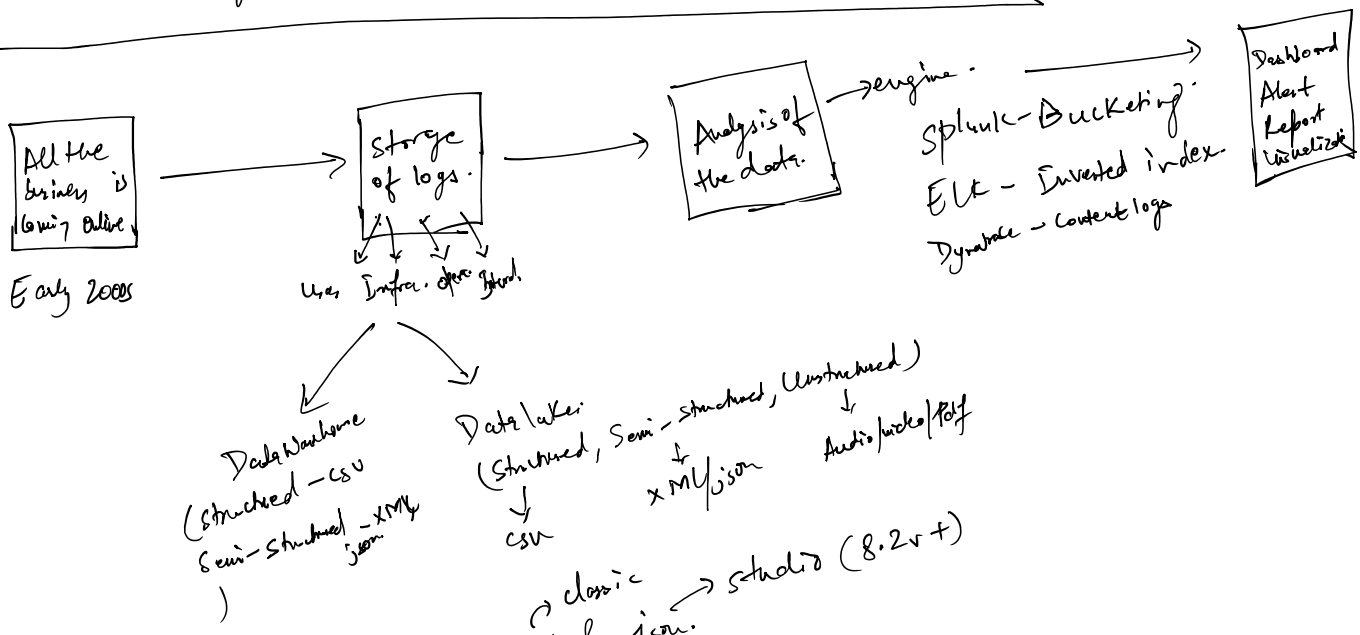
Day - 1

21 July 2025 10:03

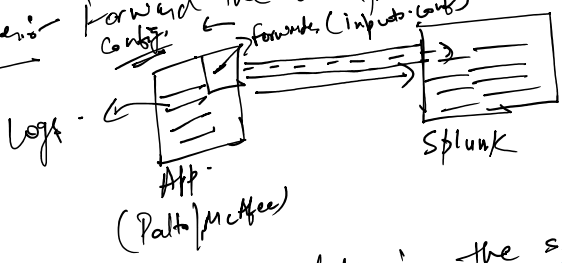
1. Splunk.
2. Components of splunk.
3. Splunk Architecture.
4. splunk Usecase.
5. SPL Query.



