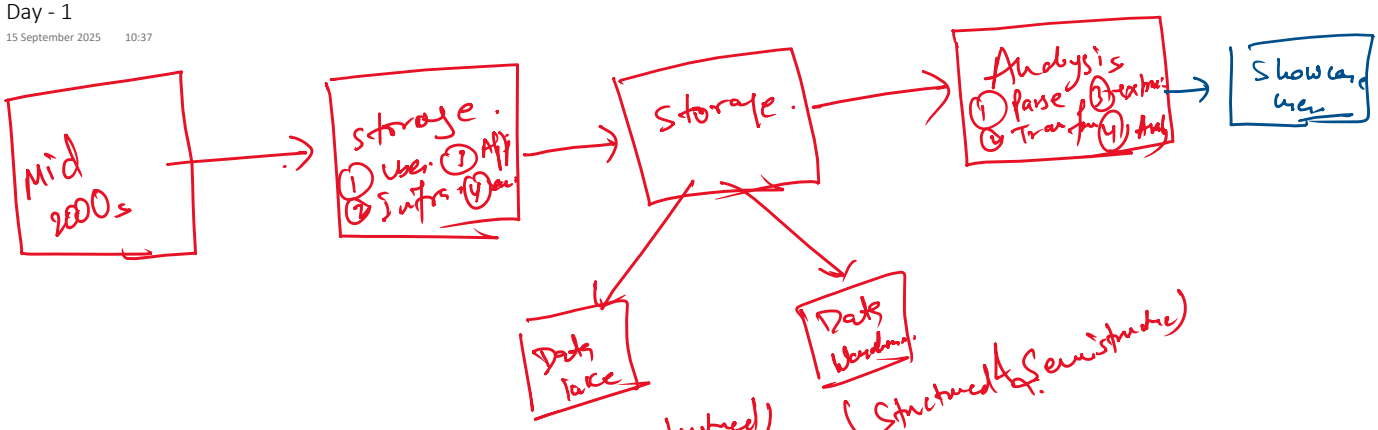
Day - 1

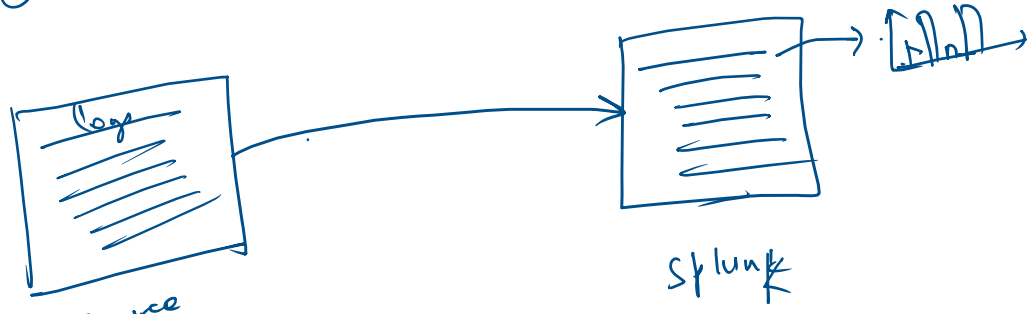
15 September 2025 10:37



(1) Analysis engine.
(2) Support - Community or Customer support.
(3) License Cost.
(4) Integration with other tools.

(1) Dashboard
(2) Report
(3) Alert
(4) Predictive Analysis

Splunk:- (1) Dashboard
(2) Report
(3) Alert
(4) Predictive
(5) Knowledge object.



