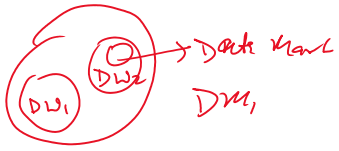
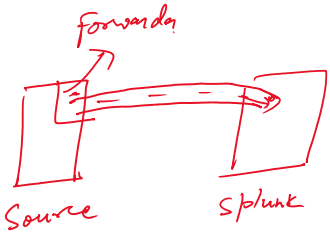
Structure → CSV
Unstructured →
Semi Structure → XML
→ Data lake.

I am going to home. My home is in India.
Home - 2



Component in splunk

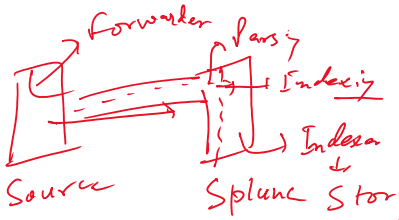
1. Forwarder



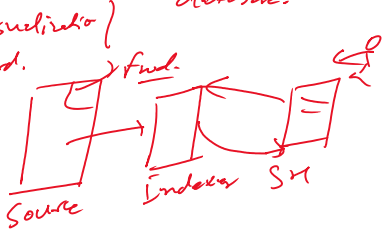
Metrics

70% → Memory
↓
timestamp → log
traces

2. Indexer



3. Search Head: GUI → search/visualization/ Dashboard.



4. License Master
↓
Agent that will Monitor

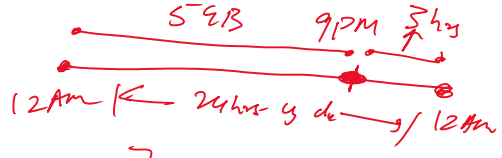
5GB/d → 1 year → license
↳ 24hrs cycle.

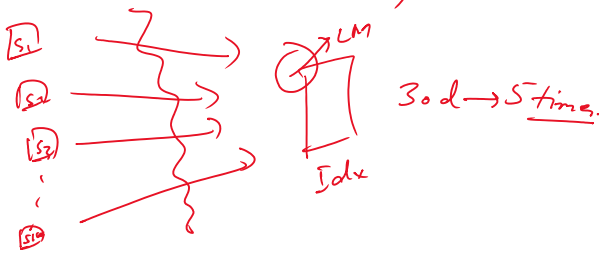
Agent that will Monitor

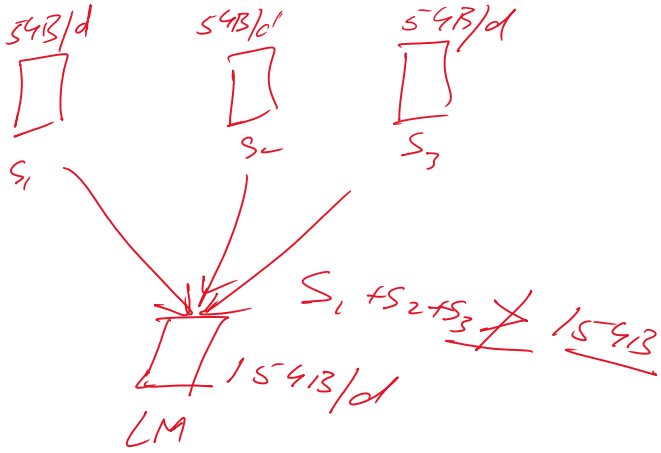
↓

Amount of data ingested in splunk on daily basis. → License Parameter

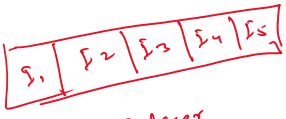
↳ 24 hrs. cycle.







Indexer



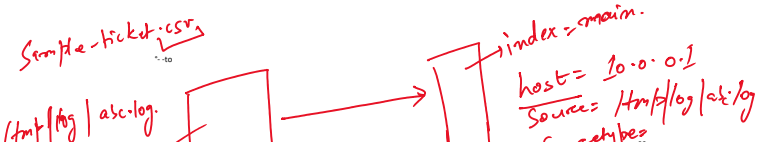
Indexer

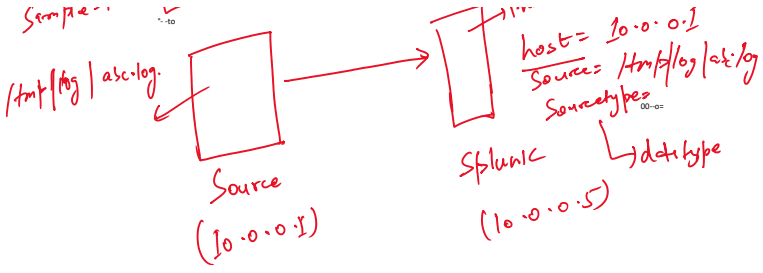
Index
- Predefined Index → _audit, _internal, _* → Reserved for splunk related logs → No license usage.
- Default Index → Custom Data → main → License Consumed.
- Custom Index → Any name → VK_idx
  - ① Custom Data.
  - ② License Consumed.

