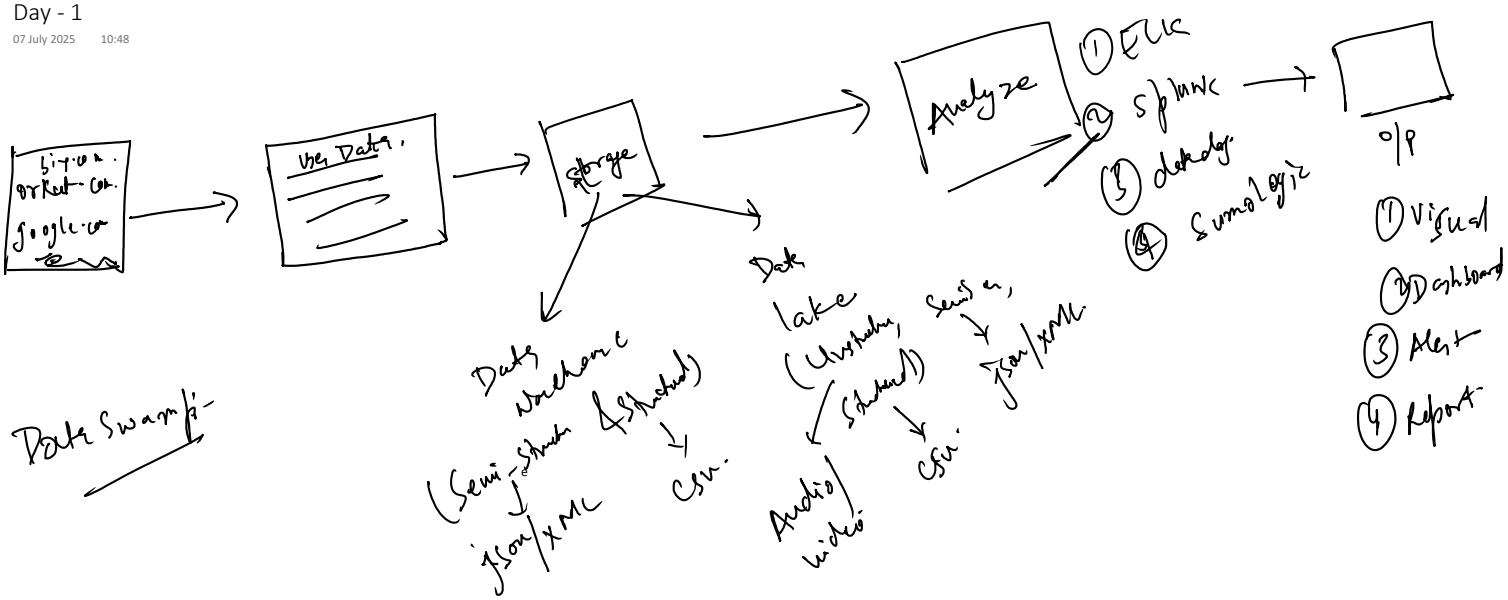
Day - 1

07 July 2025 10:48



1. splunk:- Log monitoring

(1) Dashboard

(2) Alert

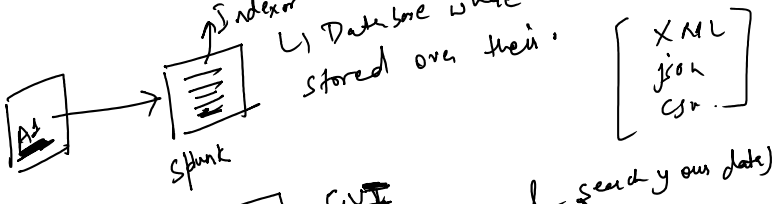
(3) Report

(4) Predictive Analysis

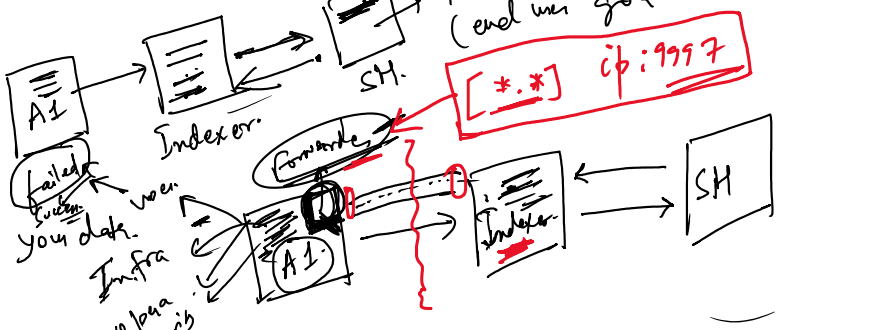
(5) MLTK → Machine learning tool kit.

Component of splunk:-

(1) Indexer →



(2) Search Head:→



(3) Forwarder → Forword your data.