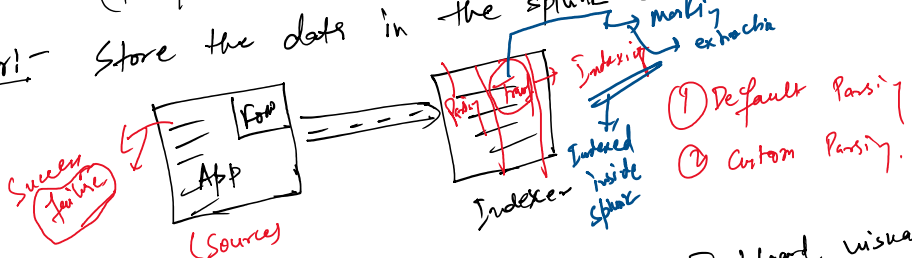
Splunk:- (1) Dashboard - xml & json. → classic → studio (8.2v+)
(2) Alert & Report.
(3) Custom Apps & visualization
(4) Predication.

Components:-

(1) Forwarders:- Forward the data from the source to splunk end.



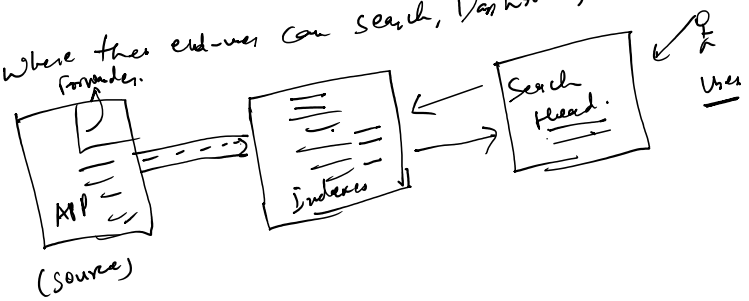
(2) Indexer:- Store the data in the splunk end.



where the end-user can search, Dashboard, visualization.

(Source)

(3) Search Head:- GUI where the end-user can search, Dashboard, visualization.



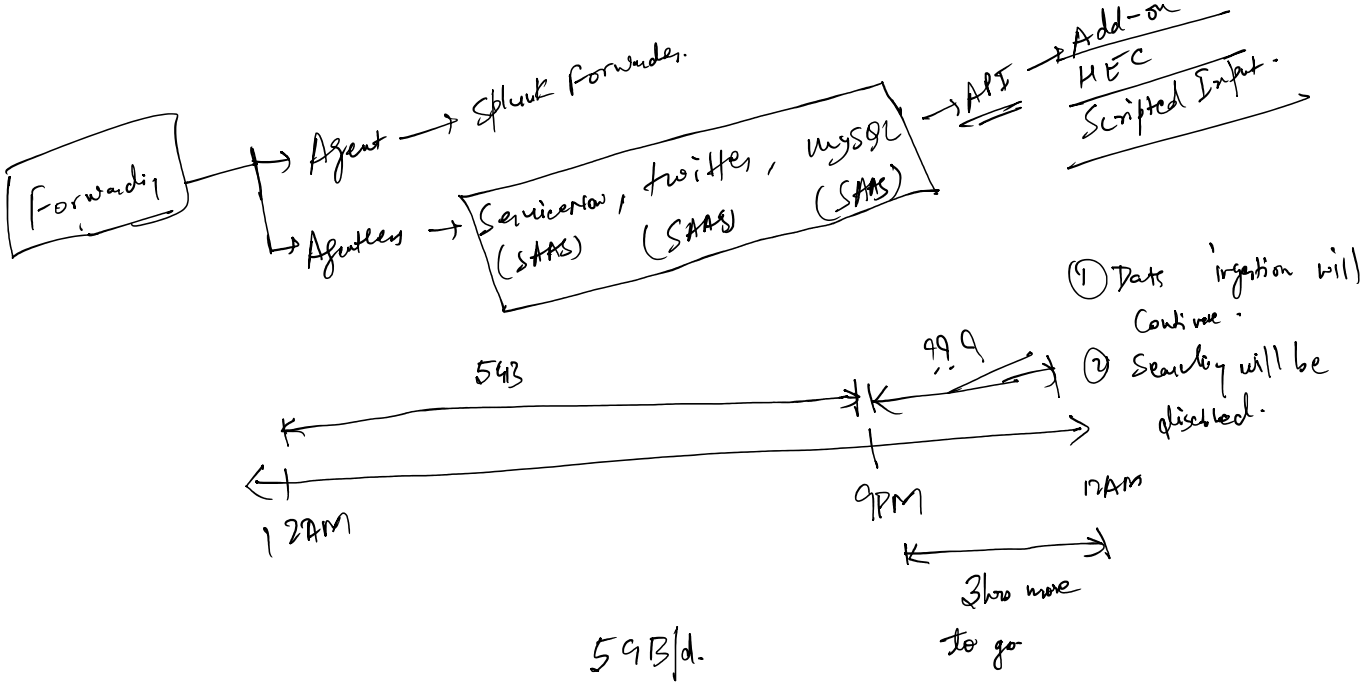
(4) Licence Master:

