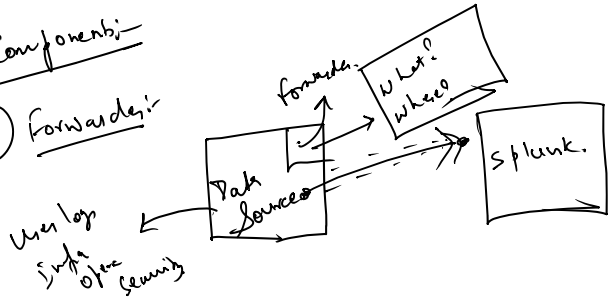
Splunk:-

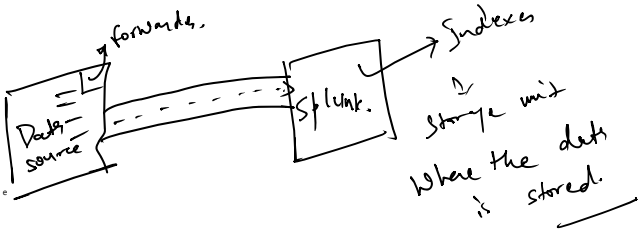
1. log monitoring.
2. Dashboards, Alerts, Reports
3. Predictive Analysis.

Components:-

1. Forwarders:-

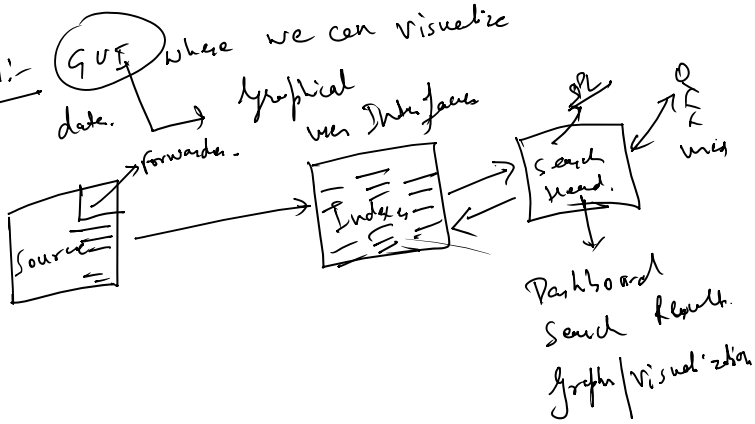


2. Indexers:-



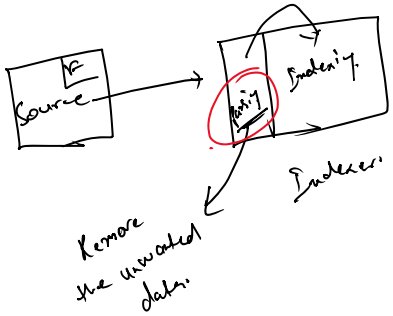
3. Search Head:-

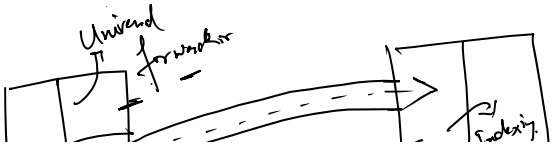
GUI where we can visualize data.



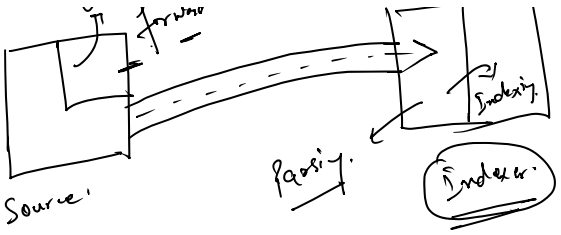
Forwarders:-

1. Universal forwarder.
2. Heavy forwarder.





1. Seperate Package we have.
2. ... 25 MB (Jar),



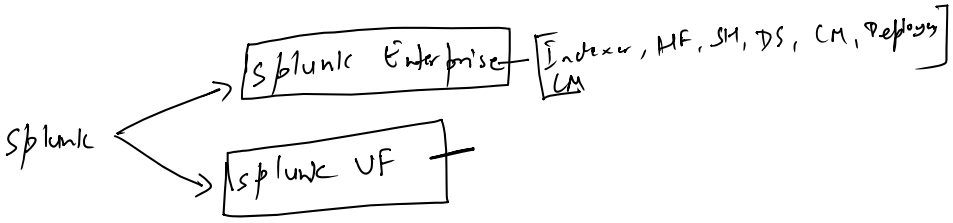
(1) ... we have.

(2) Size - 25 MB (day), 150 MB (week)

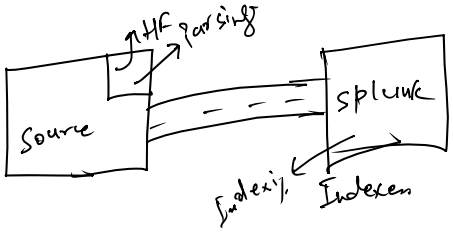
(3) No Parsing at the forwarder size

(4) Indexer will take care of the Parsing Activity.