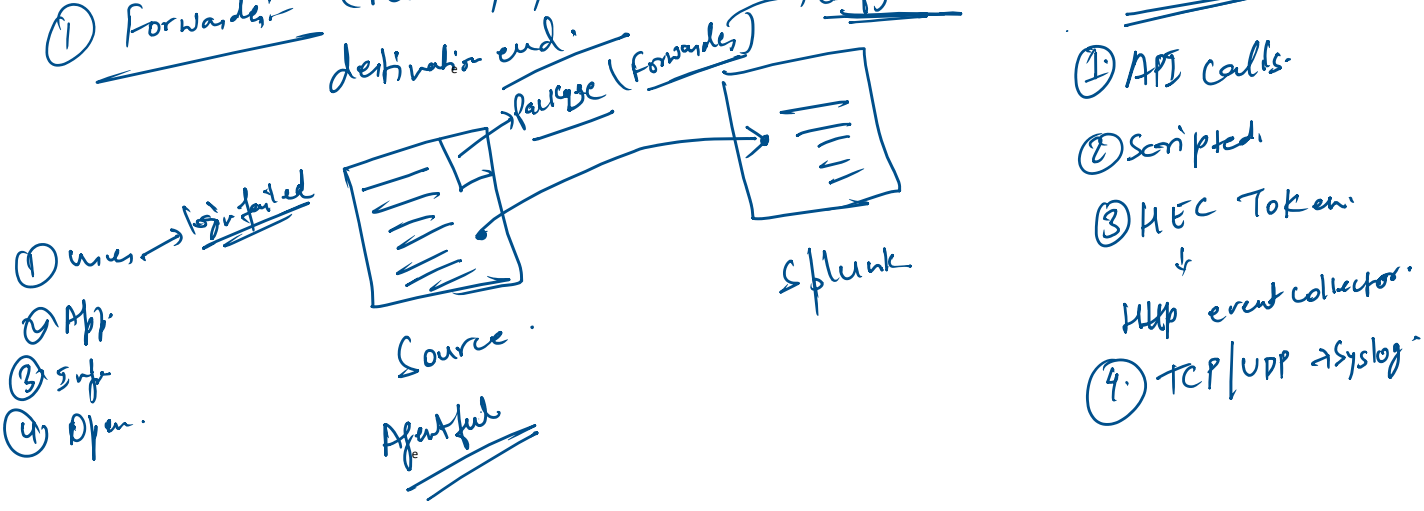
McAfee lineage.

Component of splunk:-

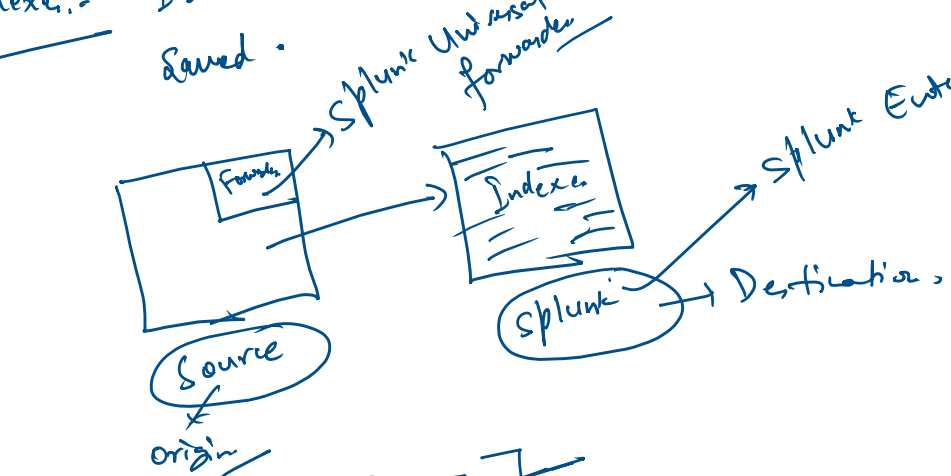
1. Forwarder
2. Indexer.
3. ~~Search~~ Head.
4. License Master.
5. Deployment Server
6. Cluster Master.
7. Deployer

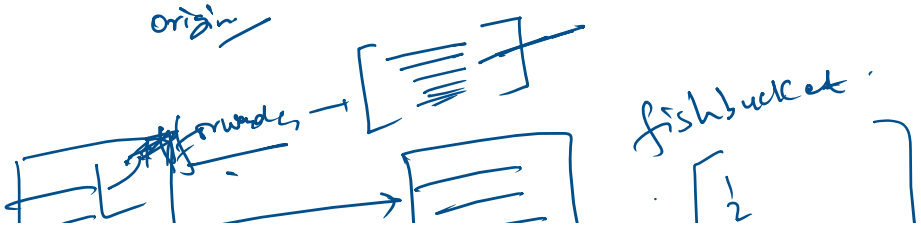
→ Management Instances.

