Day - 1

08 July 2024 10:04

1. Introduction to splunk
2. Splunk Components.
3. splunk GUI
4. User Interface.
5. splunk Commands.

---

1. **splunk:-** Monitoring Tool.

1. Application
2. website.

Data generation.

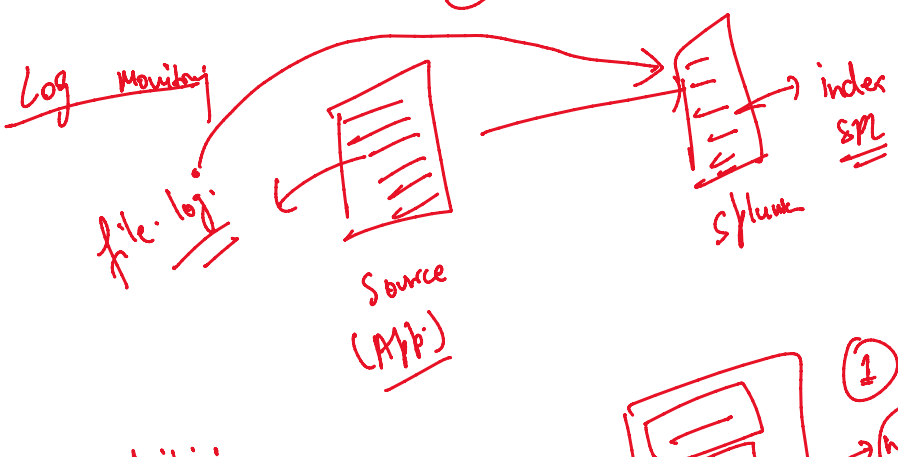
- Application
- User specific.

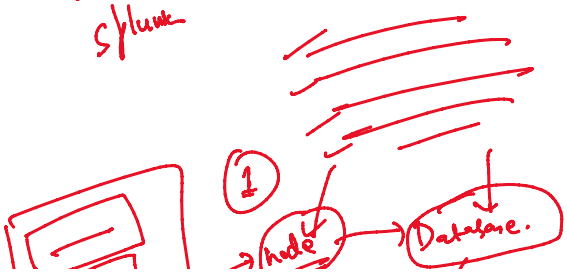
1. Data Warehouse / Store
2. Process / Analyze Data.
3. Visualization.

ETL

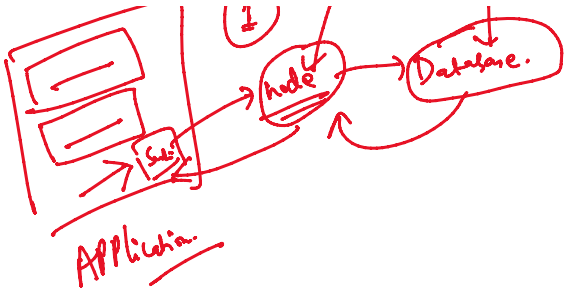
1. splunk. → log Monitoring.
2. Dynatrace → APM
3. AppD.
4. Nagios → Infra. Monitoring
5. ELK. → Log Monitoring.

Log Monitoring
APM
Infra. Monitoring.
Security (SIEM)





APM Monitoring:-



Infra:- CPU, Memory, Disk., Process

OSSEC

Splunk:- (1) No restriction on format.
(2) No restriction on data source.

Dashboard:- ↳ XML → classic Dashboard
json → studio "

Machine learning:- LR, LSP, BLL

Alert:- Rumpse alert.

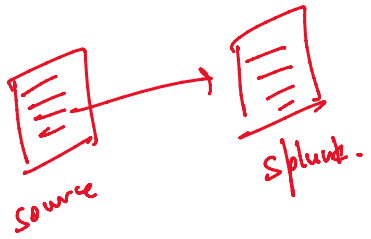
Report:-

Component of splunk:-

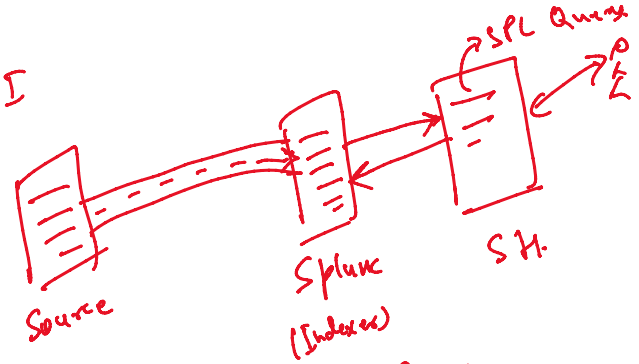
(1) Indexer.
(2) Search Head
(3) Forwarder.
(5) Deployment Server.
(6) cluster Master.
(7) Deployer.
(8) SHC:-