(5) No GUI for UF



(2) Heavy forwarder:-



(1) Parsing will be taken care at HF level

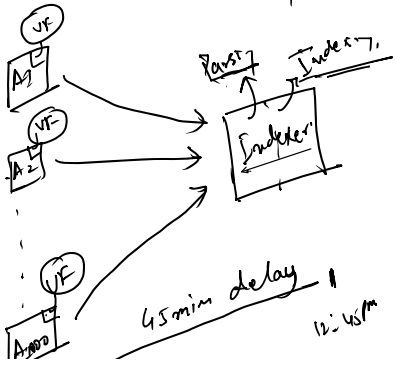
(2) Less load on Indexer.

(3) Splunk Enterprise a package.

(4) Size - 450 MB (day) 5 GB (week)

(5) GUI is available.

UF	HF
(1) Parsing will be taken care by indexer	(1) Parsing will be taken care at the forwarder level.
(2) UF - 150 MB	(2) Splunk Enterprise - 4.5 GB
(3) No GUI	(3) GUI Available.



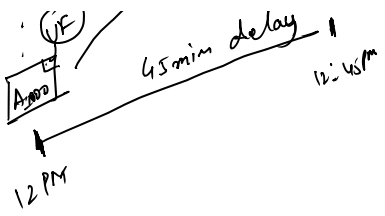
Pros:-

(1) Size is less.

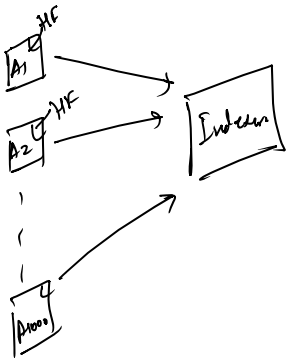
(2) No extra free ports / No extra computational resource consumption

Cons:-

(1) load on the indexer will increase



1. load on the ... increase
2. Queue of data.
3. Indexing delay.



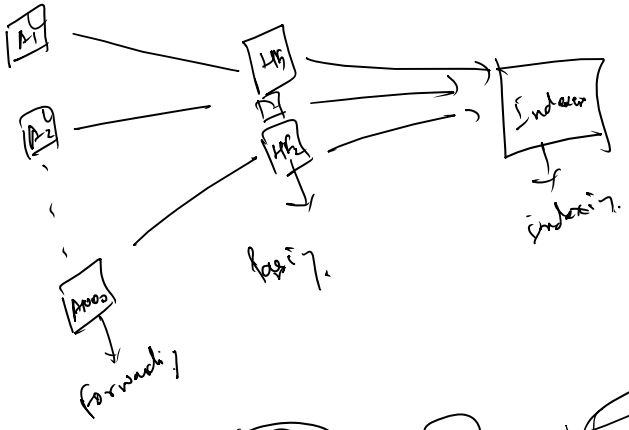
Pros:-

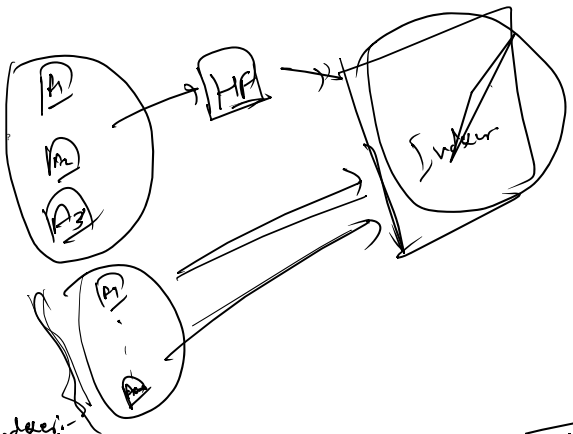
1. less / No Indexing delay.
2. Parsing will happen at source level.
3. load on indexer will be less.

Cons:-

1. Size = 4.5 GB
2. Computational resource Consumption will go up.
3. More port occupied.

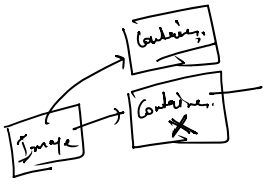
Cost will be on the Higher side. ← [Higher / Advance Infrastructure.]

