Day - 1

14 April 2025 14:19

1. Splunk & its Component.
2. Archictre.
3. SPL Query.
4. K.O. – Macros, DM, Pivot, Alert, Lookup, Tags / eventtype.
5. Dashboard

(1.) Splunk:-

Log Monitor → oper. / Infra / Security / User. / Appl.

Ebay ↓ Phone + Backcover. Shirt + Pant.

2000s → [Database] → User Info.

↓ Digital.

Data (Storage) ↓

DataWarehouse (Structured, Semistructured)

Datalake. (Structured, unstructured, semistr.)

↓ csv. ↓ video/audio/pdf. ↓ json, xml

Dataswamp → Unutilized data.

(1) splunk → Bucketing concept

(2) Datadog

(3) Dynatrace

(4) ELK → Inverted Index

[DB] → Analysis → [Search/Processing Engine]

Monitoring:- Reactive Approach.

observability:- ProActive Approach.

(1) Log → Timestamp dataset.

(2) Metrics → [CPU = 70%] [Disk = 80%.]

(3) Traces →

[Time, CPU, IP, - ...]

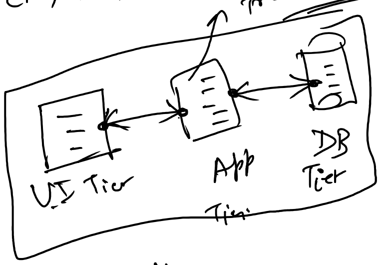
[CPU = 70%] → [Log.]

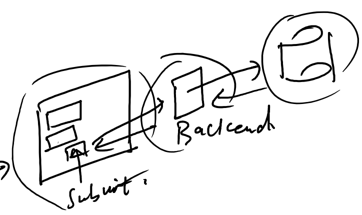
↓ [Metrics]

> 70% → Critical

< 70%. Normal

↓ Aggregation





Monitoring → Log Monitoring → Splunk.

Monitoring → APM → feature of an App. works.

Monitoring → EUM → RUM → Real User Monitoring. → [Hong-Kong.]

EUM → Syn. Monitoring. → [Bot → Location]

→ EUM → Syn. Monitoring → Bot → Location

End user monitoring

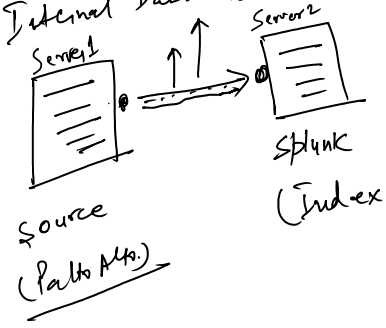
Splunk:- Log Monitoring

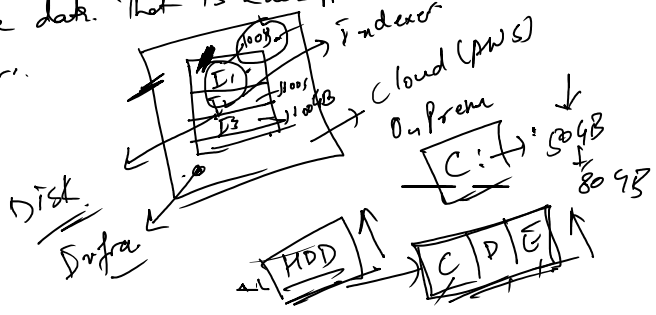
1. Dashboard
2. Alert
3. Report
4. K.O.
5. Visualization
6. MLTK
7. Cluster Master.

Components:-

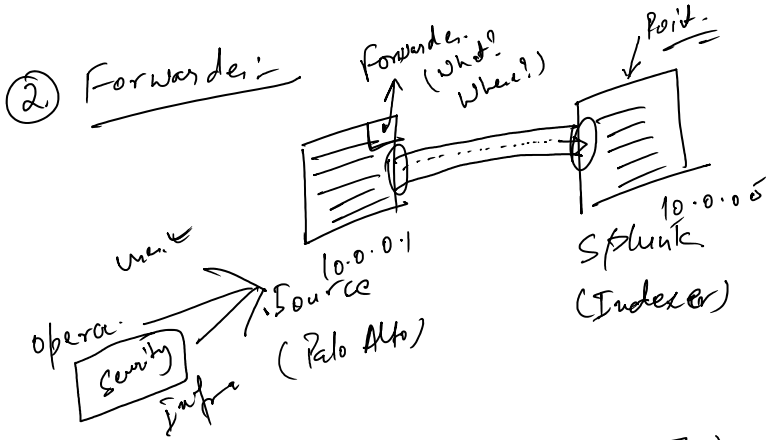
1. Indexer.
2. Forwarder.
3. Search Head.
4. Licence master.
5. Deployment Server
6. Deployer

