Day - 1

10 February 2025 09:51

Structure → CSV

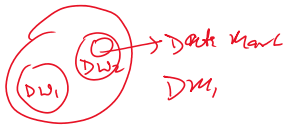
Unstructured →

Semi Structure → XML

→ Data lake.

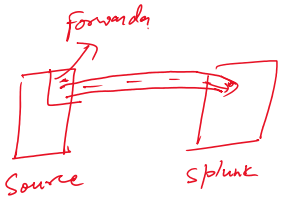
I am going to home. My Home is in India.

Home – 2



Component in splunk

(1) Forwarder



Metrics

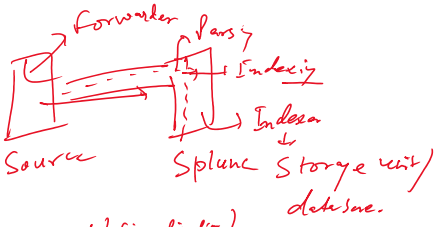
70% → Memory

↓

timestamp → log

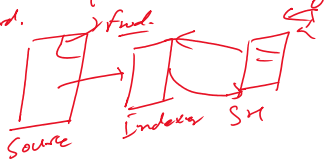
traces

(2) Indexer



(3) Search Head

GUI → search/visualization Dashboard.



(4) License Master

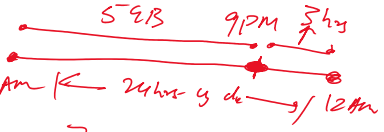
Agent that will maintain

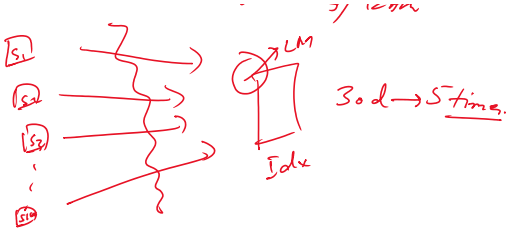
5GB/d → 1 year → License

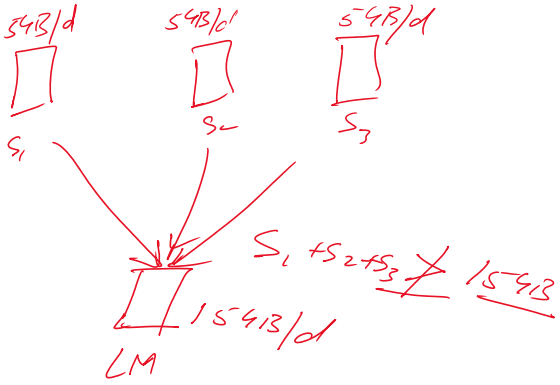
↳ 24hr cycle.

↓

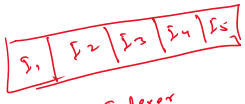
Amount of data ingested in splunk on daily Basis. → License Parameter







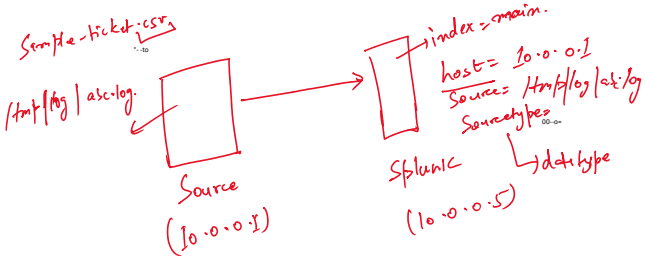
Indexer

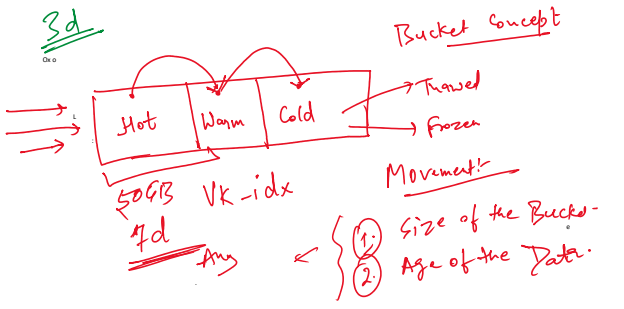


Indexer

Index
- Predefined Index → _audit, _internal, _* → Reserved for splunk related logs → No license usage.
- Default Index → Customer 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 "_"



