Day - 1

03 March 2025 19:46

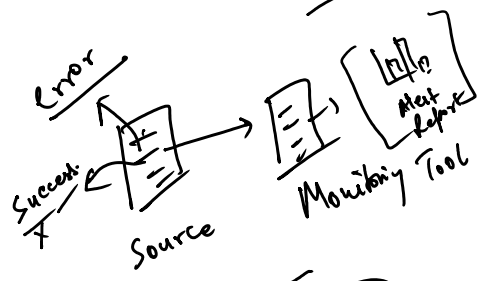
Splunk?

① Data Monitoring.

② Dashboard, Alert, Report, Knowledge object.

└ Logs (Security, operational, Infra.)

Power BI, Dynatrace, ELK, Splunk



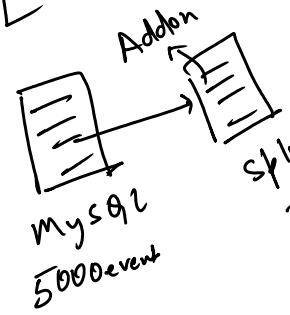
① store.

② Analysis ← Parsing. → Removal of Unwanted data.

Splunk: ←

① Any source → Network, security, Windows/Linux, IOT

② Any type of data. → XML, json, csv, Unstructured, Semi-structured.



→ Diag Report → Splunk support.

→ Diagnostic

Components of splunk:-

① Indexer.

② Forwarder.

③ Searchhead.

④ License Master.

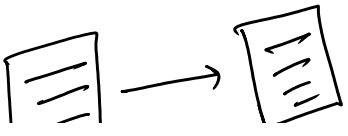
⑤ Deployment Server.

⑥ cluster Master.

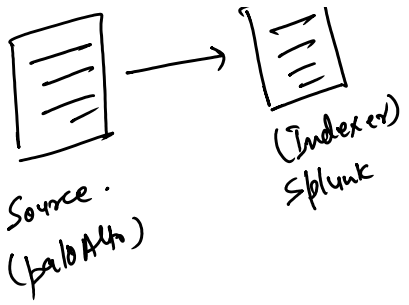
⑦ Deployer.

→ Management Servers

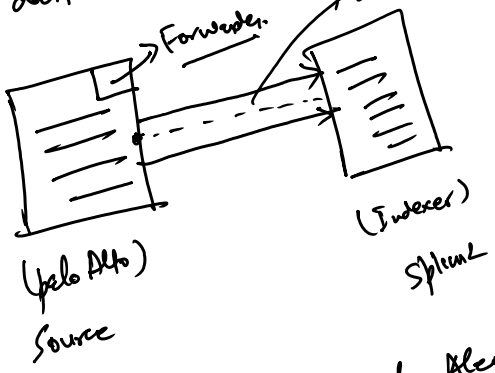
① Indexer:- Database that will store the incoming Data.



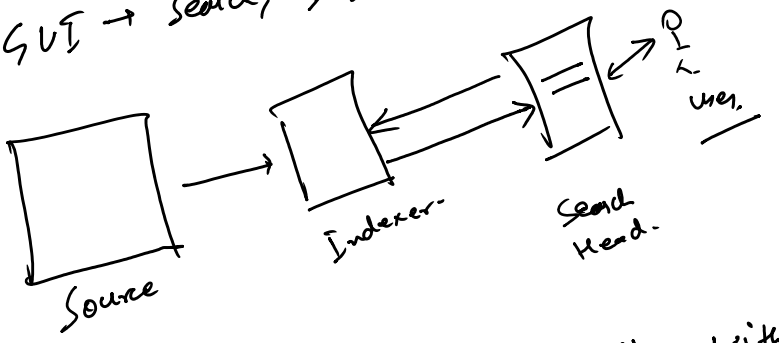
(1) Indexer:



(2.) Forwarder: Agent that you will install on the source level. It will forward your data to the splunk end (Destination)



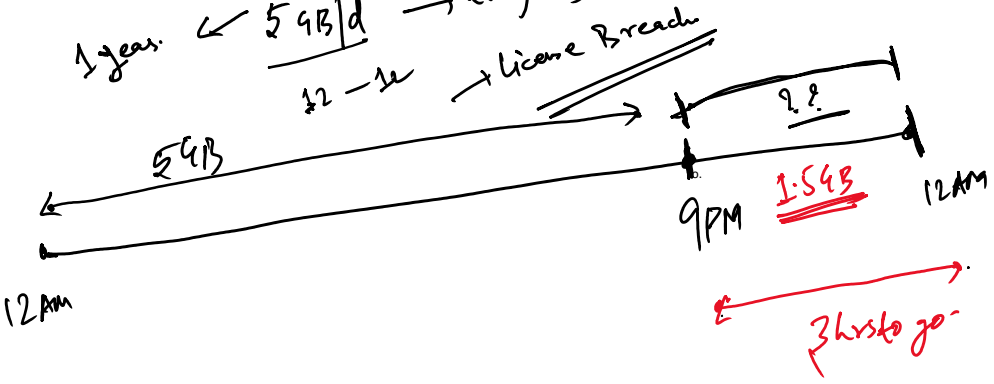
(3.) Search Head:- GUI → search, Dashboard, Alert etc.

