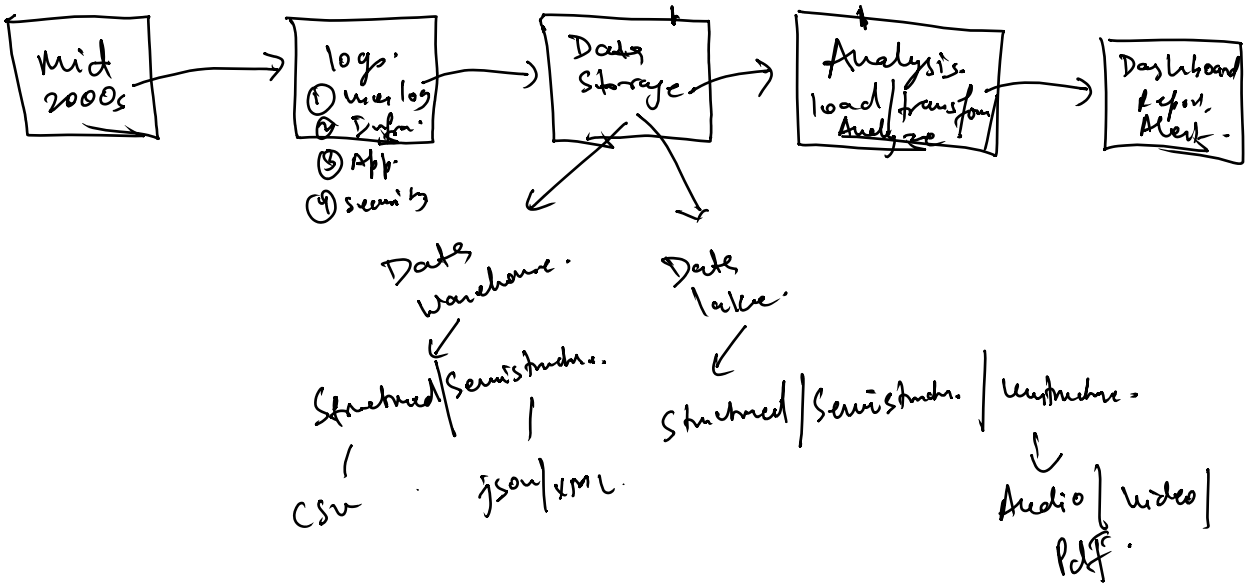
Day - 1

16 October 2025 09:42



① Monitoring → Reactive.

② observability → Proactive

① CPU → APP Hang → App↓

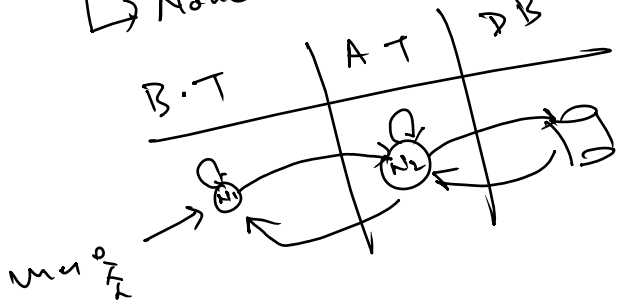
Pillars of observability

① Metrices. — Aggregate Value. CPU, Disk, Memory.

② logs — Detailed about the Activity having timestamp. detail.

③ Traces —

↳ Node level view.

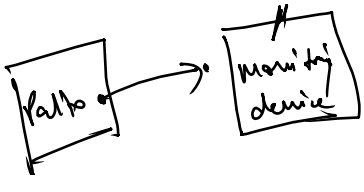


Splunk:-

① Dashboard
② Report
③ Alert.
④ Predective Analysis

→ end user.

① Data type.

