**Splunk admin session**

Why Splunk?  
- Volume of data ->Data in tera even Peta byte is common and using Splunk we can do easily compared to DB  
-Types of data -> we can have structured or non-structured data. We can do both in Splunk without changing schema.  
-Dynamics analytics use case ->here search happen simultaneously in Splunk.

Because of all these main challenges analytics tool comes into picture that’s were Splunk introduced , but Splunk initially introduced for log analysis But later on it upgraded with its feature to full-fledged analytic tool.

**Splunk Architecture:**

Single server environment ->All components will work under this and using webserver we can upload data and do analysis. But if it goes down, then no body cant access and if data grows, then it impact performance issues. **Its recommended when we have small amount of data or for testing.**  
Distributed environment 🡪 here we have multiple linux server. And those servers helps to replicate data. Since there are multiple nodes, we will get much much better performance.

**To install software:**

* You should use, Splunk.com
* Where you can create account and click free Splunk.
* And check for Splunk enterprise for full-fledged instance.
* And install Splunk software depends on OS.

For linux, depends on flavors obuntu(.deb) ,redhat(.rpm) etc.. eg. Fedora linux used by redhat and release it with .rpm version. Similarly, if aws use fedora linux and release as dif version.

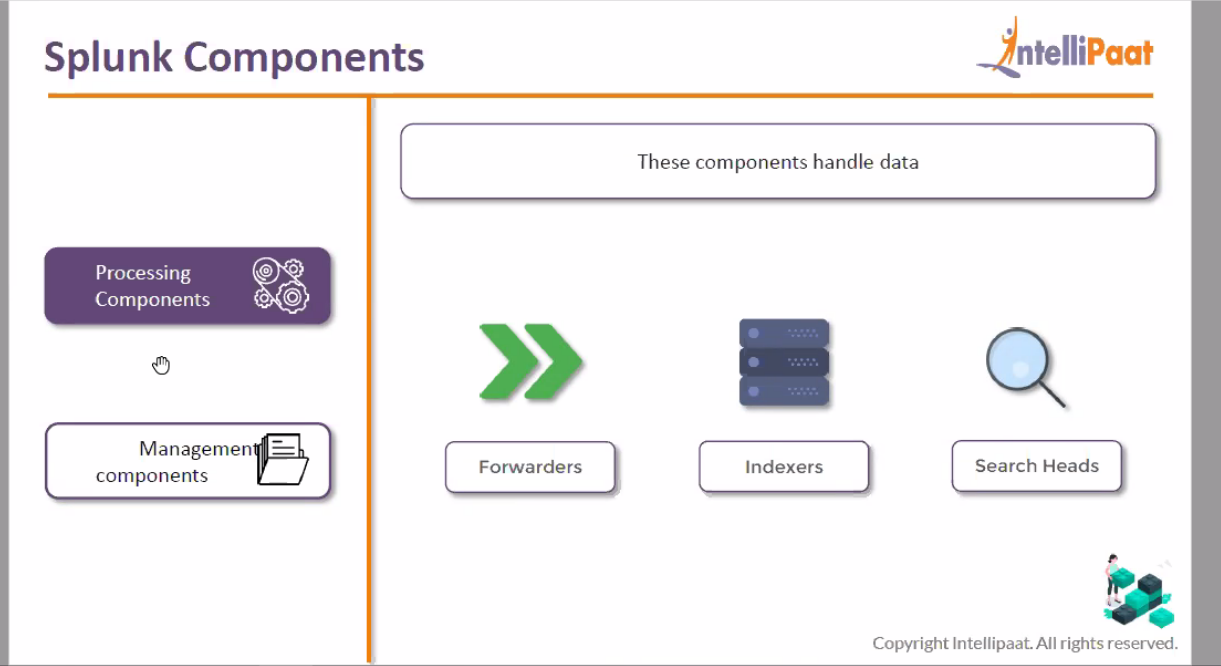
Fedora (contributed by multo ppl. Aws, redhat) so it has regular updates which will not good for pdicution. So we shd check for proper vendor and take proper version. So for productin,its good to have redhat or other vendor. For pslunk, we shd use .rpm. and obuntu is paid one(for this we shd use .deb)

Fedora ->fedora server would be preferable.

