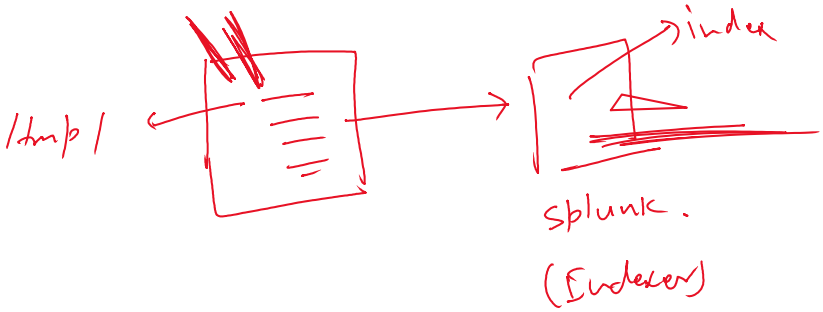
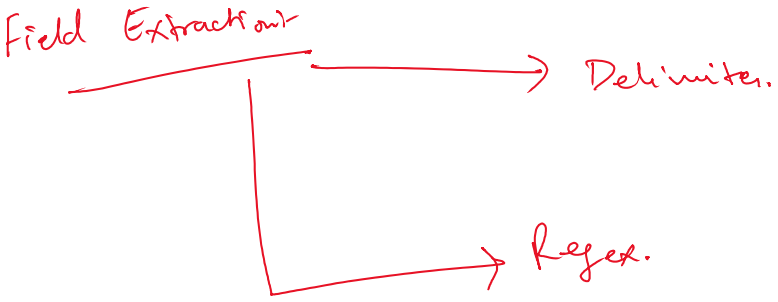
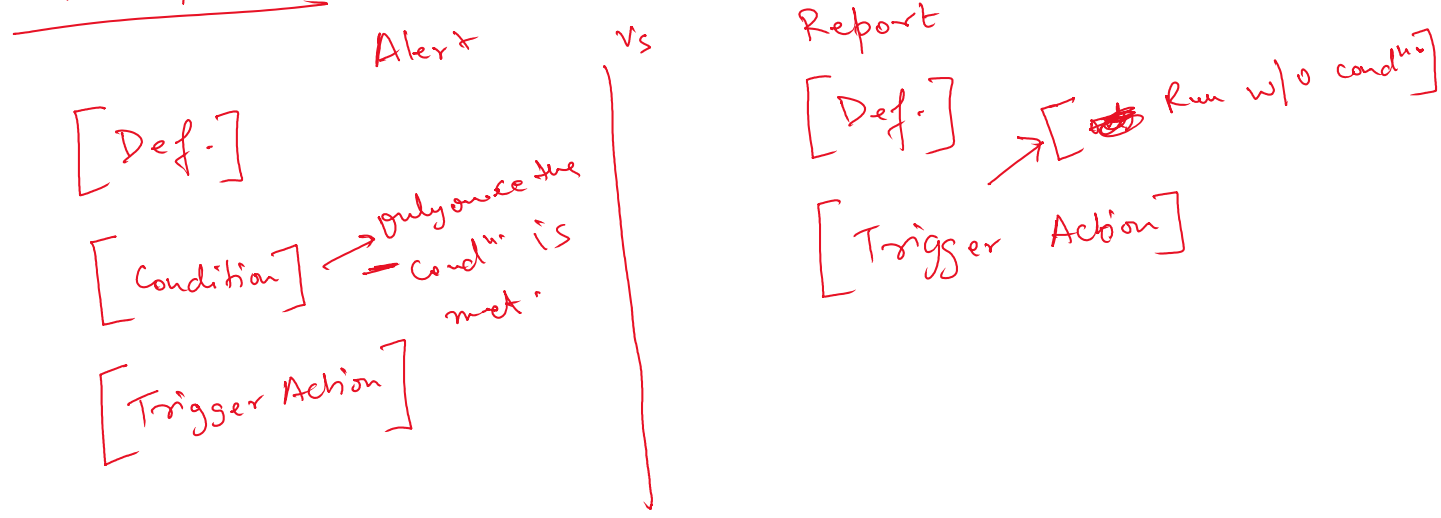
Day - 4

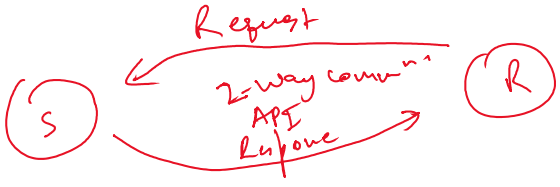
10 July 2025 10:08

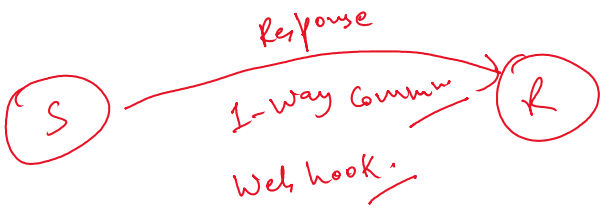


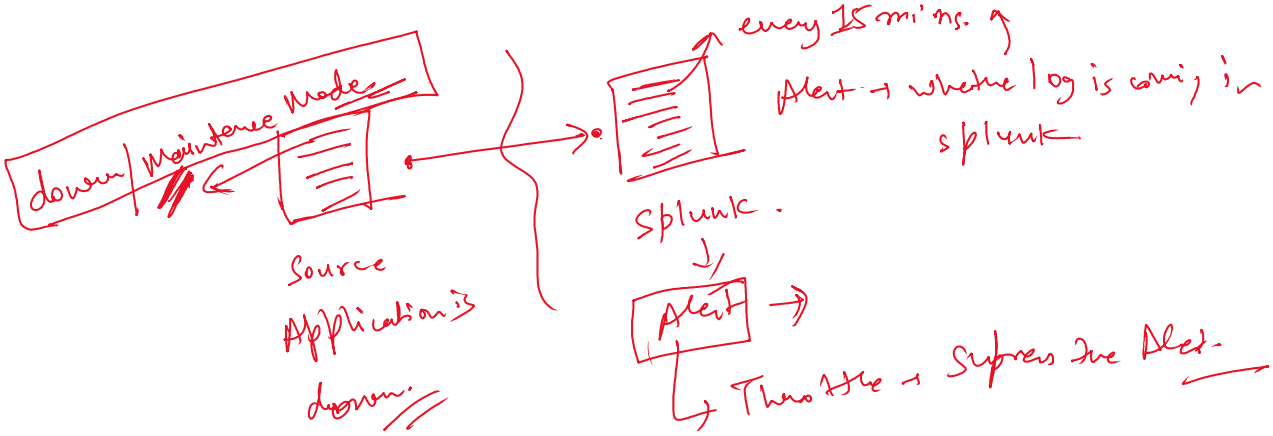


Alert & Reports:-









Data Model & Pivot:-

① Increase your searching speed.

① → Searching → Event
→ Field → Define the field in Advance.

② Hierarchy concept → Root
→ child
→ sc'
→ ssc'

Chart, timechart. → index

Pivot → DM

Transaction:- Categorize the event on the basis of certain condition.

Alert:- ①

Schedule → every 15min.
Data range → last 15min.

① → 5GB → Trigger Alert

Midnight to current time → Data range

11

splunk licence > 5GB → Trigger Alert

check schedule → 30 min.

Data range → current time