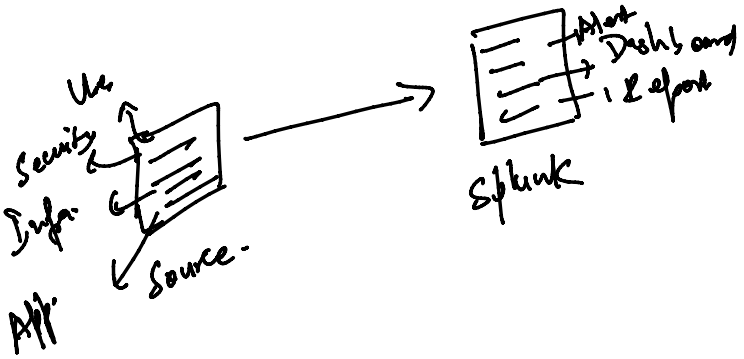
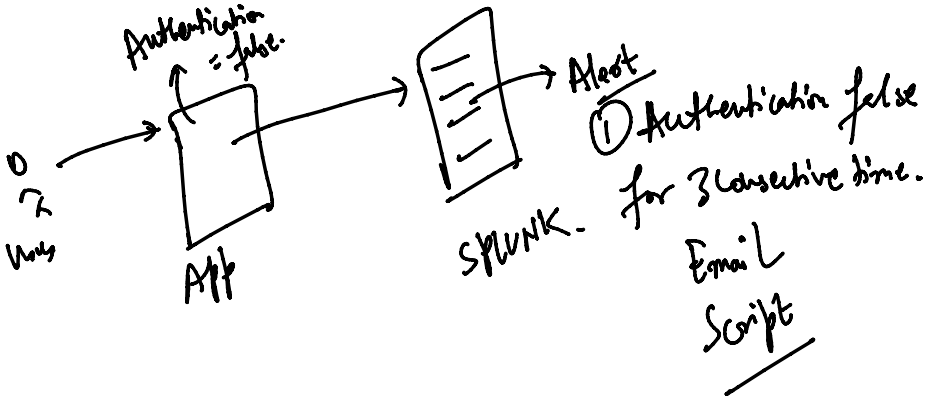
Day - 1

22 July 2024 10:18

1. Splunk.
2. Component of splunk
3. Use Case
4. Basic Commands :-
   1. table
   2. Rename
   3. stats.
   4. eval
   5. chart
   6. timechart
   7. Addcoltotal
   8. Addtotal.
   9. Rex
   10. join.



2. ELK
4. Splunk
3. Major.
4. Dynatrace
5. AppD
6. Datadog



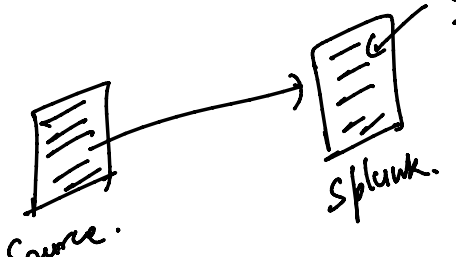
Splunk:-

1. Dashboard
2. Report
3. Alert
4. Prediction
5. MLTK

Components of splunk:-

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

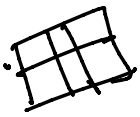
1. Indexer:- Internal Database where all the data storage works.



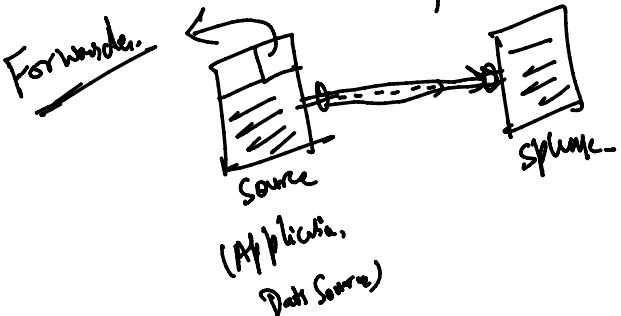
1. Type of Data
2. Amount of Data
3. Avg of source.

