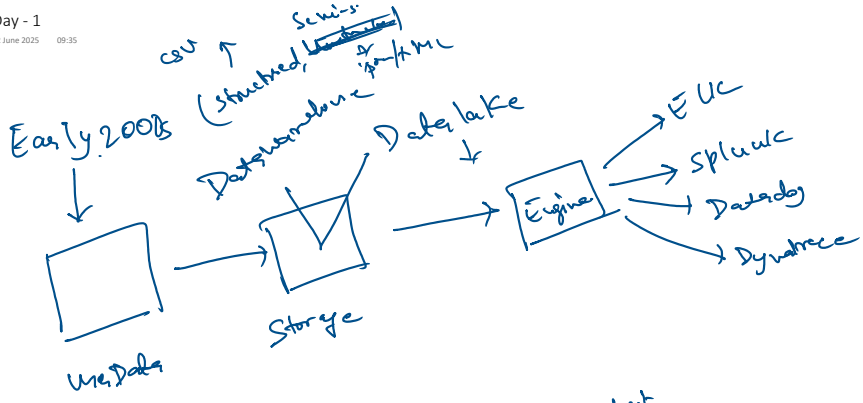
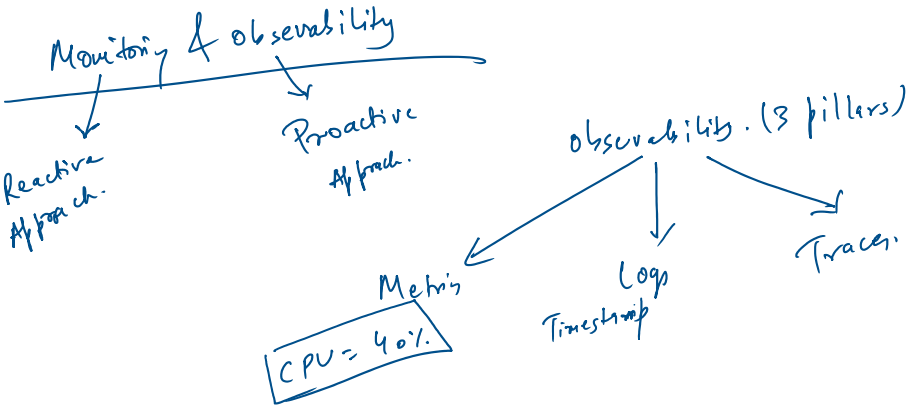
Day - 1

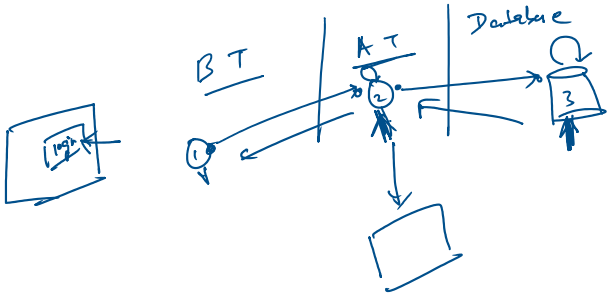
02 June 2025 09:35



Splunk enterprise → log Monitoring TOOL → logs → Alert, Visualization, Report, Dashboard.

1. Splunk ES
2. Splunk ITSI
3. Splunk Phantom → Splunk SOAR
4. Splunk APM
5. Splunk Victor
6. Splunk UBA





SLI vs SLO vs SLA

SLI → Service level Indicator

SLO → Service level objective

SLA → Service level Agreement
Aggrement b/w two parties.
(98.5%)

B/w your team.

all down priority.

B/w your ...

99% → SLO

Error Budget:- 1% (1/-) → either effect App down. (or) any kind of updates/patch.

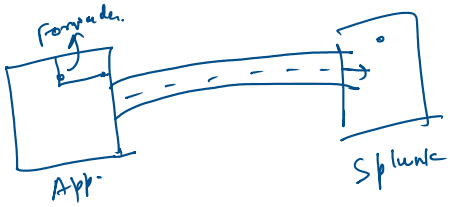
→ Splunk Enterprise

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

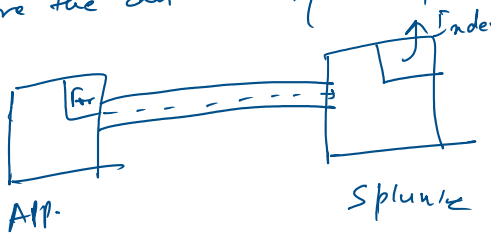
5. Cluster master
6. Deployment Server.
7. Deployer

