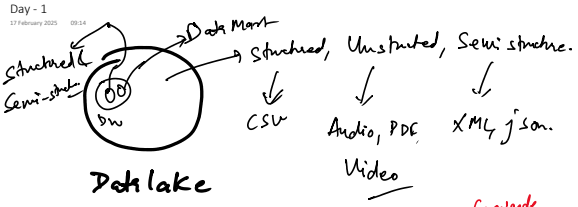
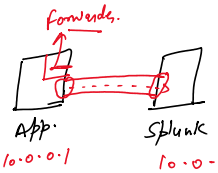
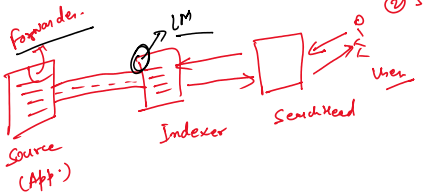


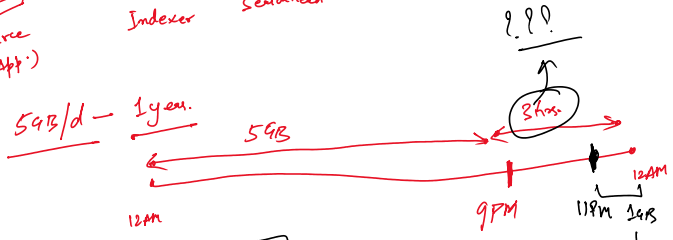
Component of splunk :-
Core :-

1. Forwarder :- Forward your data from source to the destination
2. Search Head :- Gui, where you create report, Alert & Dashboards
3. Indexer :- Database where the data is stored.
4. License master :-

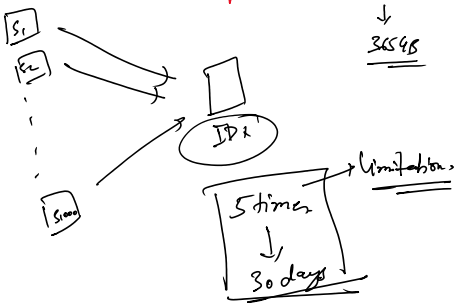


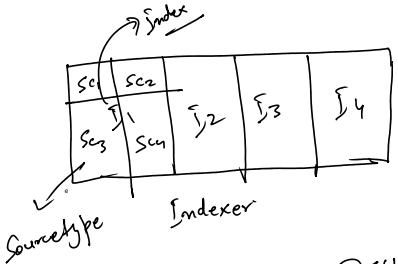
Forwarding data.
1. Serverfull
2. Serverless



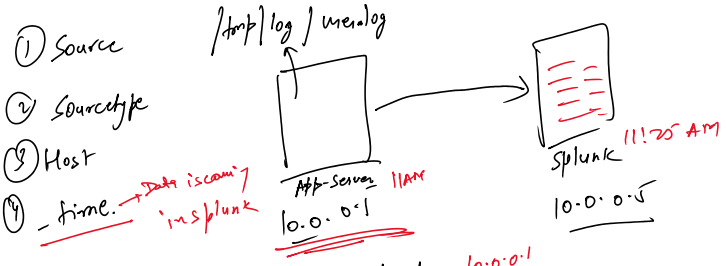


VVIT
* Indexing will continue but Searching will be disabled.





VVIT
Index
Predefined :-
1. Splunk App. logs
2. _*
3. No License Consumed.
Default —
1. index = main.
2. License Consumed.
Custom Index
1. VK-idx, sample-idx.
2. License Consumed.



host = 10.0.0.1
Source = /tmp/log/main.log
Sourcetype = main/log

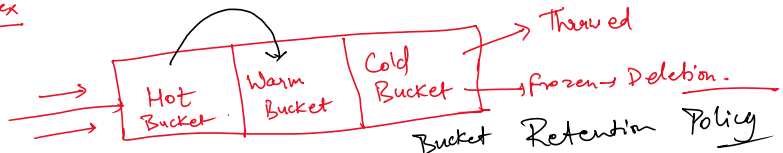
3 Searching Modes:

1. Fast Mode. → count — Pull the events. — fastest.
2. Smart Mode. — Pull + extract → Use Case
   — Max. Time taken → Deep Dive
3. Verbose Mode

index = _internal.

1. Pull the events
2. Extract the fields.

Index



Bucket Retention Policy

VK_idx

Any Condn is true ← Data will move

1. Size of the Bucket.
2. Age of the Data.

Table:- Tabular output.

|table f1, f2, f3 - - -

Rename:- Rename the field with new name → Search level.

|rename old-name AS new-name

Stats:- Statistically o/p.

