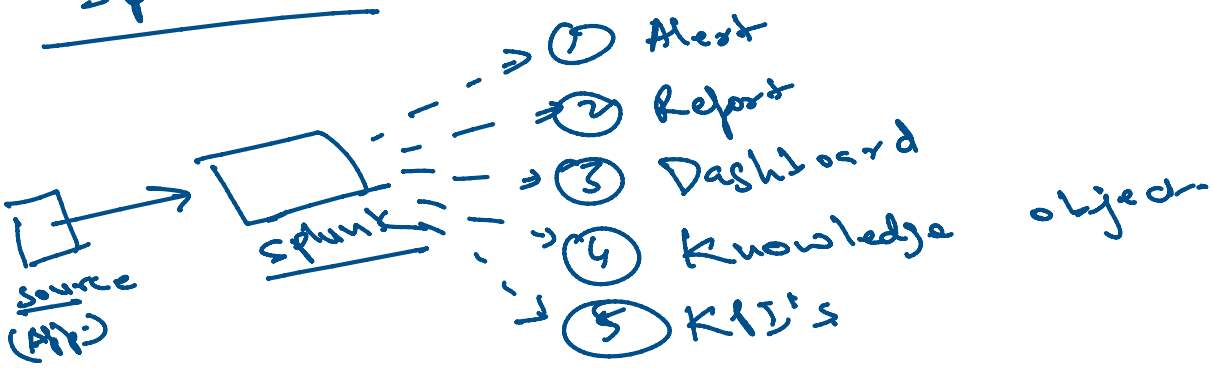
Day - 1(27th May)

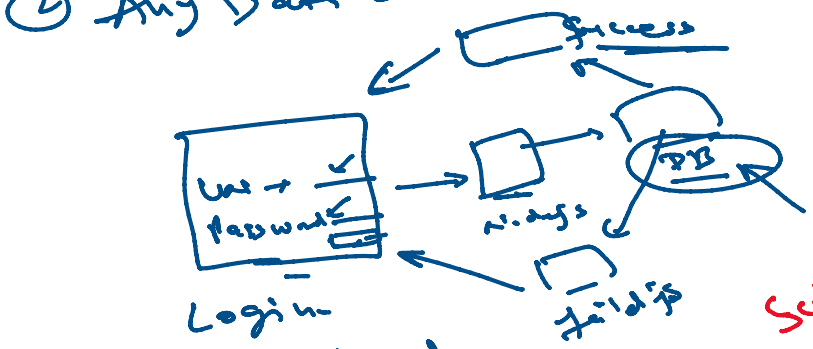
27 May 2024 09:43

Splunk:- Monitoring platform.

