Day - 10

16 January 2026 09:19

1. Studio - Savedsearch.
2. splunk Roles.
3. SplunkBase App.
4. Linebreaking & timestamp extraction.
5. Uf vs HF.
6. Inputs.conf

Splunk Roles:-

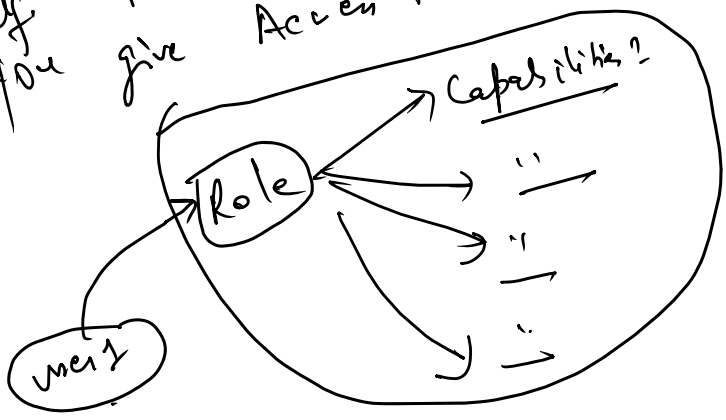
1. User. → Basic write. Read/ Access only to your KO
2. Power. → Default roles
3. Admin. → overall Acces.
4. Can-delete → Acces to delete the data from index.

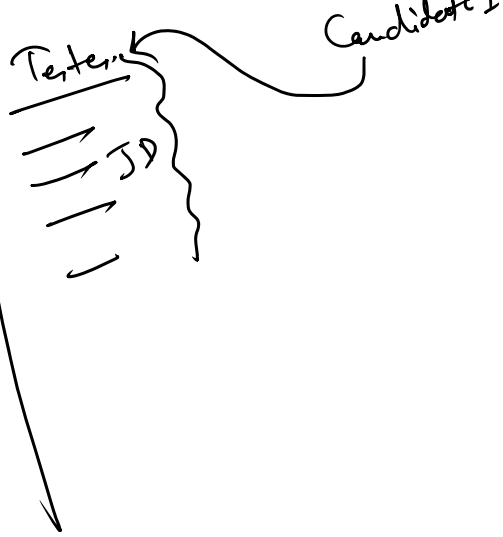
Admin don't have the can-delete access by Default

↓

explicitly Add the role itself

You give Acces to Role, not to user.





Splunkbase App:-

splunkbase

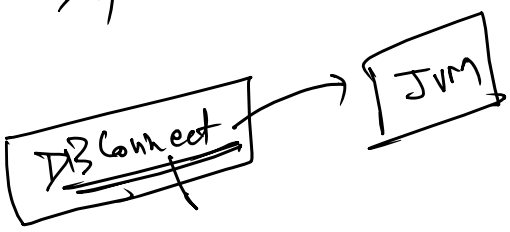
1. Splunk Enterprise / Splunk Cloud.
2. Universal splunk

② Version of splunk

③ Who has create the app?

- Splunk LLP
- Palo / Microsoft
- Individual Developer.

④ Dependent App.



① Version of JVM.
② Version of splunk
③ Drivers support.

Line Breaking & Timestamp extraction:-

Line Breaking:-

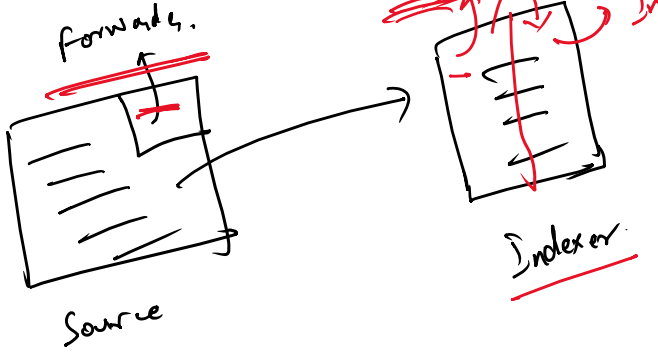
① Break_only_before.
② Line_Breaker.
③ Must_Break_after
④ Must_not_break_before.
⑤ MAX_DAYS_AGO