→ Management Server

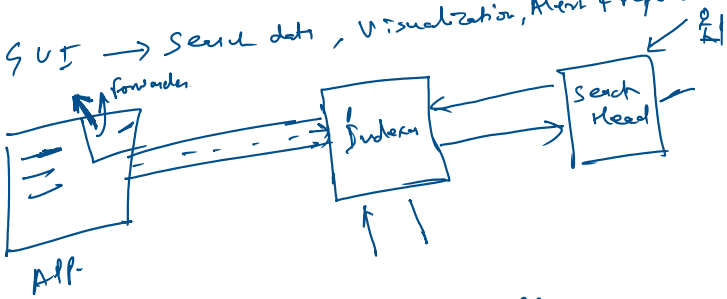
① Forwarder:- Forward the data from the Source to Splunk



② Indexer:- Store the data coming in splunk.

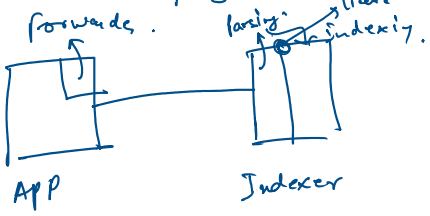


③ Search Head:- GUI → Search data, Visualization, Alert & report.



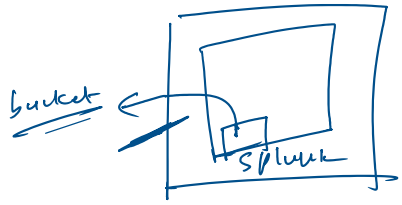
④ License Master:- Agent → check the license usage.

5 GB/day → 1 year.] → $$$

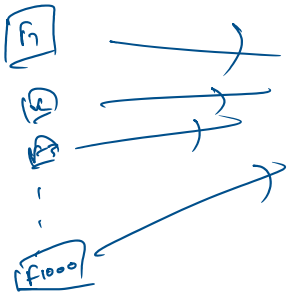


500 GB/day → 24 hrs cycle - 12AM - 12AM

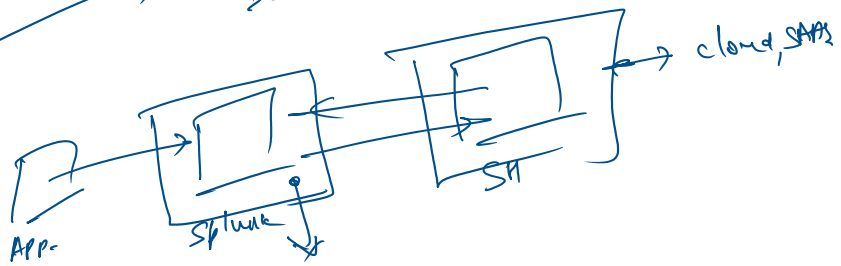
5 GB/day → 24 hrs cycle - 12AM → 11AM
9PM

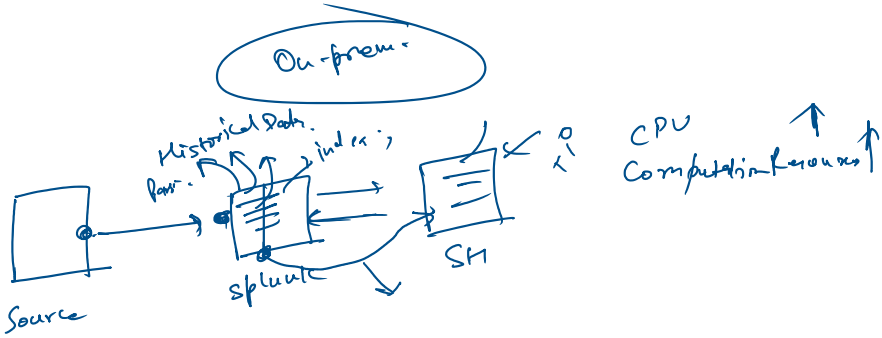


Server
On prem / cloud.