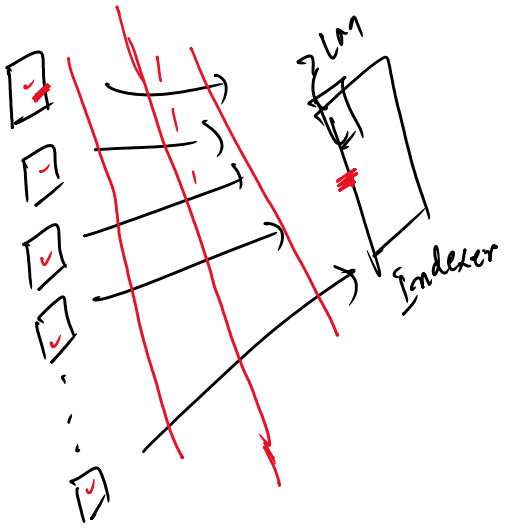


(4) License Master:- Agent that will make sure, you will adhere with license agreement.

How!!

Amount of Data ingested in splunk on a daily basis.

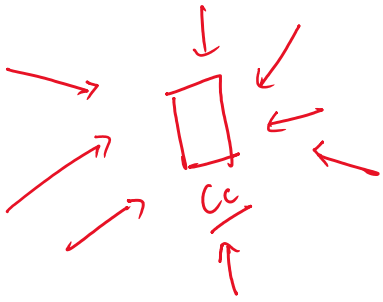


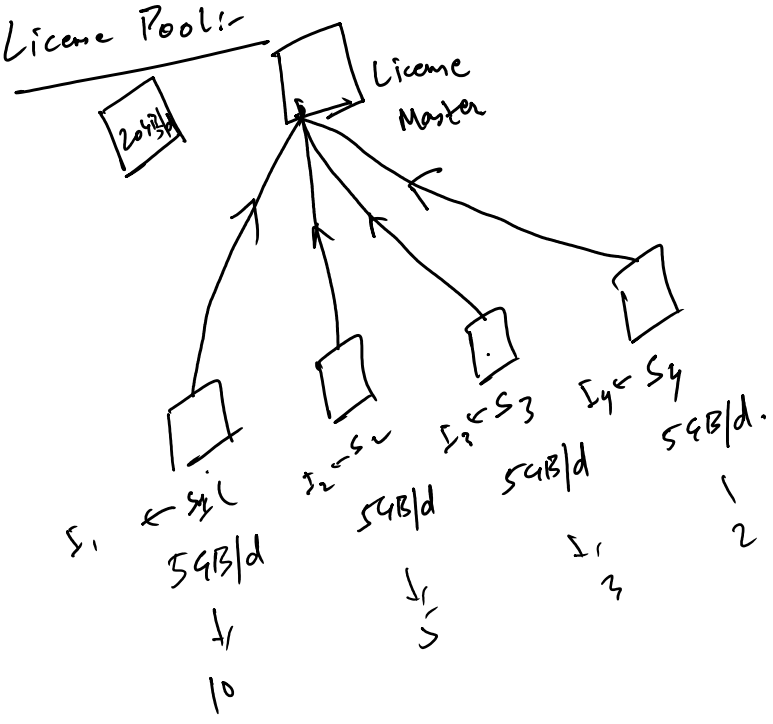


1. Indexing will continue.
2. Searching will be disabled
(Alert, Report, Dashboards)

↓
5 times - 30 days windows

↓ ↓
Blacklist Max license breach





$S_1 + S_2 + S_3 + S_4 \leq 20\,GB/d.$

1. Flexibility
2. Cost of licence cheap.
3. Managing the licence

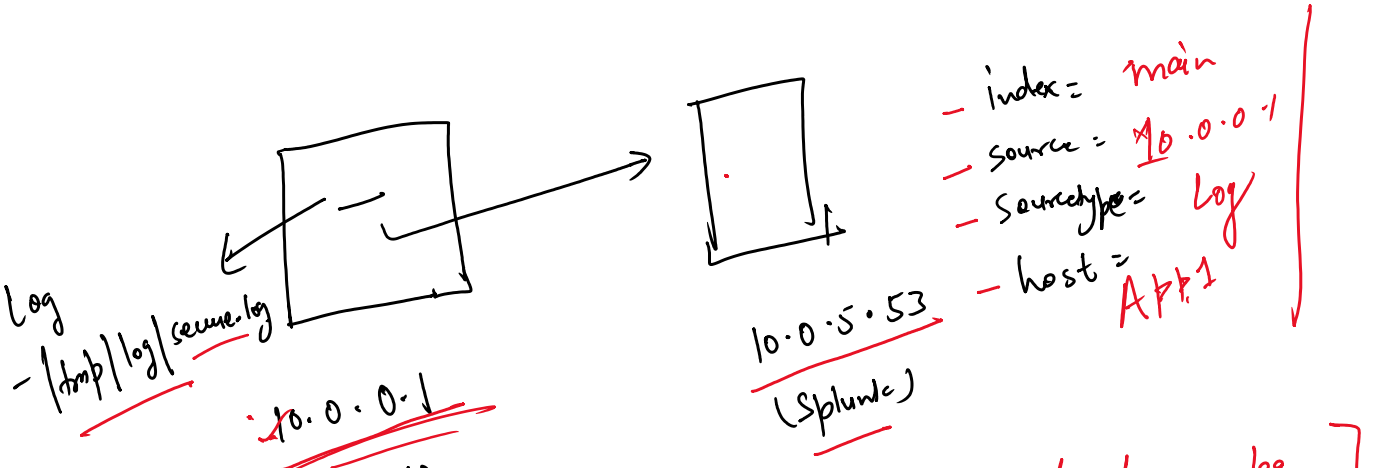
Splunk

1. Predefined Index → * (_internal, _audit, _introspection, ---)
→ Reserved to have splunk Application logs

① Predefined Index :-
↳ Reserved to have Splunk Application logs
↳ No License consuption.

② Default Index = main
↳ if you don't define the index name, By default it will go to main index.