Database → SQL
→ NOSQL → Json, XML

4. Disk size.



2. Forwarder:- Forward the data from Source to the destination.



1m → 30MB
Unix → 250MB

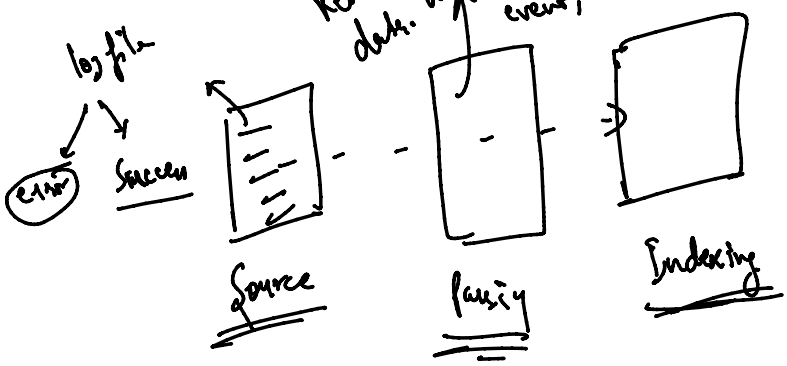
(App / Data Source)

Two Type of forwarder → Unix, 25

① Universal forwarder - Standalone package for Universal forwarder

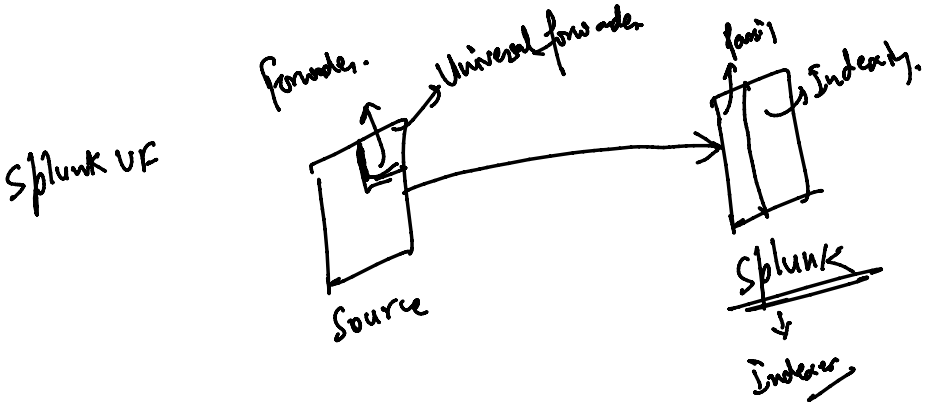
② Heavy forwarder - Splunk Enterprise. → 4 85MB+ths, 5GB → Unix.

↓ SH, Indexer, LM, HF, ...



① Default Parsing → Cleaning, removing corrupt data.

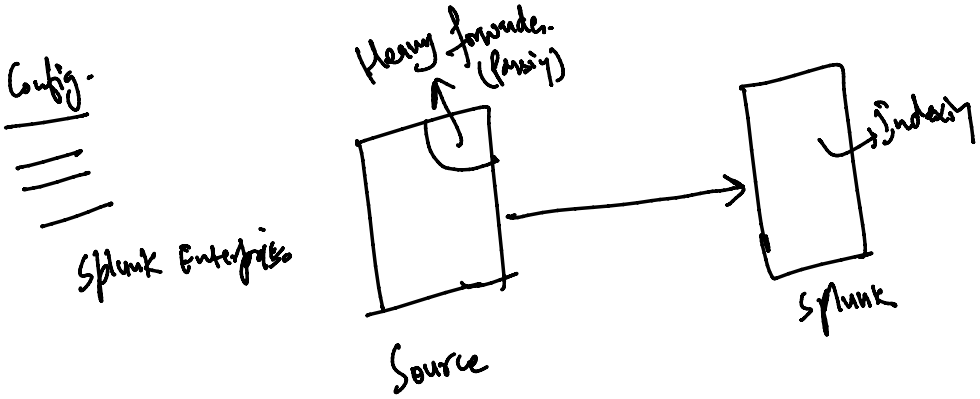
② Custom Parsing - Specific event by a specific log/string.



① forward the data same as it is.

② Parsing will be taken care at the Indexer level.

③ Indexer = Parsing + Indexing.



① forwarding of data is being taken care after Parsing.