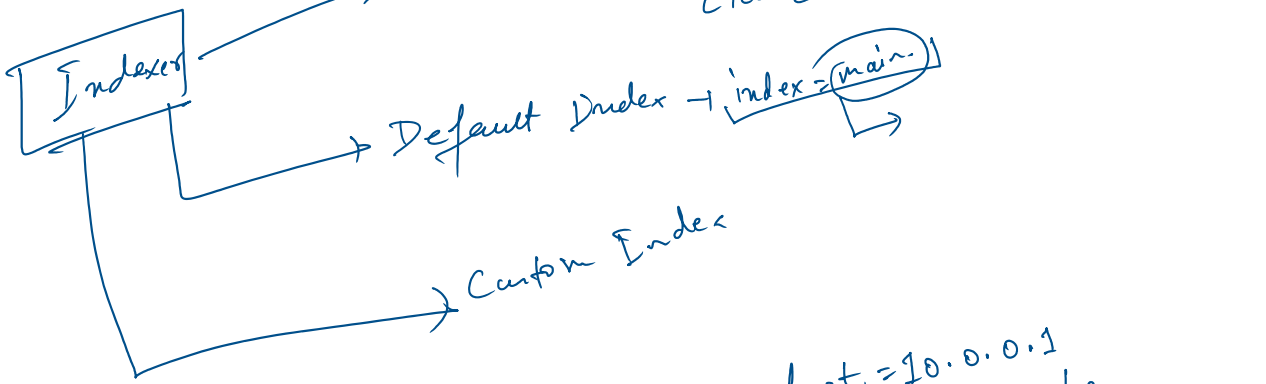


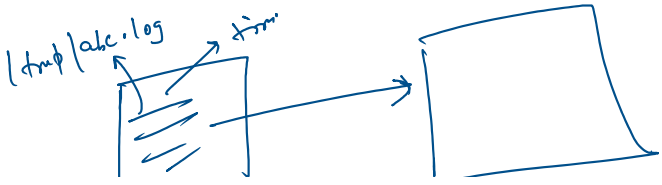
① Data ingestion will continue
② Searching of data will be disabled.



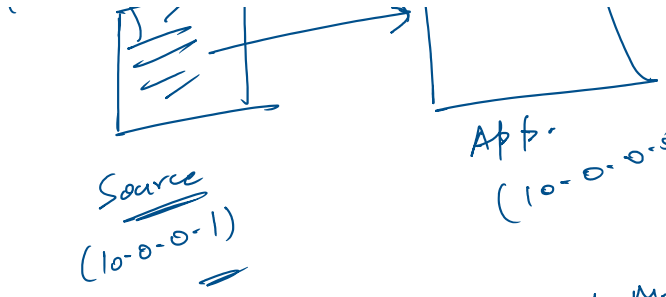


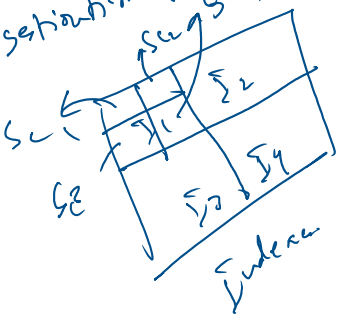
Real Time.

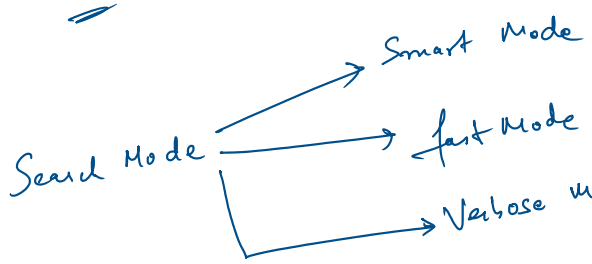




host = 10.0.0.1
Source = /tmp/abc.log.
Sourcetype = Type of data.
Insertion time.







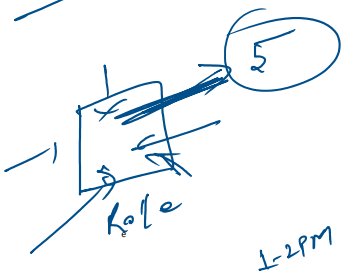
Search → Pulling the events
+
Extraction of fields

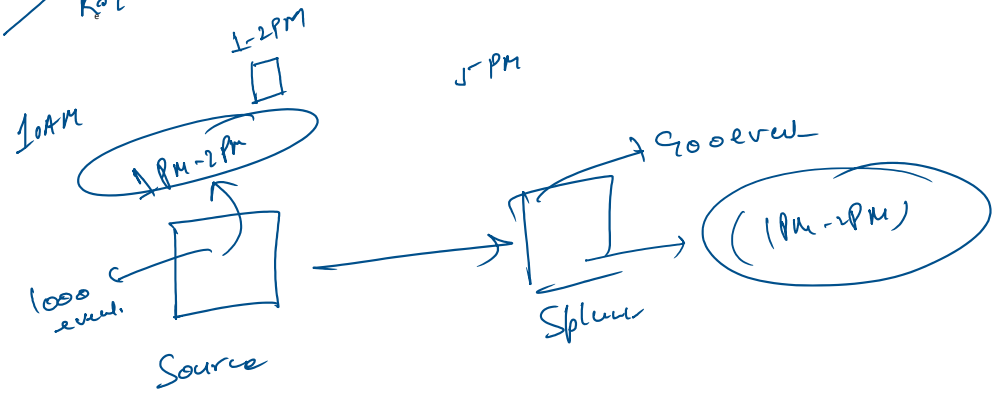
Smart Mode:- Pull the data.
As well as extraction of fields.