1. Indexer:- Internal Database to store the data. That is known as Indexer.

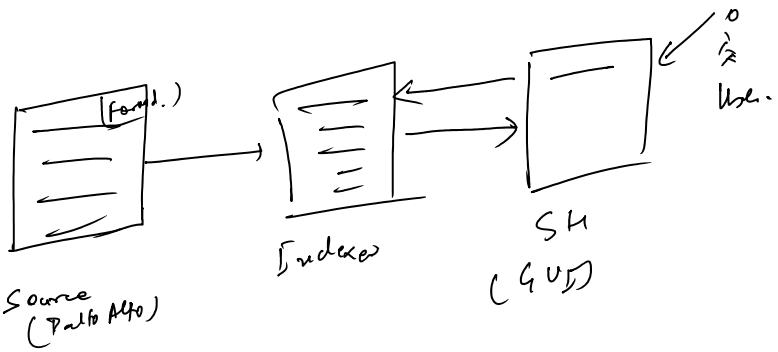




2. Forwarder:-



3. Search Head:-



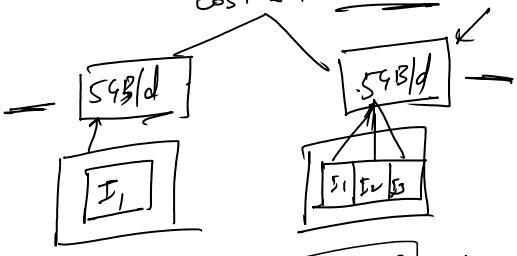
... ...ented in splunk in 1 day.

4. License Master —

Amount of data ingested in splunk in 1 day.

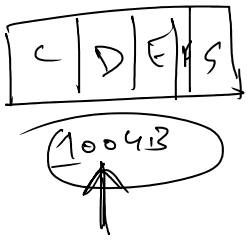
5 GB/day – 1 year → $$$

Cost will be same.

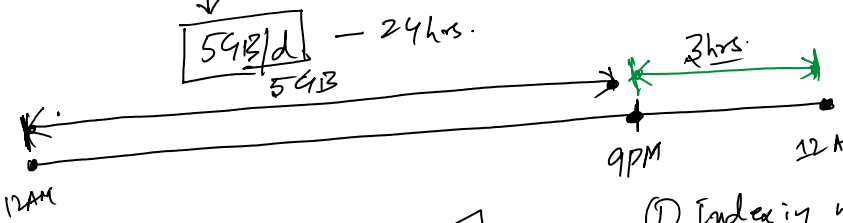


100GB – per GB

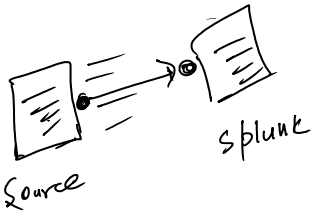
5 GB – per GB



License.



① Indexing will continue.
No searching.



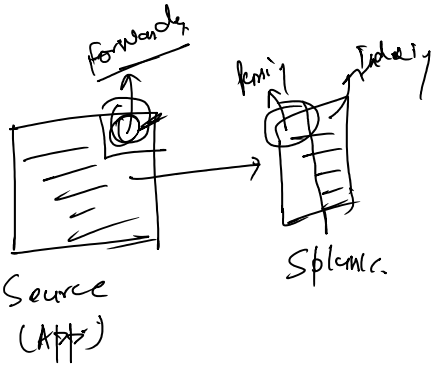
5. Parsing —

Remove the unwanted data.

junk character | issues | gaps | symbols.

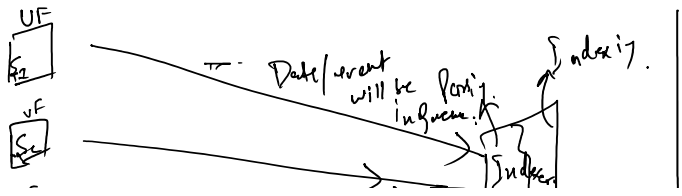
Forwarder → Heavy forwarder

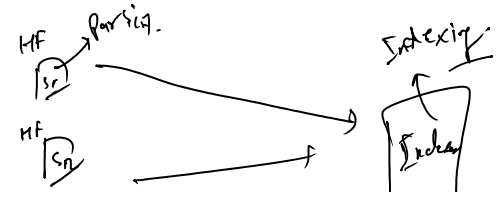
Forwarder → Universal forwarder.

