED BY ANOTHER ZONE”**

**“APPLICATION WILL BE INSTALLED IN PRIVATE SUBNET ONLY”**

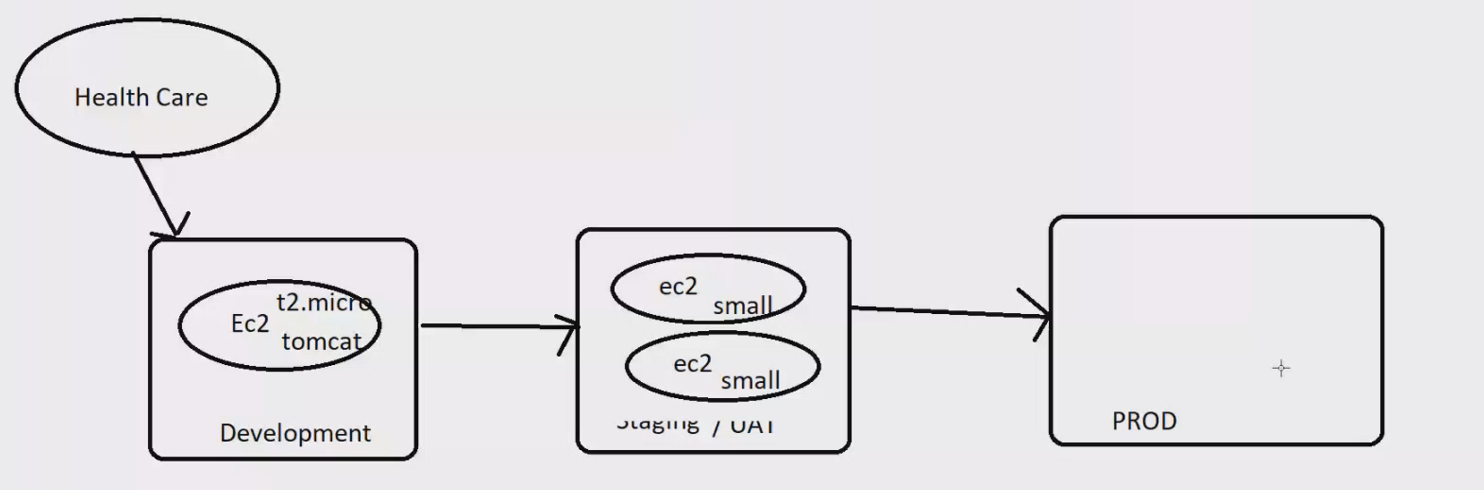
**\*\*Architecture points:-**

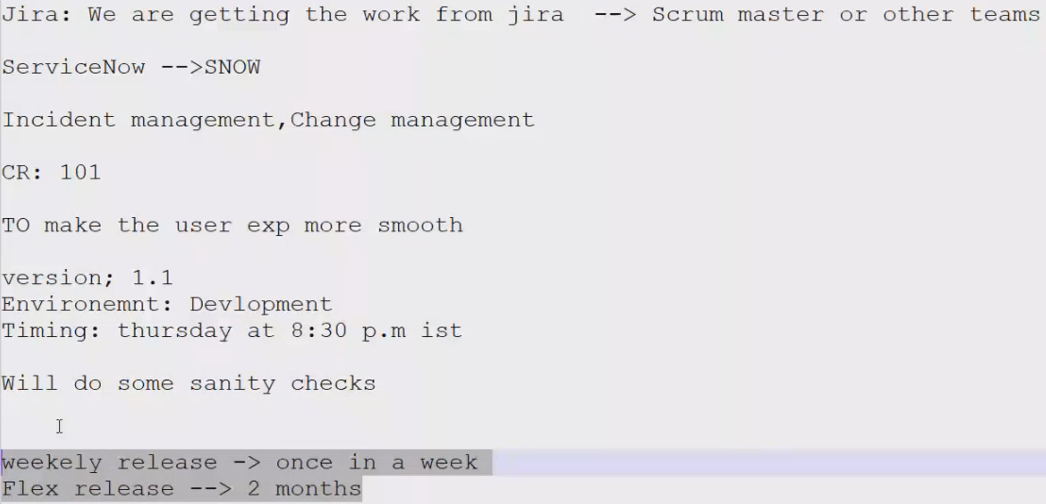
* **User will hit the WEB-URL(**[**www.shrinidevops.com**](http://www.shrinidevops.com)**) the request will goes to the Route 53 and it will check for the DNS validations**
* **DNS VALIDATIONS ( By which domain to which Aws-resources)**
* **IN Route53 we are using (simple-routing-policy) we can connect to aws-resources via Alias**
* **Once the DNS get validated the only way to enter the VPC is IGW,**
* **By “IGW” we get connected to our “ELB-ALB” /And it will route the traffic to subnet according to their “prefix, rules, or network-protocol”**
* **Then we have a (NACL)-firewall which works on subnet level it will check the IP’s are white-listed or not**
* **After that in the subnet we have our instances and there is another firewall named “Security Group” which will check the ports, after checking the ports it gives the access to our applications**
* **AUTO-SCALING-GROUP will scale up/down based upon load and on certain metrics**
* **There are different services which we are using outside the VPC Like s3,IAM,cloudwatch,SNS,VPC-Peering**
* **S-3 are using for our deployed static applications, also for getting the logs of ELB,VPC**
* **Cloud-watch for monitoring our aws service resources**
* **With the help of SNS we will get alarm-alert of our configured Aws-resources in cloud watch**
* **And IAM will help to create user and attach some permission through policy to that (user group role) without given any credentials**