↳ License will be consumed.

③ Custom Index :- Users their own index.
index = VK_idx, sample_idx, ---
↳ License will be Consumed.



Source = /tmp/log/secure.log.
host = 10.0.0.1
Sourcetype = format of that file.
↳ Secure_log.
index = main.

Searching Modes

1) Fast Mode :-

① Fast Mode :-

② Smart Mode

③ Verbose Mode.

index=_internal ↵

① fetch all the events.

② Extract the fields.

Fast:- ① fetch all the events, No extraction of Field happens.

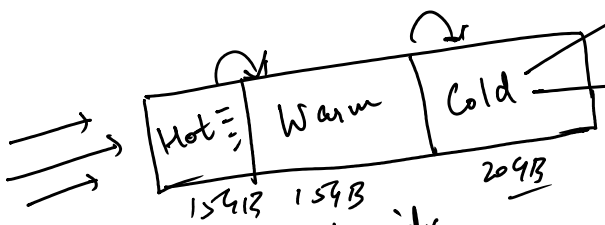
Smart:- ① fetch all the events + Extract all the fields.

Verbose:- Max Time

① Traverse b/w Multiple tabs.

Events — Statistics — Visualization

Bucket Concept:-



Hot = 10GB → Any condn is true, Data will move from one bucket to another Bucket.
Age = 7D
(Size of the Data)

Data Movement:-

① Age of the Data.

② Size of the Bucket.