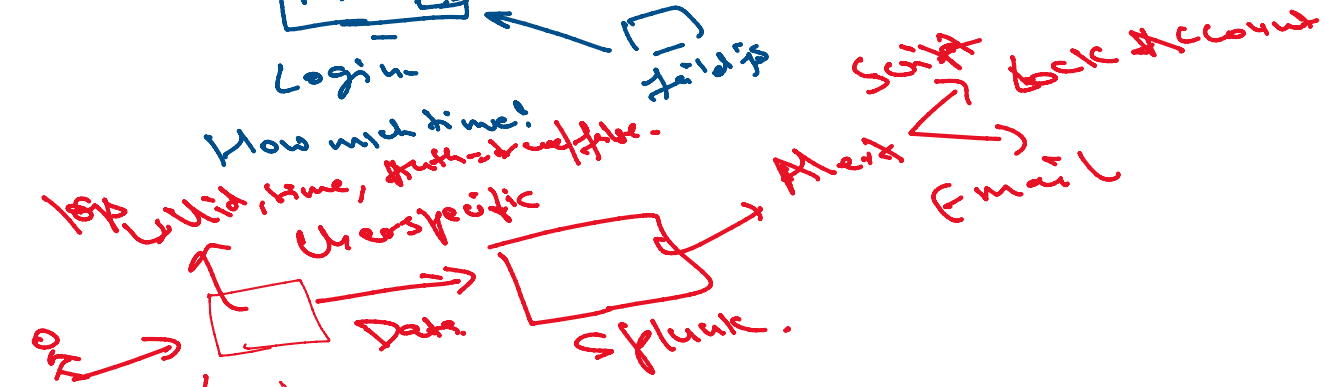


1. splunk ITSI
2. splunk ES
3. splunk Phantom (SOAR)
4. splunk Arm

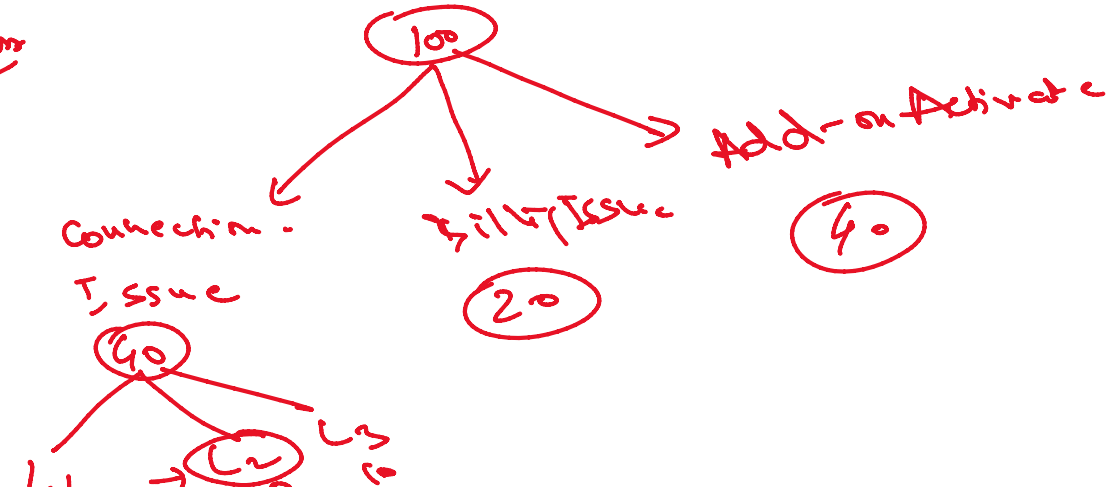
1. Any type of Data.
2. Any Data Source.



How much time!



Authentication : fail/success



Components of splunk :-

→ Day-4.

1. Forwarder
2. Indexer
3. Search Head.
4. License Master.
5. cluster Master.
6. Deployment server.
7. Deployer

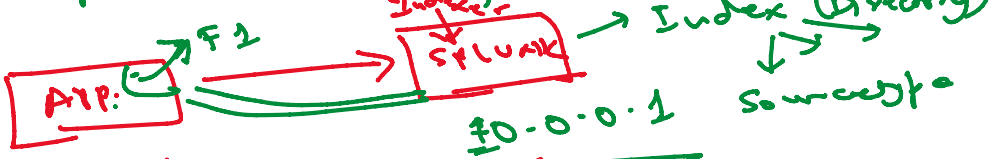
Data Swat :-

(1) Forwarder :-

→ splunk UF

splunk end.

Forward data from the source to the Indexer



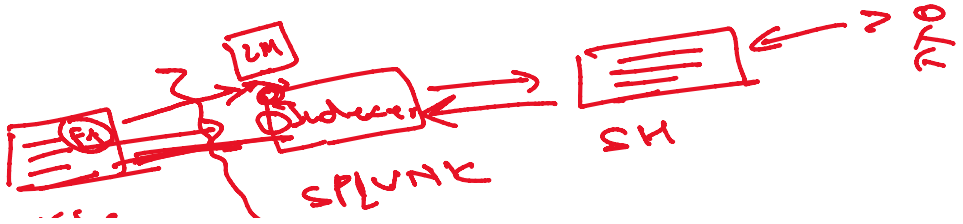
1. Splunkserver details. server-1 : 10.0.0.2
2. Specific log which need to be forwarded
3. Define the index name to forward the data.
4. Define which sourcetype data to be forward.
   ↳ Data type.