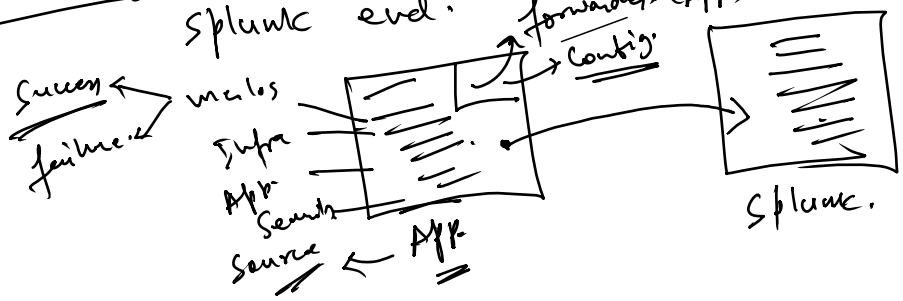


1. Data type.
2. License Cost.
3. Customer Support.
4. Integration with diff Sources.
5. Community Support.

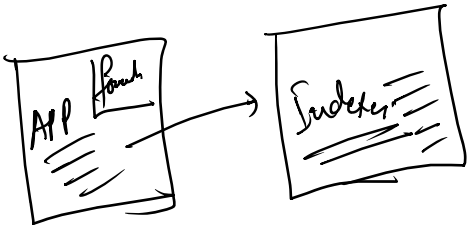
Component of splunk:-

1. Forwarder.
2. Indexes.
3. Search Head.
4. License Master.

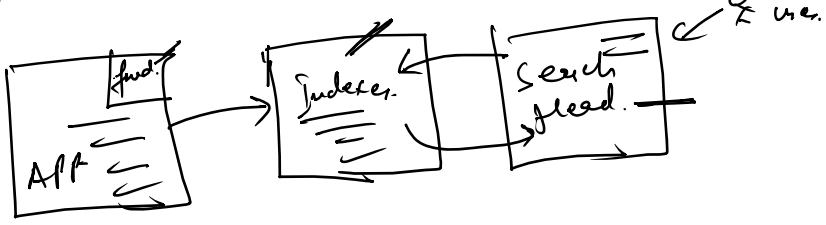
1. Forwarder:- Forward data from the source to the splunk end.



2. Indexes:- Store the data on the splunk.



3. Search Head:- GUI where the user will do the searching Activity.



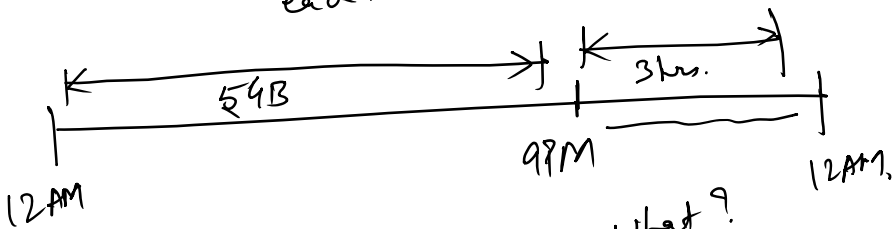
4. License Master:- Pay to splunk to leverage the access.

4. License Master → Pay to splunk to leverage the access.
LM → Monitor whether you are breaching the license limit or not.

What? — How much data you ingest on the daily basis?

5GB/day → 5GB data.
↓
each & everyday.

5GB/day → 1 year
↓
each & everyday.



What?

1. Indexing will continue.
2. No Searching of any data for those 3 hours.

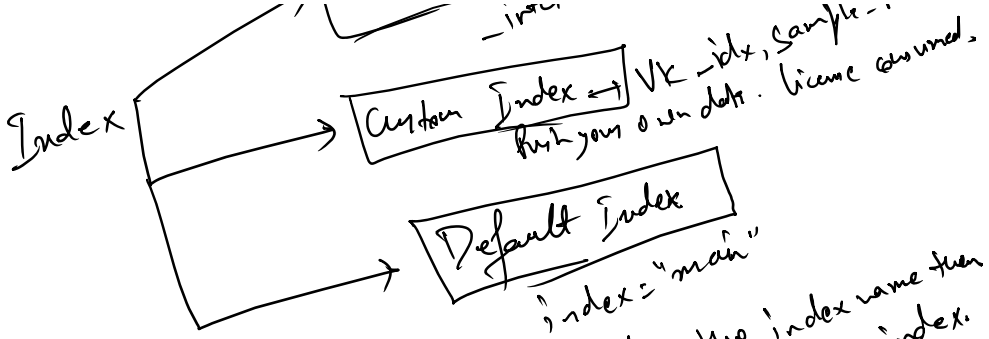
SPL (Search Processing language):—

1. table
2. Rename.
3. Stats
4. eval.
5. top
6. Rare.
7. dedup
8. sort
9. fillnull.
10. addtotal.
11. addcoltotals
12. chart.
13. timechart.
14. geostats.
15. SingleValue Visualization;

→ Visualization.

