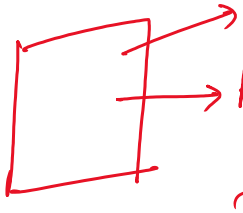
Day - 1

18 March 2025 18:41

① Splunk

Monitoring →



→ up & running.

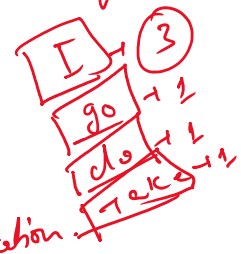
→ Application, User, Security, operational

① Data Warehouse & Datalake.

Ebay

Analysis of data → Search → Output (Insight)

I go I do I take

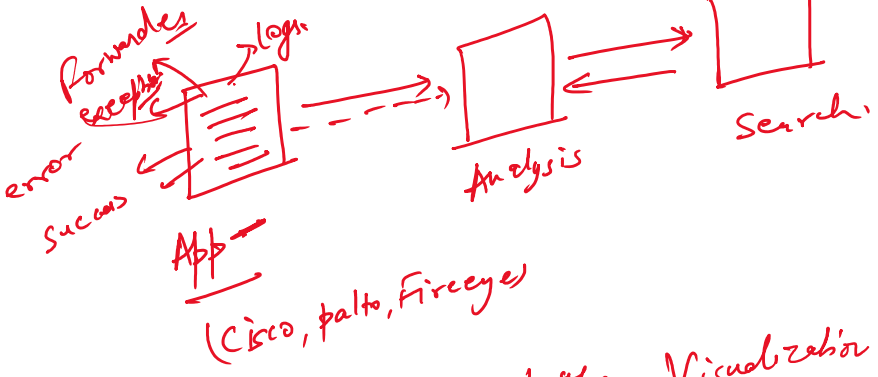


Splunk → Monitoring of data.

① Dashboard
② Report
③ Alert
④ Predication
⑤ MLTK (ML Toolkit)
⑥ Chart

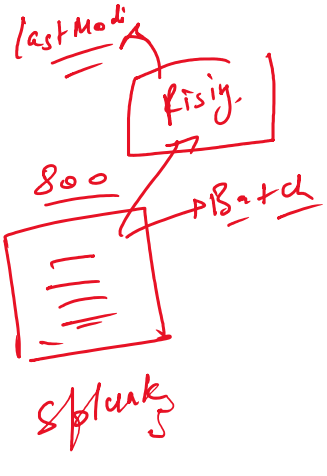
ETL

① Any Source ② Any Type.



(Cisco, palto, Fireeye)

Integration → Analysis, storage, Visualization.



- Customer Support.

Dis:-

Dis:-

1. Cost of splunk license.

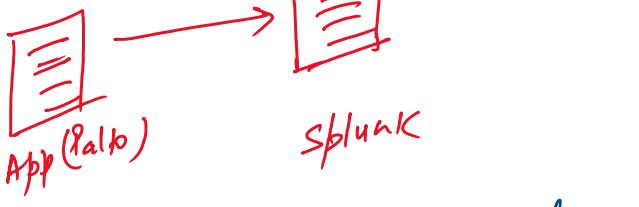
Components:-

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

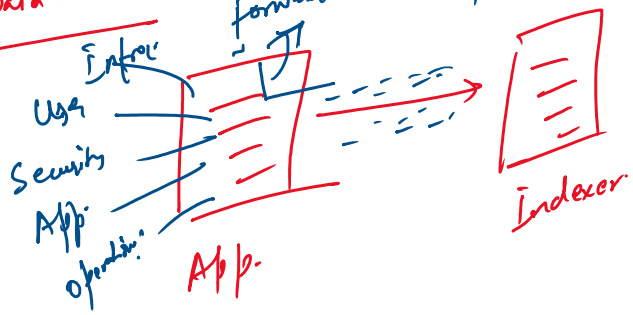
→ Managent Server.