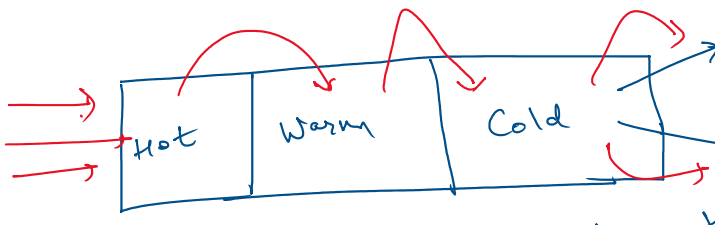
Fast mode:- Pull the data. No extraction of field

Pull + extraction + Navigate b/w diff. tab.

Verbose Mode







UK-idx

Define the retention period:

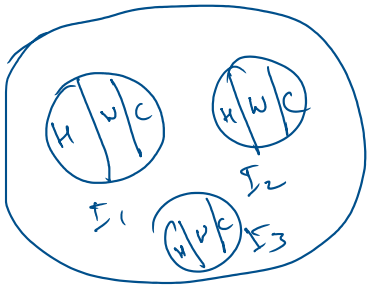
(1) Age of the data ✓ → 30d

→ 100 GB

UK-idx

Any condition matches, Data will move from hot to warm or warm to cold.

Defin
1. Age of the data
2. Size of the Bucket → 10 GB



Indexer

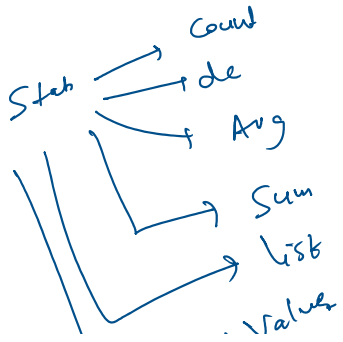
SPL:-

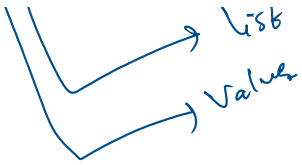
1. Table
2. dedup
3. Stats
4. Sort
5. rename
6. fillnull

1. Table:- Tabular output.

ex- |table field1, field2, field3

fieldName - Case sensitive
field value - Case insensitive.





Stats → sum/avg → | stats sum(field) by field.

avg.

Sort → Ascending → Sort + field | Sort field

Descending → Sort - field

List/Value. → Categorise the data on the basis of certain values.

Eval - evaluation Activity

init a stats

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

1. Calculations. → bytes → Kb

2. if - else

if (a > 5)

→ if (a > 5, a, b) (True / false.)

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

→ if (a>b, "", "")
↓
Condition

3 Case:-

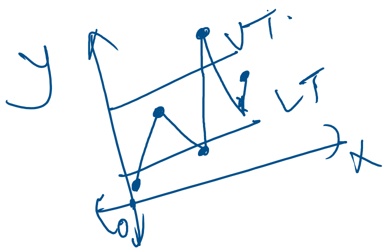
Case(Cond1, "_", Cond2, "_", Cond3, "_", 1=1, "_") → o/p

left to right

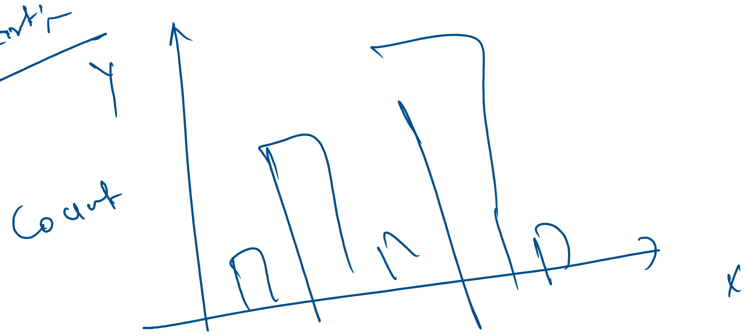
↓ Universal Cond^n

4. chart:-

| chart count by Severity.