③ Forwarder.
④ License Master
⑦ [illegible]
⑧ SHC:-

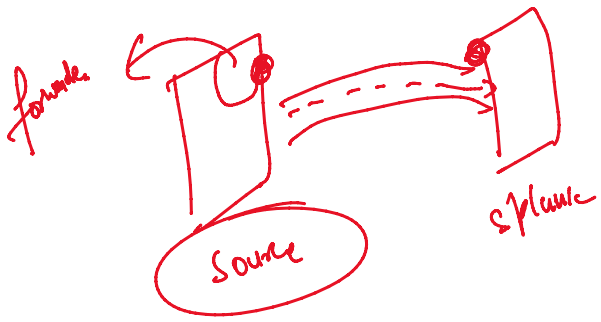
① Indexer:- Database + inbuilt.



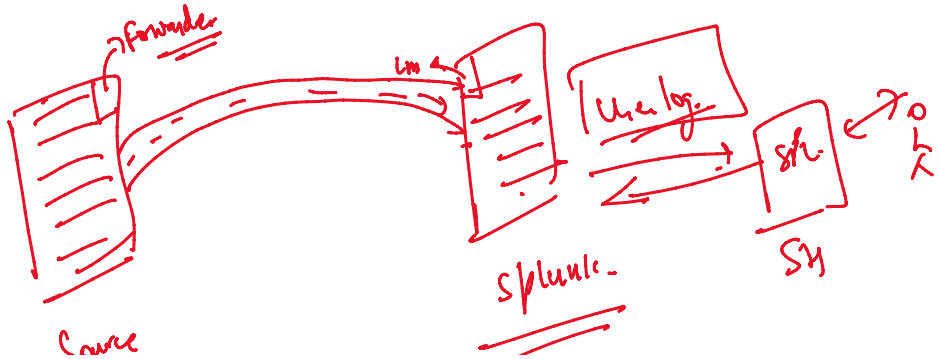
② Search Head:- GUI



③ Forwarder:- Agent that will forward the data from the source to the splunk end..



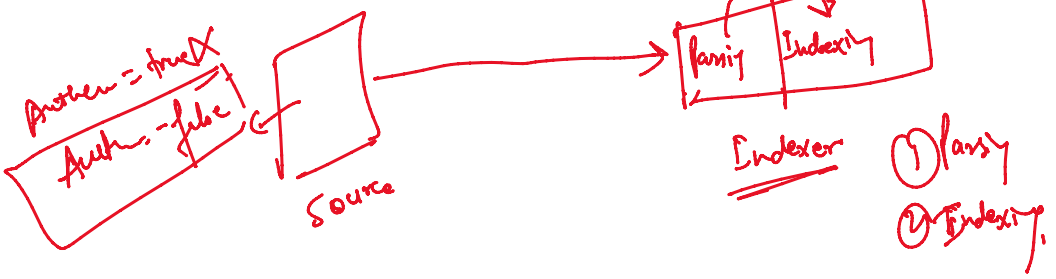
① App log
② Infra log
③ User log.
[illegible] log



3. Sys log
4. Security log

Source

splunk>



1. Parsing
2. Indexing.

License Monitor How much data / license T&C?

Policy Agent.