**Linux is must cheaper than windows and also security purpose.**

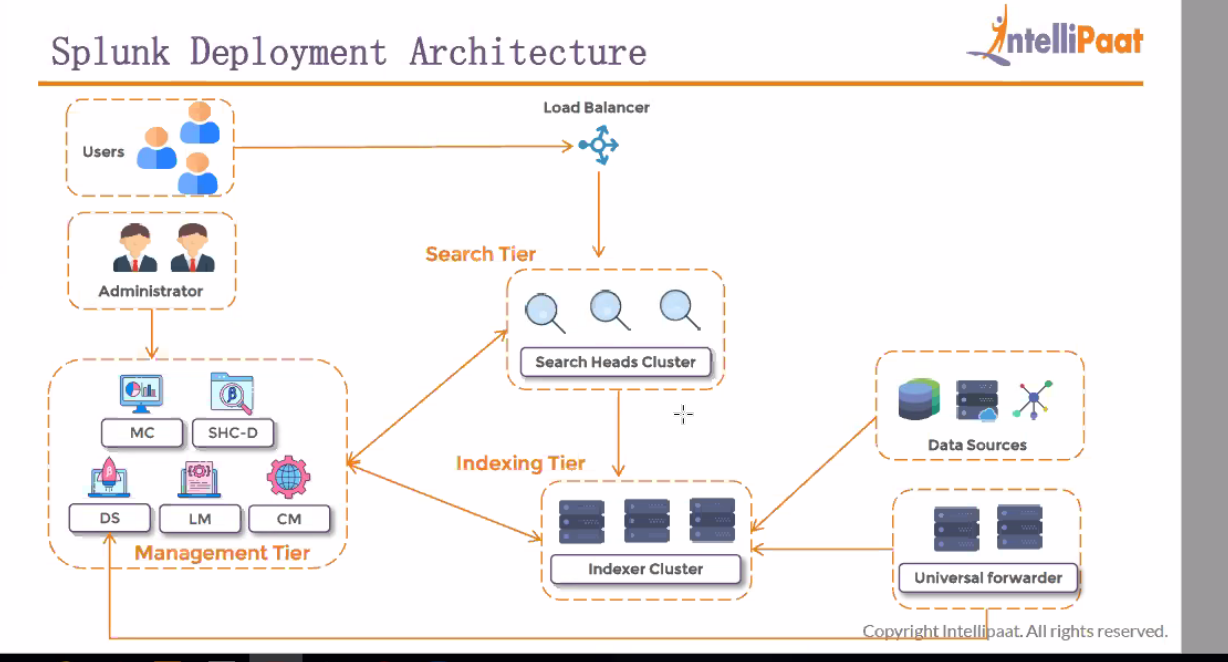
**One main advantage of using Splunk, all we can do in one. Like importing data,storing and analysis. Whereas if we take Hadoop for analysis dif and for store dif...**

Splunk **components:**

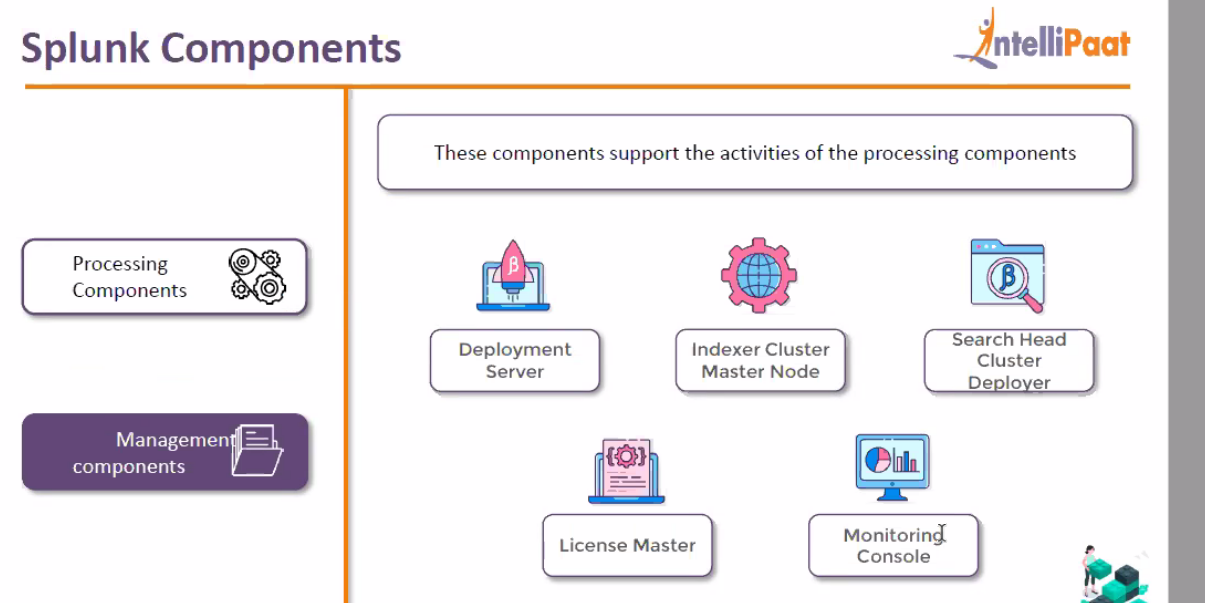
****

**You know detailed descripton of processing components such as forwarders, indexers and search heads.**

**Remember, processing happens in indexer and storing also happens at indexer. And results gets displayed on console by search head. Here serach head renders data from indexer and display on its console.**