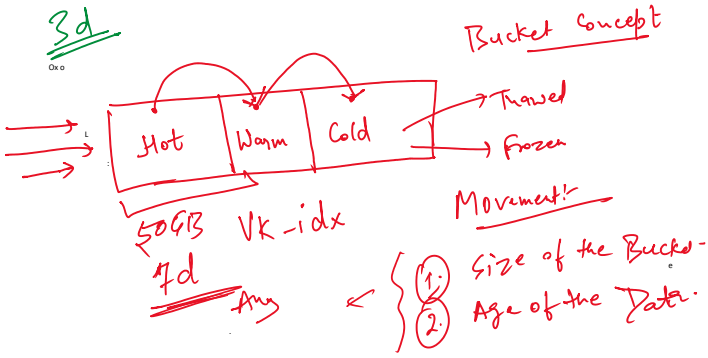
Custom Index:-

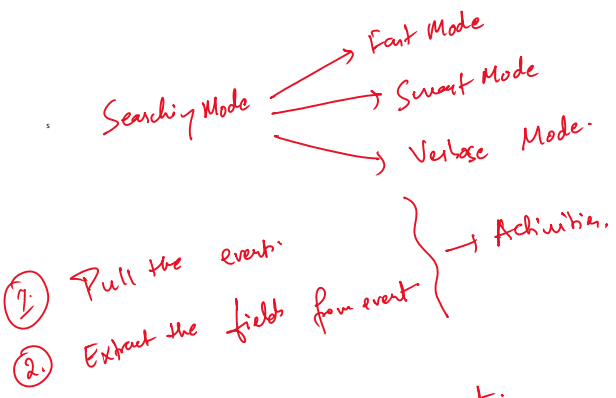
① All lowercase
② No space / no uppercase / no digits.
③ Special chars "_"

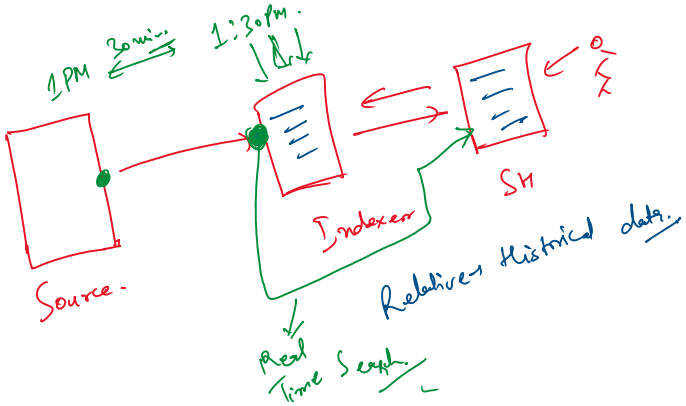
Sample-ticket.csv











SPL Queries

1. Table.
2. Rename.
3. Stats
4. fillnull
7. Where.
8. dedup.
9. Top / Rare.
10. makeresults.

3. Stats
4. fillnull
5. Eval
6. Search
9. Top / Tr
10. makeresults
11. Sort

1. Table:- Tabular output.

Syntax:- |table field1, field2, field3

VVS ** field Name is Case Sensitive & field Value is Case insensitive.

2. Rename:- rename from old fieldName → New fieldName

Search level.

|rename oldname AS NewName.

3. Stats:- Statistical output.

1. Count → Count Value.
2. Avg. → |stats avg(—) as —
3. Sum. → |stats sum(—) as —
4. List → Pull all the entries → Grouping of Values.
5. Values → Pull the unique item.

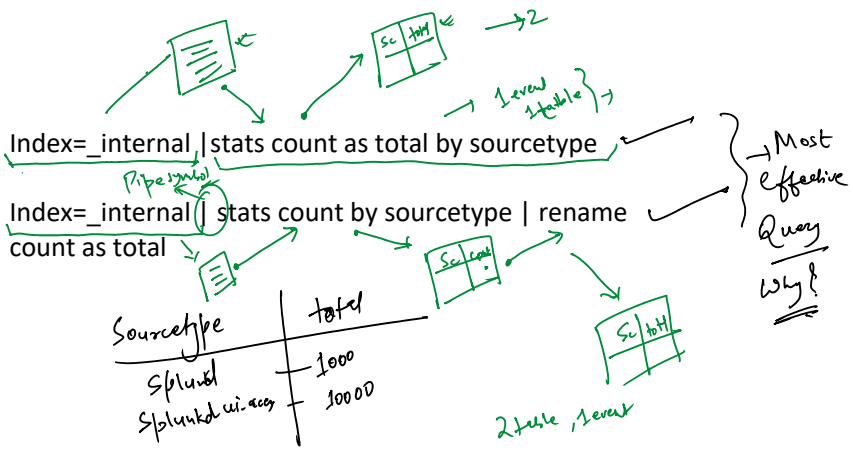
fillnull → Handle your blank spaces.