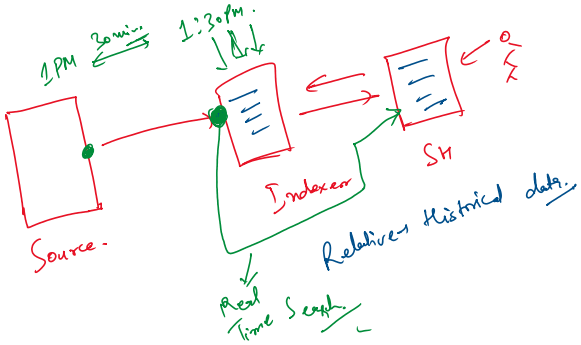


Searching Mode → Fast Mode
→ Smart Mode
→ Mode.

Searching Mode → Fast Mode
→ Smart Mode
→ Verbose Mode.

1. Pull the events
2. Extract the fields from event → Activities.

Fast Mode → Pulling the event.
Verbose Mode → Max. Time.



SPL Queries

1. Table.
2. Rename.
3. Stats
4. fillnull.
5. Eval.
6. Search
7. Where.
8. dedup.
9. Top/Rare.
10. makeresults.
11. Sort.

1. Table:- Tabular output.
Syntax:- |table field1, field2, field3

~~VVI~~ * 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.

Pull all entries ← A. List → Values → } + grouping of values

Pull the unique item.

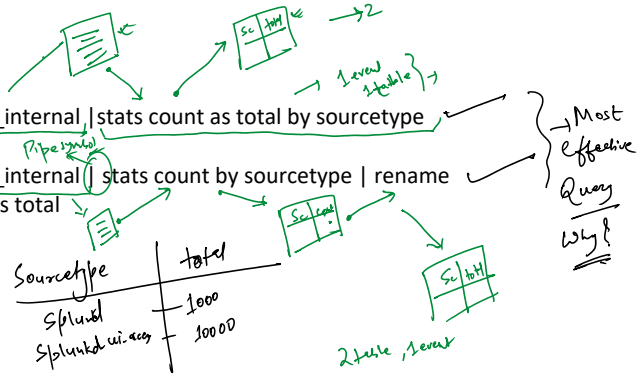
fillnull → Handle your blank spaces.

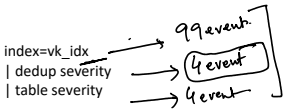
By default, fillnull value is 0

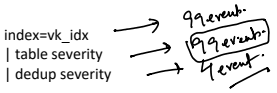
A	B	C	D
—	NA	—	—
—	NA	—	
—	NA	—	

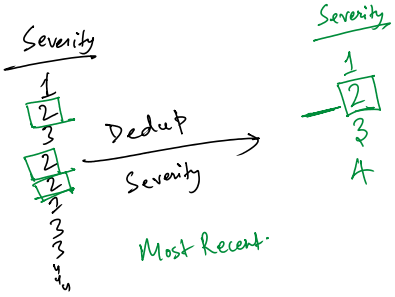
fillnull value="NIA"

B









| Sort Severity

Sort → Sorting Purpose. → By default.

Sort → Ascending

Ascending ← + / − → Descending order.

Top Commands:

Top Values.

| top Sourcetype.

↳ Default → Top 10 Values.

... 'Load Value → | top limit=0 Sourcetype

Default =

Unlimited Value → 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:-

Kb → (byte/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 → Low:

↓ ↓

Critical Medium

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

Universal Condition

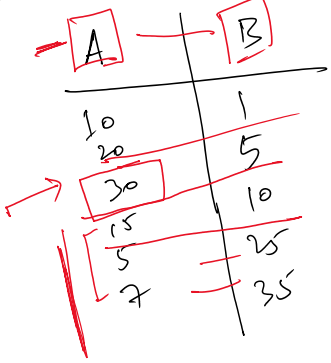
Severity

1 → True1

2 → True2

4

Search where: filtering the output.