5 GB data/day

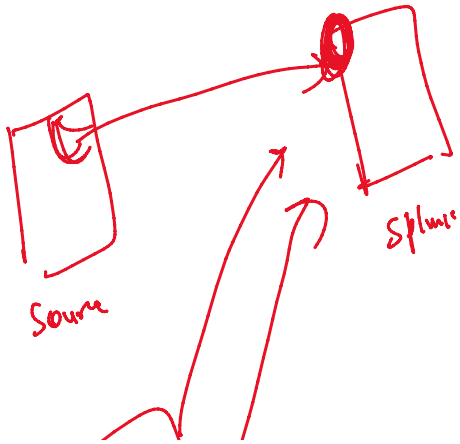
↓

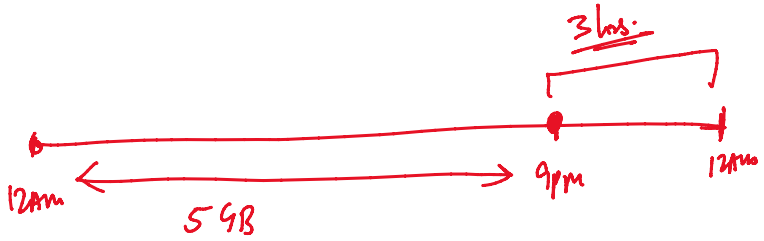
1 year

Trigger in splunk.

1. Volume of Data.
2. No. of App.
3. No. of Server.
4. No. of Index.
5. No. of forwarder.
6. Resource Utilization
7. Type of Data
8. No. of User.
9.