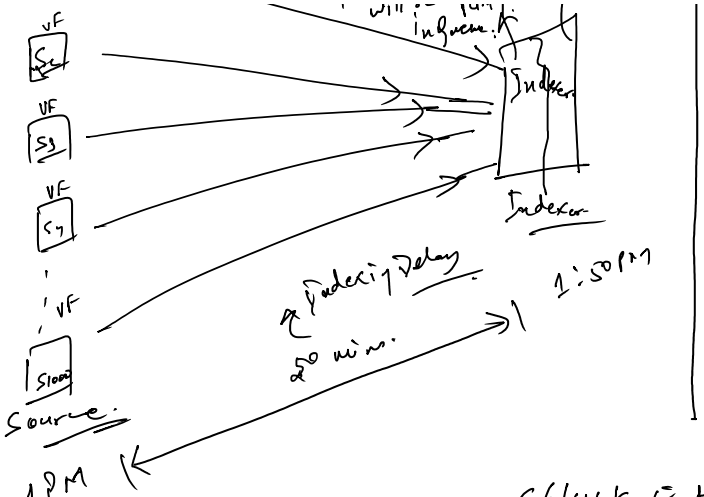


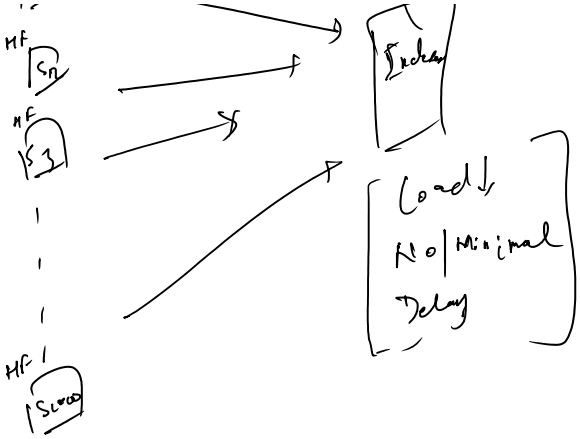
① Parsing → Compulsory
② Indexing.

Universal forwarder → Parsing at indexer.
Heavy forwarder → Parsing happens at Source



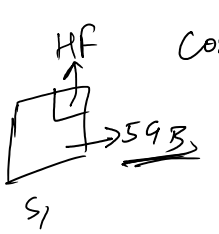




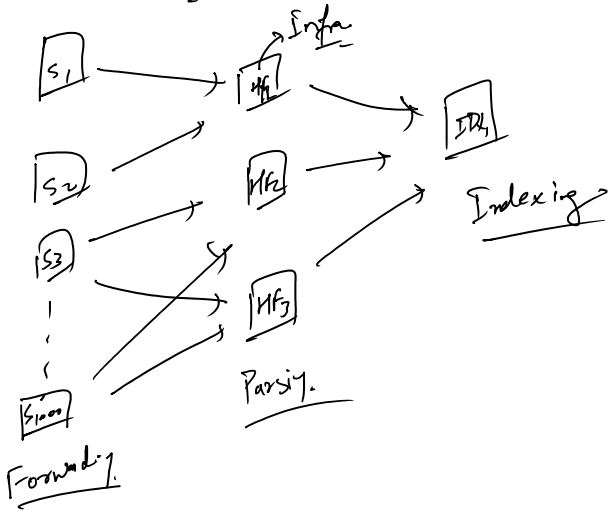


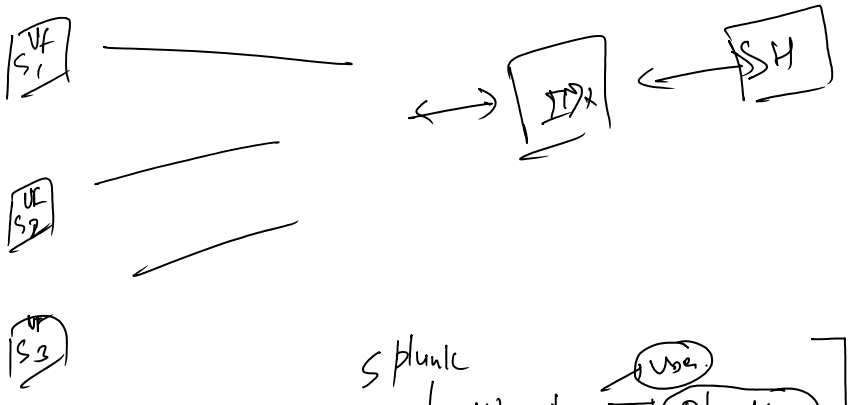
Splunk → Splunk Enterprise → HF, LM, CM, DS, Deployer, SH (5GB)