Search A > 30

↓

15, 5, 7

where: Compare two diff. field.

where. A > B

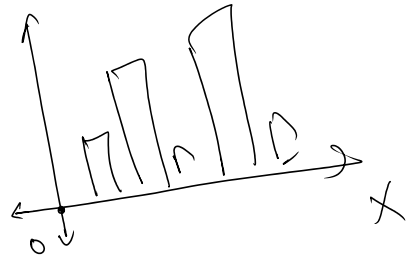
A	B
20	1
30	5
15	10

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

Regular expression.

makeresults:- Create the custom event.

Visualization:- Chart:-

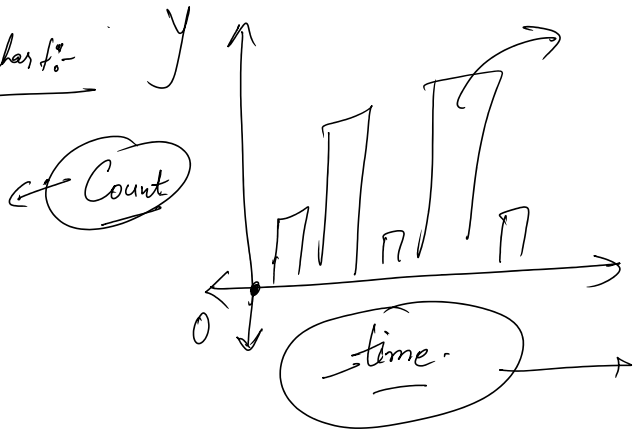


y-axis

| chart count by current_ticket_state.

↳ x-axis.

Timechart:-



Stats functions

Time Based.

CTS / ser / log_name

↓

field

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.

Strptime ⟶ epoc format → System readable form

Strftime → User readable format.

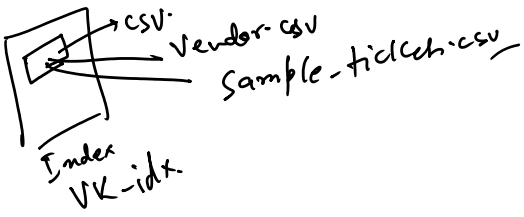
Day - 3

12 February 2025 09:07

Geo Map:-

Pin point places on the Map.

1. Latitude.
2. Longitude Value.



Custom Visualization:-

Splunk Appstore. → Developer.
→ Splunk LLC

1. Licensed / Free Version.
2. Version Compability; Product Compatability
   - Splunk Cloud (SAAS)
   - Splunk Enterprise.
3. ~~O.S.~~
4. Valid email id.
5. Dependencies
   - DB Connect → JRE
   - → Drivers

Knowledge object:-

1. Tags & Eventtype → 6. Alert
2. Field Alias → 7. Report.
3. Field extraction.
4. Lookup.
5. Data Model & Pivot

1. Tag:-

Categorize the ~~Data~~ field value.

Severity = 3 → Normal.

Config file I
tags.conf

Tag will create 2 new field.

1. tag.
2. tag::Severity

↗ or group
event/logs.

② tag :: Severity

② Eventtype:- Categorie the set of events/logs. → or group

1 error
2 exception
3 Critical
4 ~~Specific~~

→ Failure

CTS = "closed" OR CTS = "Resolved" → Completed.

Ticket-no. → 01

CTS = closed → Completed

Sev = 1 → Critical.