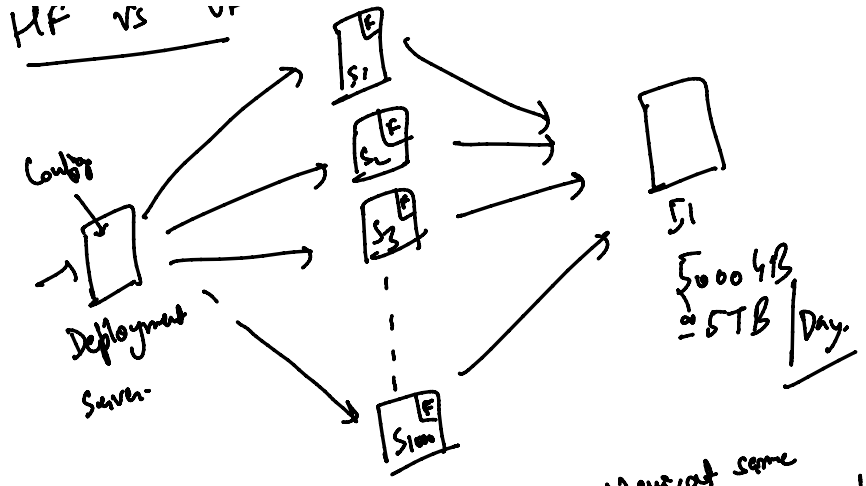
② Indexer will take care of only Indexing Activity

HF vs UF

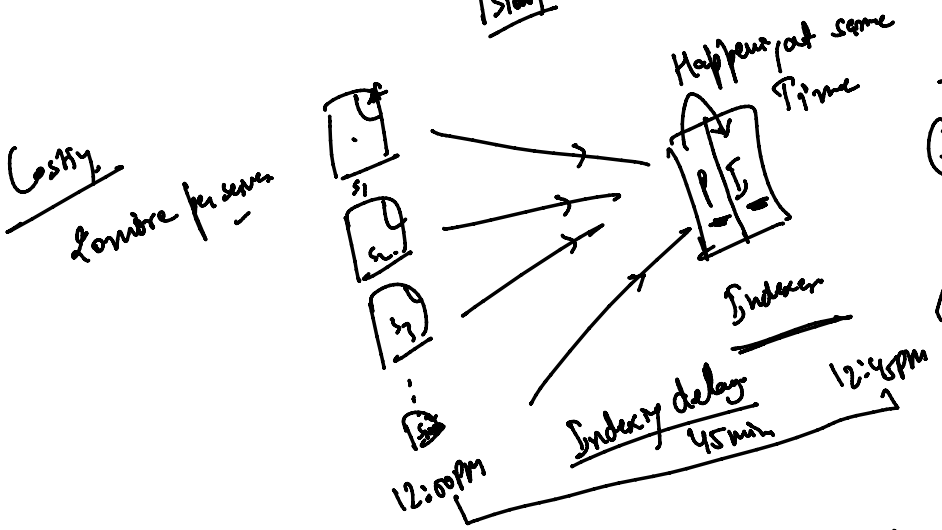
① HF

(a) less time at Indexer

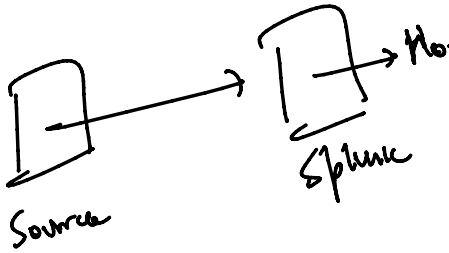
HF vs UF



① HF
② Less time at Indexer
③ Less Traffic at the n/w.

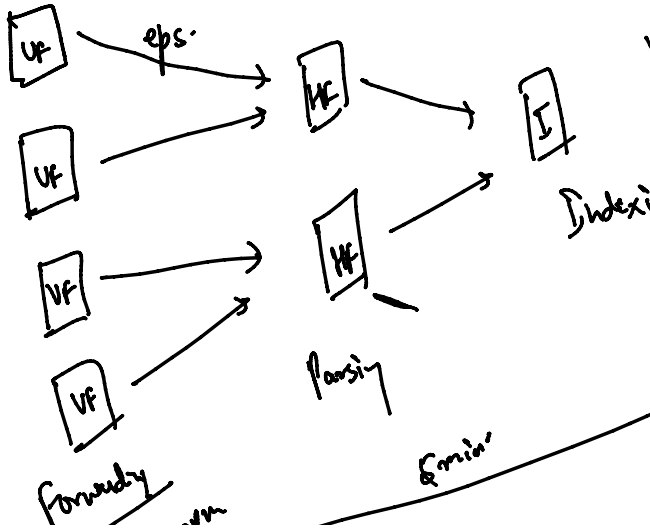


UF
① Space issue
② Cost will high
③ time taken is more.



How much data ingested per day on the basis license of splunk will be calculated.