5 GB/day.

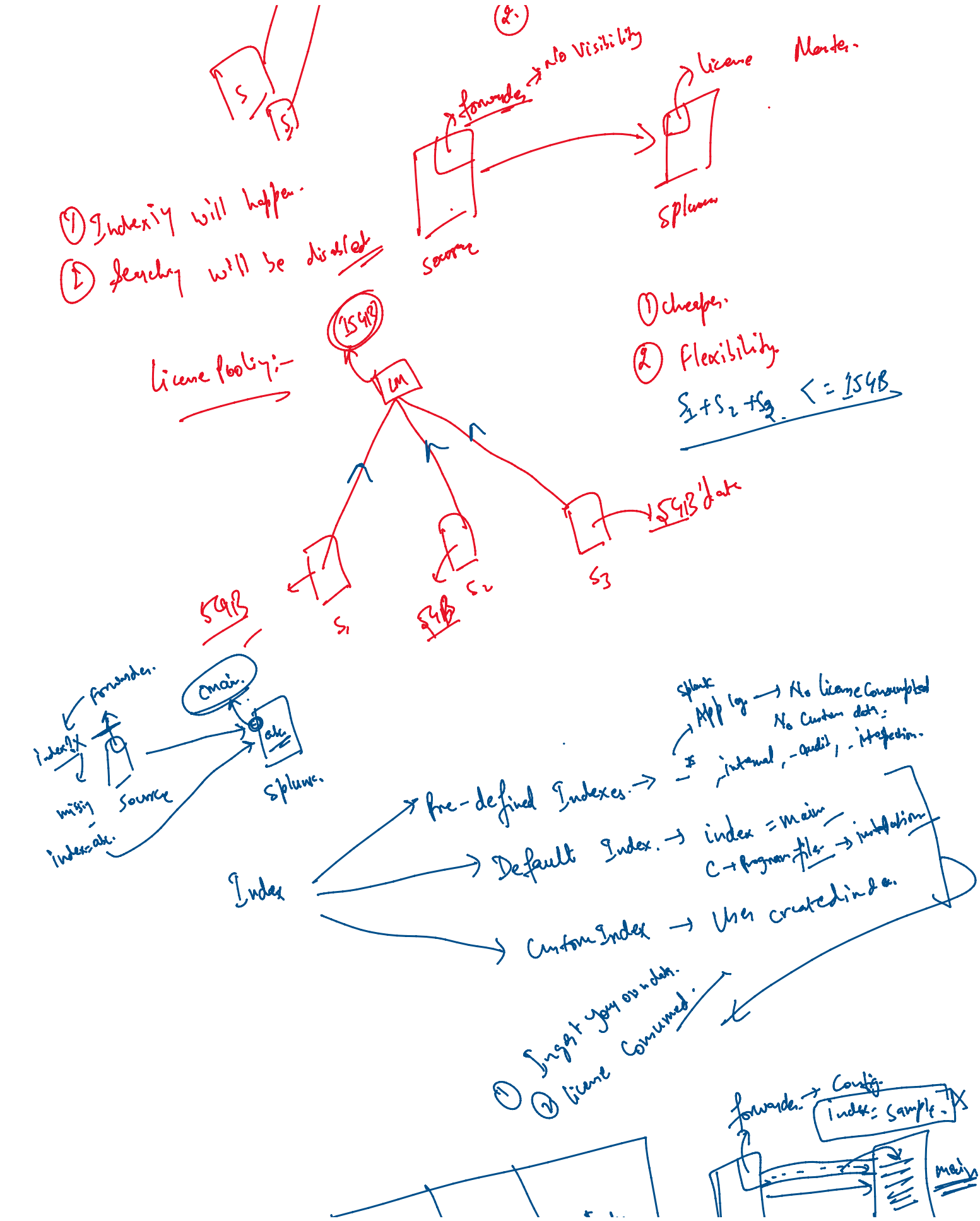


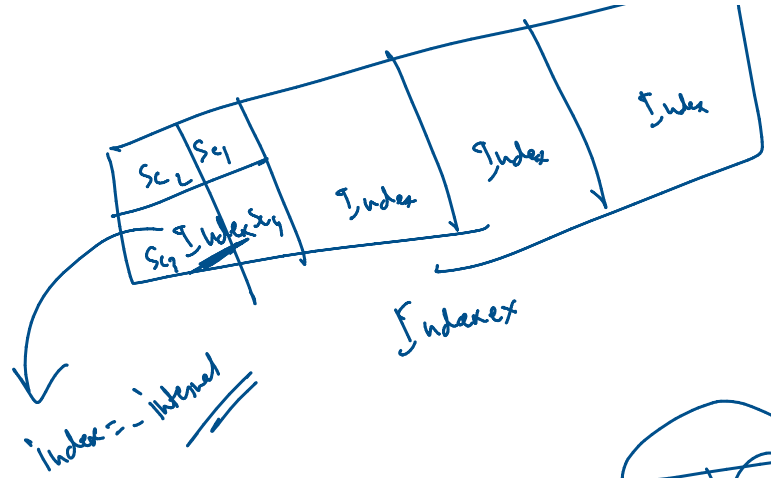


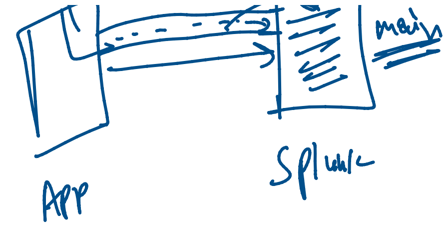
1. Stay in local server. No indexy.
2.