Policing agent that will make sure that you shouldn't be crossing the licence limit.

How much data you ingest on the daily basis?

5 GB/day → 1 year → $$$

24 hour cycle. (12-12)

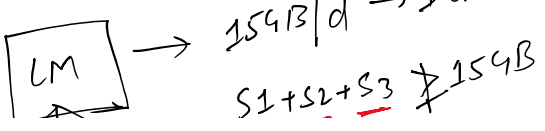


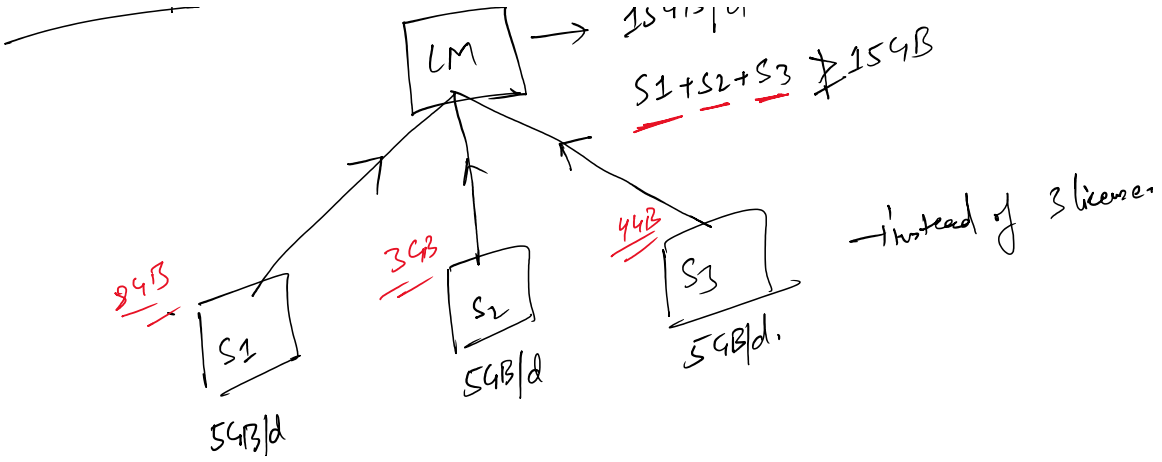
(1) Data ingestion will continue.

(2) Search will be disabled.

* 5 violation in 30days window.

License Pooling:

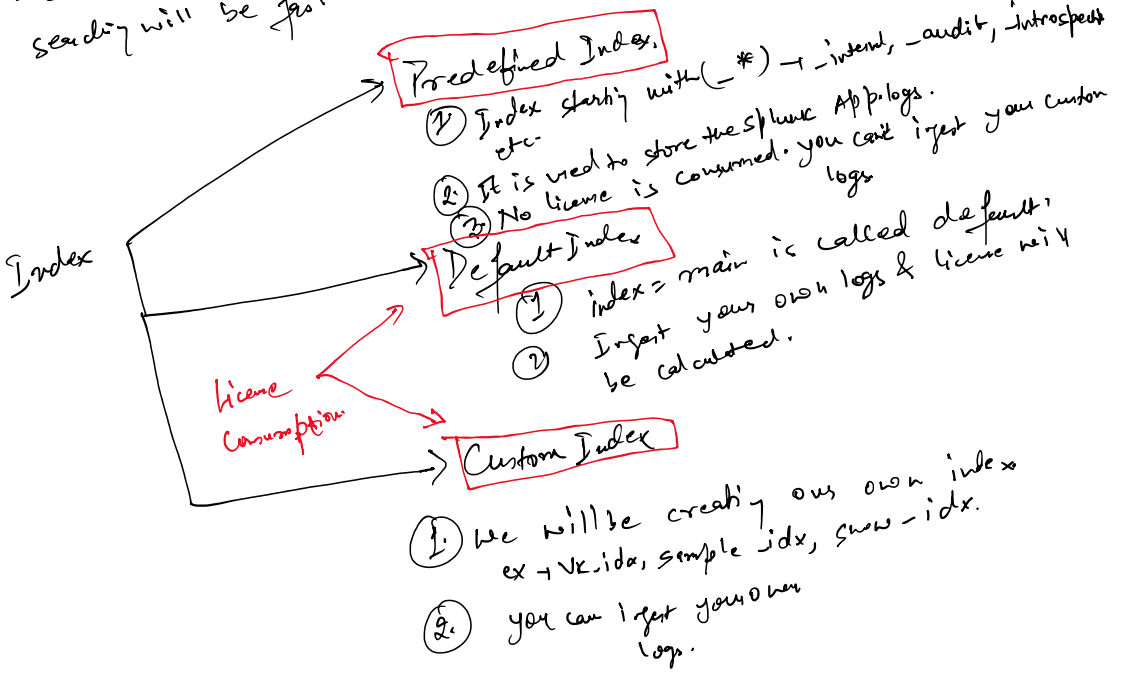




Indexes → Index1, I2, I3, I4

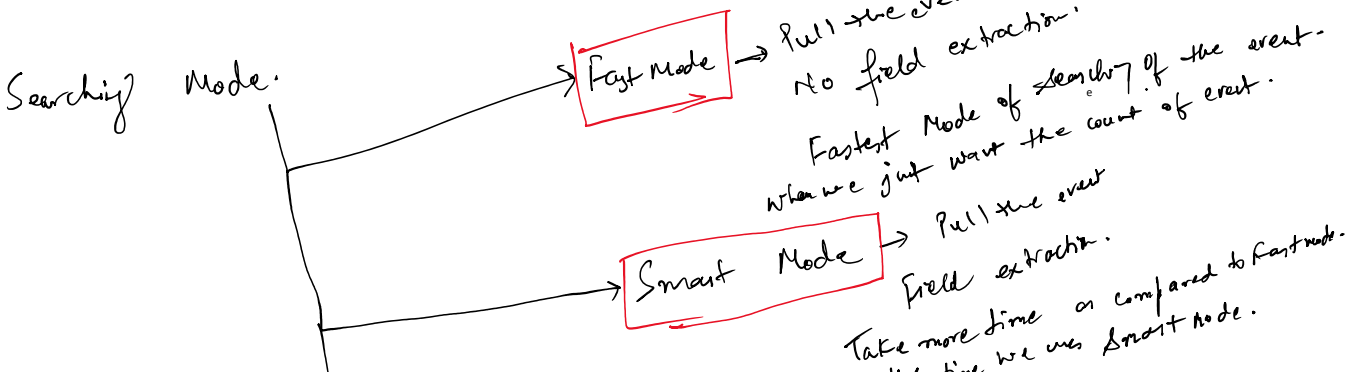
Harddisk → D:, C:, E:, F:

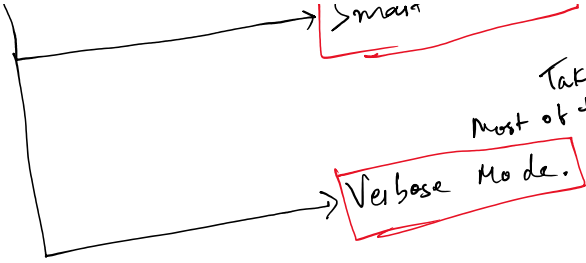
1) Segregate the data, so that searching will be fast.