1. Count → Count of the events.
2. Sum. → Summation of the numeric
3. Avg. → Average of the numeric Values.
4. list
5. Values

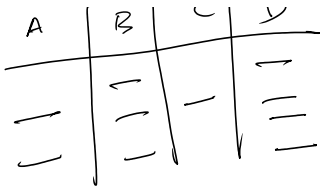
Fillnull:- That will handle blank space.

Default value of fillnull is 0

A	B	C	D
	—	_	—
			—

fillnull value="NULL"

A, C



A, C

List / Value → Function.
group your data.

Eval :- Evaluation purpose.

Bytes / 1024 → KB

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

I

```
index=_internal          → 1000 events
| eval kb = round(bytes/1024,3)." KB"   — 1000 events
| table bytes , kb       → 1000 rows
```

II

```
index=_internal          — 1000 events.
| table bytes            — 1000 rows — 1 column.
| eval kb = round(bytes/1024,3)." KB"  — 2 Columns
```

→ More optimised.

```
index=vk_idx             — 99 events.
| dedup severity         — 4 events
| table severity         — 4 value
```

```
index=vk_idx             — 99 events
| table severity         — 99 rows
| dedup severity         — 4 rows.
```

if-else statement :-

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

if (Condition, true, false)

if (a>b , a, b)

Sort → sort - / + → Ascending

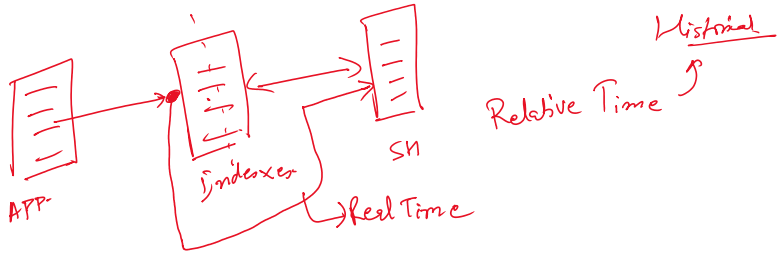
↓

severity 1, 2, 3, 4

Sort → sort -/+ → Ascending
↓
Descending

Sort + severity 1, 2, 3, 4
Sort severity 1, 2, 3, 4

Sort - severity 4, 3, 2, 1
↓
Explicitly Define over here.



Case statements

Case (Cond1, Value1, Cond2, Value2, Cond3, Value3 - - - -
1=1 " - ")
↳ Universal Condn

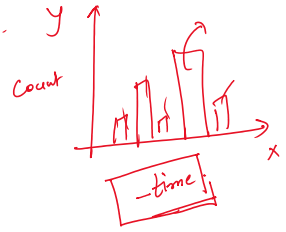
1 → Critical
2 → High
3 → Normal
4 → Low

Rex → \s
\d
\w

Visualization:-

y-axis ↗ x-axis.
① chart - /chart Count by Severity.
② Timechart -
③ Single Value Visualization.
④ Geomap.
⑤ Custom Visualization

Timechart:-



Assignment - 1:- Time taken to resolve each ticket. Diff. should be in the day wise format.

time_submitted, closed_date → ① Strptime → epoc

② Diff. → time_sub_epoc - closed_date

③ strftime → Reformat in day format.

* Single Value Visualization:

Single Numeric Value.

* GeoMap:- Geographical Map → Latitude & Longitude.

* Custom Visualization:

① Version Compability

② Product Compability

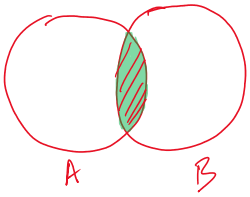
③ Dependent Compability

④ Support

Assignment - 2:- ① List of Check you need to make before & After the splunk upgrade.

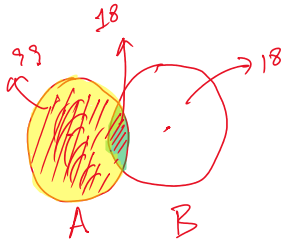
1. join Command:-

i)



Inner join

ii)



Outer join

Sample_lookup.csv.

Append / Appendcols / Appendpipe:-

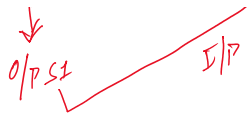
Append:- S1 | append [search S2]

Appendcols:- S1 | appendcols [search S2]

Appendpipe:- S1 | appendpipe [subsearch S2] → O/P final

S1 → O/P S1

I/P



* Top / Rare :- Top Values.

Syntax : | top Sourcetype

* By default give the top 10 values.

limit → No. of values

| top limit = 3 Sourcetype.