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

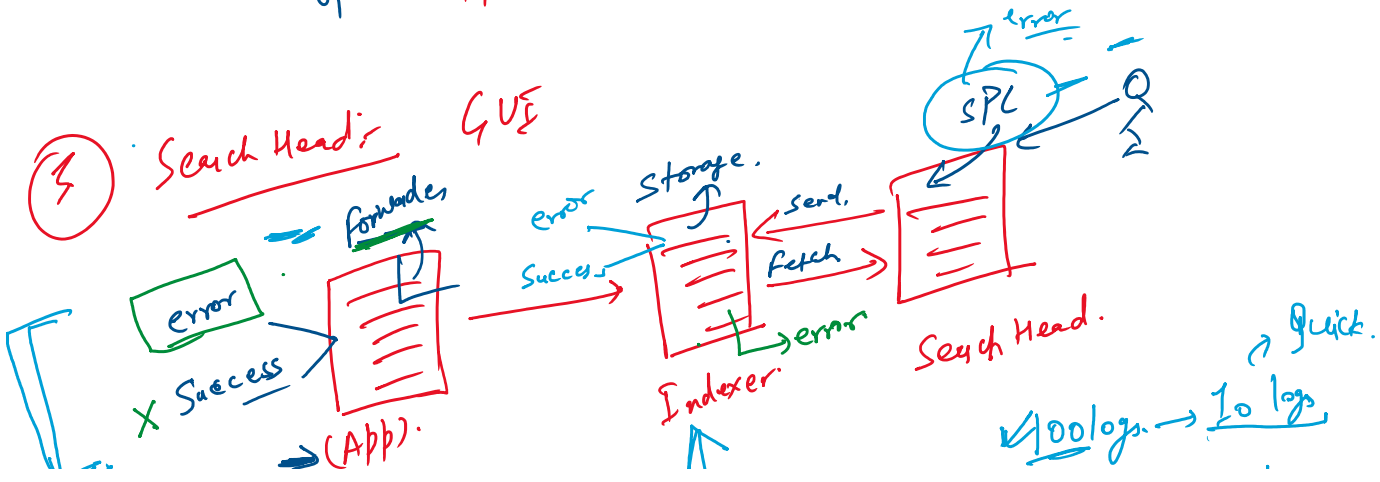
1. Indexer:- Store the incoming data.



2. Forwarder:- Forward the data from the Source to the Splunk end.



3. Search Head:- GUI



X Success

(App). Source

Indexer

Disk space

License.

100 logs → 1o logs

more 1000 logs → 1o logs

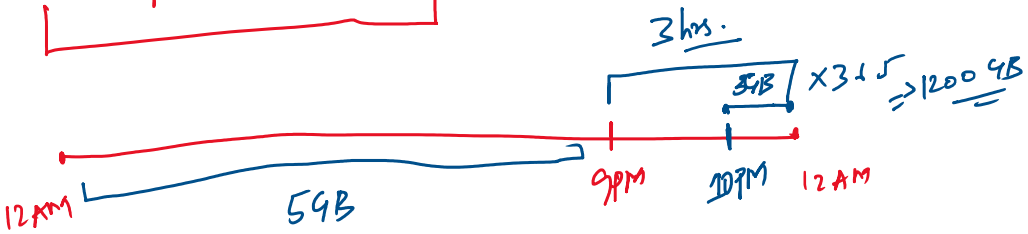
④ License Master — License

↓ Policing Agent that will Make sure that user will be adhering with the License terms.

Amount of data, you ingest on the daily basis.

12AM — 12AM

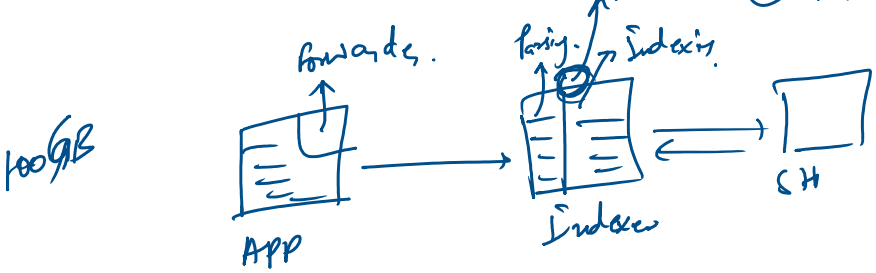
5GB/day → 1year.