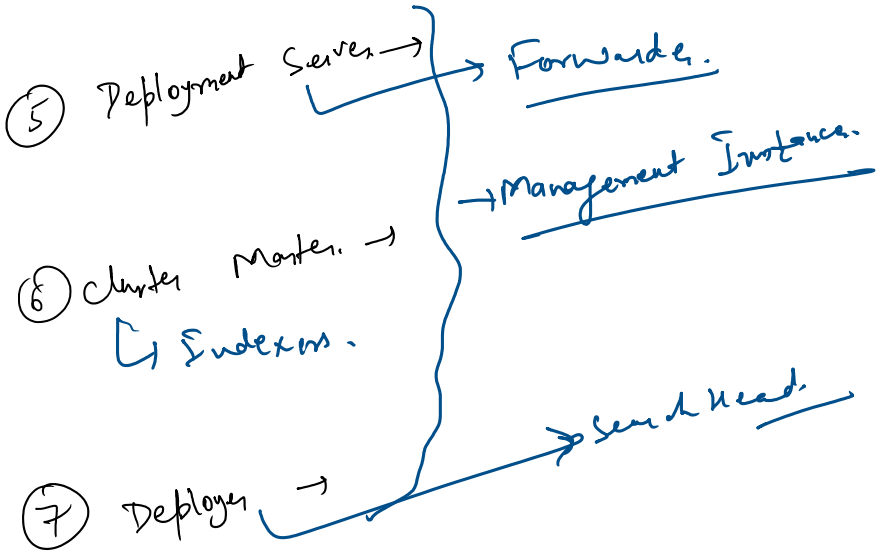
Infra
opsa
security

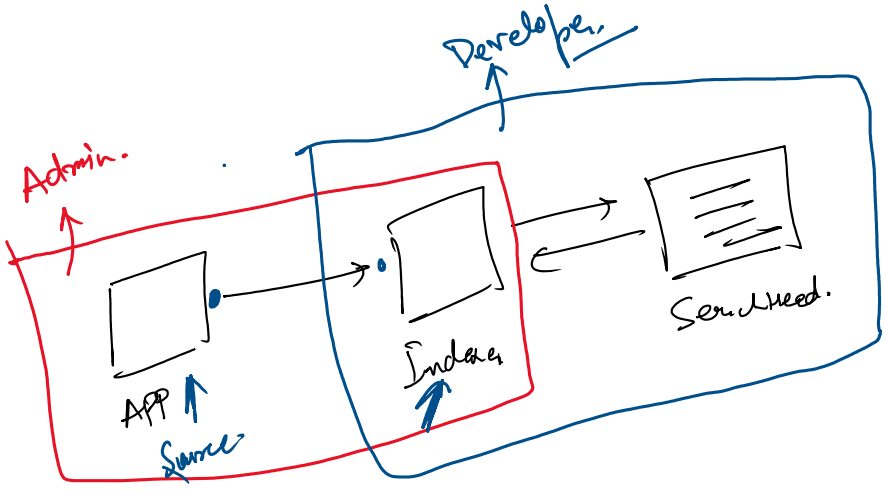
(4) License Master → Not a open source. Pay to splunk to livrage the access

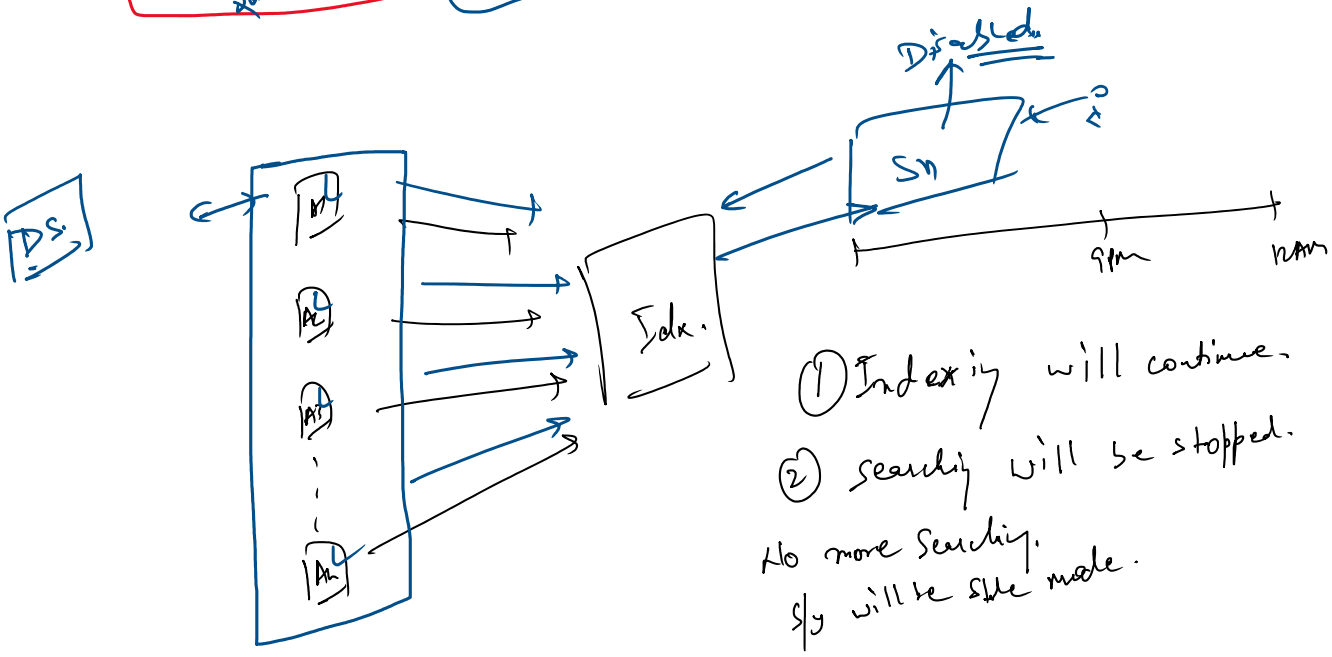
Parameter: → Amount of data indexed on daily basis.

