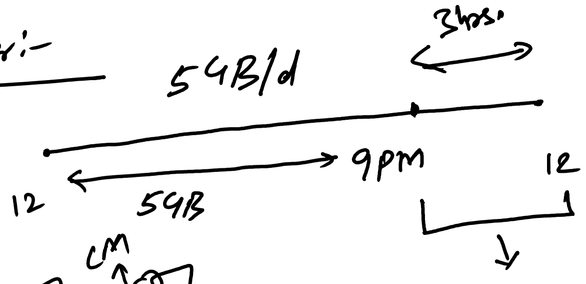
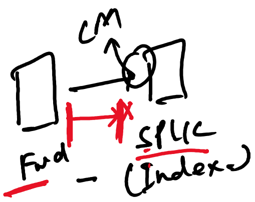
Day - 1

13 January 2025 11:25

① License Master:-



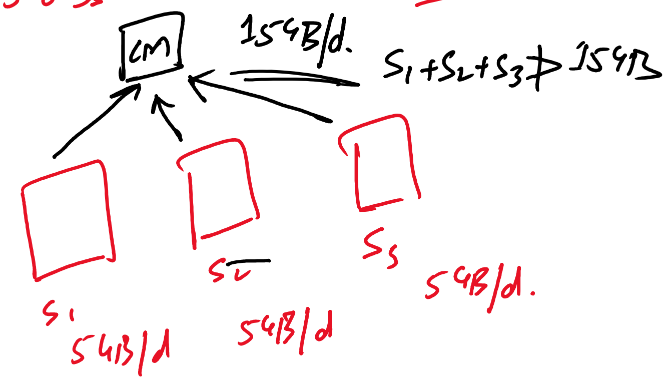


1. Stop the storage
2. Removing of older data.
3. charges will be extra.
4. Lending from the Next day.
5. Carry fowd. for previous day.

1. Indexing will happen.
No Searching.

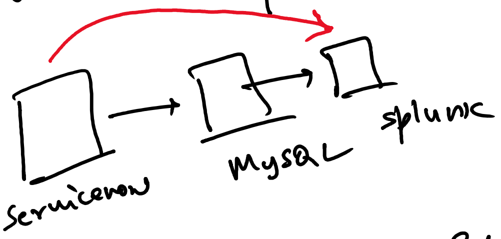
② Max. Voilation of 5 days → window of 30 days.

License Pooling:-

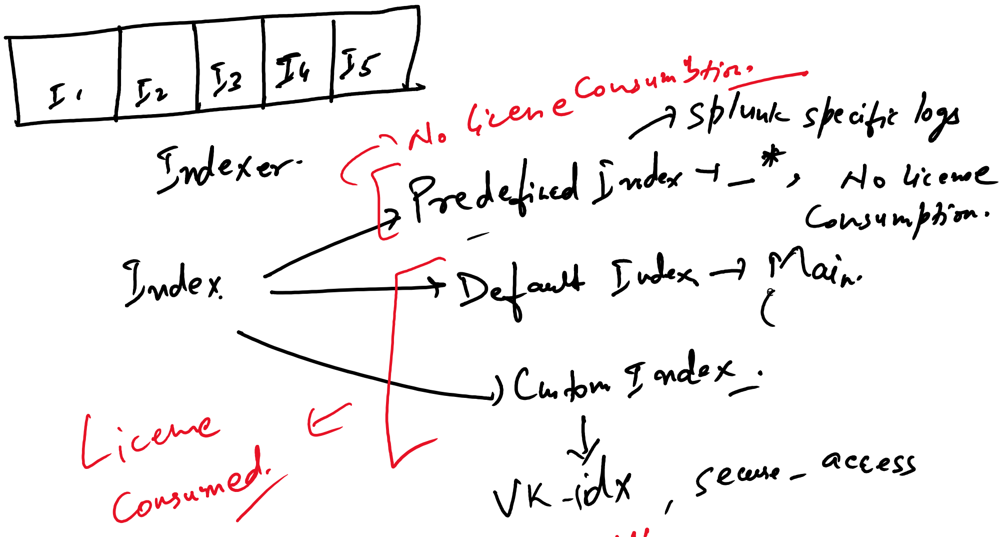


① Splunk Enterprise → Indexer, Heavy fwd, CM, SH, DS, CM, Deployer

② Splunk UF (Universal forwarder)

