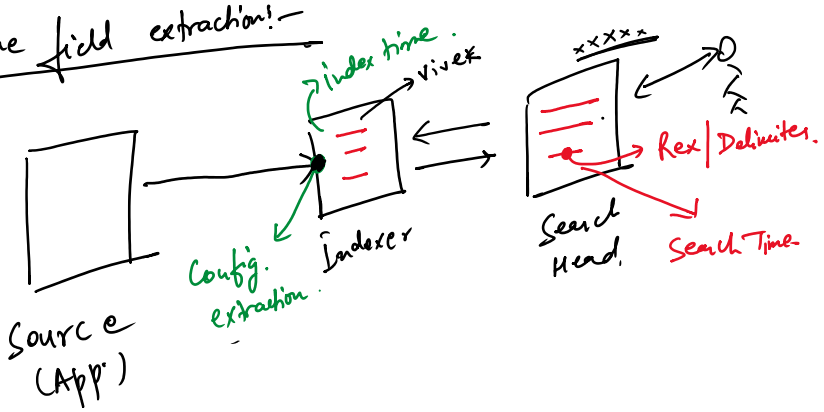
Day - 3

26 March 2025 09:26

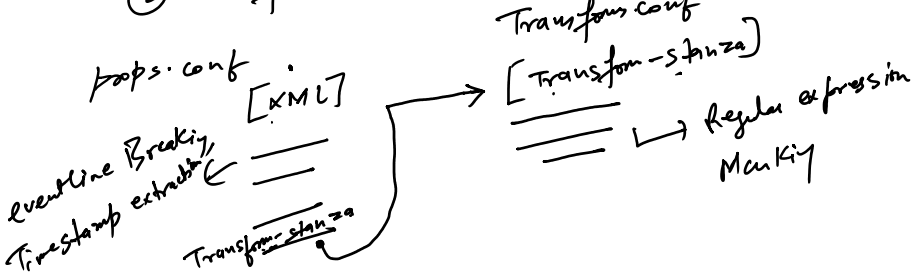
1. Index time field extraction.
2. User & Role Creation.
3. DB Connect ←
4. Syslog.

---

## 1. Index time field extraction:-




1. Props.conf
2. Transforms.conf




|

**Step-1:-** Props.conf → eventline breaking

step2:- Write the regular expression.

Step3:- Transforms.conf.

step4:- Calling Mapping stanza from Props to transforms.conf.

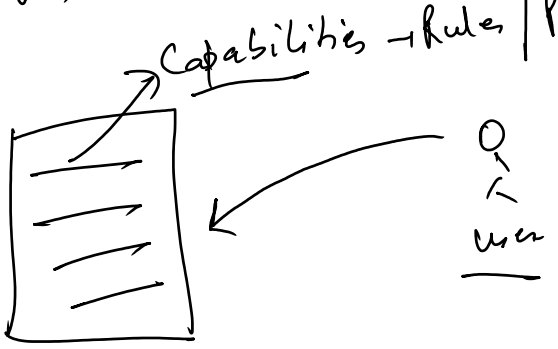
Step5:- Purity of data to validate.

## 2. User & Role Creation:-

(1) Admin

(2.) User & [illegible]

(1) Admin
(2) Developer
(3) User

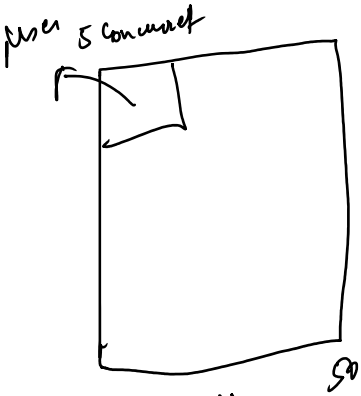



Role.

(1) Admin.
(2) User
(3) Power

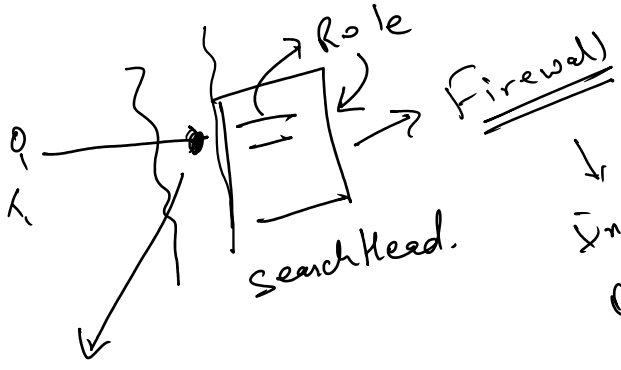
(4) can-delete → Delete the log from splunk.

*** Even Admin don't have delete privilege by default



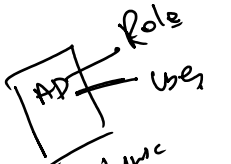

SH

SOCB → Dispatch
10 Concurrent search




Inbound – IP, Port
Outbound – IP, Port

→ Role → User




Portal →

SSO

LDAP → AD → Role → User

IAM Portal — Splunk

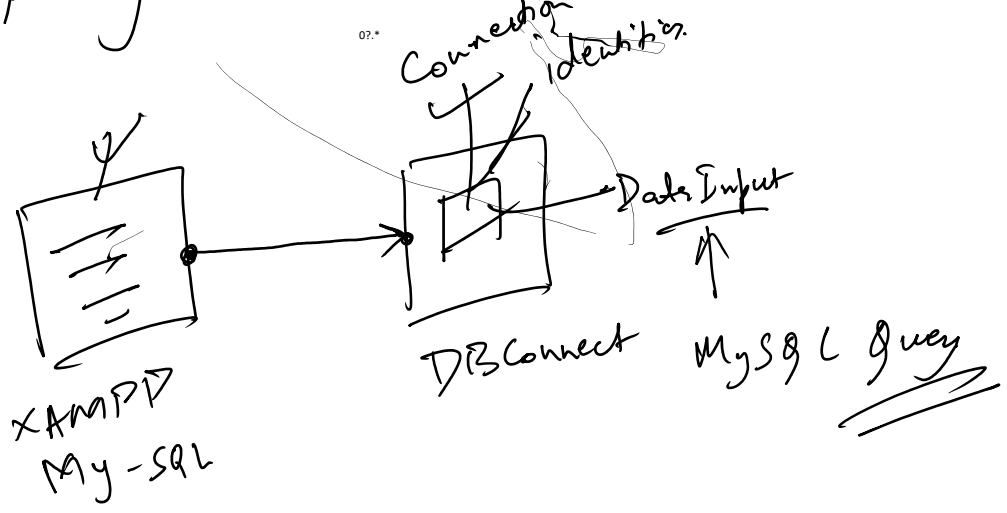
③ DB Connect

① DB Connect App.
② Driver.
③ JRE - 17

④ XAMPP - MySQL
↓
Linux.

① Identities.
② Connection.
③ Data Input

→ DB Connect App.




Data input → Batch.

Data input → Risky column. → checkpoint

↓

every 5 min → → 1 2 3 4 5