FieldName is Case Sensitive

Field Value is Case Insensitive.





Field ...
Take more time or compared
Most of the time, we uses Smart Mode.
– Max. time.
extract the fields & event
Along with that pull the detailed
field. Traverse b/w event, stats & visu.

Search your data :– (1) Extraction of field.
(2) Pulling the events.

SPL → (1) table.
(2) Rename.
(3) stats.
(4) eval
(5) chart. } → Visualization
(6) timechart.
(7) Rex. } → Regular expression.
(8) addcoltotal.
(9) addtotal.
(10) top
(11) Rare.
(13) event count.
(14) Sort

(1) Table :– Tabular output.
ex → | table f1, f2, f3 – – –
Same the seq. the output will come.

(2) Rename :– Change the name ~~of~~ at the searchtime.
ex → | rename f1 as new-f1
f1 → old name
new-f1 → new field.

(3) Stats :– It will give the statistical output.
ex → | stats count by f1, f2 – – –

(3) Stats:- It will ...

(1) Count :- | stats count by f1, f2 - -

(2) Sum :- | stats sum(f1) ——

(3) Avg. :- | stats avg(f1) ——

(4) list :- | stats list (source) as source by sourcetype.
↳ overall list of item.

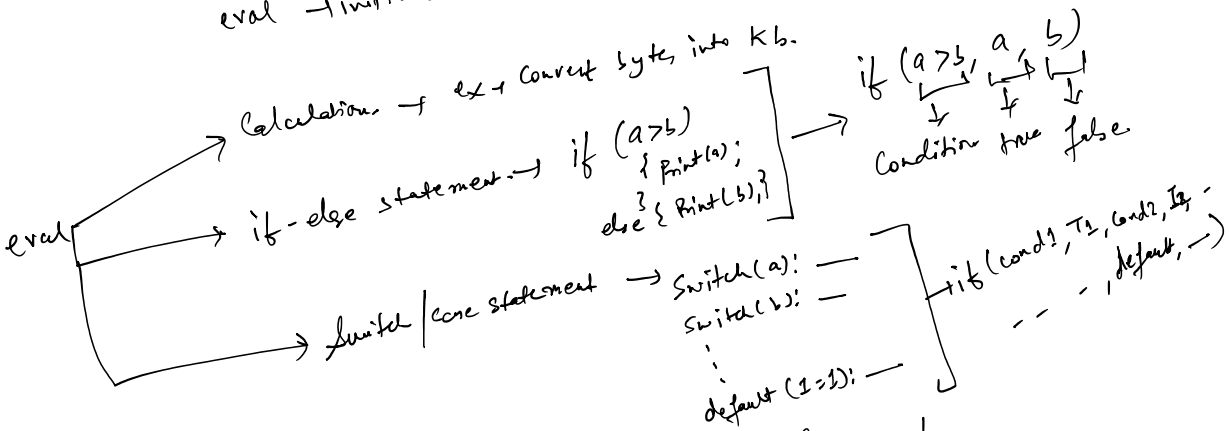
(5) Values :- | stats values (source) as source by sourcetype
↳ only unique item.

(4) Eval:-

Used for evaluation activity.

int, str, var → define the variable.

eval → initialize the variable.



field → field - f1 → Remove the field f1 from the O/P.

Sort → Sorting purpose.

Sort - f1 → Descending order.

Sort + f1 | sort f1 → Ascending order.