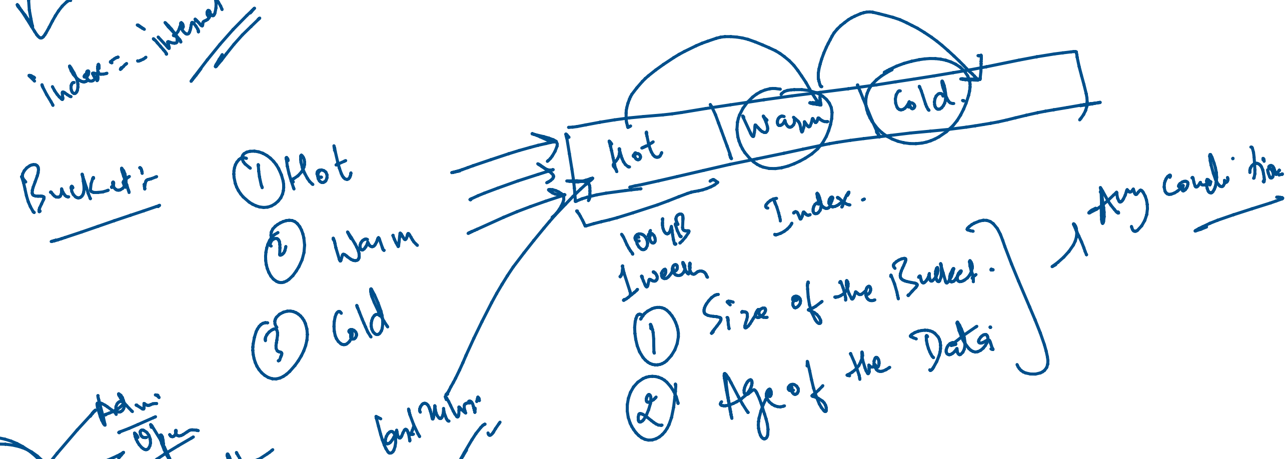
No Visibility

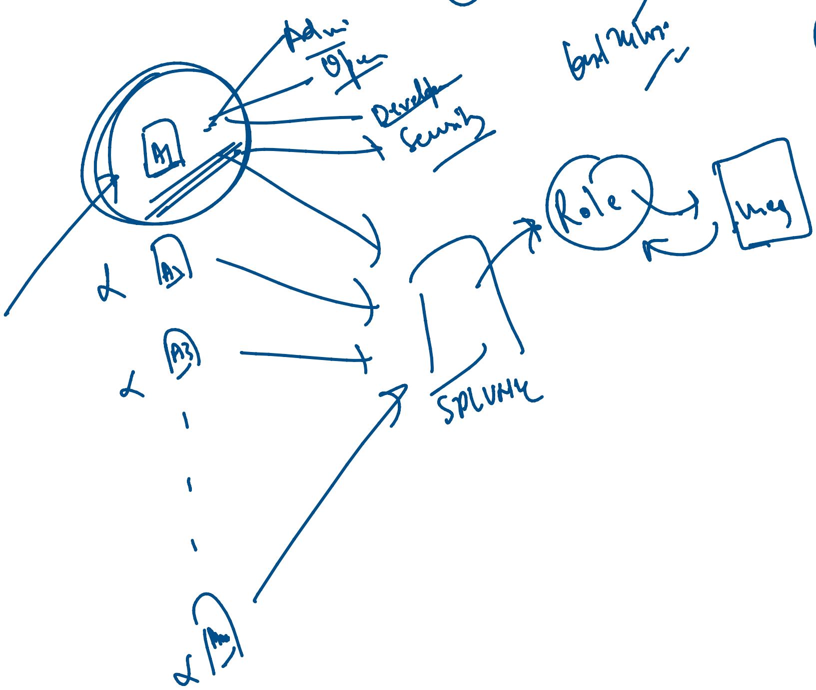
License Monitor.

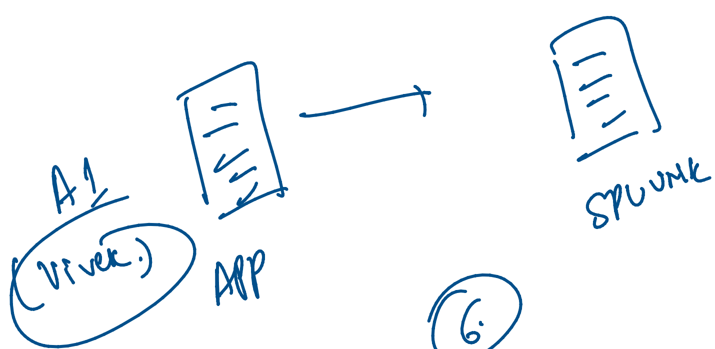

(2.)
forwarder → No Visibility
License Mgmt.
Splunk
source
(1) Indexing will happen.
(2) Searching will be disabled
License Policy:-
LM
150GB
150GB's data
S1
S2
S3
50GB
50GB
(1) cheaper.
(2) Flexibility
S1 + S2 + S3 <= 150GB
forwarder.
main.
data
Splunk.
index=X
missing source
index=abc.
Index
Pre-defined Indexes. → _internal, _audit, _introspection.
Splunk App log → No license Consumption
No Custom data:
Default Index. → index = main
C → Program files → installation
Custom Index → User created index.
(1) Ingest your own data.
(2) License Consumed.
forwarder → Config.
index = sample.
main