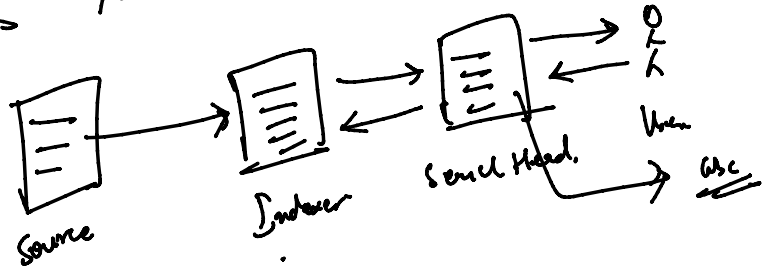
Hybrid Concept:



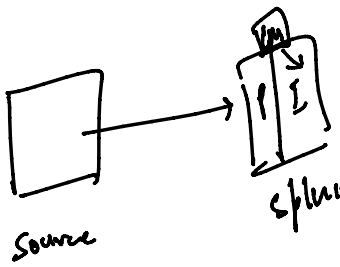
① Reliable solution.

UF → Forwarding
HF → Parsing
Indexer → Indexing

Search Head:- GUI where user can create the Dashboard, Panel, Report etc.



License Master:- Policy agent which will monitor that someone should not be crossing the daily limit.



Criteria :-

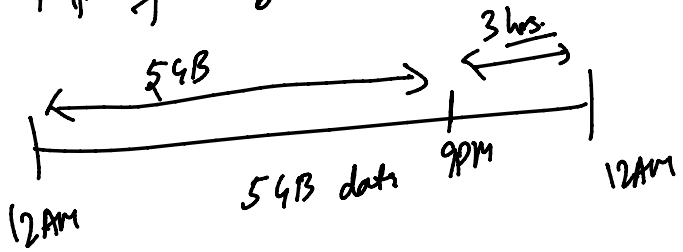
(1) LM is calculated on the basis of how much data is ingested in splunk per day? 5GB/day $$$

↳ 1 yes.

24 hrs. cycle : 12 AM — 12 AM

(1) No Carry forward

(2) No Lending from future days.



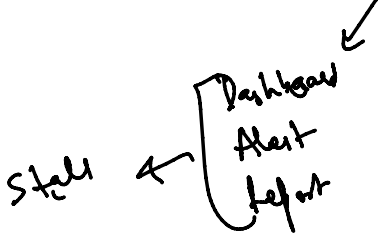
(1) Temp storage.

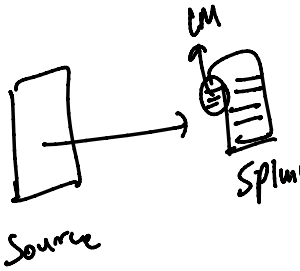
(2) Auto-extend the license.

(3) Delete old data.

(4) Borrow from Next days.

(1) Saved in indexer, Search will be disabled





(1) Data Ingest

(2) New Datasource

(3) Prediction

Stan → Depart

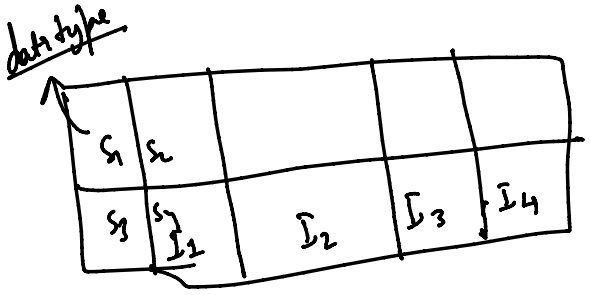
Source

⑤ Predicate

④ Buffe

Per GB cost vary.

3 times → 3 day.

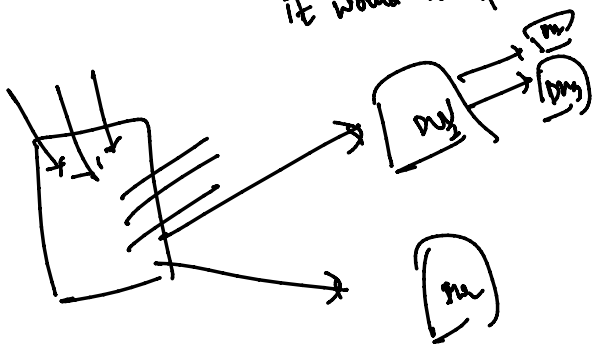


① Proper segregation.