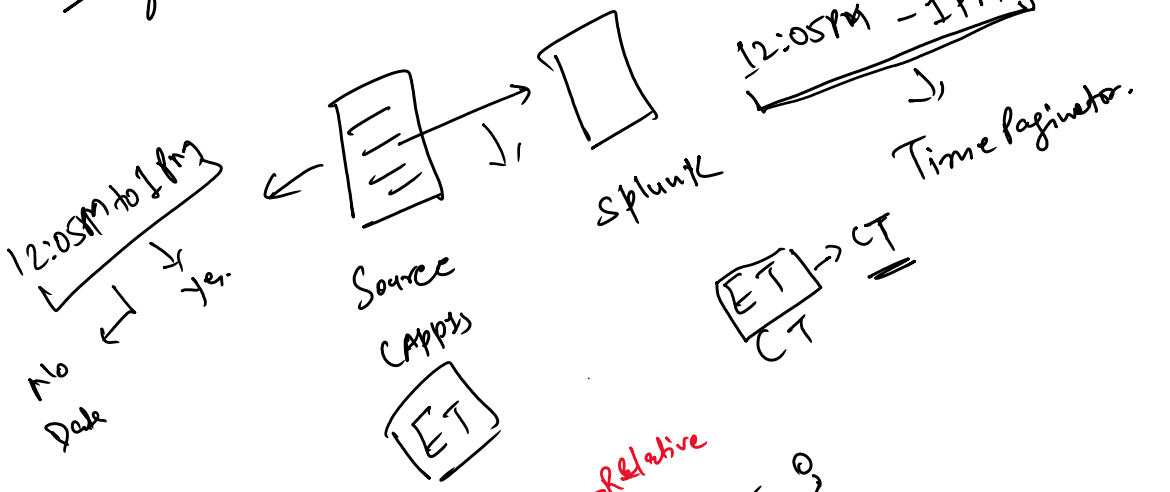
vvi

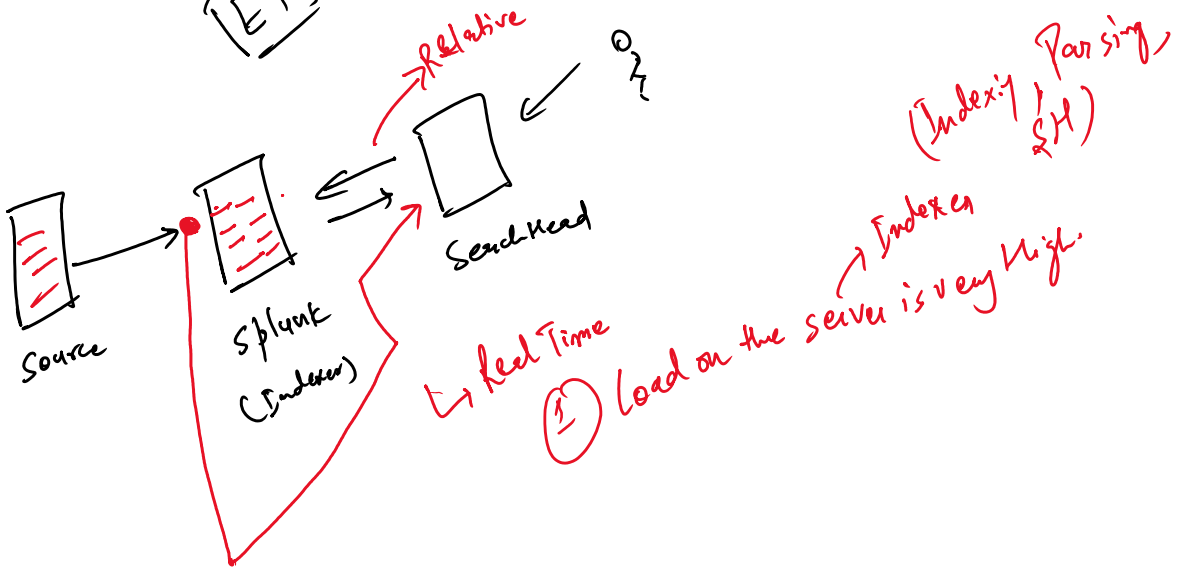
Field Name is Case Sensitive & field value is Case Insensitive

No data in splunk.

VVI

field Name is Case Sensitive & field Value is Case Insensitive





SPL :- Search Processing language.

1. Table – tabular output. Syntax: |table f1, f2, f3
2. Rename – change the name of the fields at the search level. Syn:- |rename old-field AS new-field.
3. Stats – statistical output.
   1. Count – Overall Count
   2. Avg. – Avg. Numeric value.
   3. List – Categories the events on the basis of duplicate Certain field.
   4. Value. – " " " " Unique.
   5. Sum – Summation of Numeric Value.
4. Eval – Evaluation purpose.

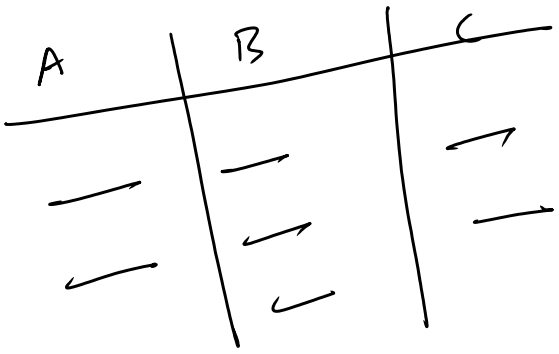
Var a
int b
str c

eval ___ = ___

Calculation →

Conditional Statement
- if else

- Cse.



| fillnull value="NA" A |

fillnull value = "Undefined" B

if-else:- (C++, java)

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

Splunk

if(Condition, True, False)

if(a>b, a, b)

Sort Command:- Sorting Purposes

Sort severity → Ascending.

