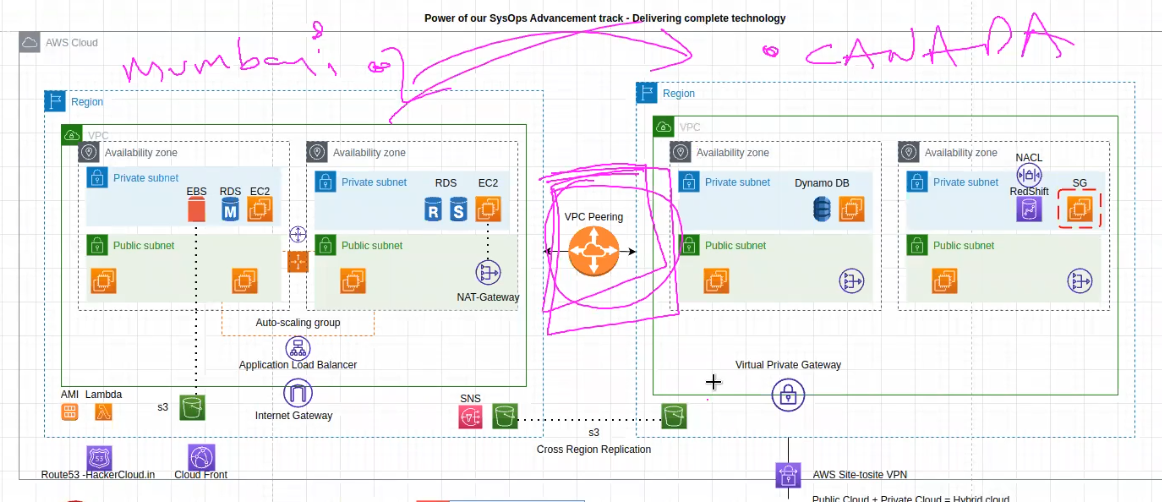
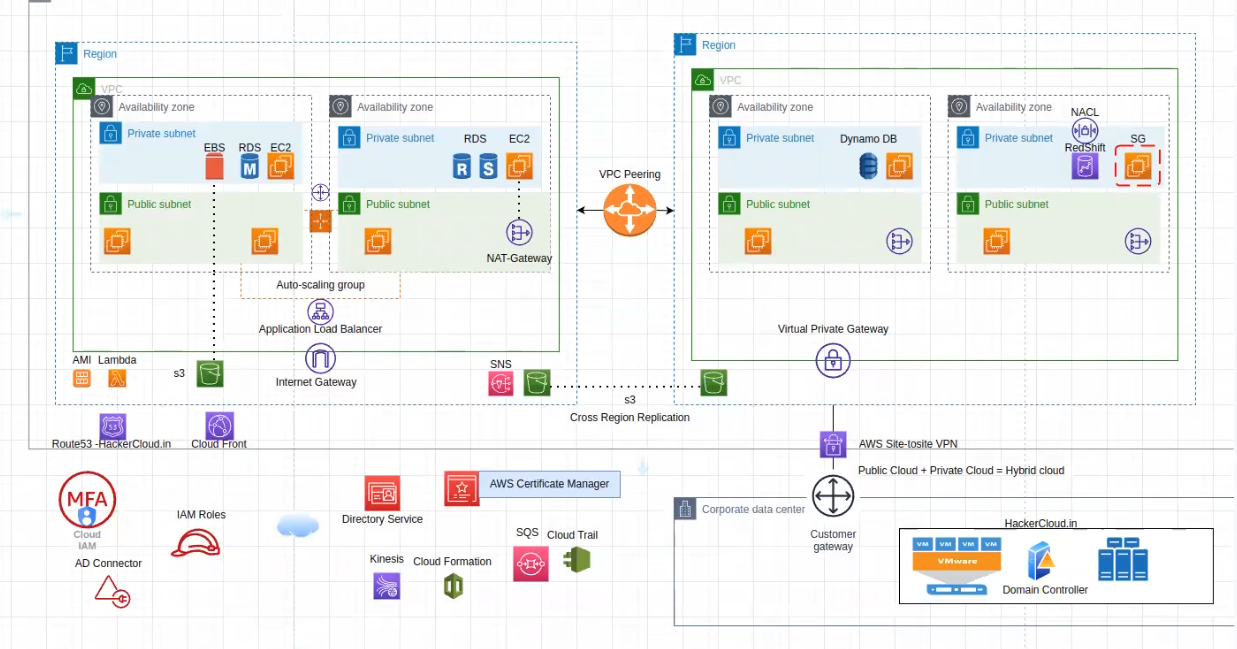
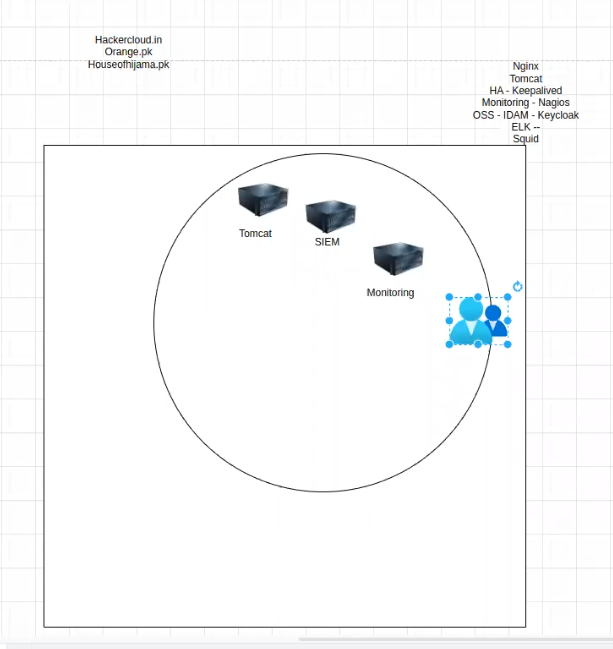
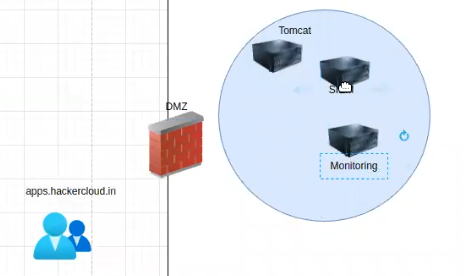
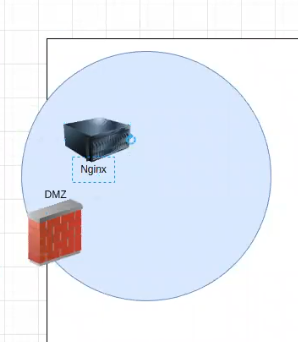
Lecture 27