****

**Here Managemetn tier is not resource hungry since it controls other component. So we install all DS,LM,CM ,MC and SHC-D all in one as mgmt. tier.**

****

**Forwarders managed by deployment server.**

**All logs which you want to collect to Splunk those configuration changes will be done in deployment server and will push those changes to deployment-clients(forwarders) using server class.**

**Index clustermaster node:** it mainly helps in manages index cluster and it also manages serach cluster as well. Here It monitor how replication happens at captain in search head and also how data getting replicate d in indexer.

**Search head cluster deployer: it helps to distribute apps or config changes across indexers and search heads.**

**License master: splunk is full fledged premium product. It will monitor hwo much data indexing and if ti exceeds license amount , it will trigger alert.**

**Monitoring console: How many users logged in to Splunk, how much CPU occupied by search head etc.. similarly we have few inbuilt alerts which we can enable if required,**

**Restart universal forwarder:**

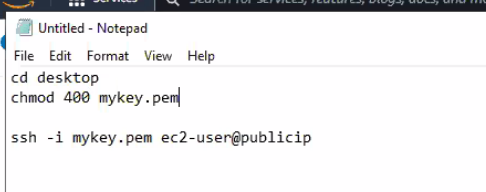
**, For version upgrade of forwarders, then we shd go for deplyemnt server but if upgrades on sale, u can go for individual one.**

**Or most of the case, u can script and push it across.**

**And most of the case, you can do restart of failed ones**

**Installation of linux instance:**

* **Launch instance**
* **If you are using moextem, there u use public ip, usre name as ec2-user and apply private key and launch linux instance by selecting ssh session.**
* **If its Mac os, then open terminal and navigate to directory where u kept .pem file. And run ssh command as below. Here we kept .pem(key pair file) in desktop.**

****

**Install splunk instance:**

**In EC2 instance, we get private address which is actual server ip address. And public address temp kind and which we use while launching instance.**

**Always keep in mind, be as splunk root user to install splunk and to isntall software always install inside a foler instead of installing in OS default folder.**

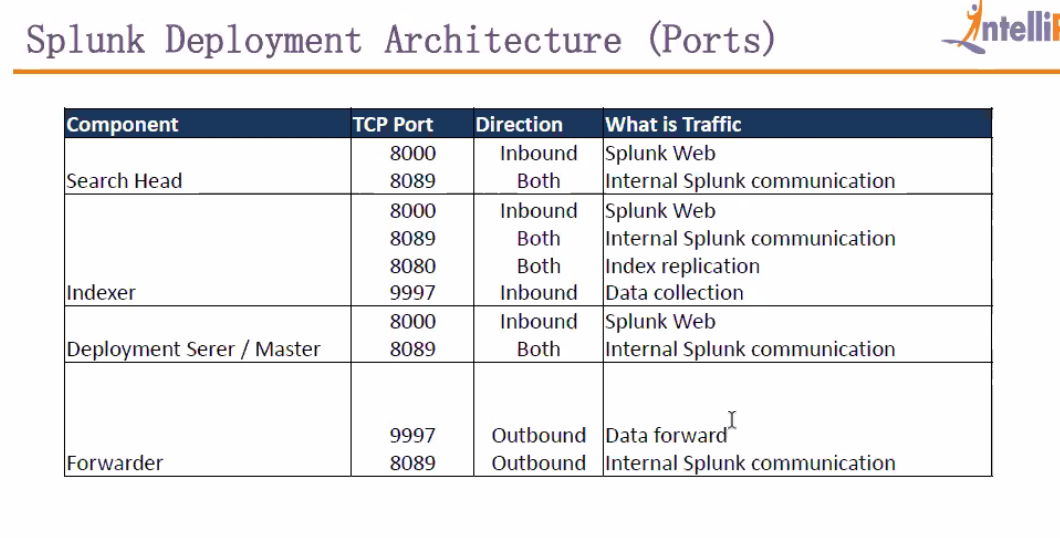
**So that if something happens, it will not crash OS.**

