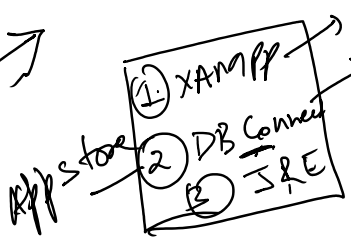
Day - 2

25 March 2025 09:29

1. HEC Token.
2. Scripted Input.
3. Event Breaking.
4. Timestamp Extraction.
5. Apps & Add ons.

Assigment:-

1. XAMPP server installation.
2. JRE installation.
3. DB Connect App Installation.
4. MySQL Driver Setup.



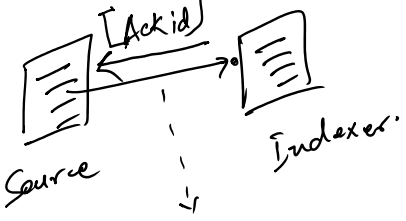
MySQL
Version of JRE

4. Driver → DB Connect
J/ mysql .jar → J/ Driver .jar

---

1. HEC Token:- Http Event collector.
   - ↳ Unique token.
     - ↳ Application Owner.
       1. Token
       2. URL
       3. index

1. Normal
2. Enable Indexer Acknowledgement.

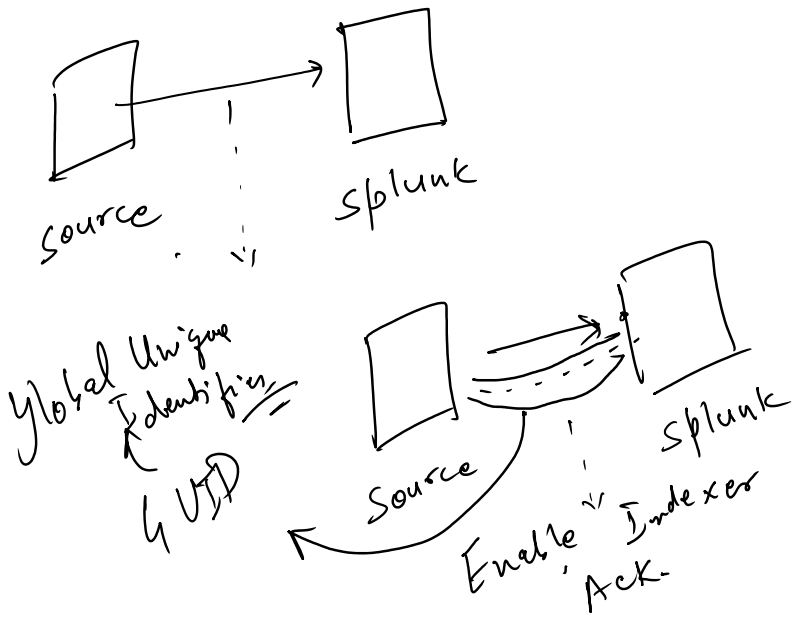


Indexer - [Server-2]

8000 - Splunk Web
8089 - splunkd
8088 - Collector

9997 - Reciever port No.
80 - Http

8191 - KV store



(2.) Scripted Input:-

Python Script (.py)

→ Path (Script)

bin folder.

(3.) Apps & Add-ons

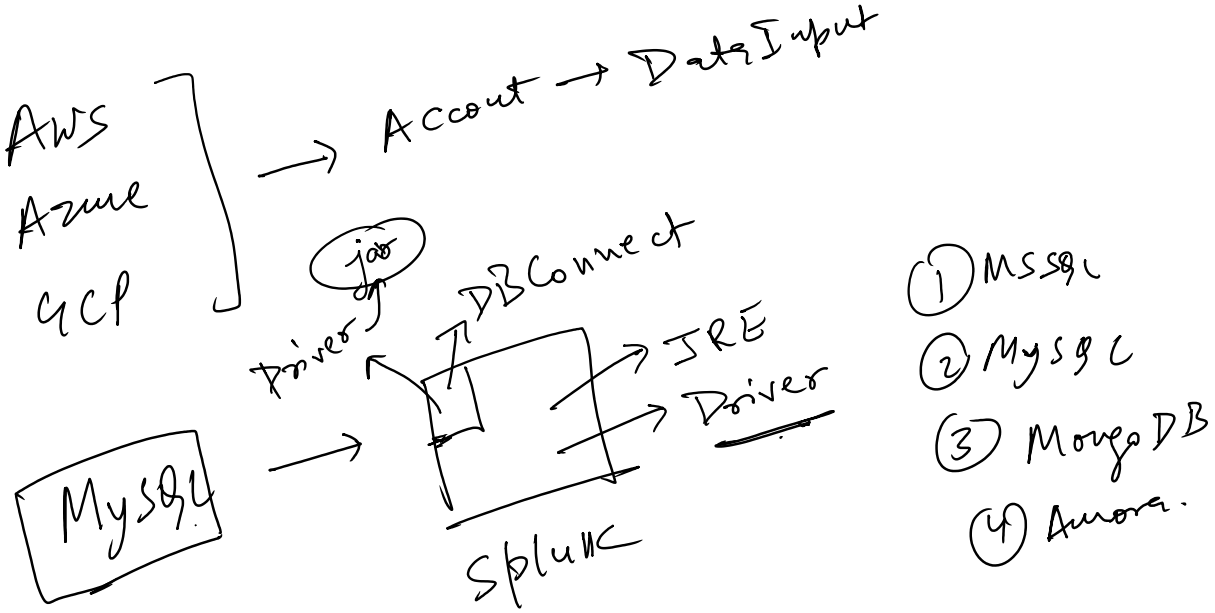
App + Splunk Appstore

→ URL, Username, password

→ what??

↳ What :-

Your instance URL:https://dev309421.service-now.com
Username: admin
Current password: A$l!z0rq7NWR



4. Event line Breaking :-

CSV → Rule → Break data & filter/extract events.

json →
xML →
apache-error →
syslog →

Raw dataset → How to write rule

Key words :-

1. Break_only_before. →

2. Must_break_after →

3 Time_Prefix →

4 Time_format →

5 Max_time_lookahead →

6 Max_time_hence. →

7 Max_time_ago →

8 Must_not_Break_before →

props.conf → Breaking & Stuching of the events.