(2) Indexer :-

Database in splunk which will store the data.

(3) Search Head :-

GUI where user can create the dashboard, Alert or any kind of Visualization



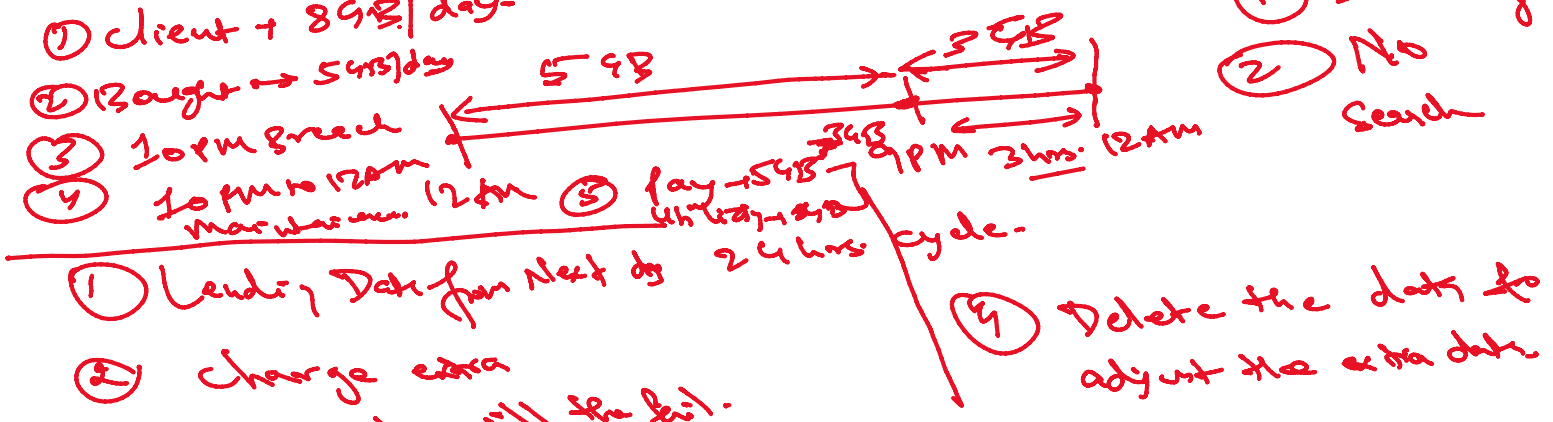
4. License Master:-

Parameter splunk charge?!?

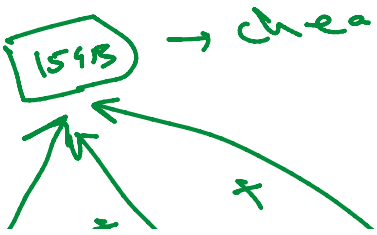
1. Amount of Data ingested → Pay Amount.
2. No. of Component involved.
3. No. of Sources
4. Searching speed.
5. Cloud or API used to call the data
6. No. of end User
7. Data Backup

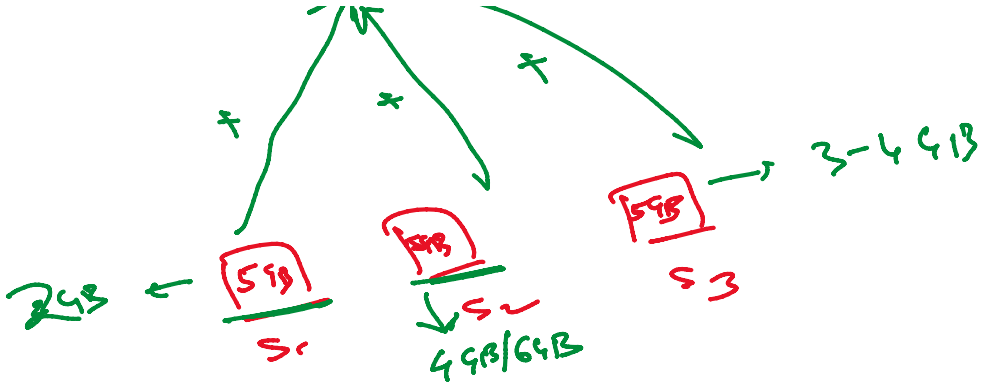
5 GB data every day → 1 year.