*If you are not admin, then ask admin to create mount folder with size of 30GB.*

*Why we are setting min space is 50MB. Splunk minimum free space requirement is 5GB. Since its free trial, while installingit occupies 4.5 GB. So to make it work, we are keeping min space as 50MB. But in production it shd have 5000MB.*

*And that comes by default. And if tis about to film then we shd create volume and apply to disk using lvcreate and fdisk commands.*

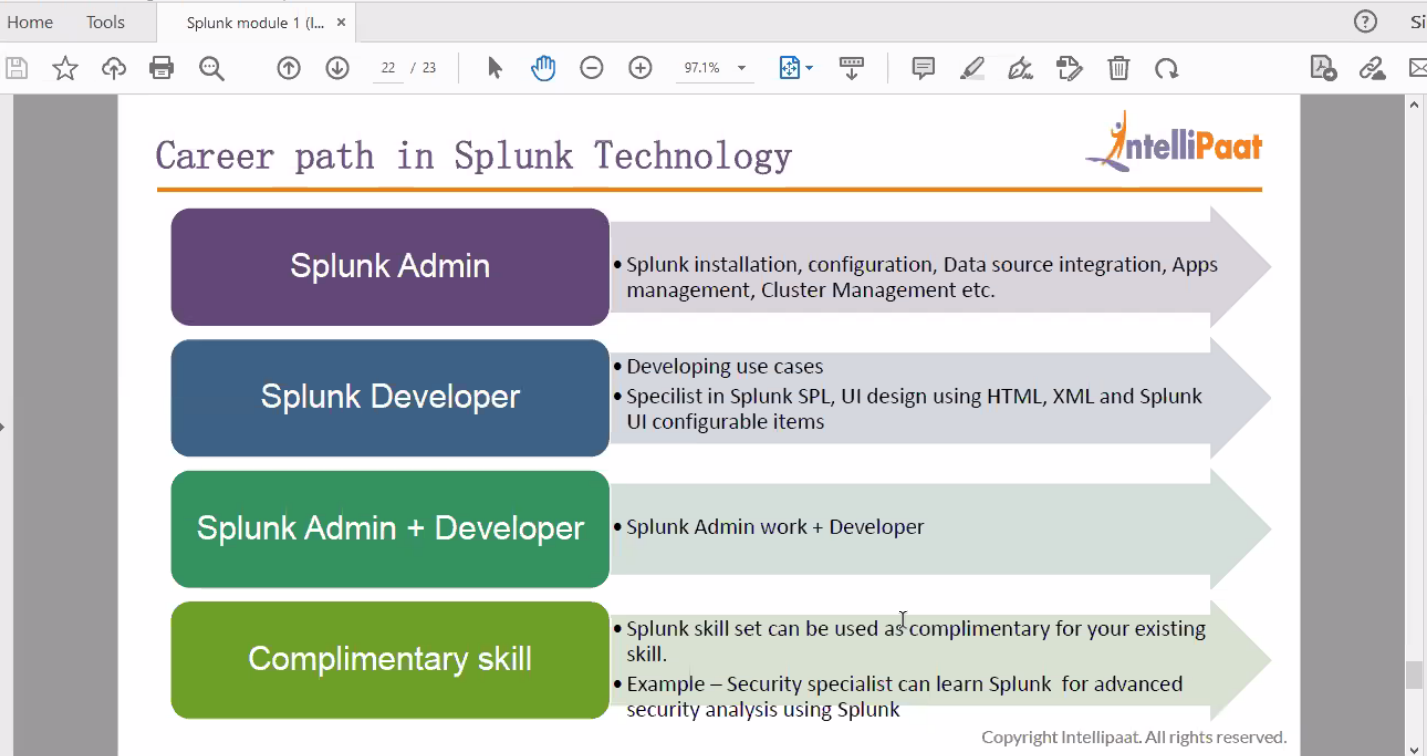
***Ports:***

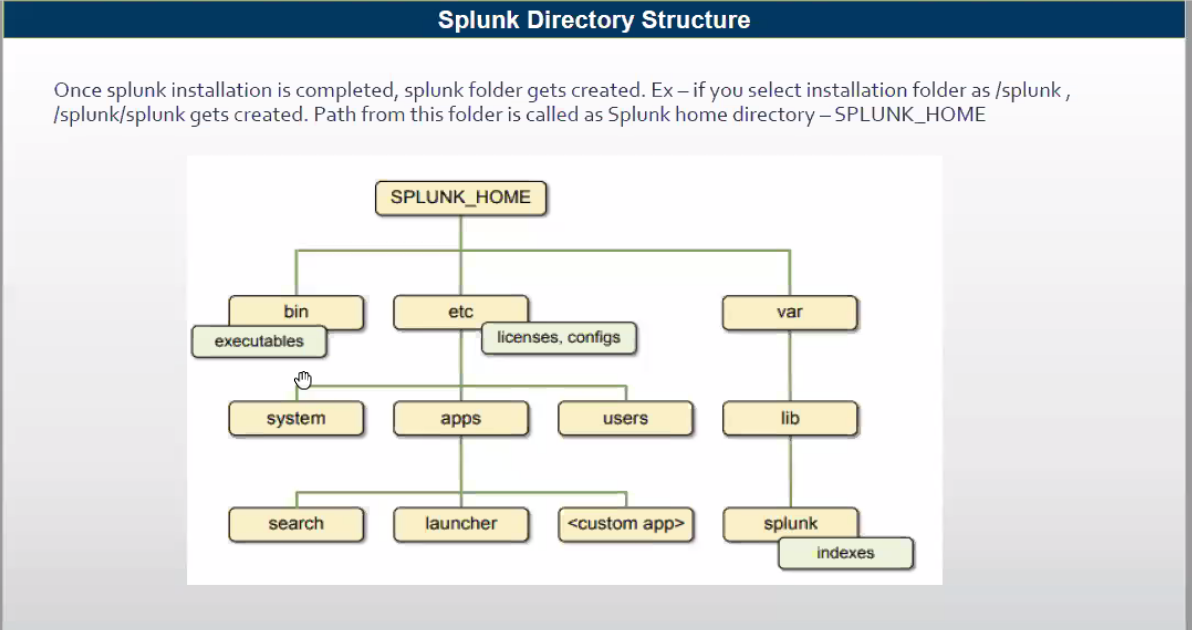
******

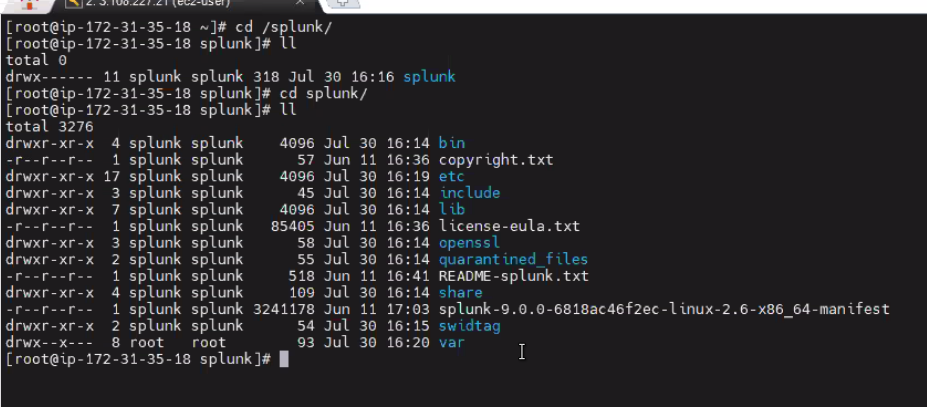
***2 types of flow we have***

***Inbound->data comes from user to search head***

***Outbound->data comes from indexer to search head***

******

******

******

***Default folder is Splunk and generally we call it as SPLUNK\_HOME***

***And inside that we have some default folders***

***Bin:***

***->here we have*** *hell no of executables. But all areused internaly by splunk. But only we use splunk execuatle file to apply config changes including start and stop splunk server.*

***Etc***

*->apps  
 ->here we will get info about apps. If u see apps in homepage all will get dsplayed here.*

*In phone, if u buy it will come with default android os and default apps. And if u need to install, u can install from play store or if u want u can create as well.  
similarly, in splunk if u want u can install from splunkbase.com or if u want u can create on ur own. And these apps gets stored under /splunk/splunk/etc <here splunk new mount folder where we installed splunk>*

*🡪system  
 default->here we have default setup/config setup. If any changes need, we shd copy frm here and paste it in local and do modification. And once done, restart splunk.  
 local ->here it has internal SSL config infomaton, disk freespacce info, And* ***files in /local folder has highest precedence. And it has customized config files.***

*->users  
-if splunk used in multi persons, then we create users. Those users foldrs are created under user folder and their metadata and user preferences are saved under their folder.*

***Var:***

* */lib/log  
  here we have log files relates to splunk. Here we get various logs. In wich important one is splunkd.log where we get to know if any transfer is nto happenng or any server is not startng.or any search head or indexer not starting.. those we can get to knw from splunkd log.*