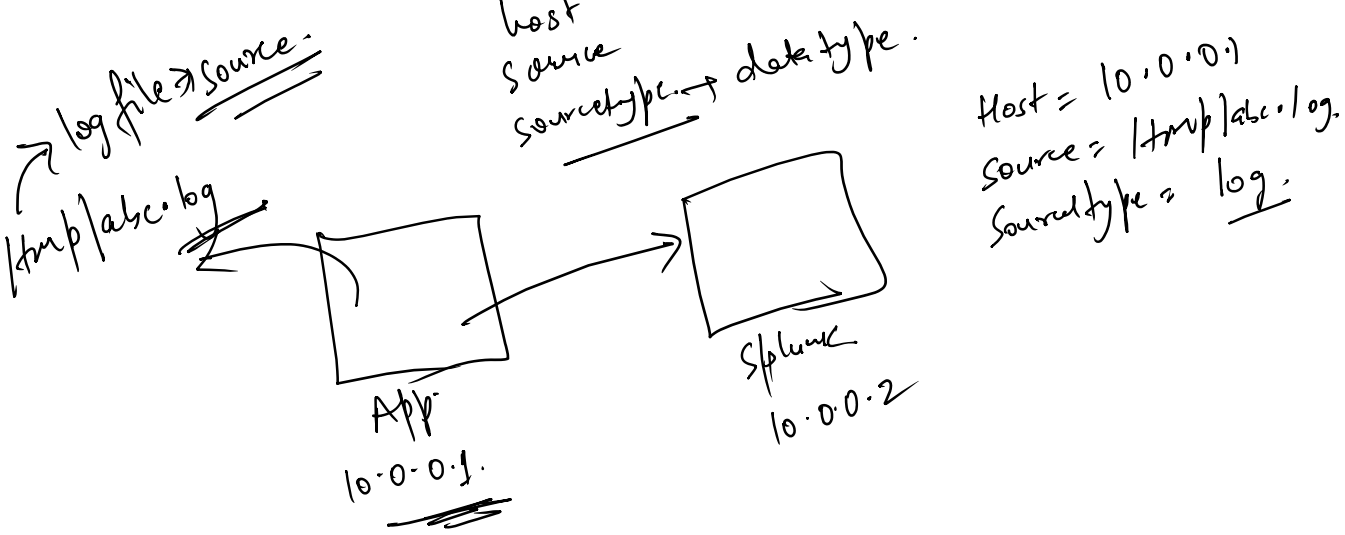
Predefined → Reserved for the logs coming from splunk. No license consumed
index starting with (_*)
_internal, _audit, _introspection...

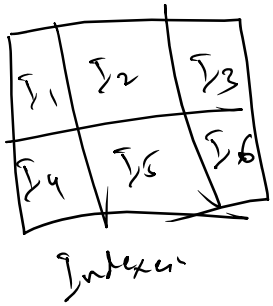
Index → VK_idx, sample_idx
idx. license consumed.