Timestamp:-

① Time_format.
② MAX_TIMESTAMP_LOOKAHEAD
③ MAX_DAY_HENCE
④ TIME_prefix

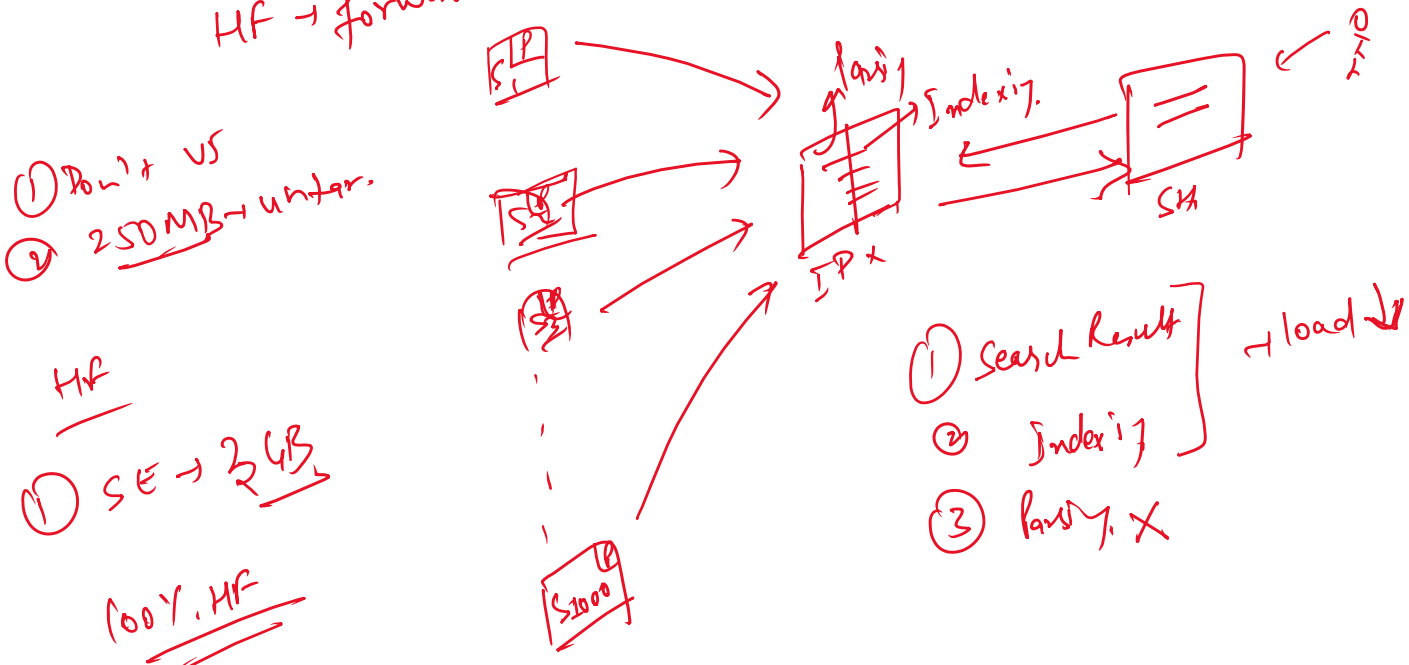
Parsing:
① Remove the unwanted data.
② Delete the corrupt data
③ You can also ignore the specific data.
Indexing

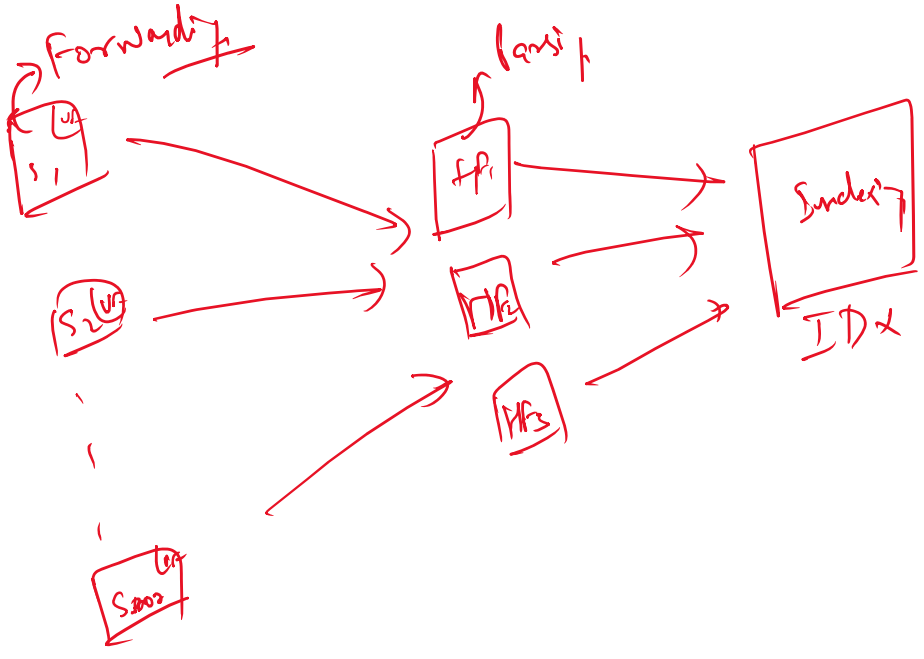
UF vs HF !

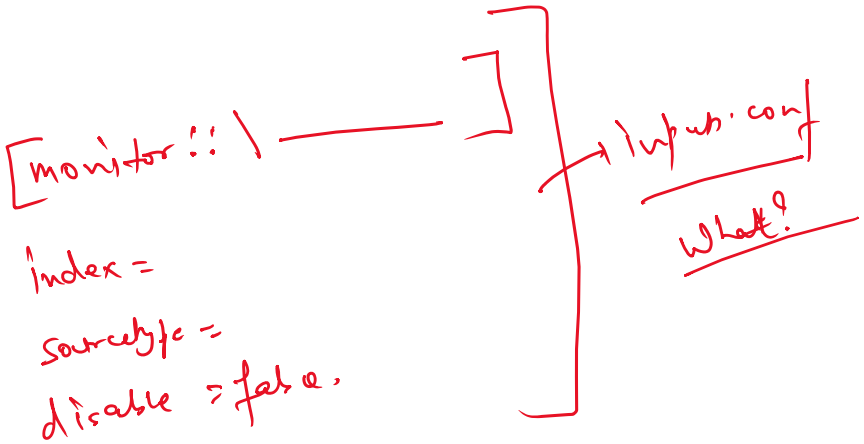


UF → forward the data but no parsing.

HF → forward the data, As well as parse it too.







Splunk certifications :-

→ optional.
→ foundational.

1. splunk certified core User → MCQ
2. splunk Certified Power User
3. splunk Certified Admin
4. splunk certified Architect

50 Question
↳ Pearson. → Centre
↳ Home.

70%

Result at same time. ← 35 question → right.
15 question → attend wrong