(Green) eventtype (Pri-4) ← highest

Ticket → 1 Sev=1 → Critical

Ticket → 1 sev = 1 CTS = closed (Red)

↳ Completed → eventtype (Pri-2) Normal

eventtype = Completed. (Red)

eventtype = " (Green)

Conf → eventtype.conf

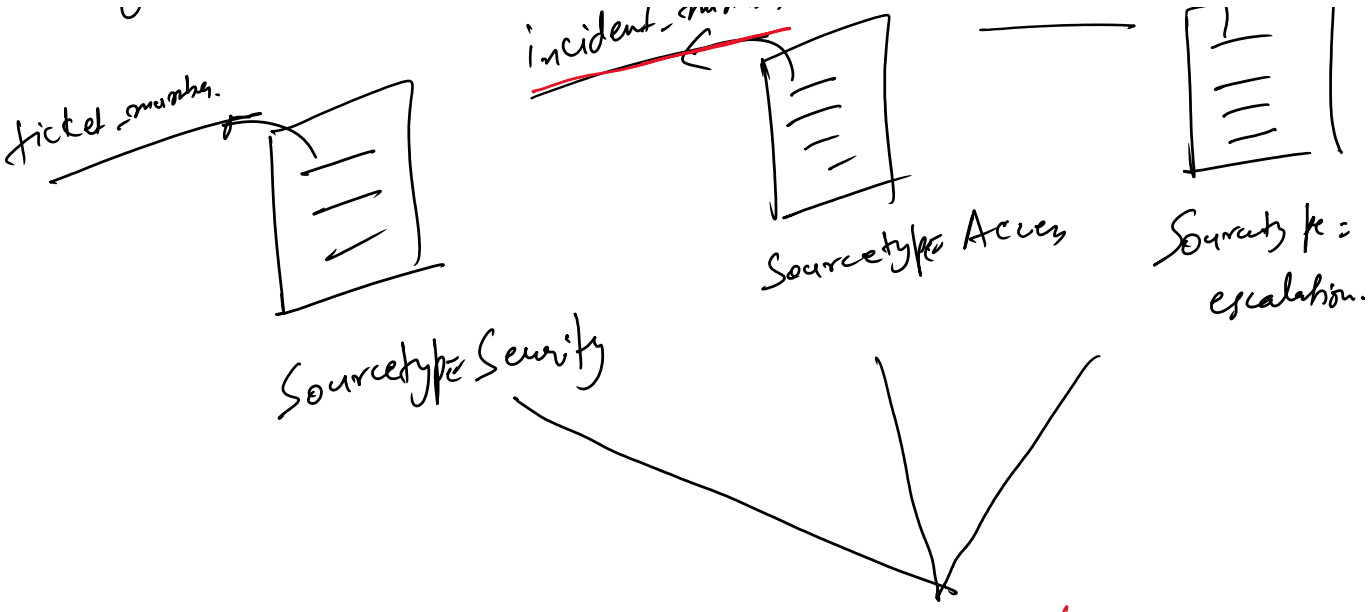
② Field Alias:-

↳ Alternate / Nick / Pseudo name.

ticket_number → ticket_number ← incident_number

ticketNumber.

number.



ticket_number.

1. New field created from field Alias. It is not going to delete the older field.

Old field, New field → Available.

Field Extraction:- Extract data → field name.

↓

Transforms.conf

↓

Config file where it will be saved.