5GB/d

① Data is saved.

② No Searching at All.



5 times → 30 day period.

Field Name is Case Sensitive & Field Value is Case Insensitive.

index = main ↵

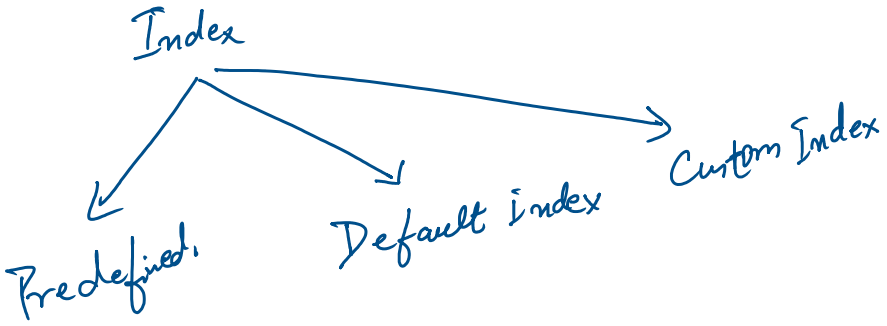
(1) Extract the fields.

(2) Search the number of events.

Fast Mode → 2 (Search the No. of events)

Smart Mode → Extract + Search.

Verbose mode → Smart + Navigate b/w diff. Tabs.



Predefined Index :- _*
_internal, _audit, _introspection,
_telemetry.

- Reserved for splunk App. Specific Data.
- No License Calculated / Assigned.
- Can't index your custom data / App data in this index.

Default Index :- index = main.

C → Program file

→ index = main.

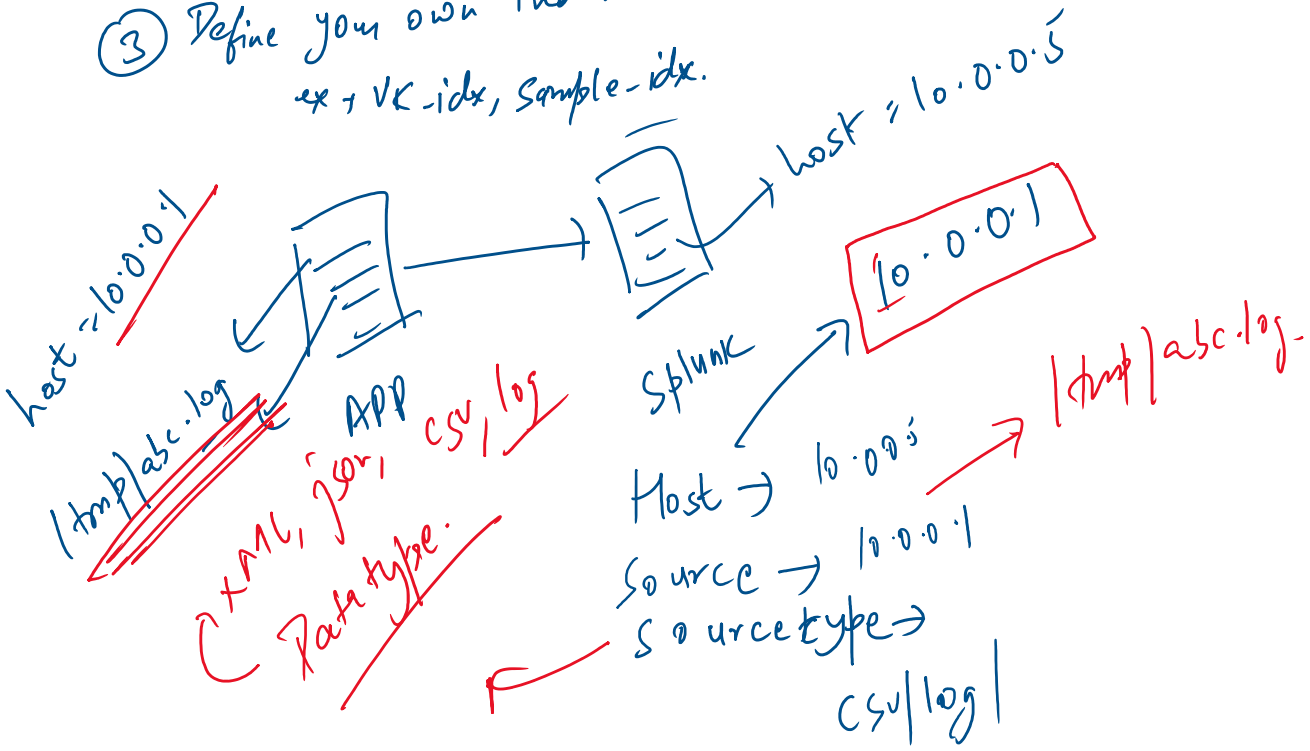
→ License is consumed.