Sort - severity → Descending,

+/- ↳ Descending

Sort + Severity or sort severity

↳ Ascending.

Ascendig

Case Statement

C++ | OOPs

C++ / OOPs

```
switch (0): Monday
switch (1): Tuesday
   :
   :
switch (6): Saturday
default : Sunday
```

→ case (Cond1, True, Cond2, True, Cond3, True, Cond4, True ...., 1=1, True)

Default / Universal Condition.

(5) Top / Rare → least values
→ top values. top command, by default it will give the top 10 values. Ext top sourcetype

(6) Addcoltotal → Addition column wise

(7) Addtotal → Addition Row Wise.

(8) Rex Command →

(9) Append → Combine the data from two different dataset.
↓ No Join

(10) Appendcols → Both the search Query will run at the same time.

(11) fields

(12) Search

(13) where

(14) Head

(15) tail.

Day - 2

04 March 2025 19:39

1. Field ✓
2. Search ✓
3. where ✓
4. Head
5. Tail
6. Rex ✓
7. Knowledge object - Tags & eventtype
   Field Alias
   Data Model & Pivot
   Alert
   Report

1. **Rex:-** Extract the field from the rawdata.

2. **field:-** Include / exclude any field from the output

ex:
- fields + — include for the o/p
- fields - — exclude the field for the o/p.

3. **Search & where :-** filter the result/event

search A >25 → filter out the result for the same field:

A	B
25	5

where A>B → Compare the value of two fields.

A	B
25	5
55	50

A	B
5	25
10	25
15	35
25	5
55	50
4	1

15 | 35
25 | 5
55 | 50
4 | 1

Head & Tail Commands

(1) Head :- First values from the start

|Head 10
↳ first 10 values.

(2) Tail :- Last values

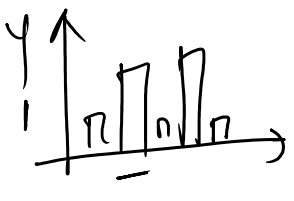
|tail 2
↳ Last 2 values

Pick from the Bottom

Visualization :-

(1) chart
(2) Time chart
(3) Single Value Visualization
(4) GeoMap.

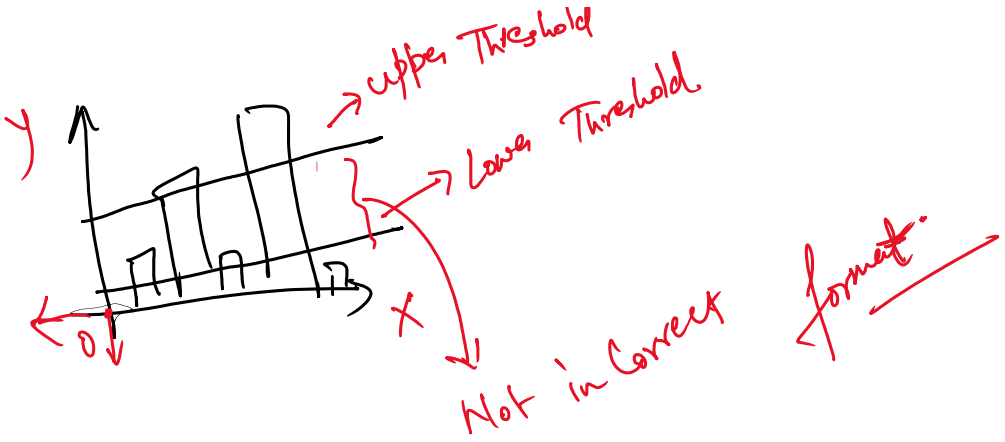
(1) chart :-



|chart count by cust_ticket_state

count → y-axis
cust_ticket_state → x-axis

upper Threshold



(2) Timechart:-

Timechart count by severity

span = interval

span = 1w ↳ weekly count

w = week M = minute

d = day S = sec.

h = hour y = yearly

(3) Single Value Visualization

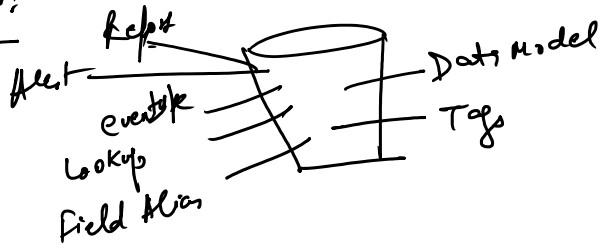
Single numeric Value as an output.