Splunk → Splunk Uf → UF (512MB)



Hybrid

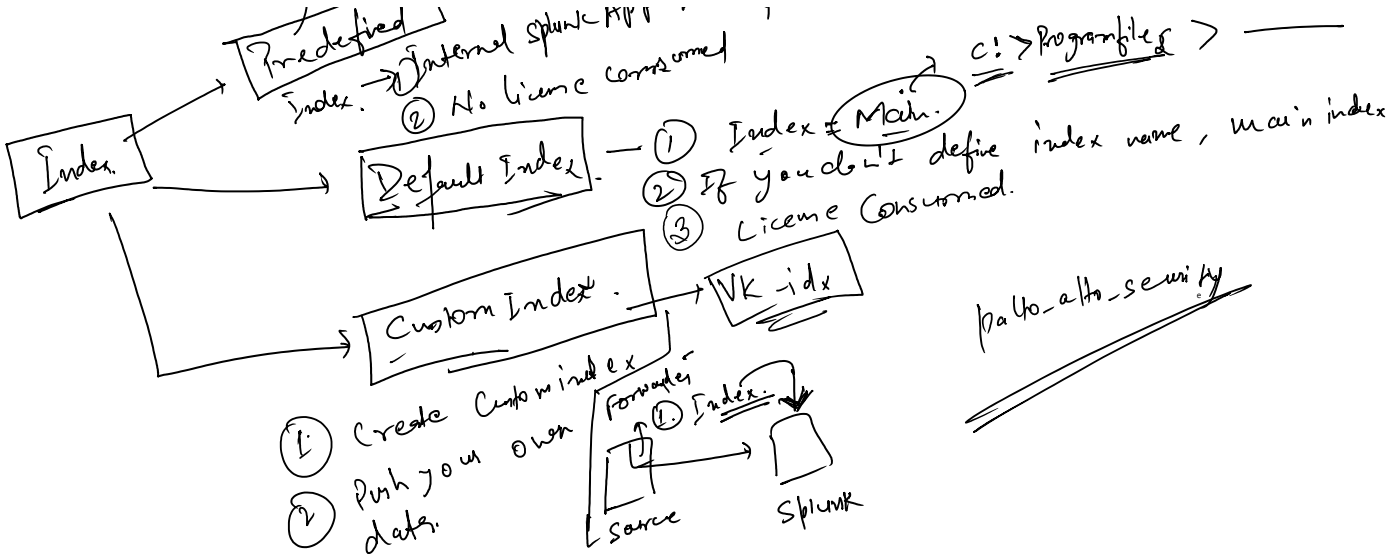


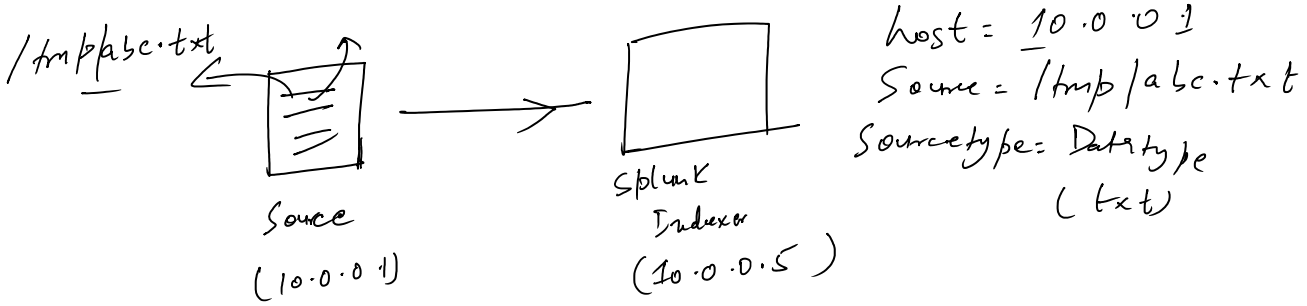


Splunk
└ App → User, Operation, Infra. → Issue

Predefined → Internal splunk App:log → license consumed

c:\> Programfiles >





Searching Mode
- Fast Mode. — fastest searching mode, Event
- Smart Mode — Event + Extraction of fields
- Verbose Mode. — Event + Extraction of fields.
  - Max. Time to Search

Search → Event + Extraction of the fields

SPL (Search Processing Language) :—

1. Table
2. Rename.
3. stats.
4. eval.
5. Top / rare.
6. Time chart
7. chart
8. fillnull
9. Sort
10. Dedup.

(1.) Table:- Tabular output

Ex:- | table f1, f2, f3 - - -

(2.) Rename:- Rename of the fields.