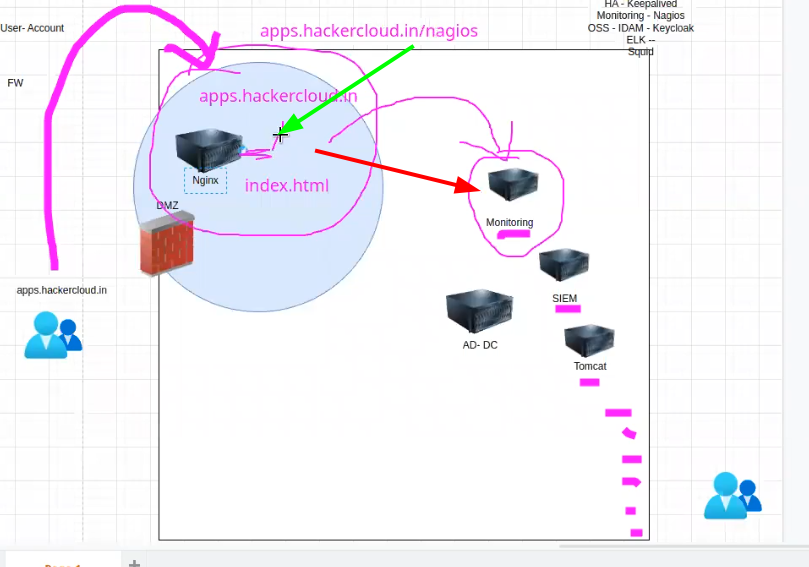
**Installing Reverse Proxy Nginx Cluster (OSS 1.20.2) to protect our Internal assets Part1 (Live Session 12 November 2022)**