② While search, it would be quick.

Indexer

I1 → Security logs
S1 → Palo
S2 → fireeye
S3 → mcaffee



Reserved to store the splunk ↑ app. specific log. ↳ License not consumed.

_internal, _audit
_introspection.
_*

No Destination

Pre-defined Index

Index → Default Index → index = main.
(click) C:\Program Files\

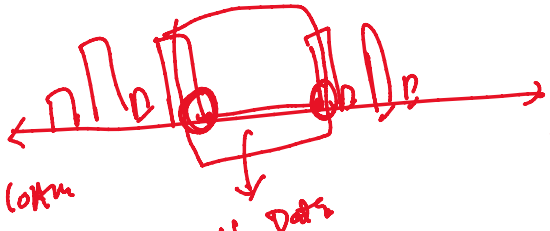
Custom Index
↳ User create specific index.

index = VK-idx

index = sno 15

While data ingestion, if you are not defining the destination → main index.

Store your custom data. License will be consumed.



Smart / Verbose Mode

the data is

Search the data:-

index=main

Fast mode ← [(1) Pulling of events. ✓
(2) Field extraction from the events. ✓] → Mode:-

Fast Mode → Most fastest Method. → Searching of data happening. No data extraction

Smart & Verbose Mode → Take More time extraction + Searching of data

Commands:-

1. table
2. Rename
3. top
4. Rare
5. Dedup.
6. Append / Appended / Appendpipe.
7. eval.
8. Timechart
9. chart
10. eventcount
11. Sort.
12. stats.

(1) Table:- Create the Tabular output.

table field1, field2, field3

Top:- it will give the top values

|top sourcetype default → Top 10 values

|top limit=3 sourcetype → Top 3 values

|top limit=0 Sourcetype → Unlimited output.

Eval:- Evaluation purpose

int — expression.
var —
str —

Var –
Str –

eval (define_variable) = expression.

Kb = (byte/1024)

⇒

① Calculation → byte → Kb
② if-else →
③ Case statement →

② if-else:-

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

if-else statement:

```
if (a>b, a, b)
```

③ Case statement:-

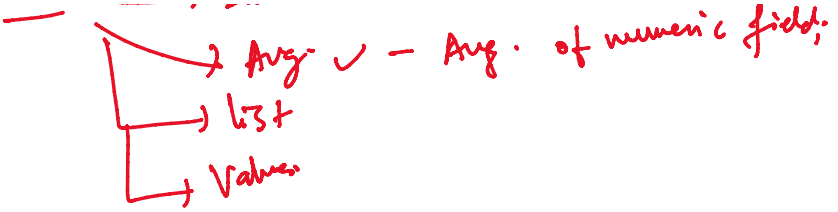
```
switch(a): —
switch(b): —
switch(c): —
  :
  :
default: —
```

Sort - severity
↳ Descending order

Sort + severity
↳ default → Ascending order.

Stab:- Statistical output -

Stats → Count
→ Sum ✓ – summation of numeric field
→ Avg ✓ – Avg. of numeric field.

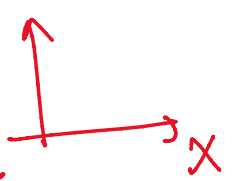


Visualization:-

① chart → chart count by severity

count → y-axis

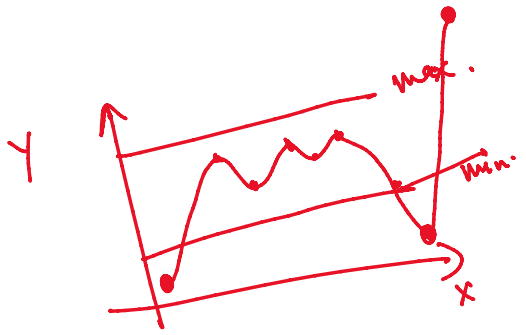
severity → x-axis



② timechart

Linear:- 10, 20, 30, 40 - - - -

Log:- 10^x = 10, 100, 1000, 10000 - - - -



Timechart:-

↳ pre-built field of Splunk. where the X-axis → _time.

timechart count by current_ticket_state

time_submitted = 09-09-09 09:09

Min

time-submitted = 09-09-09 09:09

%.d-%.m-%.y → Asia

%.m-%.d-%.y → US

%.y-%.m-%.d → Europe

date & time → epoc format → Convert into the system Readable format

Strptime → Parse the date & time field

Strftime → format the date & time field.
└→ Convert the format f1 to format f2