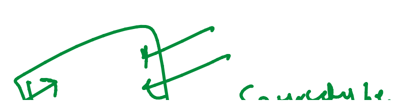


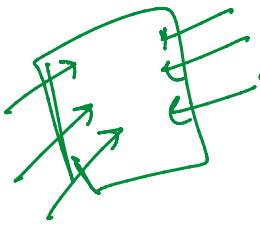




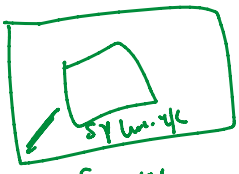


1. Create Index.
2. Alert Welcome!!
3. How much data?/Size of data!
4. Retention.
5. Permission.

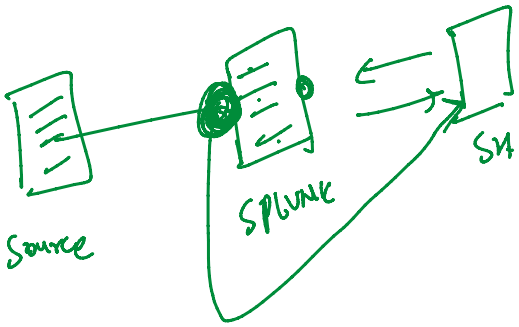




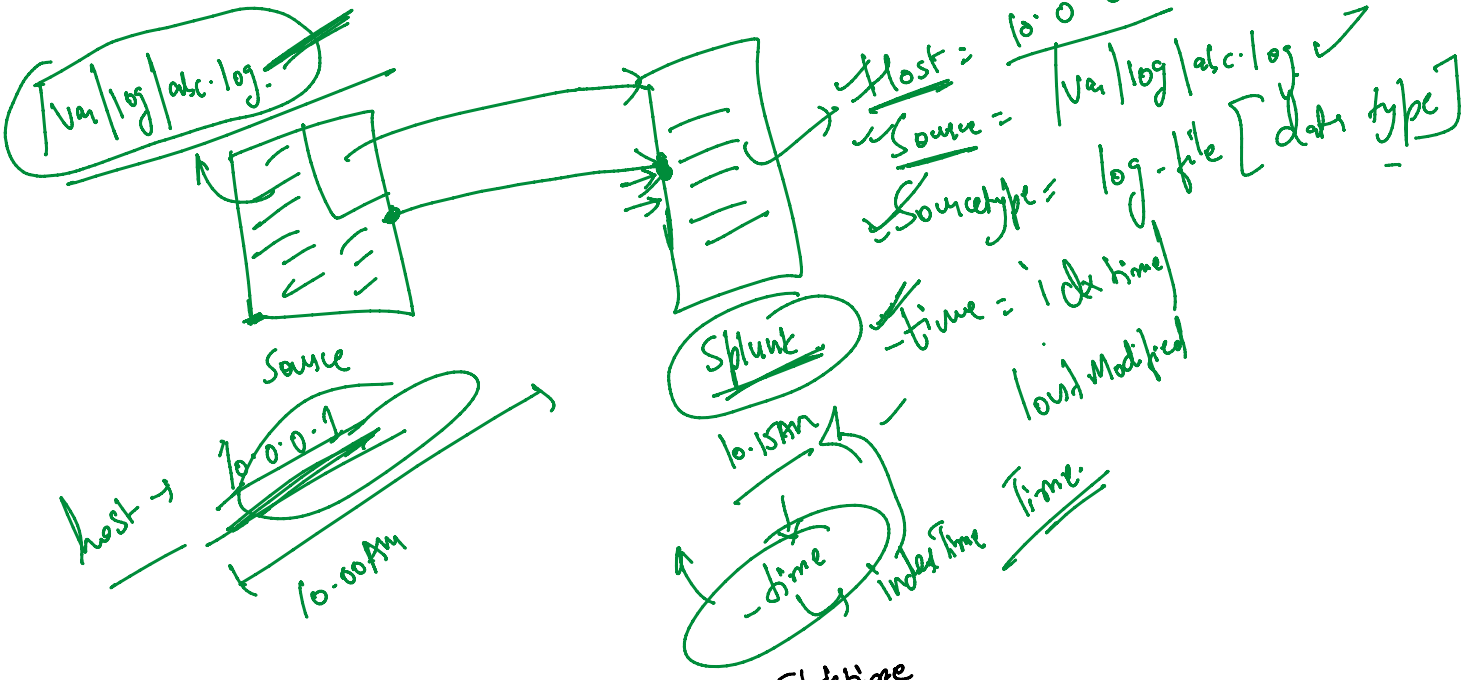
1. Data size
2. Sample data (PII, Data Format)
3. Index Creation ?? → How much.