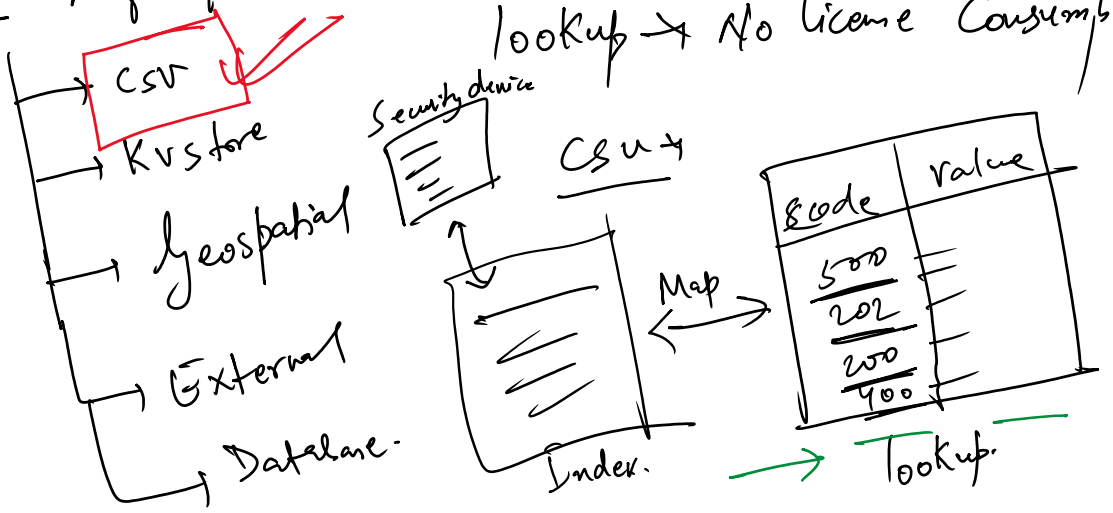
→ Regular expression —

→ Delimiter type — Splitting the events on the basis of certain symbols.

Default symbols —

1. Space
2. Comma
3. Pipe.
4. Tab.

Lookup :- A file | external



lookup → No license Consumption

Case (sc = 400, "—", sc = 300, "—")

1. Data / lookup file is small.
2. Static in Nature.

Lookup ① Upload the lookup file.

② Lookup Definition.

③ Automatic Lookup.

— Lookup Editor App.

— Combine the data available in the index & the lookup file.

LookupDefinition:- Extract the field in Advance.

LookupDefinition:- Extract ...

/inputlookup UK-sample_lookup.csv.

1. Pulling all the events.
2. Extract the fields- ex: ticket_number, time_taken.

Automatic lookup:-

lookup → Compare the data s/w index & lookup & combine it out.

inputlookup → fetch the data in the lookup table.

outputlookup → update the data in the lookup file.

Lookup Editor:-

App → Splunk Appstore.

↓

Splunk CCC

Day - 4

13 February 2025 09:21

Data Model & Pivot:-

1) Data Model:-

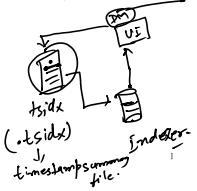
index = main source = abc.log

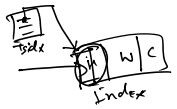
1. Pull the events/log.
2. Extract all the fields

Mechanism:-

Data Model:- 1) Tsidx file in the index + (.tsidx)

Timestamp index file Summary.





VK idx

2. Define the field required in the advance only.

3. Inheritance. Root event
   - ↳ child event +c'
     - ↳ S child +c''
       - ↳ SSCHC'''

Pros:-

1) Searching speed will increase.

Cons:-

1) Compute Resource Consumption will increase.
   ex- CPU, Memory ↑ etc.

1. Data Model Creation - Root event
2. Data Model Creation - Child event.
3. SPL Query for Searching DM.
4. Create Pivot out of DM.
5. Accelerated Data Model.
6. Basic Config./option we have with DM.

DM is created on the top of the json.

DM → Pivot → Visualization.

Index → Visualization (chart, time chart etc.)

1. Need to have DM to create a Pivot.
2. Click to Go option, no need much to write a code to create a pivot.

DM → increase searching speed

Accelerate DM → More increase Searching speed.

↳ Summary Data → Refer.

Cons:-

1) Further increase the compute resource consumption, CPU, Disk, Memory ↑

Acceleration:

→ Summary Data → [illegible]

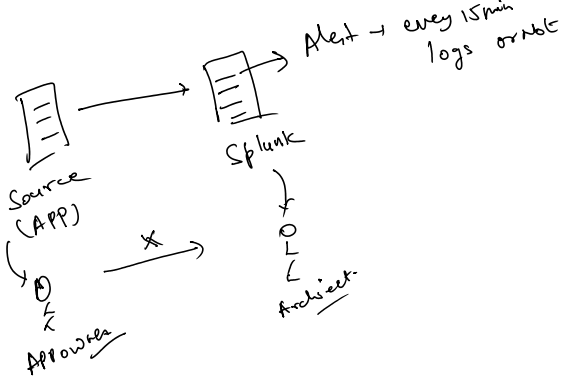
(1) [illegible]
resource consumption.
Ex: CPU, Disk, Memory ↑

Enabling the Accelerate DM → No further editing the DM.