↳ $$$



License Pooling:-

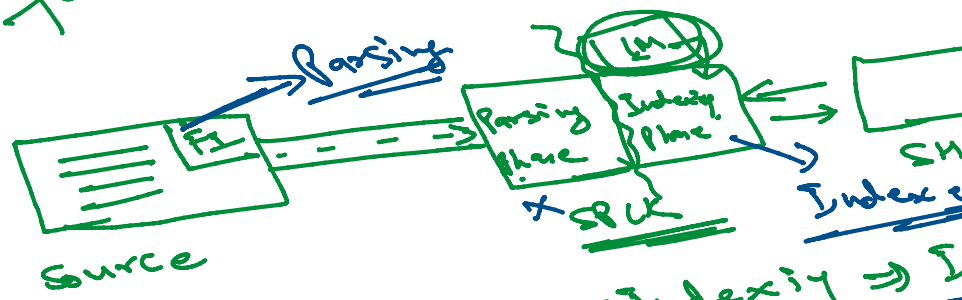




Forwarders-

UF
(Universal forwarder)

HF (Heavy Forwarder)



Forward the data basis ← UF → parsing ✗ Indexing ⇒ Indexer

Pass through ← HF → parsing (forwarded) ✗ Indexing (Indexer)

Only by source (forwarder) ✗ the Indexing is taken care by Indexer.

No GUI
Splunk UF
35MB to 40MB Unix + 150MB

GUI
Splunk Enterprise
(Forwarder, SH, IDX, LM, CM, Deployer, DS)
Lin → 4.85MB
Win → 4.5GB

UF → 150MB Unix.