Ex:- | rename old-name AS new-name.

Field name is Case sensitive & field value is case insensitive.

(3) Dedup:- Remove Duplicate Value.

| dedup f1

(4) Sort:- Sort is for sorting purpose. | sort f1

Default → Ascending order.

sort -f1 → Descending

sort +f1 → Ascending

↳ sort f1

(5.) Stats:- Statistical Command:-

(1) Count.
(2) List
(3) Avg.
(4) Sum.
(5) Values.

(1) Count:- | Stats count → overall count.

| stats count by f1

↓

clause you can split the fields.

(2) Sum – | stats sum(f1)

(3) Avg – | stats avg(f1)

(4) List – Group the fields on the basis of certain field.

(5) Value – Group the Unique field values on the basis of certain field.

(6) Eval Command :- Evaluation Activity.

c = a+b

Variable

var c
int c
str c

→ eval c = a+b

(1) Calculation → bytes/1024 → (Kb) → Variable.

Addition.

(2) If-else →

(3) Case statement →

if-else :-

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

if (a>b, a, b)

True / False

Conditional Statement

Case statement :-

Case(1) :-
Case(2) :-

Case(Cond1, "_", Cond2, " ", Cond3, " ", 1=1, "—")

case (2); —

case (3) ; —

!

!

default (—)

1=1, " — ")

↓

Universal Condⁿ.

It will be always be true.

case (byte> — OR bytes< — , " — " ; —)

Top / Rare :—

↗ highest

| top sourcetype.

| rare sourcetype

↓

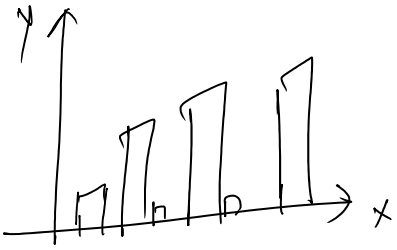
least

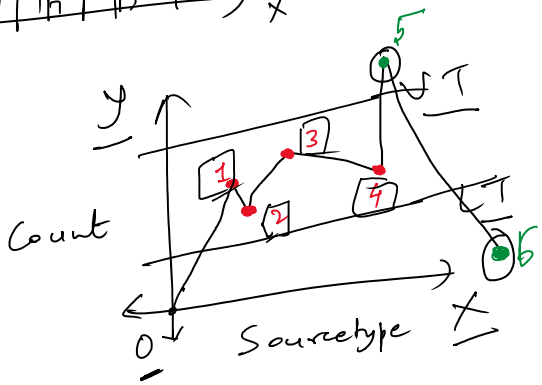
Chart :—

| chart count by sourcetype

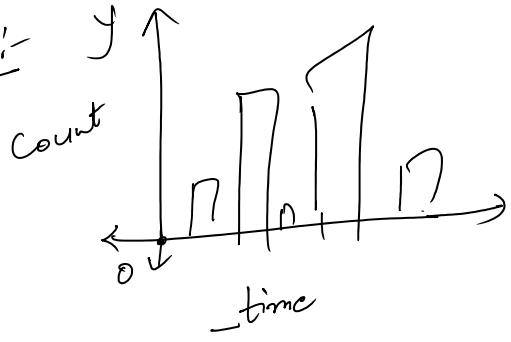
↓ ↓

y-axis x-axis.





Timechart :—



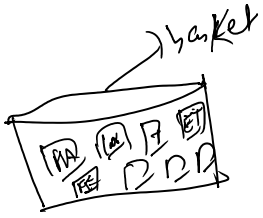
x-axis is reversed for "_time"

y-axis = count/sum/avg.

Single Value Visualization — Single value o/p in graphical manner.

| stats count

- Knowledge object :-



① Tag & Eventtype
② Alerts.

① Tag :- Categorise / Segregate the data.
Sourcetype + firewall
2 new fields generated :-
① tag = search
② tag :: action → search

② Eventtype :- Categorize the set of events.
Eventtype :

③ Alert :-
[Definition] → Name, SQuery, Schedule
[Trigger Condition] → When ? How ?
[Trigger Action] → Email, Mobile, Webhook