How to setup whole infrastructure of an organization on **AWS**

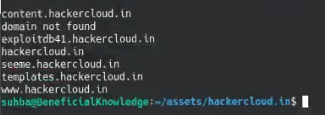
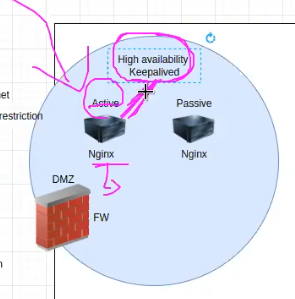
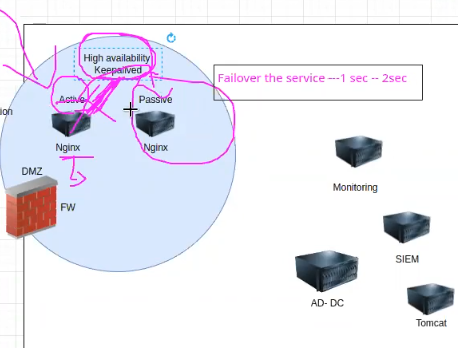
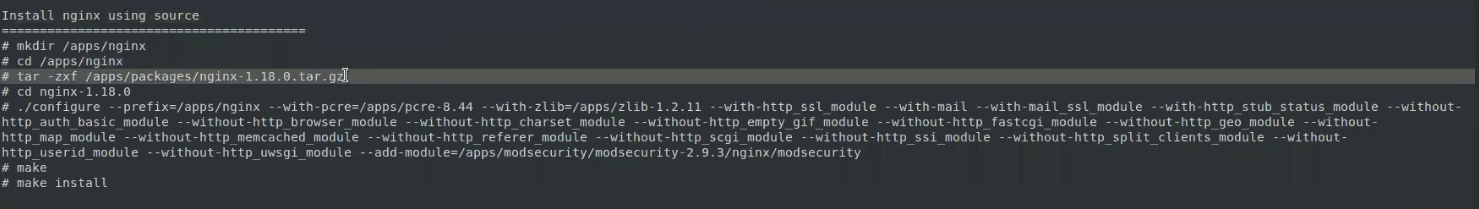
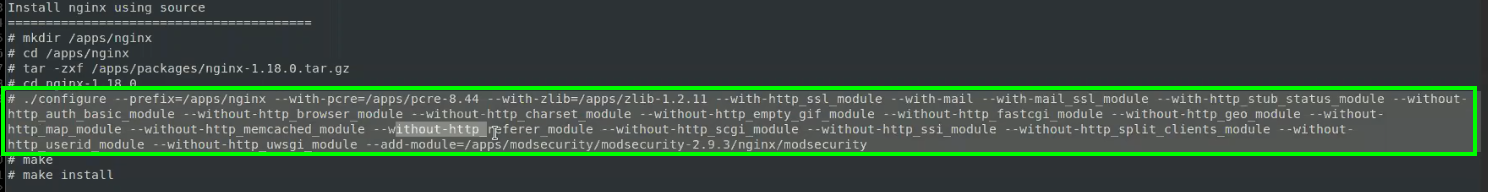
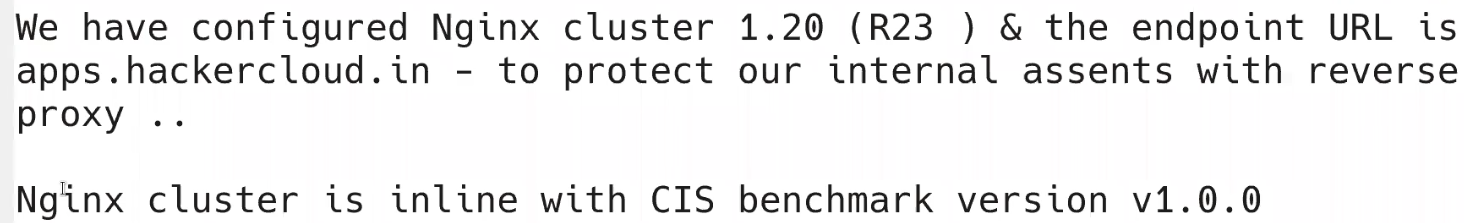