24hr cycle — 12AM — 12AM

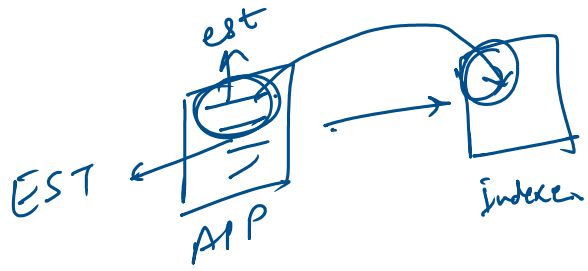
9PM

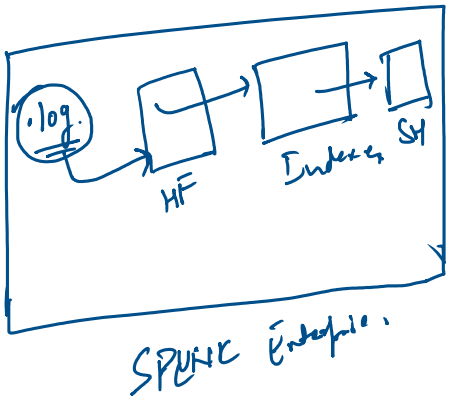

5 Deployment Server
Forwarder.
Management Instance.
6 Cluster Master.
Indexers.
Search Head.
7 Deployer

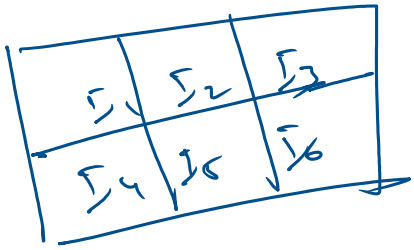

Developer.
Admin.
App
Source
Indexer
Search Head.


Disabled
SH
9pm
DS.
Idx.
1 Indexing will continue.
2 Searching will be stopped.
No more Searching.
SH will be Idle mode.

1. Why?
2. What?
3. P II
4. Ingestion limit







Indexer

→ No license consumed
Push No custom Data.