**\*\*WHAT IS THE PROCESS TO DEPLOY AN APPLICATION;**

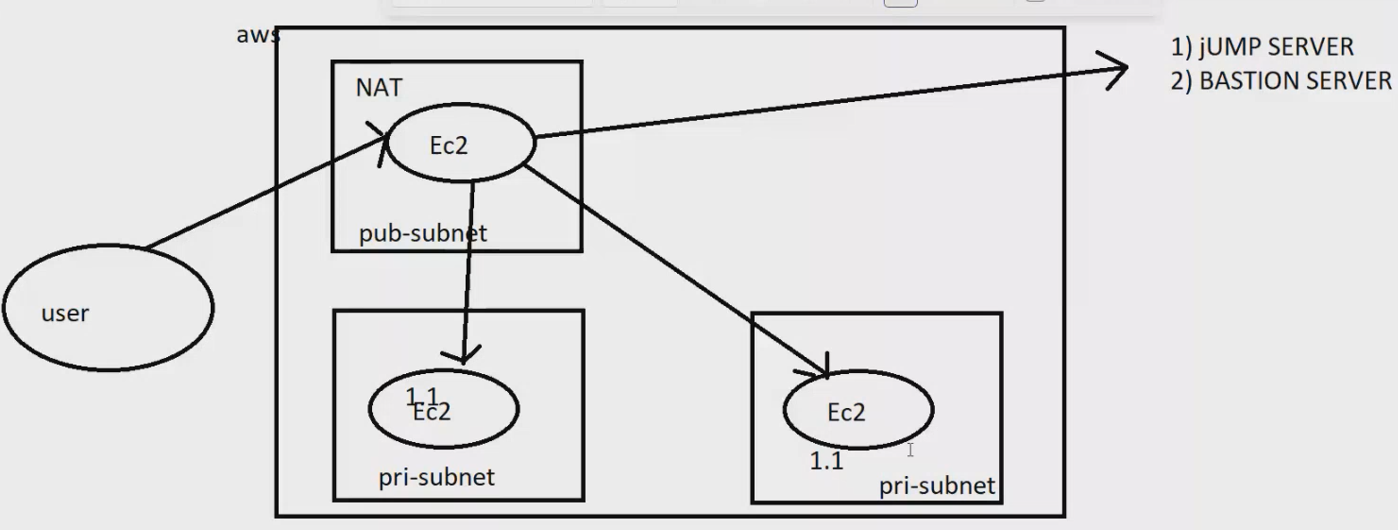
**HEALTH CARE –APPLICATION**

**1.DEVOLPMENT- ENV  
2.STAGGING-UAT-ENV : WE PUT THE LOAD AND VERIFY IT CAN SUSTAIN OR NOT  
3.PRODUCTION-ENV : FINAL/RELEASE STAGE**

****

****

**TO CONNECT A PRIVATE SUBNET WITH PUBLIC THAT SERVER WILL BE CALLED AS “JUMP/BASTION-SERVER”**

****

**-------------------------------------------------------------------------------------------------------------------**