Alert:- Notify the user on the certain incident.

Alert
- [Definition] → SPL, Time Range, Schedule.
- [Trigger condition] → Scenario ???
- [Trigger Action] → How to notify!!!

1. Alert.
2. Avoid creating false Alert.
3. Settings.



API

Request

2 Way Comm

Response

Sender

Reciever

Webhook

Response

1-way Comm

Sender

Reciever

Notification Service.

Work flow Action:-

→ Drilldown Activity / Deep Dive on the

Get

Post

→ Drilldown Activity / Deep Dive on the raw data.

Alert vs Report

Reporting:-

Report

[Definition] → SPL
→ Schedule
→ Interval.

[Action] → ~~Email~~
→ message
→ Script

Alert:- Time Range

Cron Expression / Schedule.

24hrs → ~~Cron~~ Schedule

TR = S - I

TR ≤ S - I

TR ≥ S - I

(1.) License Consumption - Alert-

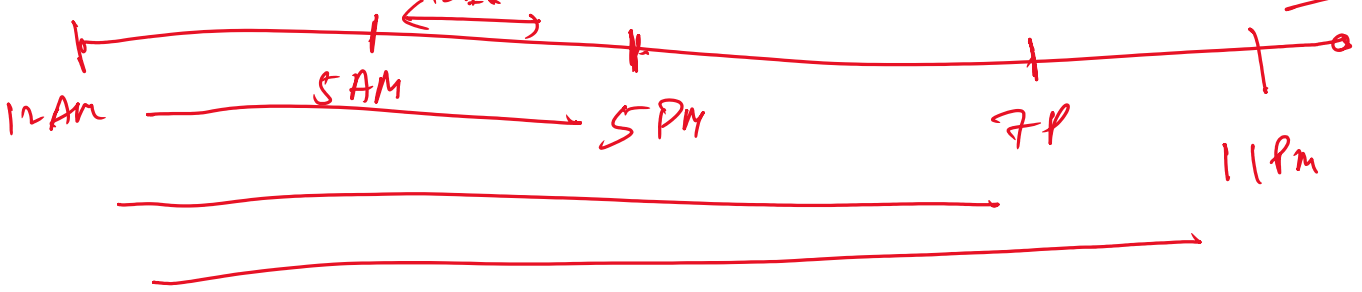
① License Consumption - Alert

60% → 30 min

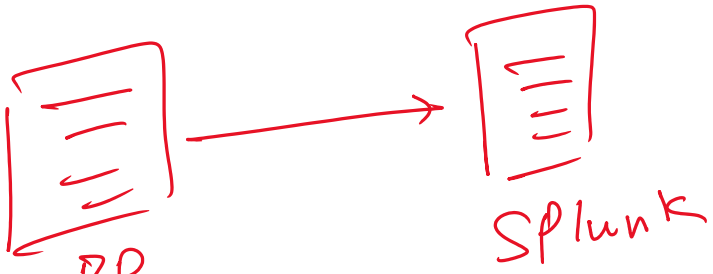
SI = 30 min.

TR = Today's day

daily Basis + license calculated



②



① every 30 min.

