Day - 10

16 January 2026 09:19

1. Studio - SavedSearch.
2. Splunk Roles.
3. Splunk Base App.
4. Linebreaking & timestamp extraction.
5. VF vs HF.
6. Inputs. conf

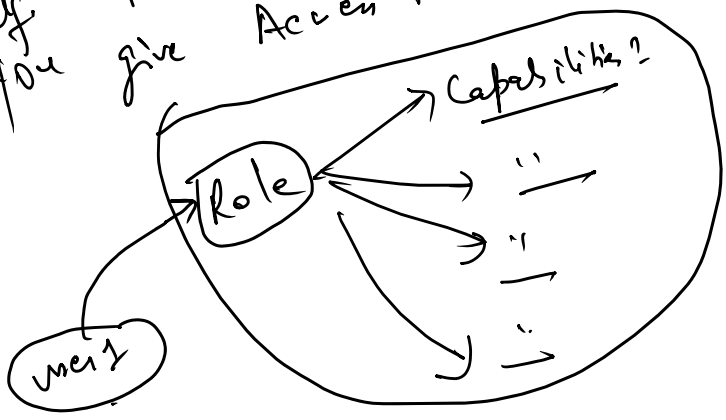
Splunk Roles :-

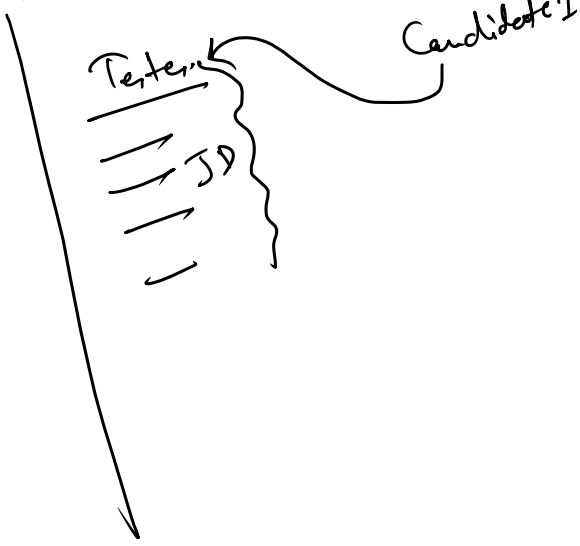
1. User. → Basic. Read/write. Access only to your KO
2. Power. → Default roles.
3. Admin. → Overall Access.
4. Can-delete → Access to delete the data from index.

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

explicitly Add the ~~Acc~~ Role itself

You give Access to Role, not to user.





Splunkbase App :-

splunkbase

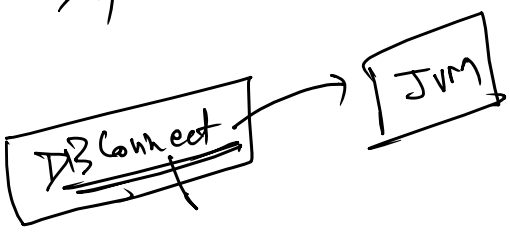
1. Splunk Enterprise | Splunk Cloud.
2. Version of splunk

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:

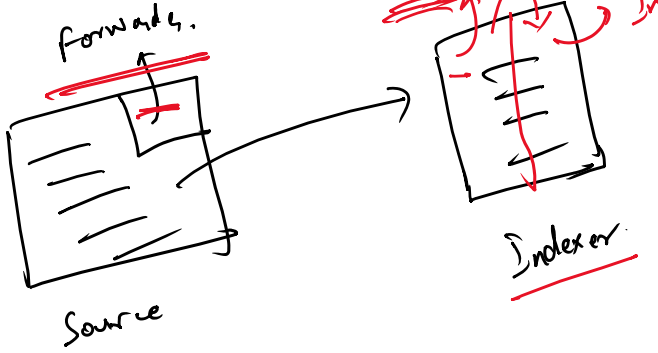
① Remove the unwanted data.

② Delete the Corrupt data

③ You can also ignore the specific data.