② App. runtime → SI

Disk ↑

SI

Indexer

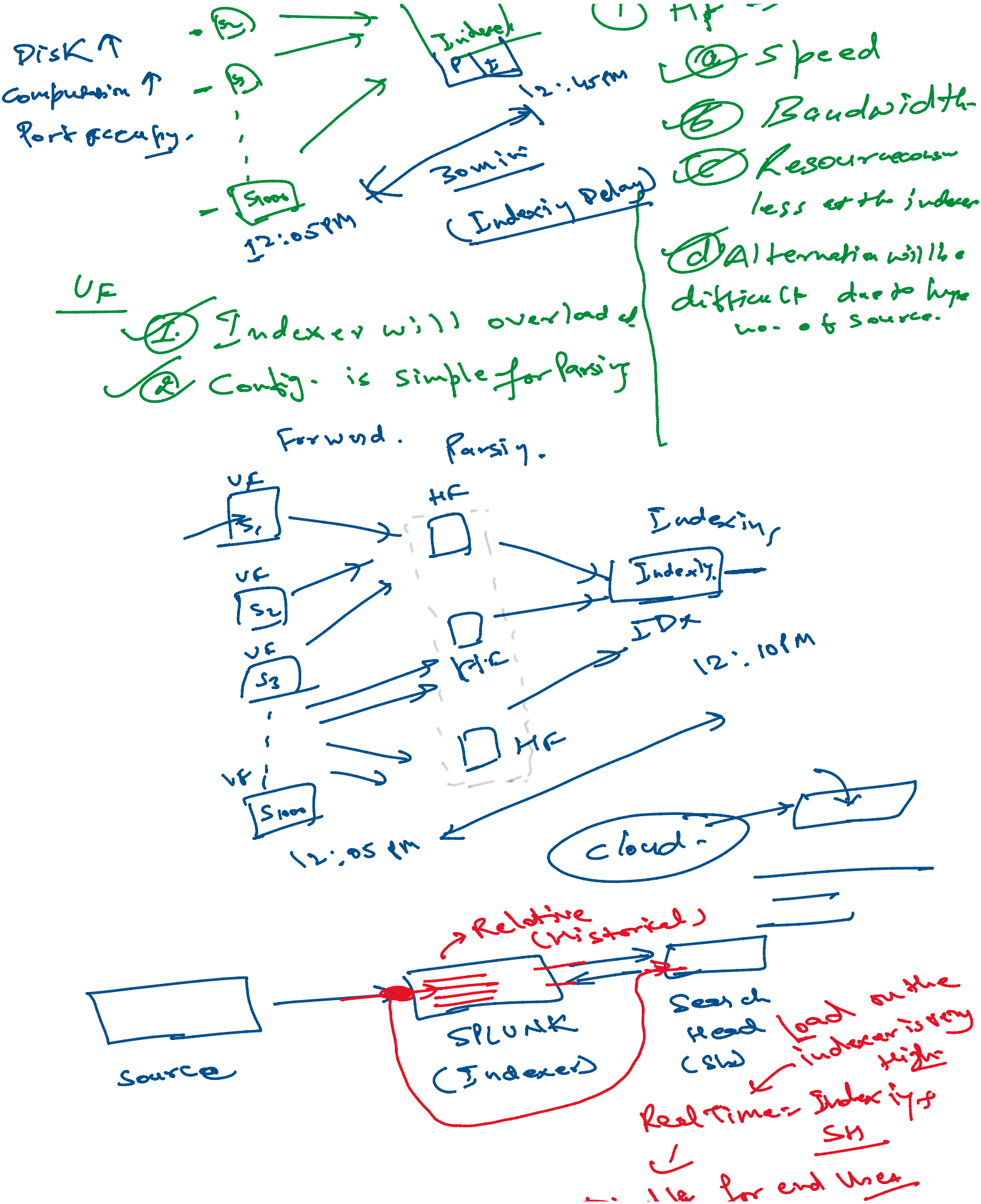
HF → 4.8 ≈ 5GB

Optimize -

20GB 5 USD

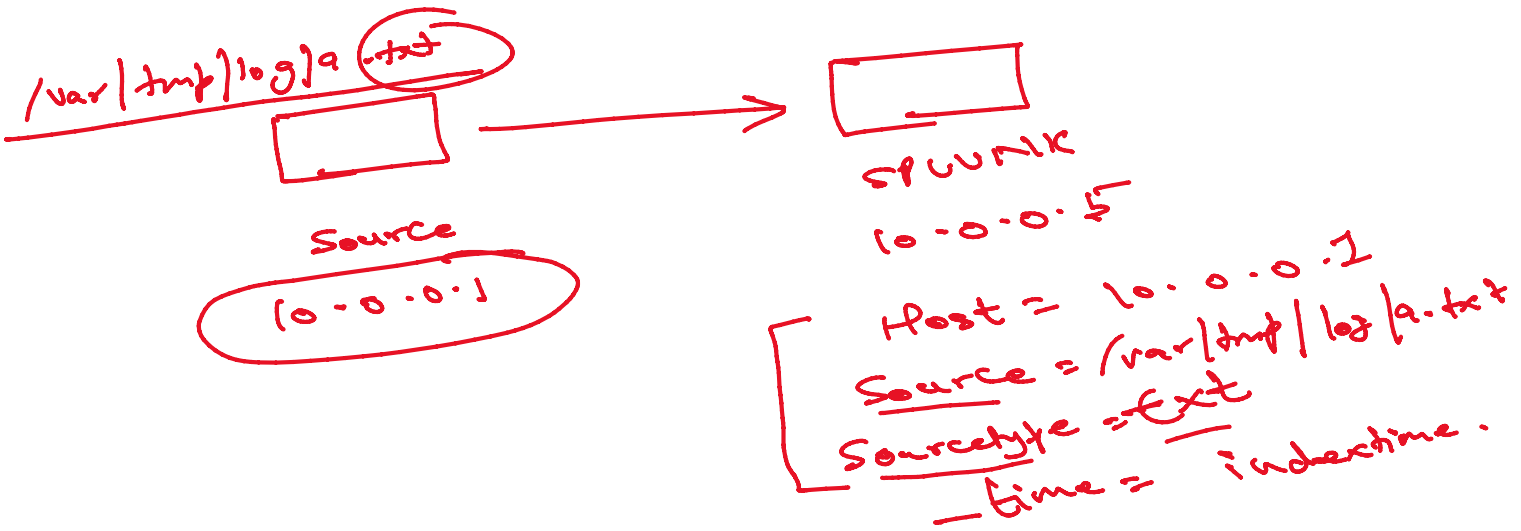
① HF → 50 USD

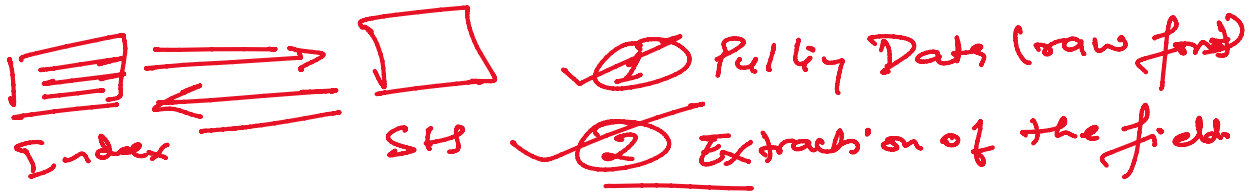