* Establishments of private network
* Assigning of Subnets, IPs etc.
* Make it HA (High Availability)
* Make it redundant.
* Auto scaling (severs will added automatically, if demand drops and server usage is dropped servers will be reduced)
* Internet gate way
* S3 bucket
* 
* **DevOps + SysOps** (these tracks can open immense opportunities InnSha Allah)
* .
* A company 🡪 develops applications 🡪 service based company 🡪 how to set it up?
* Requirements are ,
* **3 servers**
  + 1 for monitoring
  + 1 for SIEM (incident event monitoring)
  + 1 for application
* 
* To give access to global users through internet
* We need to set up a portal apps.hackscloud.in
* Users will create accounts.
* Firewall will be setup to secure the DMZ zone (that’s 1 way to do it)
* 
* A **DMZ** (demilitarized zone) is a network zone that is designed to provide an additional layer of security for an organization's internal network. The DMZ is a buffer area between the organization's internal network (intranet) and the public internet. It is often used to host services that need to be accessible from the internet, such as web servers, email servers, and FTP servers.
* We will setup an Nginx server in DMZ
* 
* Nginx will have our URL (hackerscloud.in) 🡪 index.html (its our page in Ngnix

Nginx 🡪 works

* + It hosts index.html page.
  + It revers proxy to private network (it connects to private network and provide that specific service suppose Nagios or SIEM or Tomcat to the user)
* If a user wants to access nagios 🡪 hackers.cloud.in/nagios
* But Nagios is not exposed to internet (only Nginx is exposed)
* The request will come to Nginx server 🡪 and then to Nagios (in private network) which is not exposed to internet)
* 

Security of this network

* To secure this network or to give limited access to the resources
* *We device it into 2 scenarios 🡪 depends upon requirements, (minimum clients 🡪 whitelist) but for (unlimited clients 🡪 open internet is the solution)*
  + **Whitelist 🡪 source restriction**
  + **Open internet**
* As our urls are exposed to internet
* 
* The hackers may try to attempt to hack the password through brute force attack.
* How to secure it then?
* *According to Microsoft 99.9% attacks can be prevented by activating,*
* *MFA (multifactor Authentication) or 2FA (2 Factor Authentication)*
* Question?
* If Nginx is down ?
* Availability -🡪 CIA 🡪 SLA with user is breached 🡪 penalty.
* .
* If the Nginx is attacked by a hacker and the service is down?
* **Solution: -** we need to create HA (High Availability) so that in case of a failure our application does not stop.
* On premises 🡪 keepalived is a great option and open source package.
* 
* keepalived will keep checking if the server is working or not
* if the active service is down (not alive) 🡪
* it will “failover” the service to the available Nginx server 🡪 within 1 or 2 sec
* 
* It will make the active sever (2nd server) master and the 1st one slave.
* And after maintenance 🡪 “failback” to server 1
* In case of patching (upgrading the packages) 🡪
* Patch the server 2 and check it
* Then fail over to sever 2 and patch server 1
* .
* If same thing is to be implemented in “cloud” 🡪 load balancing is the solution. “keepalived” will not work on cloud.
* Installing “Nginx” 🡪
  + Yum
  + Rpm package
  + Source code.
* Sir Kazim recommended to install it through “source code”
* 
* We can customize and decide what packages to exclude 🡪 this is the beauty of SCI
* 
* It will make it lite 🡪
* Source code installation 🡪 u can again choose what package to include or exclude on the fly (running)
* .
* In production environment 🡪 a note is made as below (to be explained in interview)
* 
* .