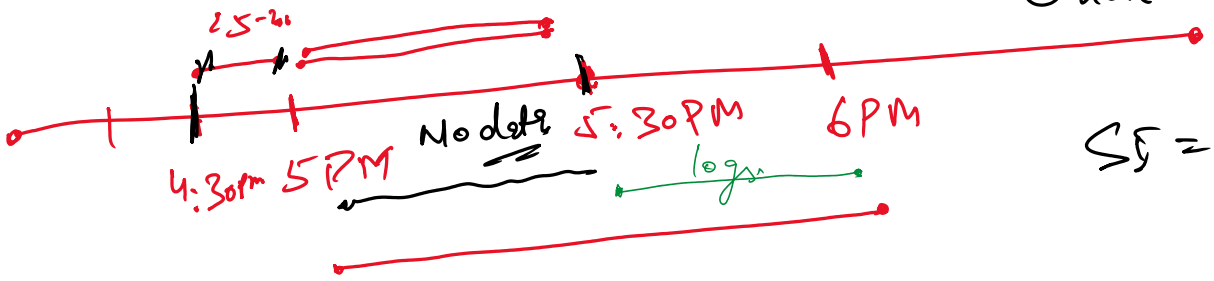
SI = 30 min

TR = 30 min

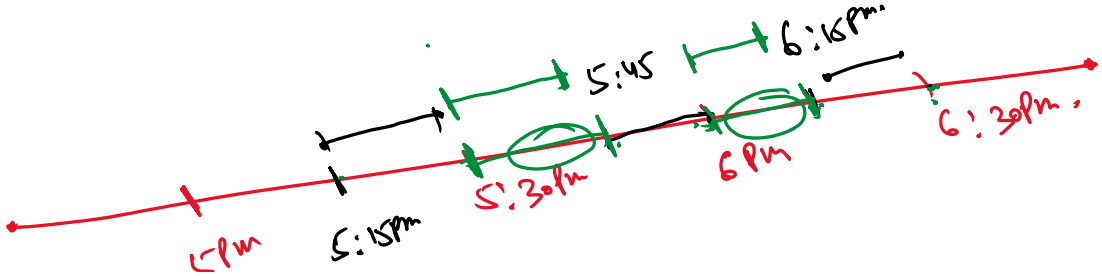
60 min.

30 min.

Condi — No re



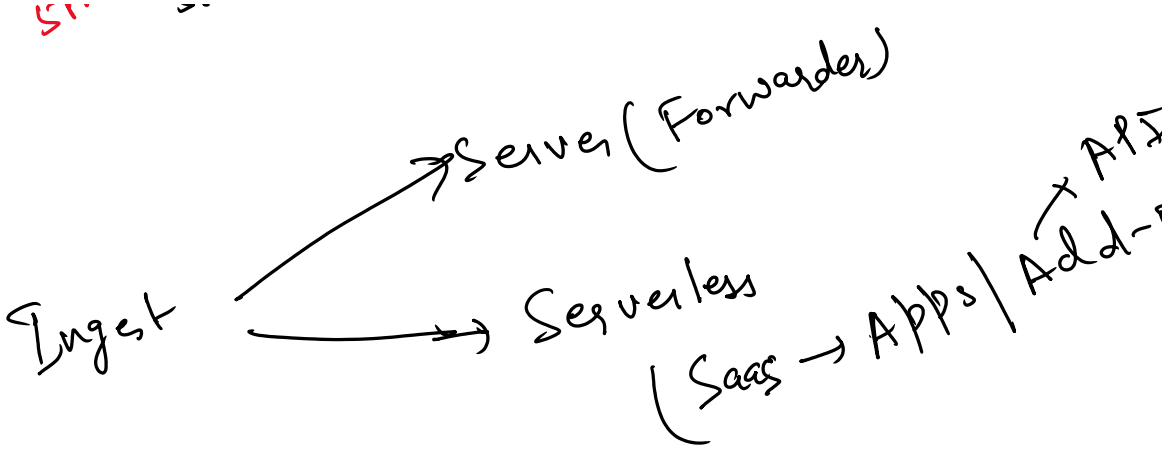
SI = TR



sult mean
No data.

= 15 min.

= 30 min.


Server (Forwarder)
Ingest
Serverless
(Saas → Apps | Add-
API

Day - 5

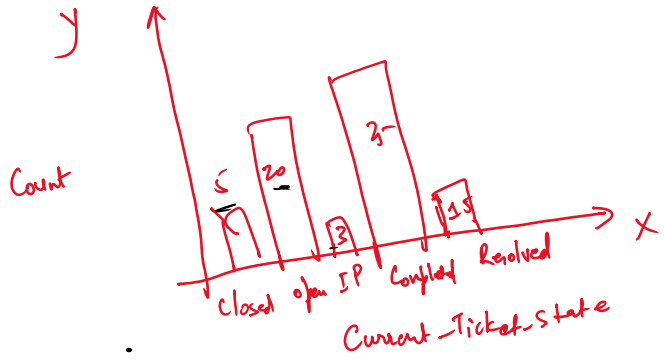
14 February 2025 09:17

1. Dashboard - classic
   1. Dashboard Creation.
   2. Addition of filters.
   3. Drilldown option.
2. Subsearch - 1. join. → inner/outer.
   2. Append. → Append/Appendcols/Appendpipe.