Reserved for the Splunk logs, N.A. consumed

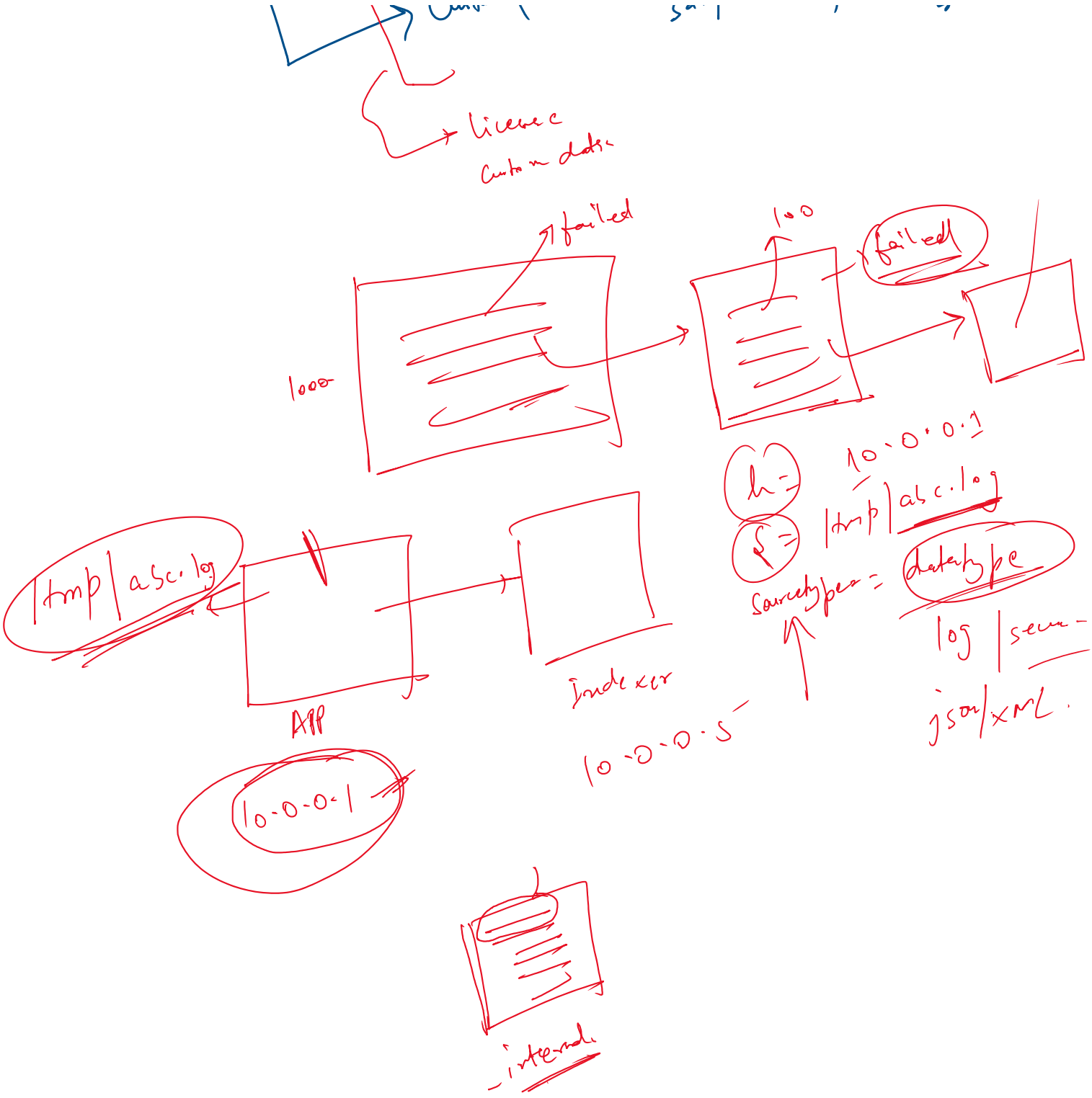
Predefined → * (_internal, _audit, _introspection)

Index → main (Data will go by default)

Default → Push the custom data.

Custom Index → VE-idx
sample-idx.

→ Push custom data license will be consumed



Search your data.

Fast Mode. ✗ — (1) Extraction of field. (2) Searching your events. → 2 step process.

(1) Table → Tabular format.

| table field1 field2 field3 - - -

(2) Rename → change the name of the field

| rename old-name AS new-name.

(3) stats:-

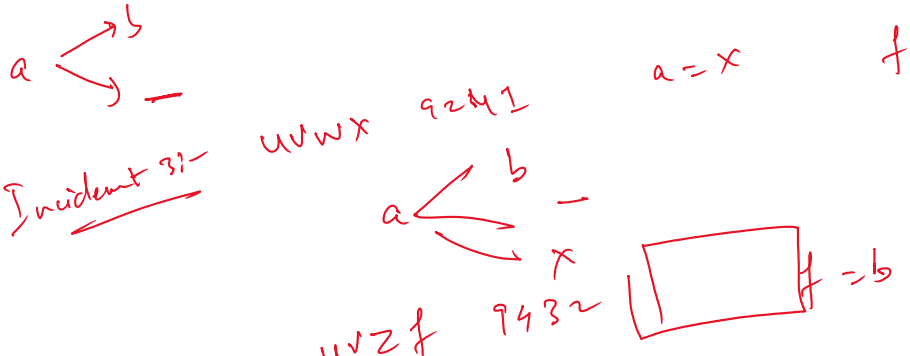
1. Count → count value
2. Sum. → Summation
3. Avg. → Average
4. list → list
5. Values → value.

asset-id: [ ]

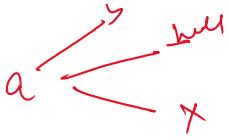
Incident1:- a b c d 1 2 3 4 a=b c=d

Incident2:- x y z f 4 5 7 8 a=- f≠g.

Incident3:- u v w x 9 2 4 1 a=x f=2.



Incident4:- u v z f 9 4 3 2



filldown :-

a	b	C
10	host01	ok
11		Warning
12		Critical
13		
14		

filldown host

a	b	C
10	host1	
11	host1	
12		
13		
14		