② Speed



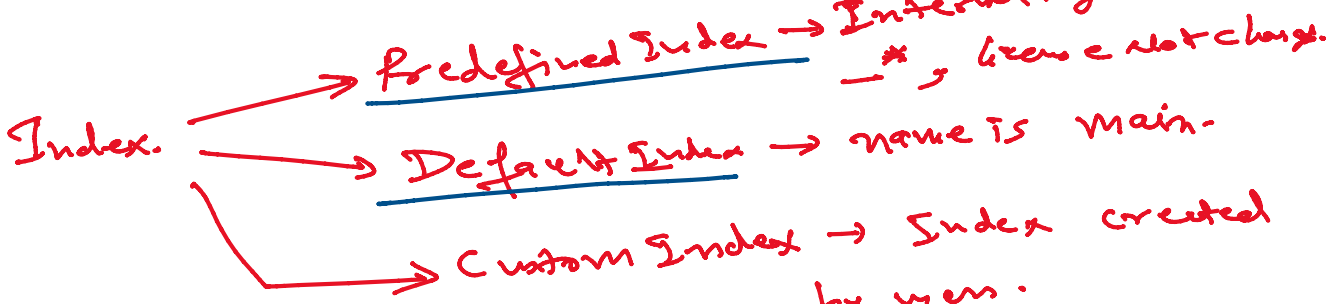
(1) HF
(a) Speed
(b) Bandwidth
(c) Resource consumption less at the indexer
(d) Alternation will be difficult due to huge no. of source.