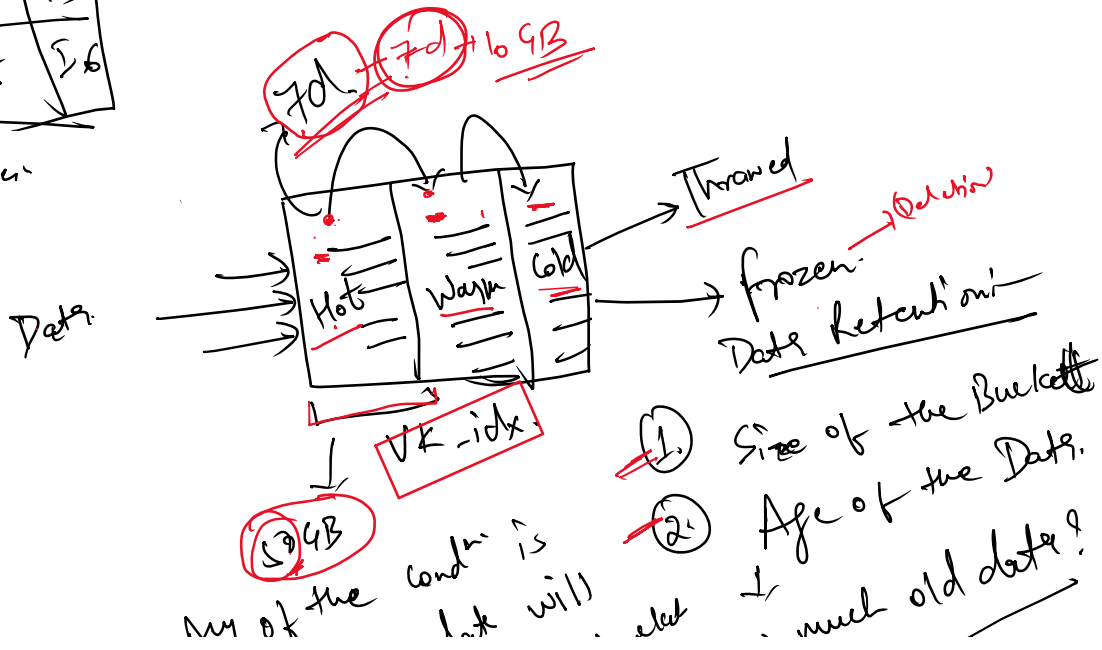


If you don't define the index name then it will be send to the main index.

Selected fields → ① field which will come by default







Any of the cond^n is met, the data will move from one bucket to another

How much old data?

Bucket

(1) Table :- Tabular output.

ex:- | table f1, f2, f3 - - -

Field Name is Case Sensitive.

(2) Rename :- It is used for rename activity.

↳ Search level.

for ex:- ex- | rename old-field AS new-field

(3) Stats :- used for statistical output.

count - No. of events → | stats count by f1.

avg → | stats avg(f1) as f1

sum → | stats sum(f1) - - -

list } → categorise the data.

value }

| stats list(f1) by - - -

(4) Eval :- evaluation purpose.

int a

int b

var a

var b

→ | eval a - -

(1) Calculation → (bytes → Kb)

Kb = (bytes / 1024)

a, b

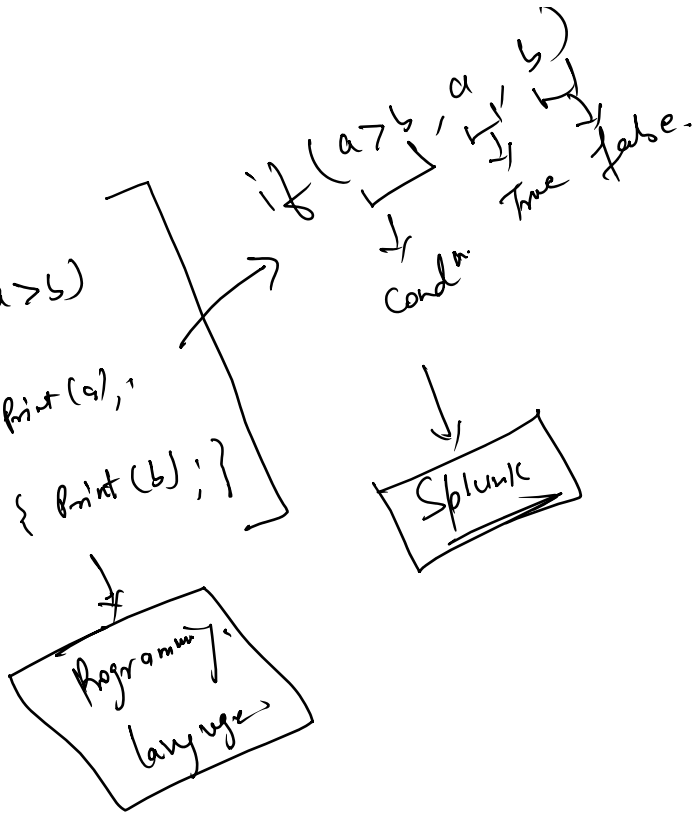
(1) Case

(2) if-else

(3) switch/case.

if-else:

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



Switch & Case statements:-

```
switch:-
- case(a) : ———
- case(b) : ———
:
- default() : ———
```

→ case(Cond1, "True", Cond2, "True", Cond3, "True" --- 1=1, "—")

Universal Cond^n

Top:- |top sourcetype.

top 10 sourcetype by default.

|top sourcetype limit=3

top 3 values

rare:- least value - |rare sourcetype

Ascending order

rare:- least value - | rare ... -

Sort:- Ascending → | sort → Ascending order
count →

Descending → | sort - count.
↓
Descending order.

3	Vivek	3	Amit
3	Bhargys	3	Bhargys
3	Amit	3	Vivek

Addcoltotal:- Addition column wise.

ex:- | addcoltotal field_name label-name.

Addtotal:- Addition Row wise.

ex:- | addtotal fieldname.