---

1. Dashboard:-
   - → classic Dashboard → XML
   - → Studio Dashboard - V8.5+ → json

iii) Drilldown:-



- X-axis
  - click.name = Current_ticket_state.
  - click.value = closed, open, In-Progress, Completed.
- Y-axis
  - click.name[2] = Count
  - click.value[2] = 5, 20, 3, 15, 25

2. Subsearch :-

1. Append:-

Appendcols:

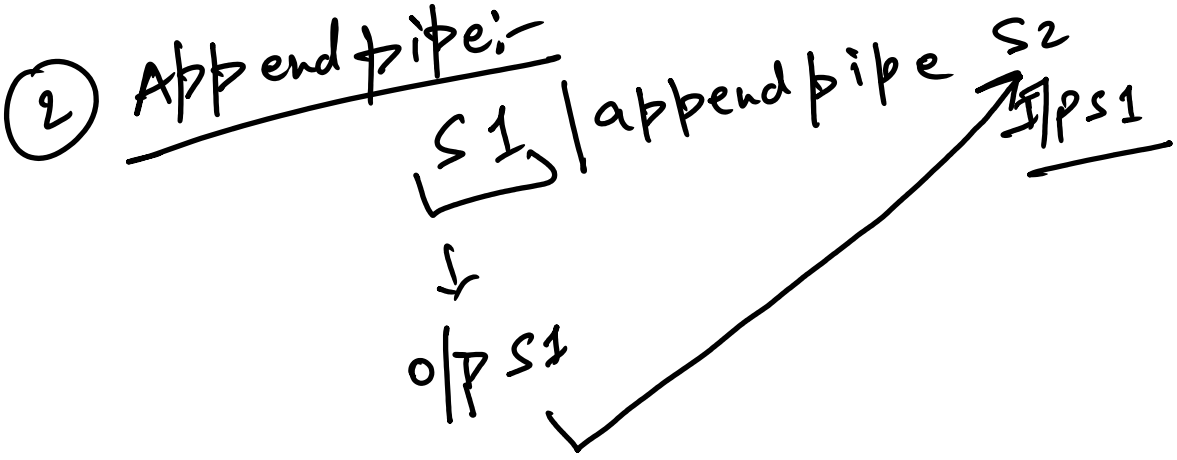
[S1 | append S2]

Combine two output

Combine two o/ps

a	b	c	d

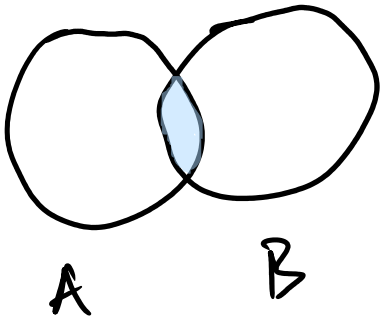
② Append pipe:-

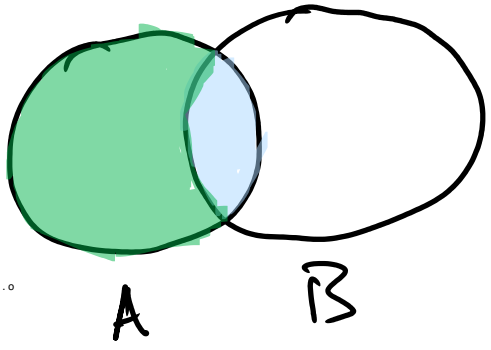


③ join:-

① Inner join.

② Outer join.





Inner join

Outer join

1 - Sample_ticket.csv → index
Lookup.csv → index
→ join

2. Sample- 100Kup.csv → inner