→ Custom / App data.

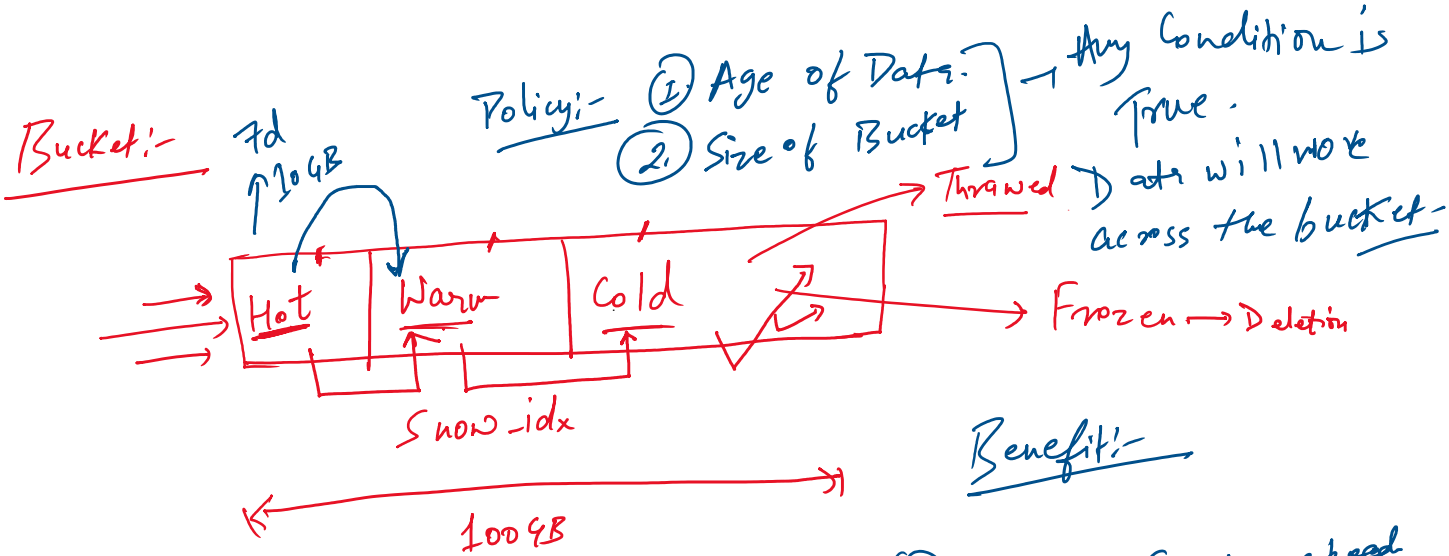
→ License is consumed.
→ Push your own / custom / App. data.
→ if you don't specify the index name, it will go to index = main.