Rare :- Min-Max Value. limit = 0

Filter Command :- Search & where.

A	B
10	15
5	8
15	3
25	30
35	25

Search A > 5

A	B
10	8
15	3
25	30
35	25

where
↓
compare two diff. fields.

A	B
10	15
5	8
15	3
25	30
35	25

where A > B	A	B
o/p →	15	3
	35	25

Knowledge objects :-

1. Field Alias :-

Alias → Alternate name / new Name

(HR) Source1

(Project) Source2

(Account) Source3

employee-id

Props.conf

(HR)
Source1

E_id → FA → emp_id

Source2

emp_id

employee_id → FA → emp_id

(1.) Create new field & will NOT DELETE OR Replace OLD or Original field.

(2.) Tag :- Categorise → field Value wise.

sev → 1 → Critical.

sev → 3 → Normal.

2 Additional field :- severity >3 → Normal (Tag)

(1) tag = Normal.
FN FV

(2) tag :: severity = Normal.
FN FV

Tags.conf

(3.) Eventtype :-

Completed.

InComplete.

Completed - Resolved, closed - 1, 2, 3, 4

eventtype.conf

Completed - Reso...

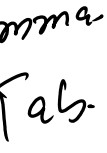
Critical - Severity = 1 → eventtype.conf

4. Field Extraction

- Regular Expression
- Delimiter Type (Symbol)
  - Expression
  - Default Symbol
    - ① space
    - ② Pipe.
    - ③ Co...
    - ④ ...

5. LookUp :-

① csv
② Kustre
③ Geospatial.
④ External.
⑤ Database.



1. CSV:-

(1) Small & static file.

(2) upload the file → No Cl

Status_code	Value
400	
200	
500	
505	

(1) upload & fetch detail from lookup file.

(2) Combine data from index & lookup file -

(3) Lookup Definition.

(4) Automatic lookup

(5) Outputlookup Command.

(6) Lookup Editor App. → splunk L

Automatic Lookup:-

erse.

→

ookup

↓

sample_lookup.csv.

C

outputlookup → Update the lookup file.

Data Model:-

index = VK_idx.

1. Pull all the events.
2. Extraction of the fields.

Mechanism:-

1. Define the fields required in the starting
2. Data model → Tsidx file → Index (Buckets)
   ↓
   Timestamp index.
3. Inheritance structure is follows:

Pros:- (1) Search speed is very high.

Cons:- (1) Increase in Computational Resource consump

(1) Visualization purpose. → Pivot and

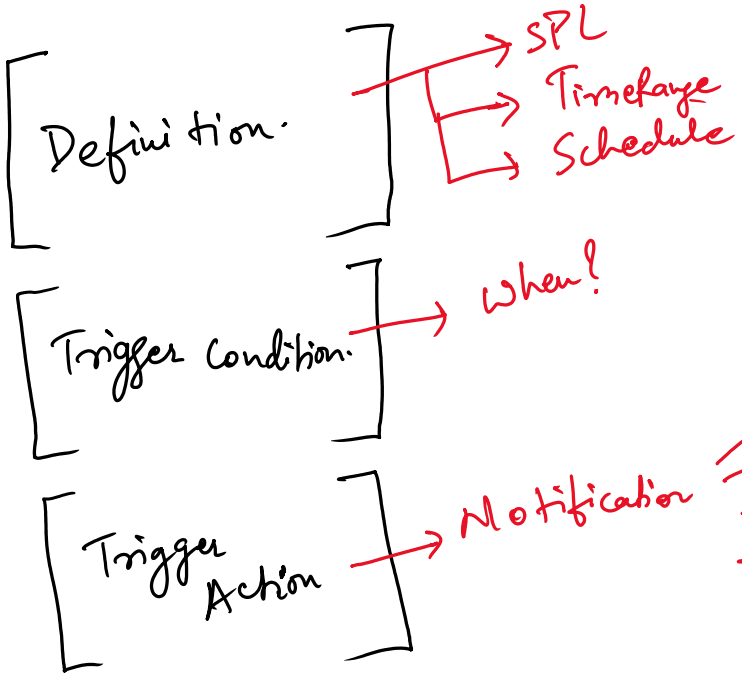
) itself.