(4) GeoMap:- Define / Showcase the things in the Geographical Map.

Coordinates: Latitude, Longitude.

(5) Knowledge objects: Apps → Data Model

(5) Knowledge objects:



(1) Field Alias:-

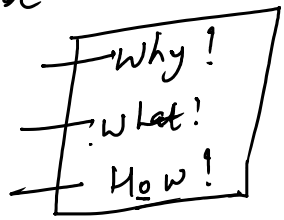
↳ New Name / Nick Name.

Nick Name / Alias Name we are giving to a field.

old field ← Severity → 1, 2, 3, 4

New field ← Priority → 1, 2, 3, 4

old field & new field both will be available.



Why!

HR
emp_id
FieldAlias
e_id

Account
e_id
No Need to create field Alias

Project
employee e_id.
Field Alias
e_id

e_id → Standard field

(2) Tags & Eventtypes:-

Tag → Categories the event on the basis of the field value.

Severity = 3 → Normal.

7 new fields generated:-

2 new fields generated:-

① Tag.

② tag::severity = Normal.

Eventtype:- Categorization of the event on the basis of certain criteria.

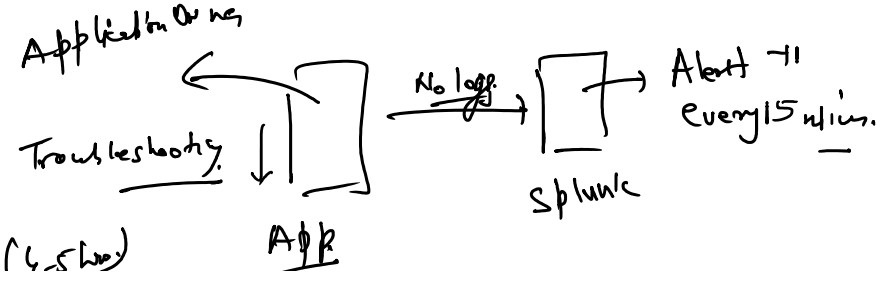
CTS = closed OR CTS = Resloved

↓

Completed → eventtype

③ Alert:- Condition, Trigger, Action.

- Definition → SPL query, Timerange, Schedule, Frequency
- Trigger Condition → Condition - a> - event.
- Trigger Action → Email Notification, Script, SMS, Triggered Alert, SNOW Ticket.

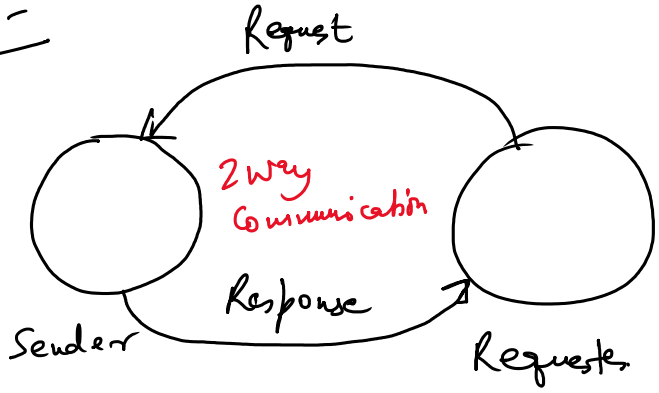


(4-5 hrs)

API

Splunk

API:-



Webhook:-

Report:-

- Definition
  - SPL
  - Schedule
  - Time range.
- Trigger Action
  - Email
  - sms
  - script