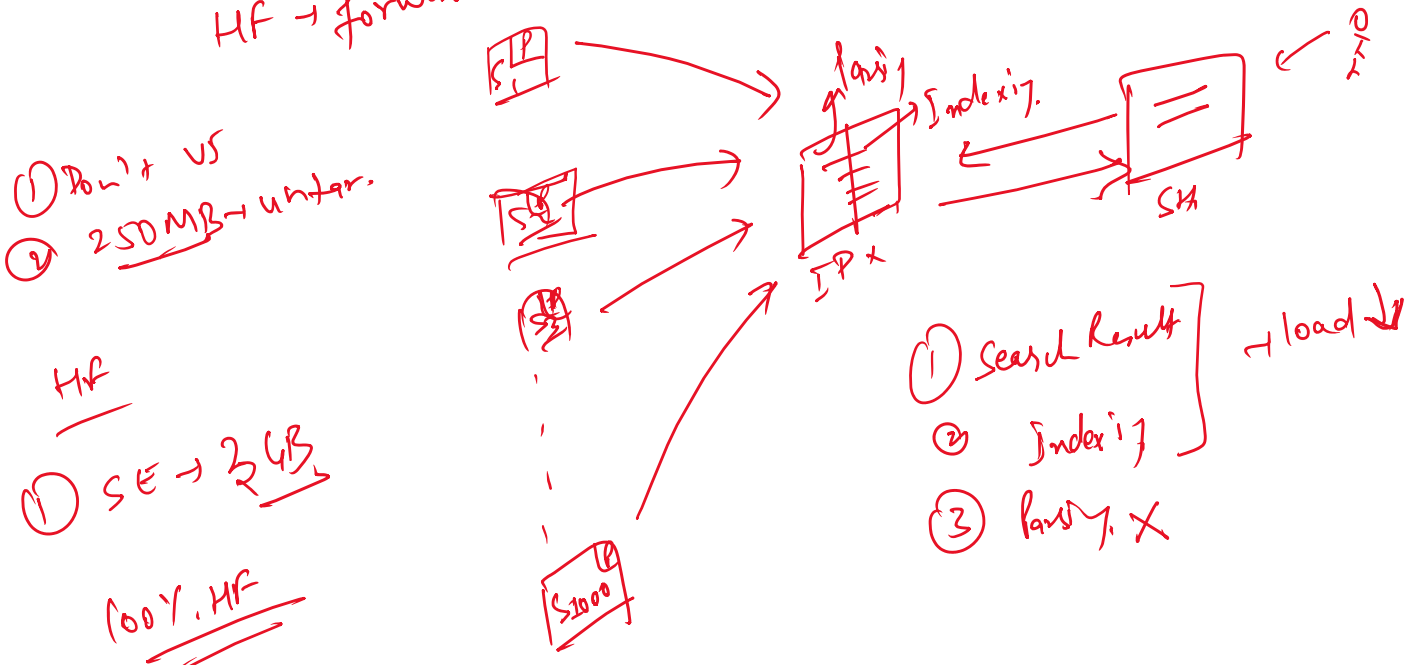
Indexing

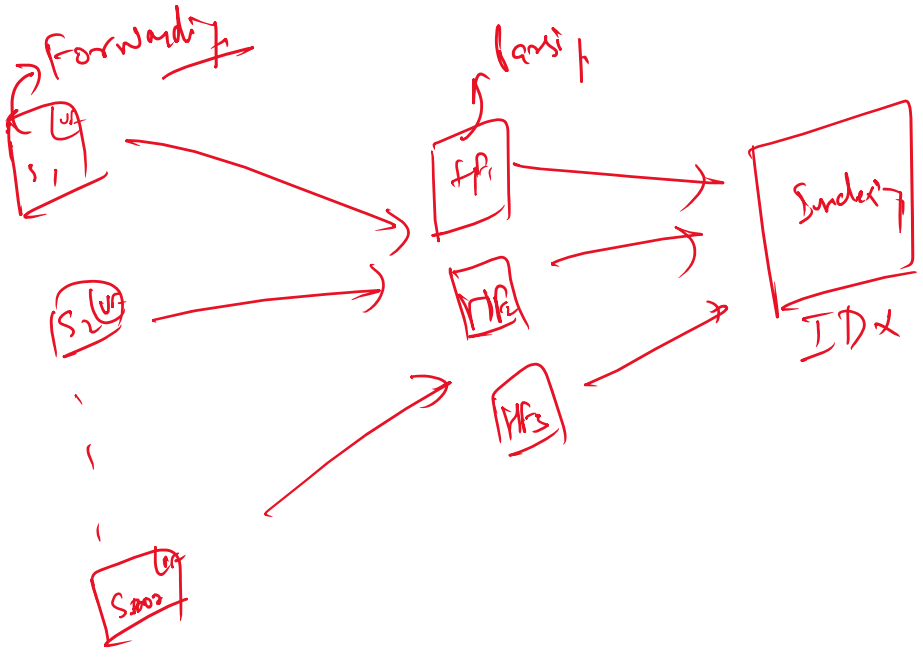
UF vs HF !



UF → forward the data but no parsing.

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





[monitor :: \ ———]

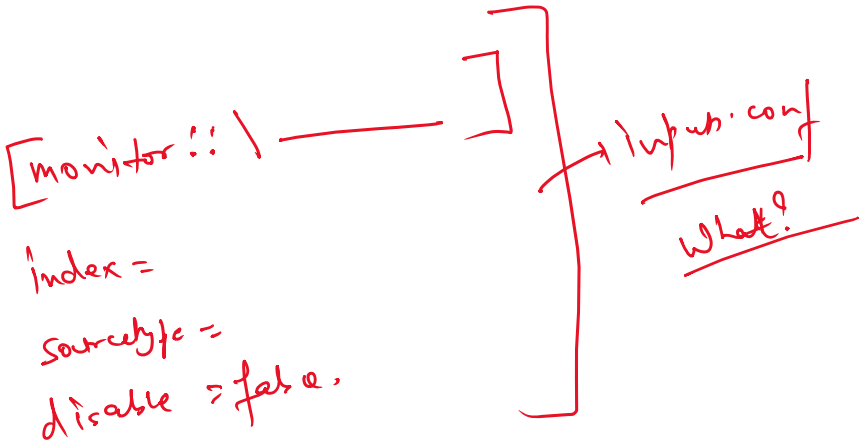
index =

sourcetype =

disable = false.

→ Inputs.conf

What?



Splunk certifications :-

1. splunk certified Core Users → optional. → Foundational.
2. splunk Certified Power User
3. splunk Certified Admin
4. splunk Certified Archiect.

50 Question → MCQ

↳ Per ason. → Centre, ↳ Home.

↓

70%

↓

35 Question → right.

15 Question → afford wrong

Result at same time. ←