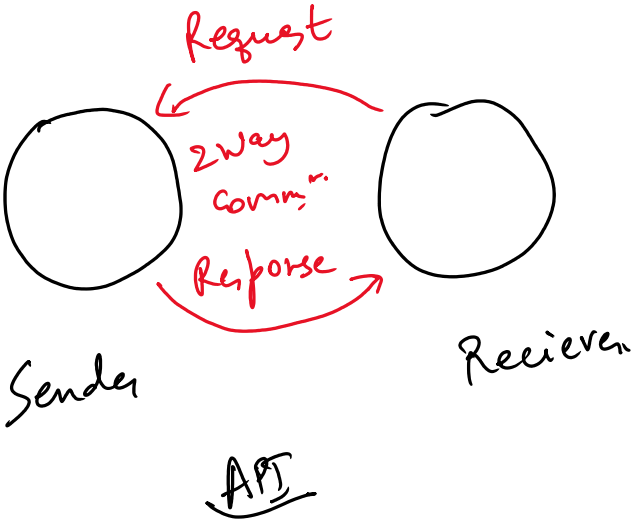
ation.

Pivot:- ① Visualization purpose. → Viz
② chart & timechart → Data Model

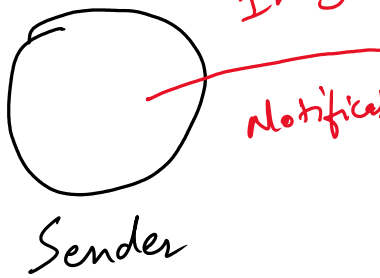
↓
index

Alert:-





API

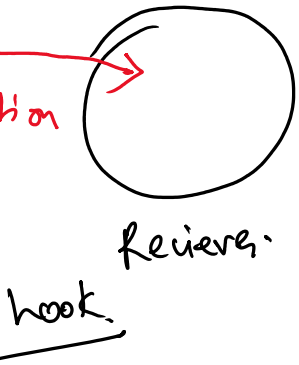


Web

Report:-

SPL
Timerange

Alert



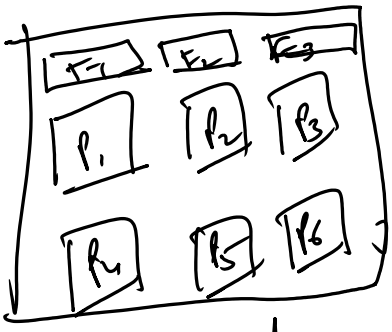
hook.

Report:

[Definition: → SRC, Timerange, Schedule]

[Trigger Action] → Notified
1. email
2. Notifica
3. Mobil

Dashboard:-



1. Combination of Panels

Classic Dashboard → XML → Features.

Studio Dashboard Dashboard → json → V8.4 + → Cosmetic

Input filter:-

tion

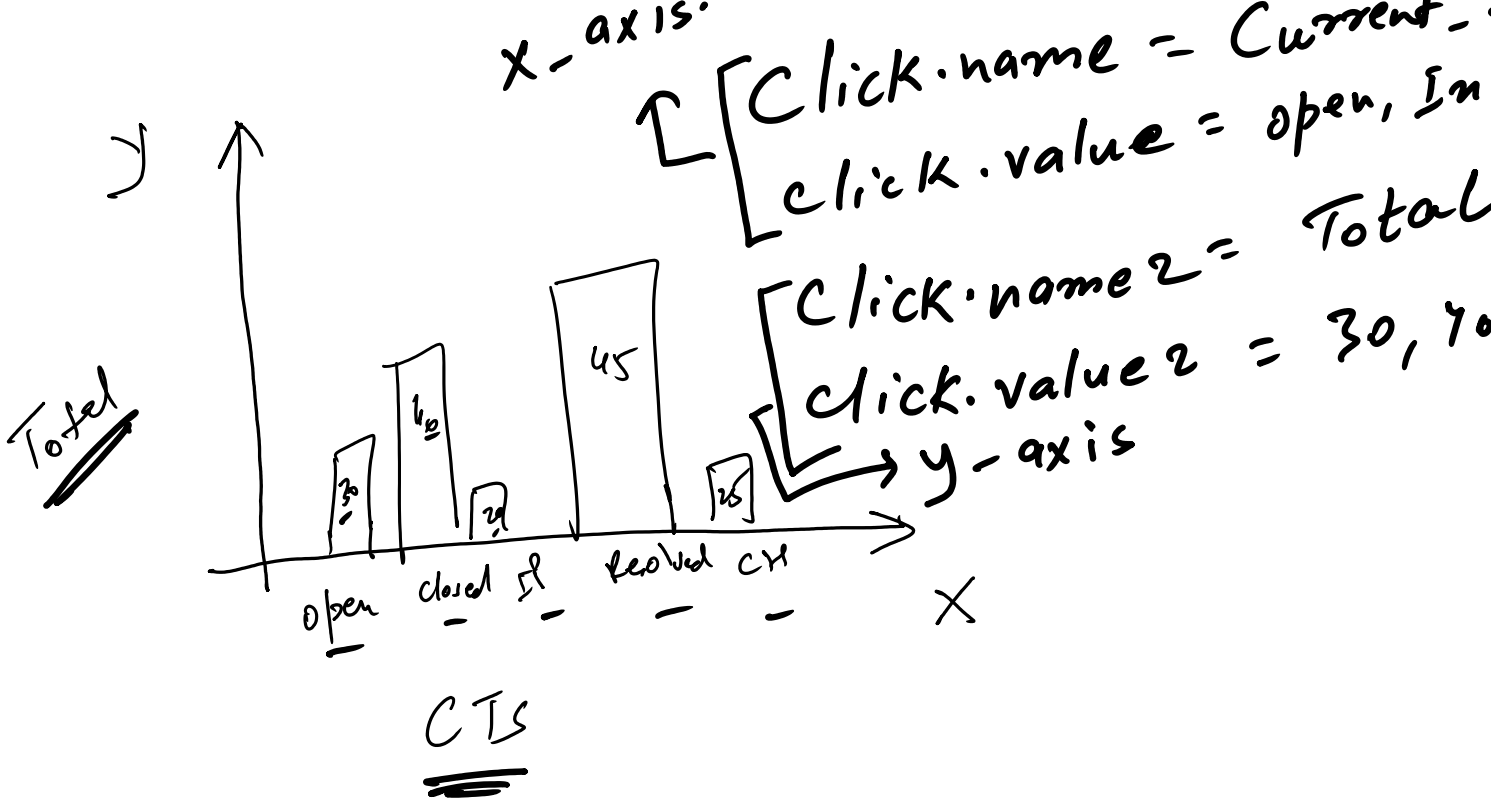
e.