It is to run & send the configured Notification

Day - 3

05 March 2025 19:39

1. Dashboard

① classic Dashboard

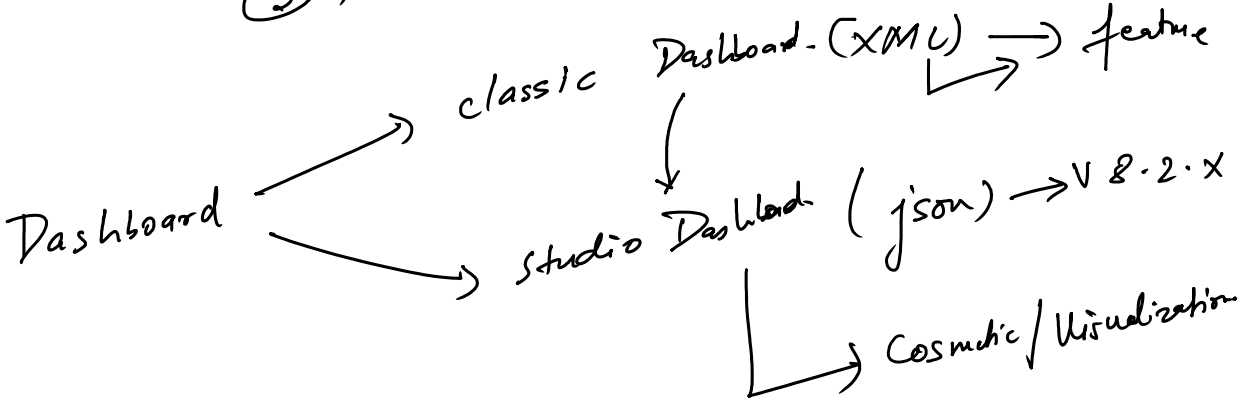
① Panel

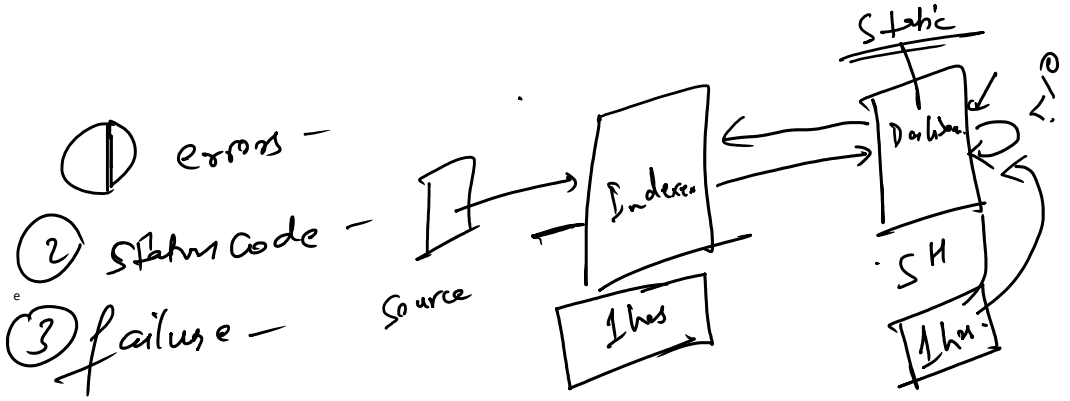
② Add the Panel.

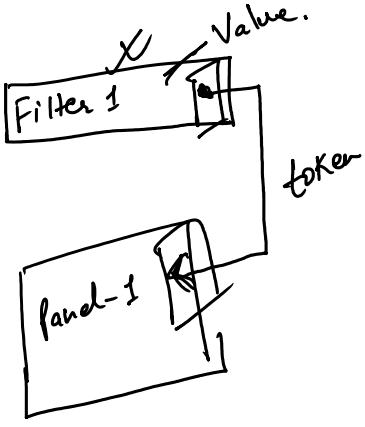
③ Input filters.

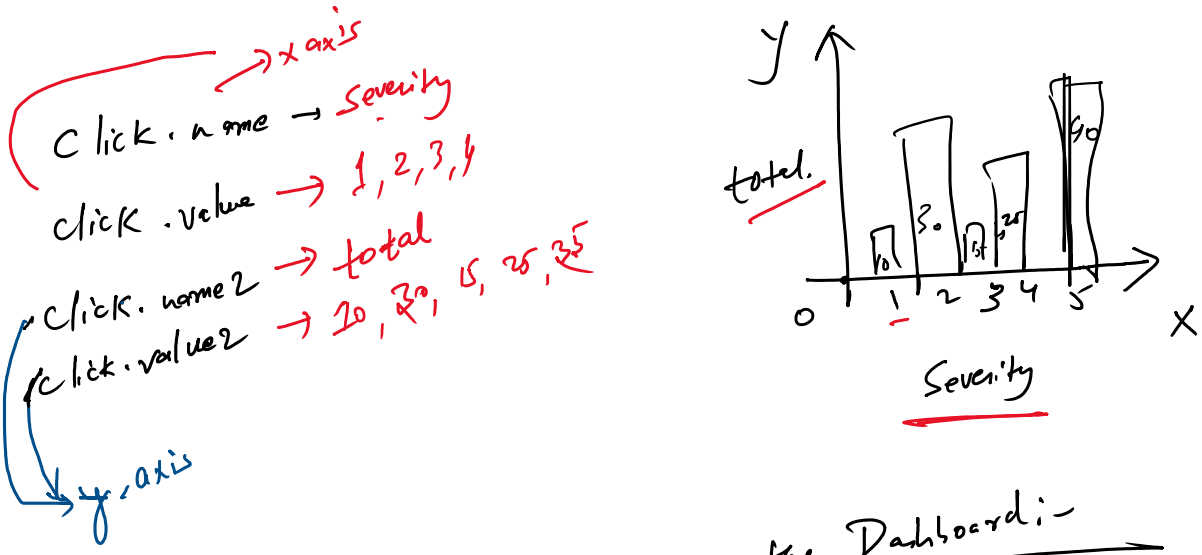
④ Drilldown Concept

⑤ XML Creation.