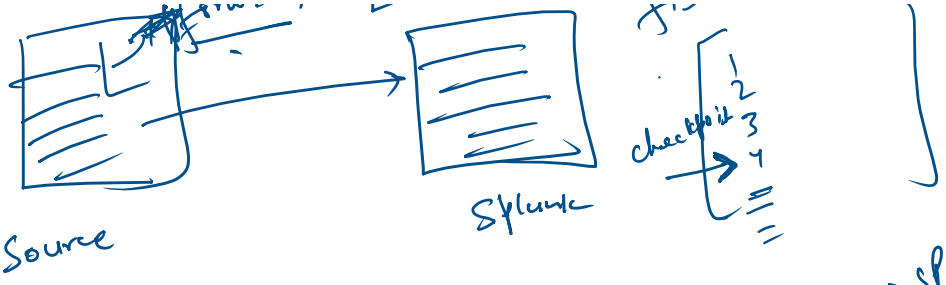
1) Forwarder:- Create a pipeline & send the data from the source to the destination end.

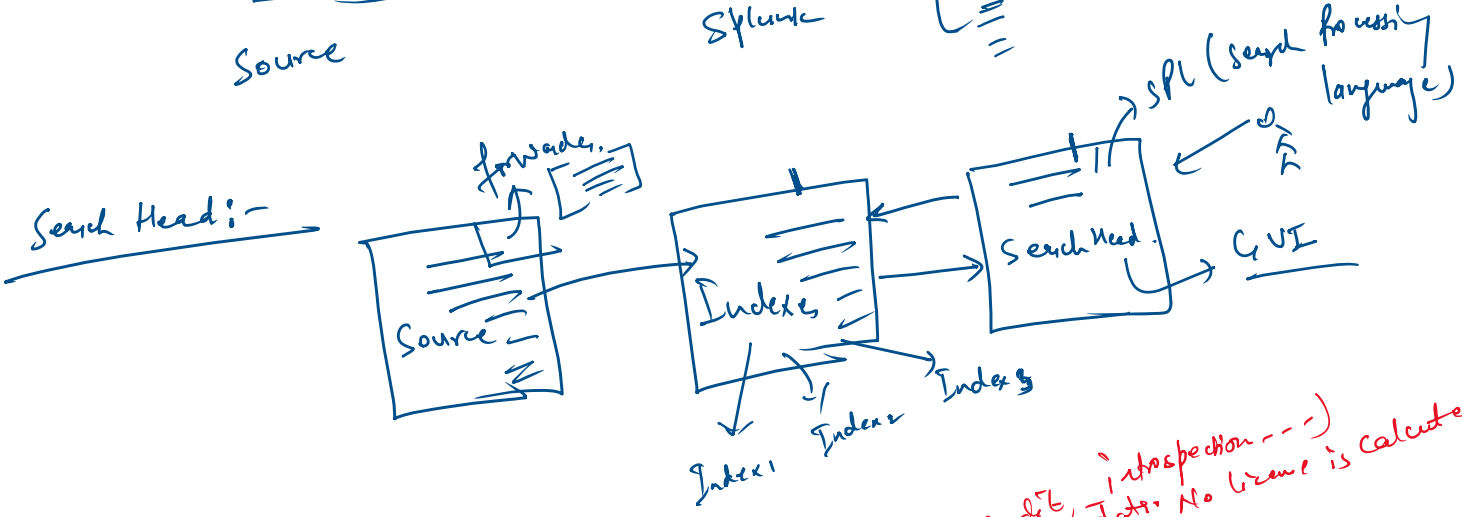


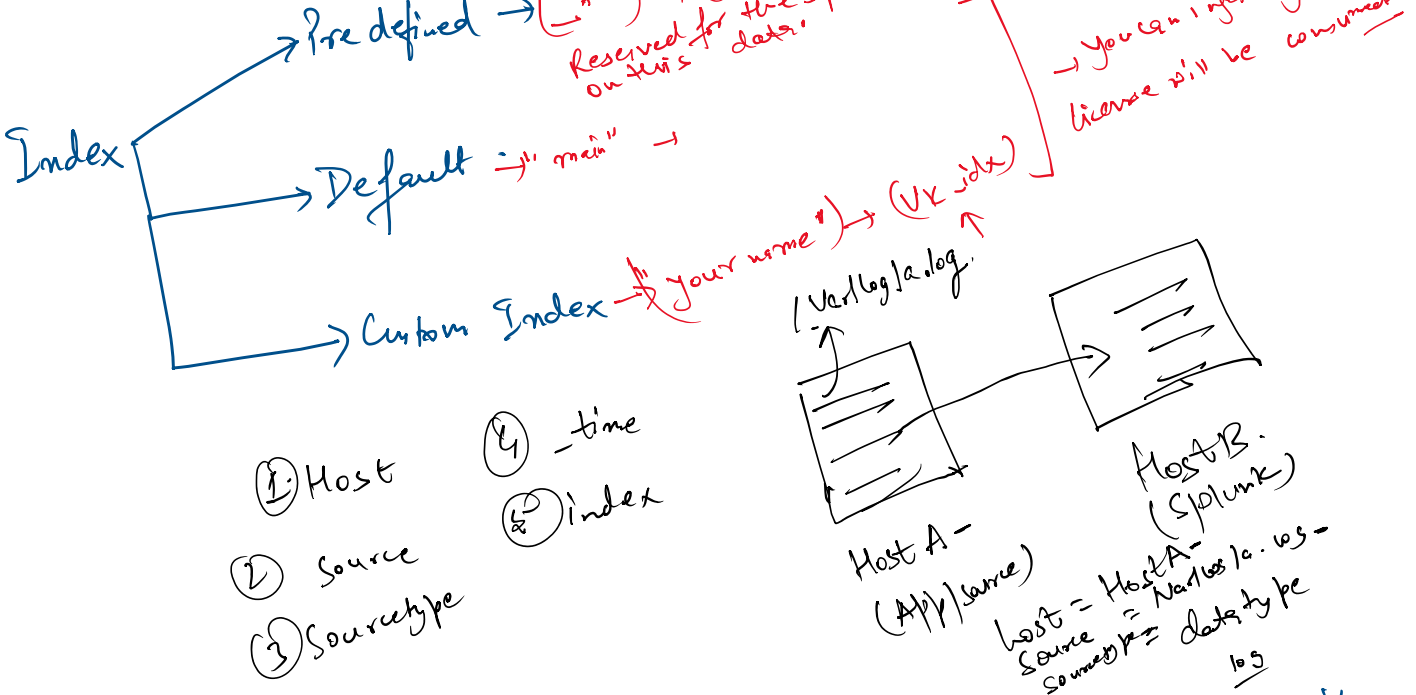