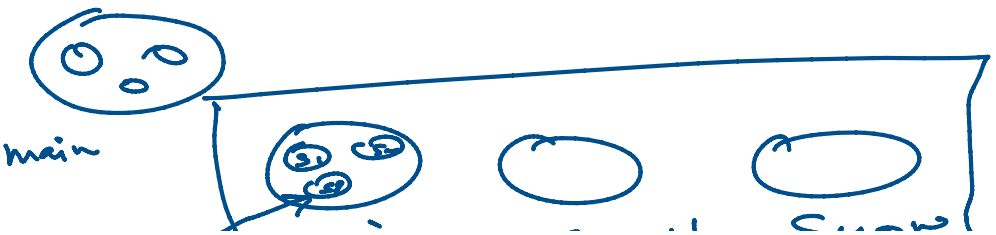
Disable for end user

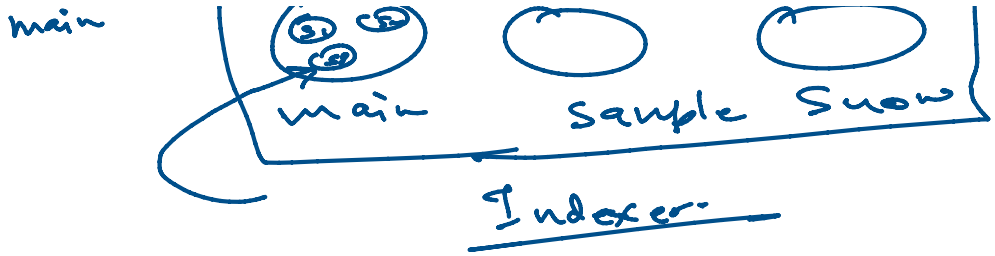


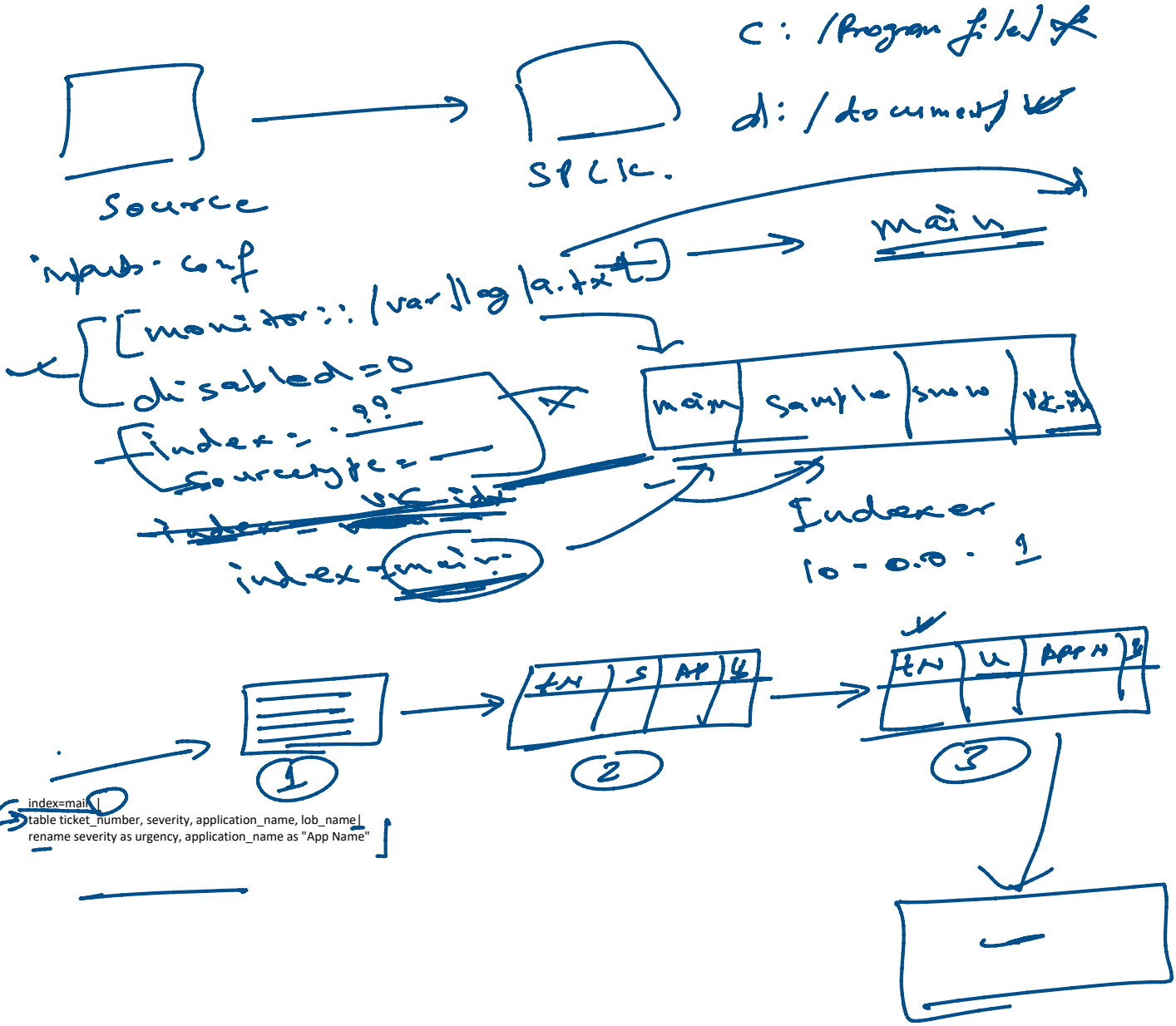


Smart Mode :- (1) Pull the Data.









Command Section :—

1. Table
2. Rename
3. stats.

8. Rex, erex, Regex.
9. join
10. timechart
11. chart
... fadd collect.

3. stats.
4. eval.
5. top
6. rare
7. append | appendcol | appendpipe.
11. chart
12. addtotal fieldname=colto total.
13. Dedup.
14. Eventcount
15. where.

stats →
- 1. Count
- 2. Sum.
- 3. Avg.
- 4. List
- 5. Values

Statistical.

6. dc.

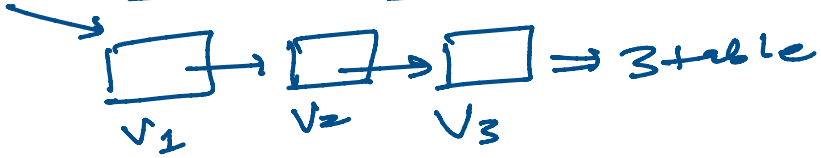
(1) Count:- No. of event with certain condn / group wise.