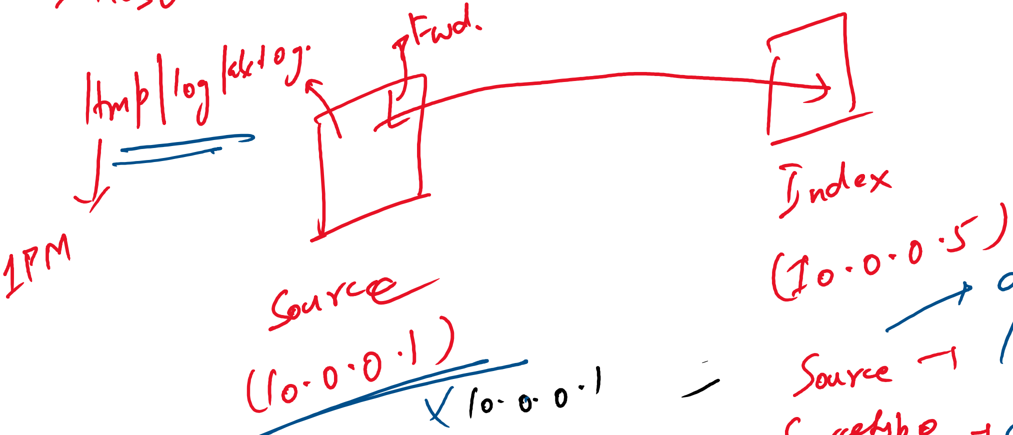


Splunkd	8090
Mang. Port	8089
Web Port	8000
Kvstore	8191
Recieving Port	9997
Collection Port	8088



Default Fields:

1. Source
2. Sourcetype.
3. Host.
4. Index
5. _time.



data Path.

✗ 10.0.0.1	—	Source → /tmp/log/abc.log.
	—	Sourcetype → data type.
✗ 10.0.0.5	—	host → 10.0.0.1
ingestion time.	—	time → Last modified time.
10.0.0.6	—	Index → main / Custom one.

Searching Mode:

1. Fast Mode. → Fastest method
2. Smart Mode. → optimized.
3. Verbose Mode. → Max. time.

③ Verbose Mode. → Max. time.

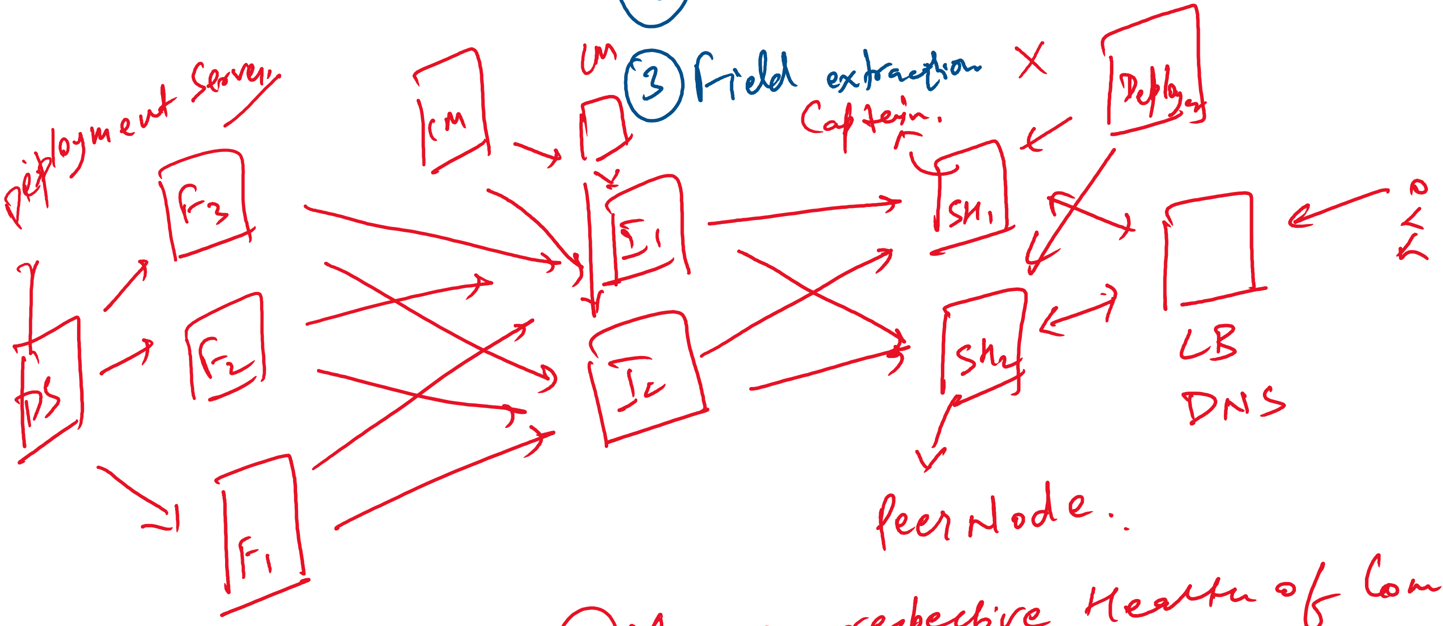
index= _internal :-

① Index ✓

② Pull the event

} Fast Mode.

③ Field extraction X



① Manag. respective Health of Comp.

② Config.