4. ~~Retention.~~
5. What is the final objective!!? → WTF



1. Historical Data / Relative Data.
2. Real Time.



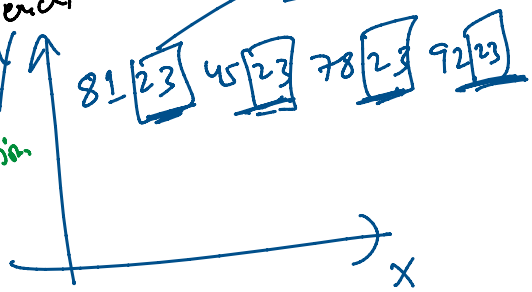
Command :-

1. Table
7. timechart
8. chart
13. Rare.
14. Where

Command :-

1. Table
2. Rename
3. Stats.
4. fillnull
5. sort
6. eval
7. Dedup
8. chart
9. Rex
10. addcoltotal
11. addtotal.
12. Top
13. Style Value Visualization
14. Where
15. eventcount
16. field
17. Rare.
18. Search.

Value that is repeatedly occuring in mode data set

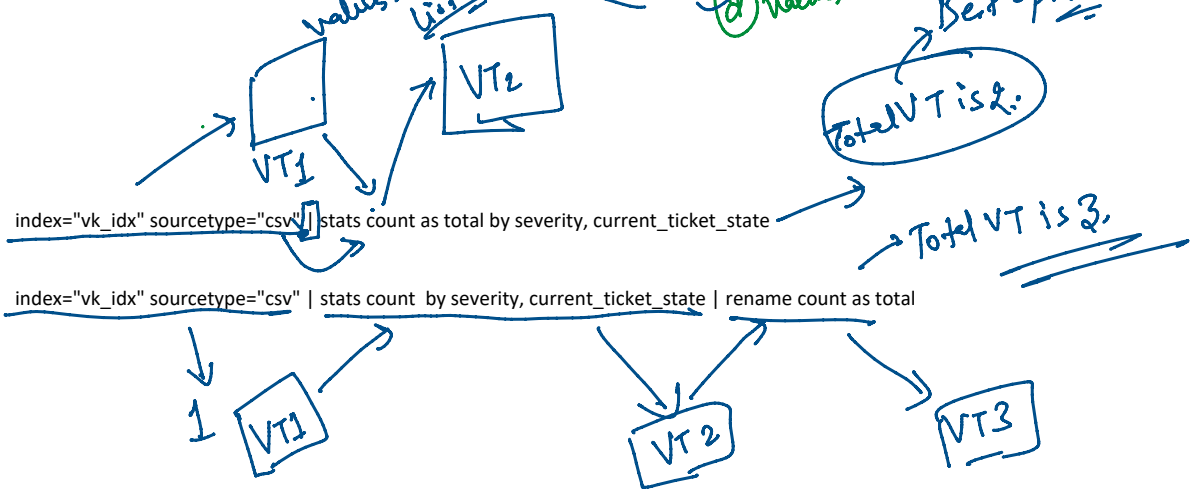


(1) Table :- o/p in the Tabular format.

(3) Stats :- Statiscal output

- (2) count
- (3) dc
- (4) list
- (5) values
- (6) sum
- (7) avg.

Unique dc → count values → array list



(4) Dedup | Sort.

↳ Duplicate value.

Sort (-) → descending.

Sort + → Ascending order.

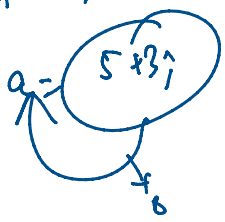
Sort severity, Sort + severity → Both are in the Ascending order

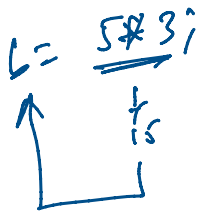
Eval → Evaluation purpose.

int —
str —
var —

→ Eval [define variable]

int a;

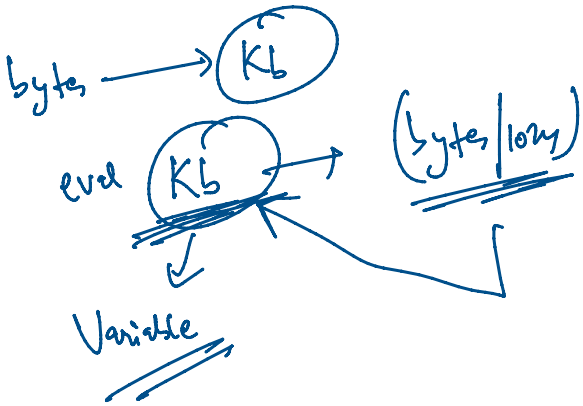




(1) Calculation
(2) if - else
(3) Case statement.