2) Indexer:- Internal database of splunk where the data will be saved.





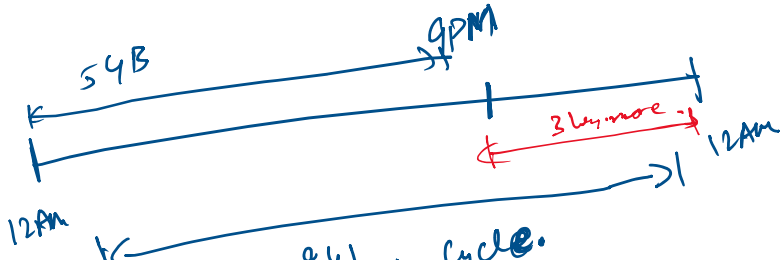






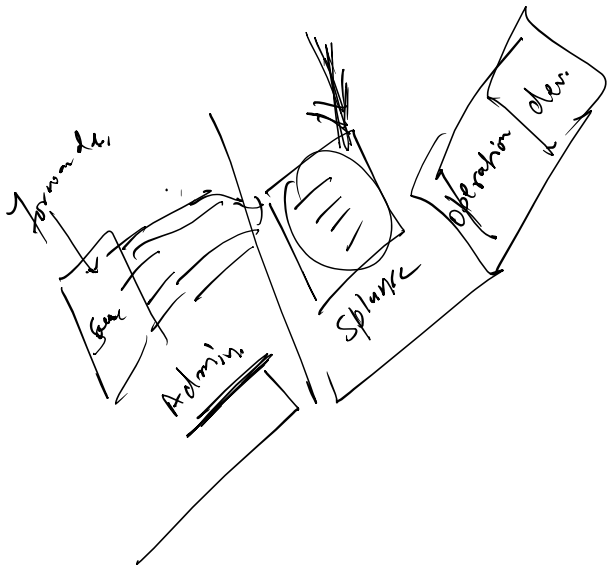
License Master:- Agent that will make sure, you will be in it in the license limit.