5 Timechart:-



(4) Single Value Visualization:-

Trend Analysis where you define the trend.

(5) Addcoltotal / Addtotal:-

Addcoltotal → Addition Columnwise
Addtotal → Addition Rowwise.

(6) Top / Rare:-

Top → Top 10 values by default

|top sourcetype ↳ default is 10 values.

|top limit=3 sourcetype
↳ Top 3 values

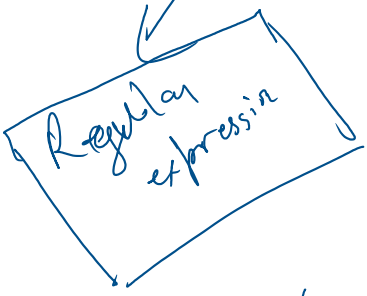
|top limit=0 sourcetype.
↳ Unlimited values.

O/P

sourcetype	count	percent.

Rare → least value
default 10 values
|rare limit=3 sourcetype

7. Rex:- field extraction.



Apply the rex ← Dataset

↓

extract the fields.

→ Both is same.

1. Tag & eventtype.
2. Field Alias.
3. Calculated field.
4. Macros.
5. Data Model & pivot
6. lookup (SW)

1. Tag & Eventtype's-

↓

Normalize the data on the basis of certain

Categorize the data on
field value.

Severity=3 → normal.

2 new field will be generated

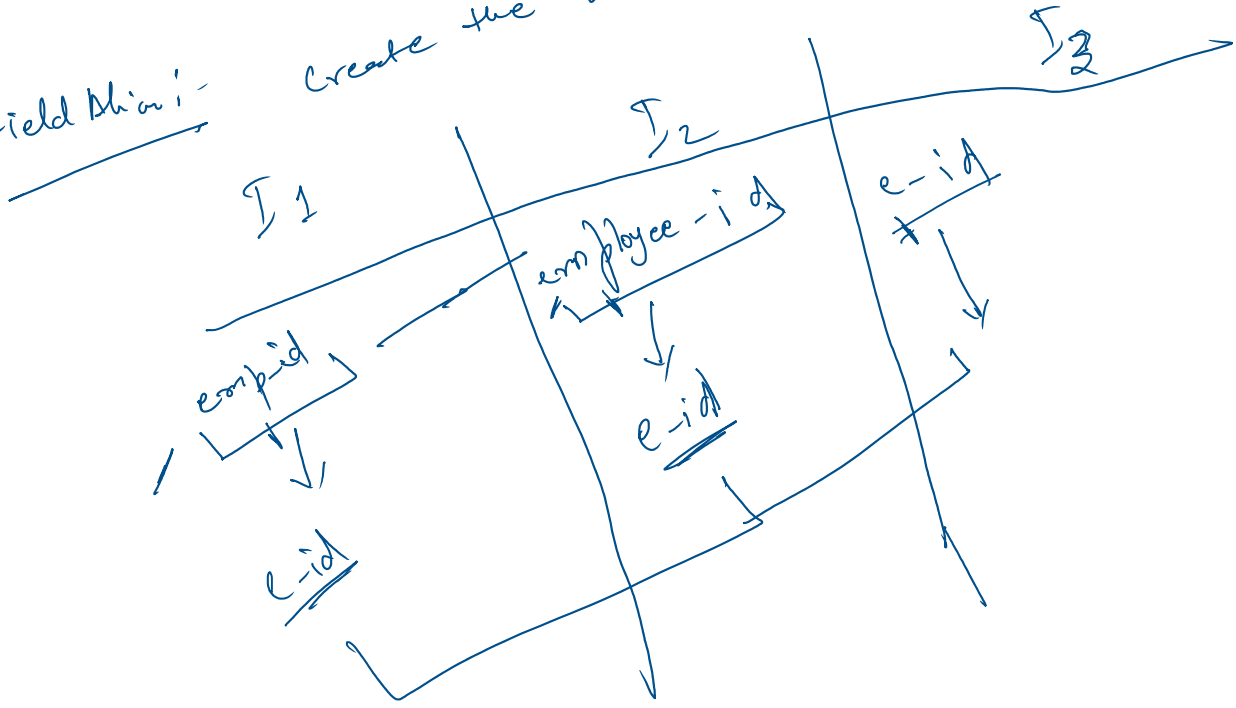
① tag

② tag :: severity

Eventtype →

Categorise the event on the
basis of certain category.

Field Alias: create the new field name from the old name.



Add new Alias field. It will not
[illegible] any existing field.

Add new

delete any existing field.