Most efficient one-

⇒ 2 table.

```
index=main | stats count as total  by severity, current_ticket_state
```

```
index=main | stats count  by severity, current_ticket_state | rename count as total
```



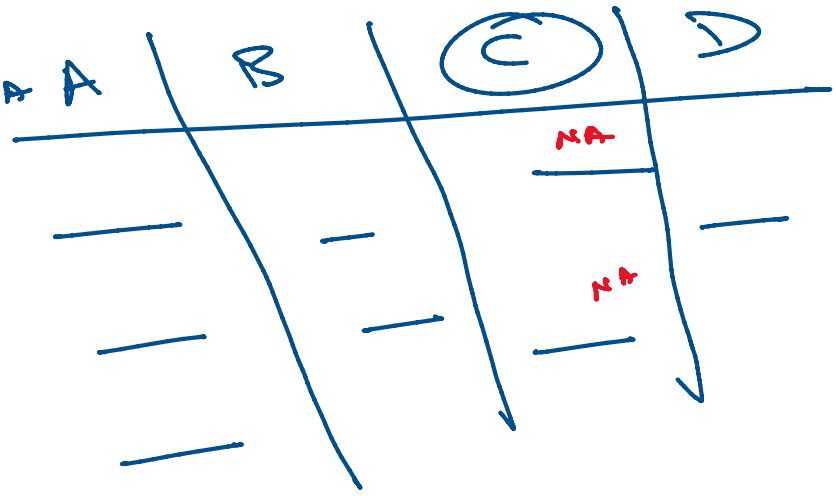
⇒ 3 table

(2) DC → Distinct Count.

fillnull value = NA C

fillnull

fillnull values=NA



3. List & Values:- Group the item on the category
   - → Unique items-
   - → All the items-

Bucket in Index :-

Thrawed Bucket → Deletion.

VK - idx.

① Size of Bucket

② Retention Period of Bucket.

→ 200 GB

→ 30 days

500 GB

Searching speed

index = VK - idx last 15 days