Day - 1

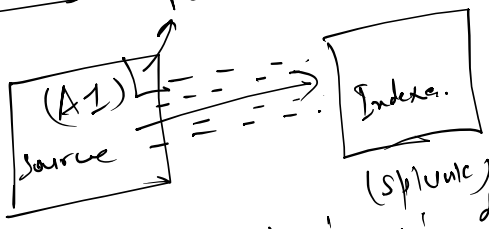
17 September 2025 19:35

Splunk :- Log monitory tool.

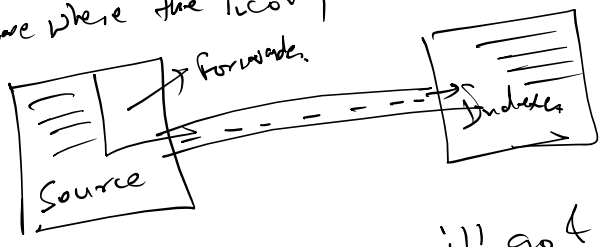
1. Dashboard
2. Report.
3. Alert
4. Predictive Analysis.
5. Knowledge object.

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

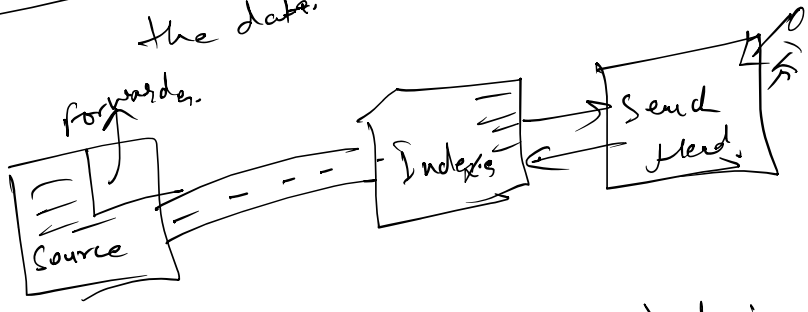
1. Forwarder :- Forwarding the logs from the source to the splunk side.



2. Indexer :- Database where the incoming (splunk) data is stored.

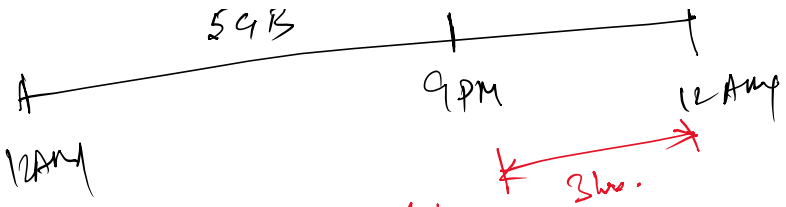


3. Search Head :- GUI where the user will go & search the data.



4. License Master :- Amount of data, you are indexing on the daily Basis.
24hrs. cycle.

5GB/d - 1 ~~month~~ year.



(1) Indexing of data.

(2.) Searching will be disabled.

30 day → 5 violation only.

↓

Blacklist.

↗ License is consumed.

Reserved for the internal data/ splunk app. logs.

NOT Post your own data.

Predefined index → (_*) → (_internal, _audit, _introspection - - -)

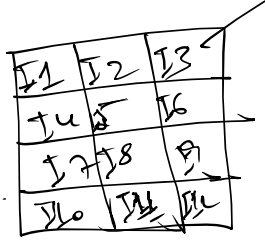
Index

Default Index → (main) → index = main

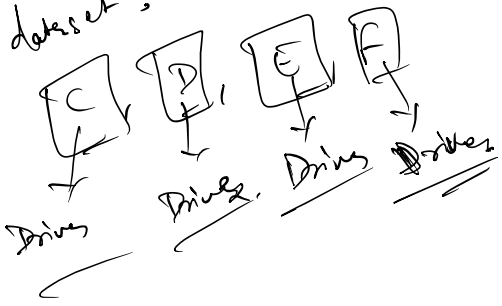
↳ By default, it will store index named main.

Custom index → which is user created one.

(VK_idx, sample=idx)

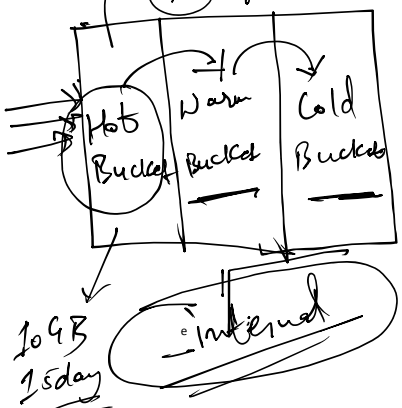


→ Different dataset.



(1) Size of Bucket

(2) Age of Data



less the event ↑ faster it would.

SPL:-

table

where

addcoltotal

(11) timechart

(12) Append | Appendcol | Appendpipe

join.