1. How much data you ingest on the daily basis? 5GB/d → 1 year.



1. Indexing will continue.
2. Overall security will be disabled.
   - No Alert
   - No Report
   - No Dashboard

→ All the system will come to the stable mode.



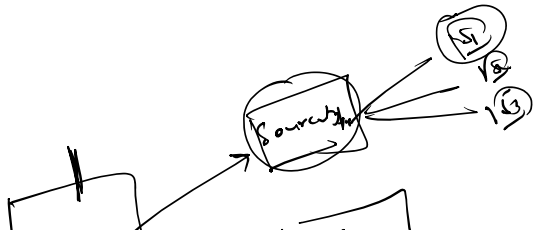
SPL Queries

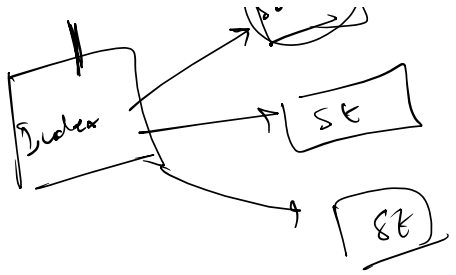
1. Table.
2. Rename.
3. Stats.
4. eval.
5. Addtotal
6. Addcoltotal.
7. dedup.
8. Sort
9. rex.
10. chart.
11. timechart
12. Top
13. rare.
14. join.
15. Field.
16. Where
17. eventstart
18. fillnull

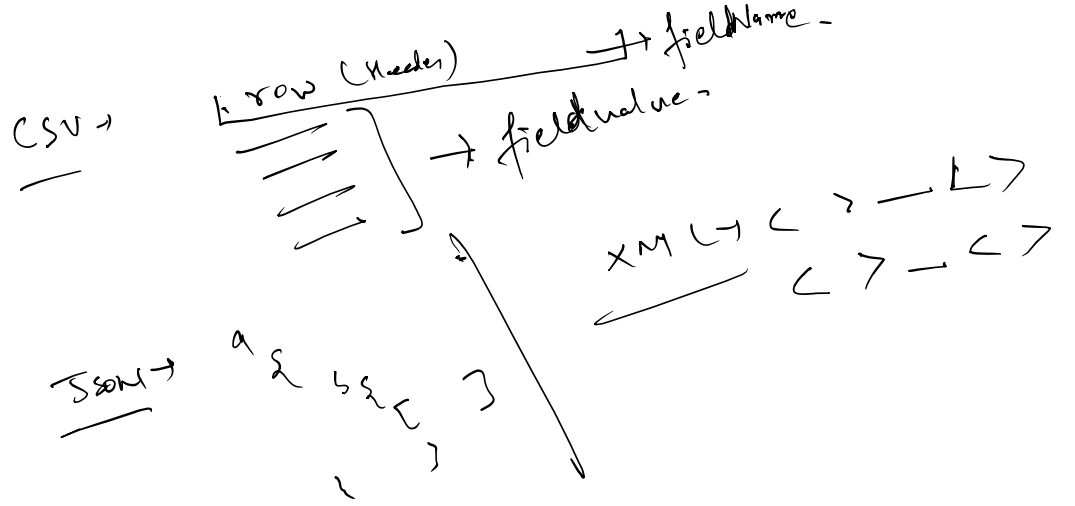
1. Table:- Tabular output.