C = a+b = 8+15 = 23

(1) Calculation

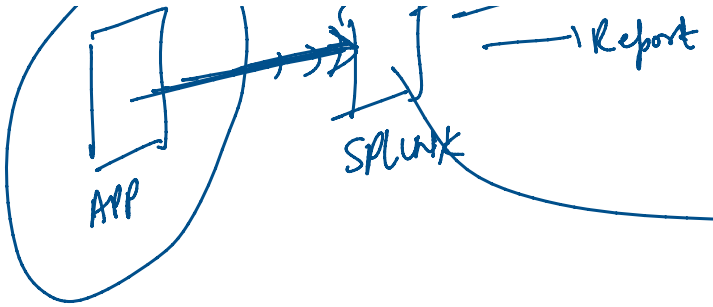


(2) if - else

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

eval — = if(condition, true, false)

condition → a>b
true → a
false → b



↳ last 15 minutes.
triggered → email / Notification.

3. Case Statements:-

Case1:- Mon
Case2: Tue
Case3: Wed
.
.
.
Default: Sunday

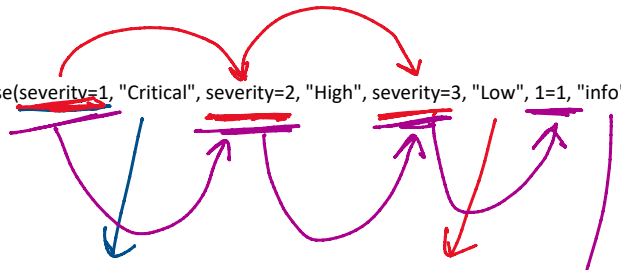
Case1:
Case2:
Case3:
Case4:
default:

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

case(Severity=1, "Critical", severity=2, "High", severity=3, "Normal", 1=1, "Low")

↳ Default Universal condition.

index=vk_idx | dedup severity | eval priority=case(severity=1, "Critical", severity=2, "High", severity=3, "Low", 1=1, "info") | table severity, priority | sort severity



o/p:

Low.

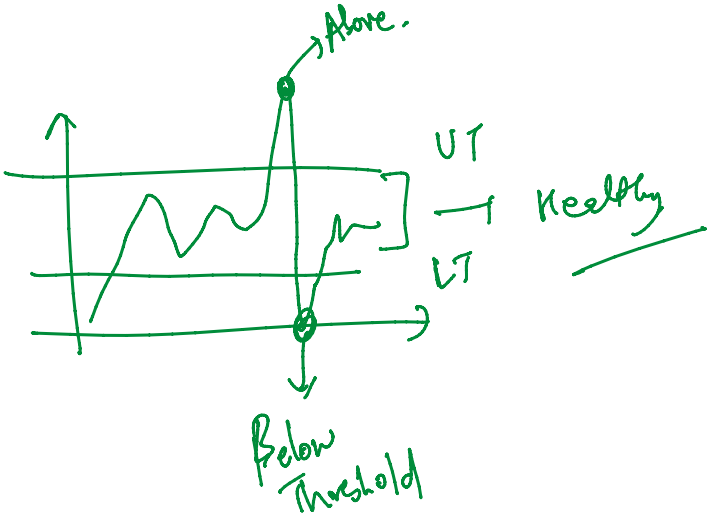
Severity=3.

Severity=5 'info'

Top & Rare:-

Top → top values

Rare → least values



Where & Search Commands

A	B
10	30
20	20
30	10
40	5
50	15

Search A > 20 → filter in the same field

Where A > B → filter b/w two fields.

9th july:-

→ striptime

9th July:-

1. Timechart → strptime
   → strftime.
2. Install Custom Visualization App
3. Addtotals & Addcoltotals.
4. Rex. → field extraction, Data Masking.
5. Eventcount
6. Fields