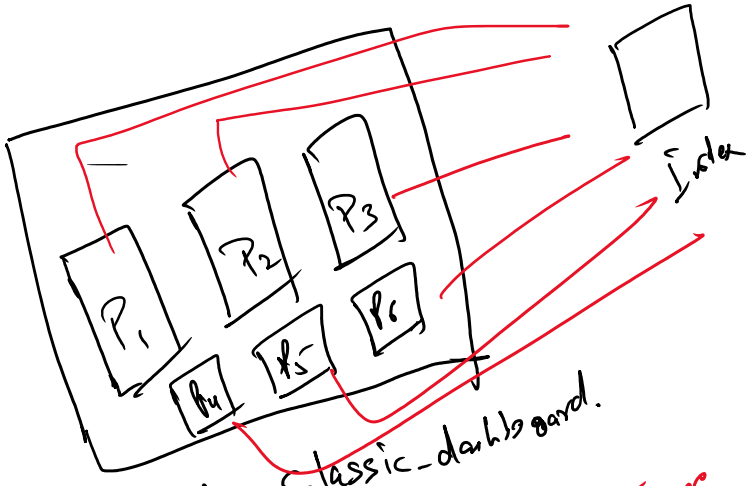


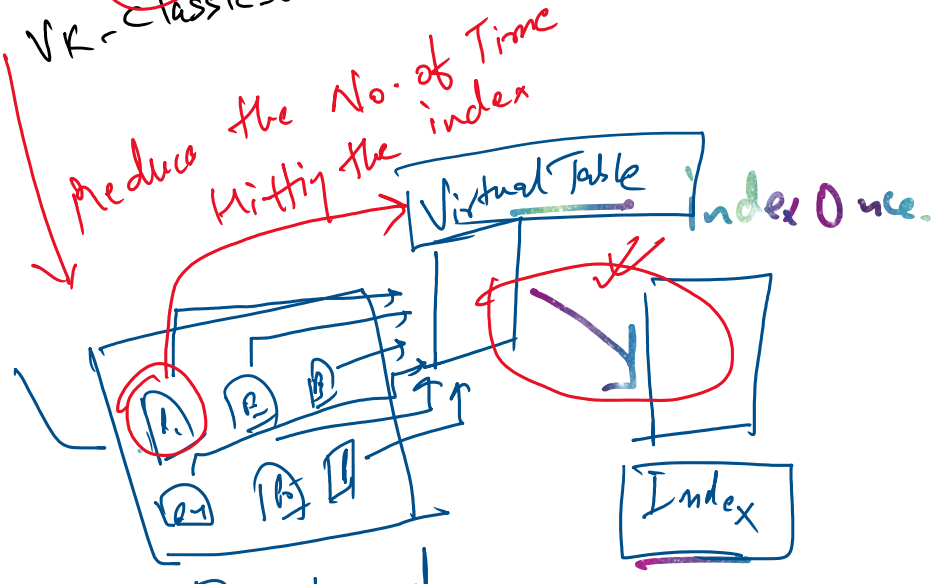




Optimize the Dashboard:-

1. Base Search →
2. Saved Search →
3. Summary Index →





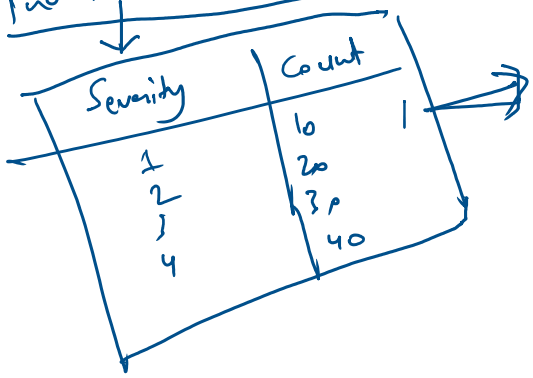
Panel → VT → Same index

Panel → Same index

Dashboard

Summary Index

1. index = vlc_idx | stats count by Severity



New Index