Custom Index:-

1. License Consumed.
2. Push your own / App / Custom data
3. Define your own index.
   ex: VK_idx, Sample_idx.



Bucket:-



Policy:-

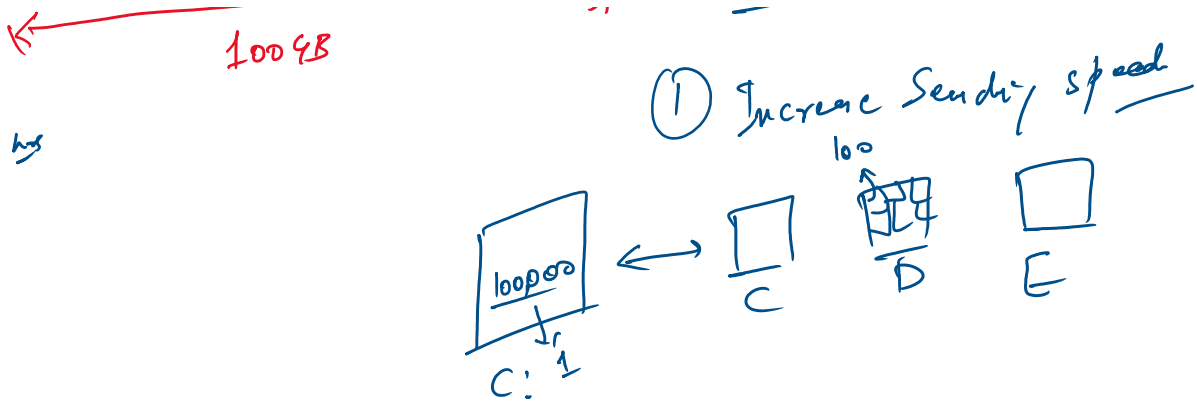
1. Age of Data.
2. Size of Bucket

→ Any Condition is True.

Thawed → data will move across the bucket.

Benefit:-

1. Search Speed



Stats - Statistical output

2. Count - Count of the event in a certain index.
3. Avg.] → stats Avg/sum →
4. Sum
5. List -
6. Values -

Eval:- Evaluation Activity

byte → kb

variable - r(byte/1024) "kb"

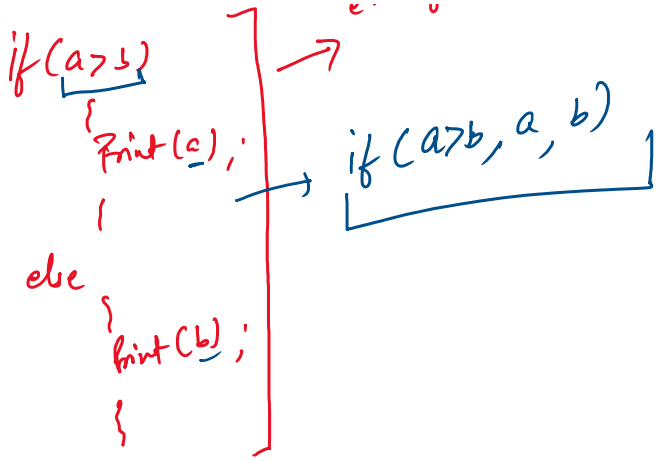
Var a
int ?
str a

1. Conversation →
2. if-else →
3. Case statement →

eval field1 = if (Condition, True, False)

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

→ if(a>b, a, b)



Switch → switch:
case (a) : ——
case (b) : ——
case (c) : ——
default: ——→

① table
② Rename
③ stats.
④ Eval.

⑤ Sort
⑥ Top
⑦ rare.
⑧ dedup.

⑨ chart.

Sort → Sorting purpose.
Default → Ascending Order.
Ascending → + → Sort severity or Sort +severity
Descending Order → "-" → explicitly you need to define.
Sort -severity

Top/Rare:
Top Value — Top — Top 10 Values by default. → Limit
Least Value — Rare. — Least 10 Values by default
3 field returned

3 field returned

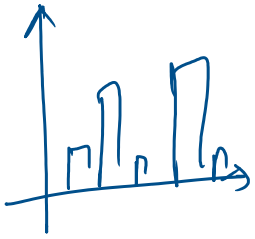
fieldname, Count, Percentage.

limit = 0 → Unlimited Values

Dedup:- Remove the duplicate Value.

| dedup Severity.

chart:-



| chart count by Severity

count → y-axis

Severity → x-axis.