1. table
2. Rename
3. stats
4. eval
5. search
6. where
7. addcoltotal
8. addtotal
9. fillnull
10. chart
11. Append
12. join
13. rex
14. makemv
15. mvexpand
16. multivalue
17. top
18. rare

(1) Table – Tabular output.

| table f1, f2, f3 - - -

(2) stats:- Statistical output.

| stats count → count the no. of event.
avg — → Avg & Sum of Numeric field.
sum —
list — → categorise the data.
values —

| stats list(—) by —
↓
all the values

| stats values.
↳ All the unique values.

(3) Eval:- evaluation purposes.

1. Calculation.
2. if-else statement
3. Case statement.

(1) Calculation:-

bytes → KB

eval → KB = bytes / 1024 → expression

↑ Variable

int a;
a =

int a =
var a =

eval → Initialize the variable

(2.) if-else statement

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

→ if (a>b) → a → b → Condition → True → false

(3.) Case :-

Case (1):
Case (2):
Case (3):
default :

→ Case (Cond1, "—", Cond2, "—", Cond3, "—", 1=1, "—")

Cond1 → Condition
Cond2 → True
Cond3 → false
1=1 → Universal condition.

Universal Condition

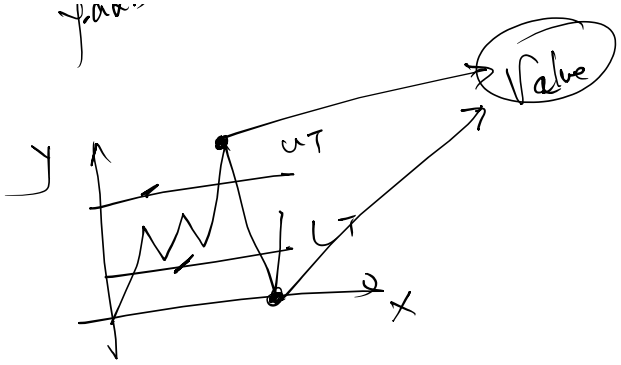
(4.) Addtotal :- Addition row wise.

addtotal — fieldname = "—"

addcoltotal :- Addition column wise.

chart + | chart y by x
y-axis x-axis

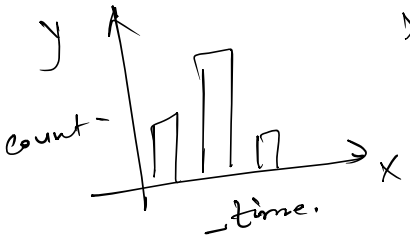
→ Value



timechart :-

timechart count by severity.

X-axis is reserved for _time.



d = day
w = week
H = hour.
M = minute
s = sec

mon = month
y = year.
q = quarter

Single Value :-

Single Numeric Data for visualization

Search & where → Both used for filter purpose

Search the value in a field.

search severity =1

A	B
5	10
15	25
35	15
45	7

where

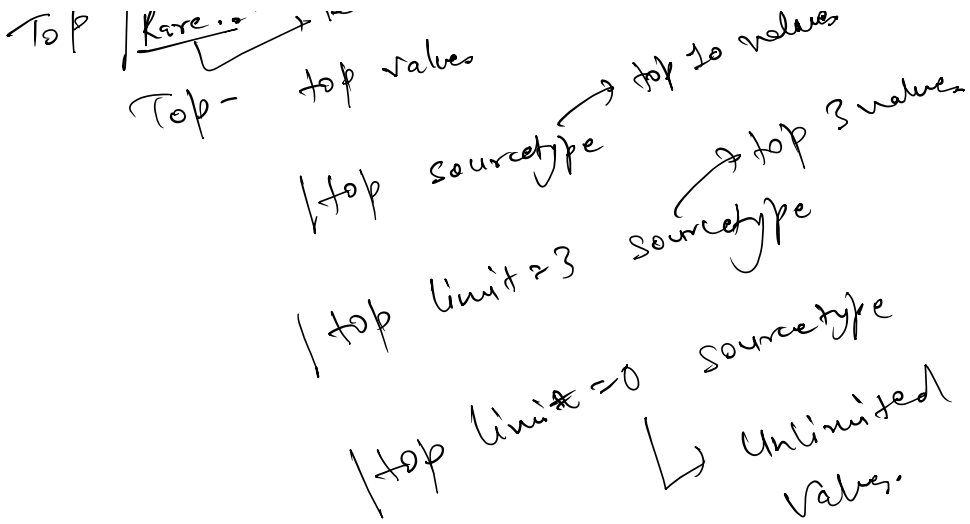
where A>B

A	B
35	15
45	7

Top / Rare :- → least value. (By Default = top 10 values, Limit=3 / 10)

Top → top values

→ top 10 values


Top | Rare..
Top- top values
| top sourcetype → top 10 values
| top limit=3 sourcetype → top 3 values
| top limit=0 sourcetype
Unlimited values.