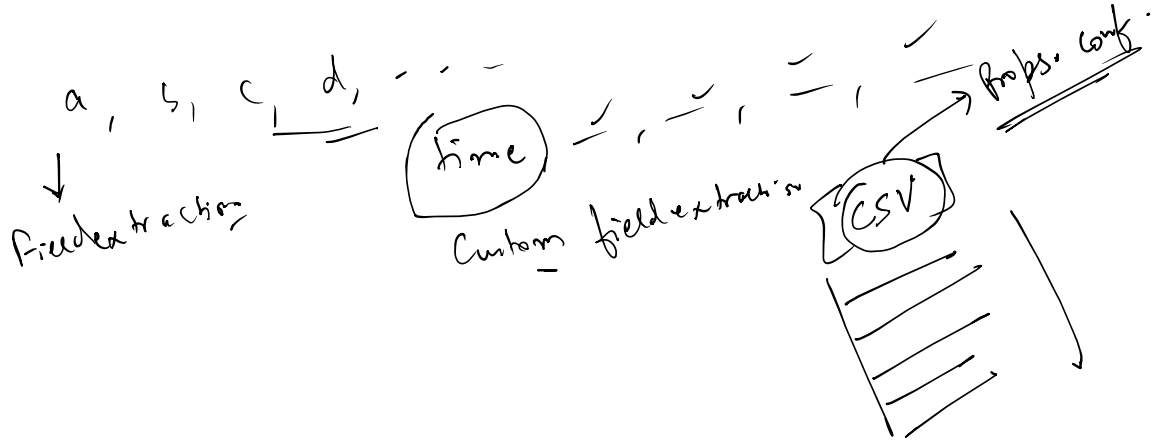
Table f1, f2, f3- - -

Field Name are case sensitive
field Value are case insensitive.









(2) Rename → change the name at the search level.

| rename count as total
↓ ↓
oldName newName

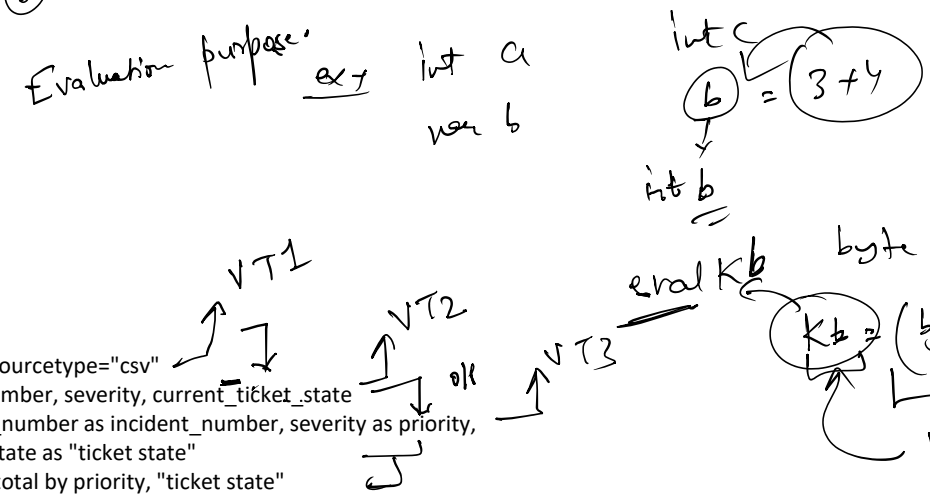
(3) Stats - Used to get statistical output -

(1) count - count of events.
(2) dc - unique count of events -
(3) sum - Summation
(4) avg - Average value
(5) list - graph purpose → duplicates
(6) values - Unique values -

(5) list - [ ]

(6) values - unique values

(4) Eval :- Evaluation purpose. ex - int a
var b



VT1 VT2 VT3

```
index="vk_idx" sourcetype="csv"
| table ticket_number, severity, current_ticket_state
| rename ticket_number as incident_number, severity as priority,
current_ticket_state as "ticket state"
| stats count as total by priority, "ticket state"
```

(2) if -else statement :-

```
if (a>b)
    { print(a);
    }
else { print (b);
     }
```

→ if(a>b, T, F) → false statement.

Condition. True statement

(3) Case statement :-

```
switch(a); —
switch(b); —
switch(c); —
    :
    :
default; —
```

→ case (cond1, "—", cond2, "—", cond3, "—")

severity = 1 severity 2

eval (a=)

Variable.

left to right.