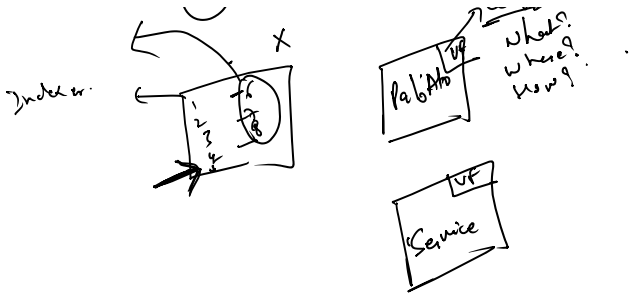




Clustered Indexer:-

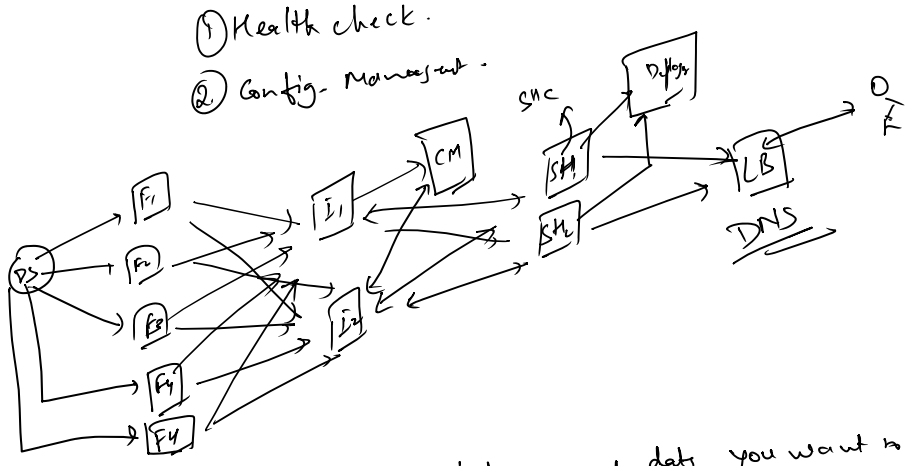
1. Backup
2. load Management -





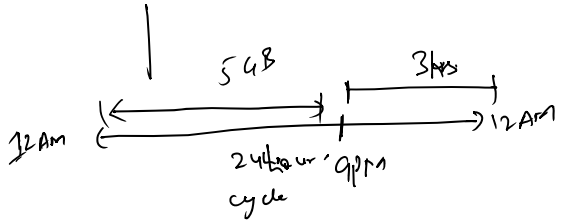
3 Management Instances

1. cluster Master. — Manage your Indexers.
2. Deployment Server. — Manage your forwarder.
3. Deployer. - Manage your search Heads



License Master:- On the basis of how much data you want to ingest on the daily basis.

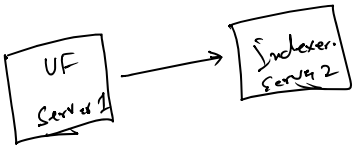
5 GB/day → 1 year.



1. Indexing will continue.
2. Searching will be disabled.

5 Times Voilation - 30days.

1. Send the data from the UF to indexer.



1. Install the UF on server 1 & monitor on server

1. Install the UF on sec ver 1 & Splunk Enterprise on server
2. Connect UF with Indexer.
3. Enable Reciving port (9997) on the indexer
4. Validate the Connn. b/w UF & Indexer.
5. Send some ~~so~~ Custom log. (inputs.conf) → ~~config~~ log file.
6. Validation & Troubleshooting.
7. Config. file involved in whole step.

(1) inputs.conf → ingestion details.

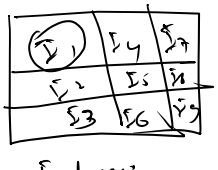
(2) outputs.conf → indexer : reciving port.

Default → By default config. files

Local → Config made from the end-user.

Local will be having higher precidense than default

Index:-



Indexer.

(1) Predefined
(2) Default.
(3) Custom index.

(1) Predefined – We are going to have index = –* internal, _audit,

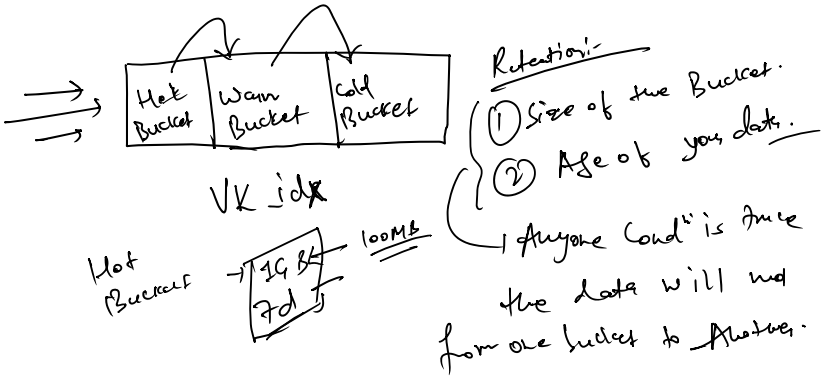
① Predefined – We are going to have index = – *

- Part of splunk app into these index.
- we can't push our own data.
- _internal, _audit, _introspection - - -
- No license is calculated.

② Default – (index = main) → ① Data from our ~~test~~ dataset
② license is calculated.
③

③ Custom index:- index = VK_idx.

1. Push your own data.
2. license is calculated.



① Create index on the source. →
② Send the data to that specific index from UF.
③ Create one sample file on the UF