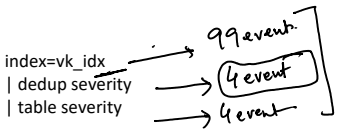
*** By default, fillnull value is 0

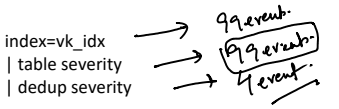
fillnull value="NIA"

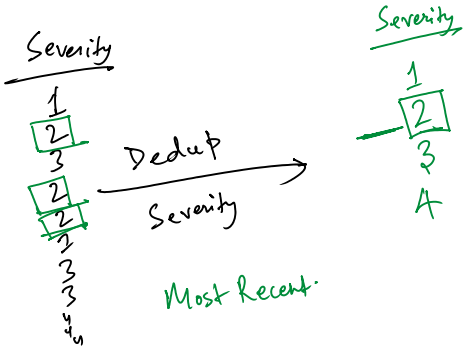
A	B	C	D
—	NA	—	—
—	NA	—	
	NA	—	

B









| sort Severity

Sort → Sorting Purpose. → By default.

Sort → Ascending

Ascending ← + / − → Descending order.

Top Command:-

Top Values.

| top Sourcetype.

↳ Default → Top 10 Values.

Unlimited Values → | top limit=0 Sourcetype

↓

Unlimited Values.

Eval:- Initialize Variable.

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

int a

Var

Str

a = b + c

a = 3 + 4

1. Calculation: → (bytes | log)

1. Calculation:-

KB → (bytes | kb)

eval Variable

2. If-else statements:-

```
if (a>=b)
{
Print (a);
}
else {
Print (b);
}
```

→ eval a = if(Condition, "True", "false")

eval x = if(a>b, "a", "b")

Severity → 1, 2, 3, 4

↓ High ↓ Normal

3. Case Statement:-

```
Switch(a):
Switch(b):
Severity = 1, 2, 3, 4
```

↑ High ↓ Low:

↓ Critical ↓ Medium

Case (Severity=1, "—", Cond2, "—", Cond3, "—", 1=1, "—")

Universal Condition

Severity

1 → True1

2 → True2

4

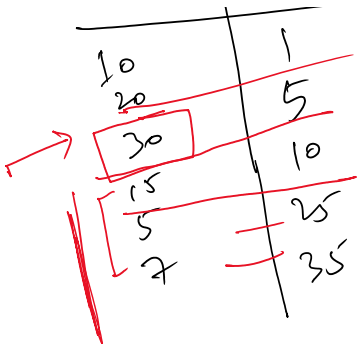
Search & where: filtering the output.

A	B
10	1
20	5

Search A>30

15, 5, 7

1.11. field.



15, 5, 7

where Compare two diff. field.

where. A ?B

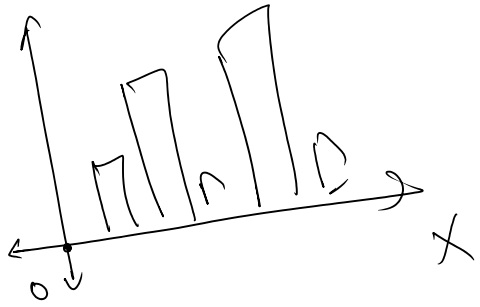
A	B
20	1
30	5
15	10

Rex:- It is used to extract the field from the Raw data

Regular expression.

makeresults:- Create the custom event.

Visualization:- Chart:-

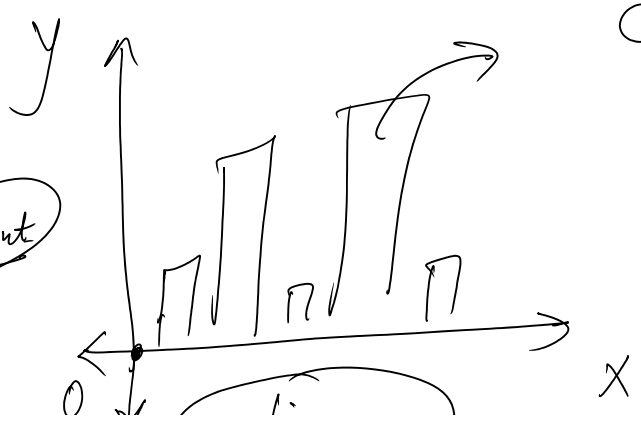


| chart count by current_ticket_state.

y-axis

x-axis.

Timechart:-

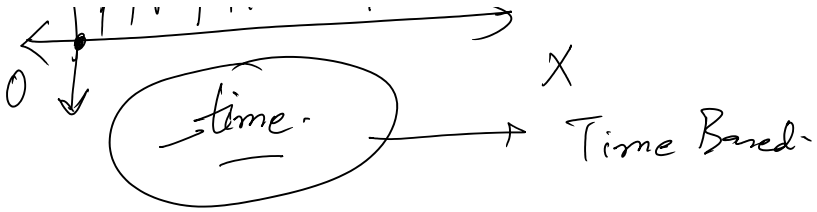


Stats functions

CTS/ser/ log_name

field

function



Single Value Visualization

1. checklist on the item you need to check b/f installing any new splunk application for splunk Appstore.

2. timesubmitted, closed date. timetaken to close a incident.
   ↓
   day/Minute wise.