4 filter.

on.

Input filter:-

1. Multiselect:-
2. Radio
3. checkbox.
4. Submit
5. Drilldo
6. XML



1. Macros.
2. Workflow Action.
3. Post Quiz.

wn.

ticket_ state
_Progress, closed.. -

..

, 20, 3- - -

. 1

(2.) Post

(1.) Macros:-

```
function a(b,c)
{
d = b+c ;
return d;
}
```

a(5,
a(-9

Workflow Actions

(1.) Alert:-

TimeRange Schedule Interva

=

No Correlation.

1

4)

, 3)

l

S = every hours.

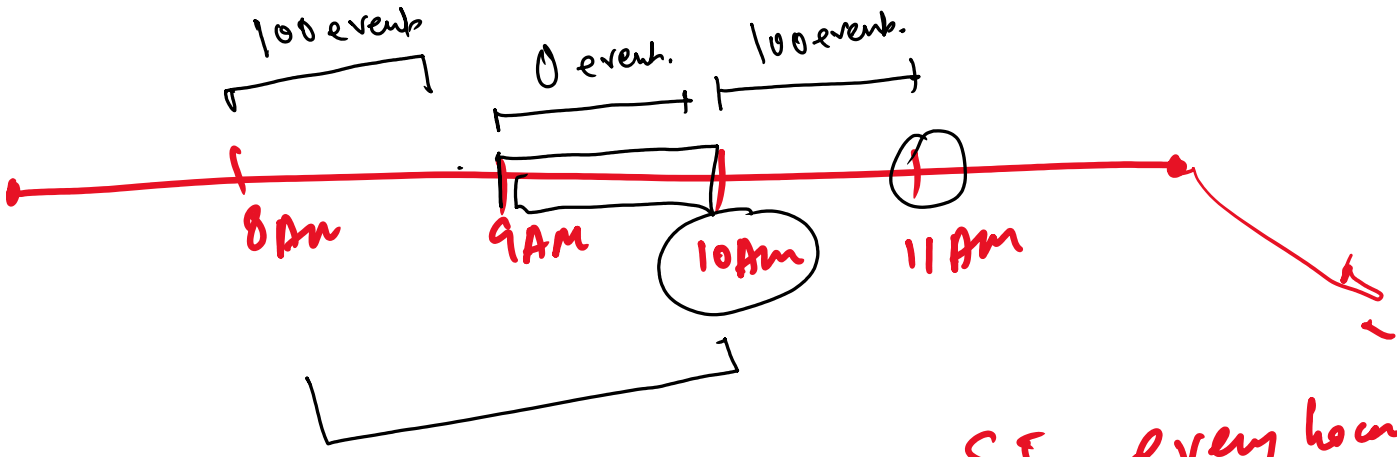
TR = ① Last 1hr.

② All time

③ Last 24hr

9AM 10AM 11AM

License -> 70%.



SI = every hour

TR = 2hr.

TR =

(3) East 24th