Training – Day #8

15 June 2023 06:14

#Event Breaking

Define at what point the one event can break into multiple.

Source type = type of data

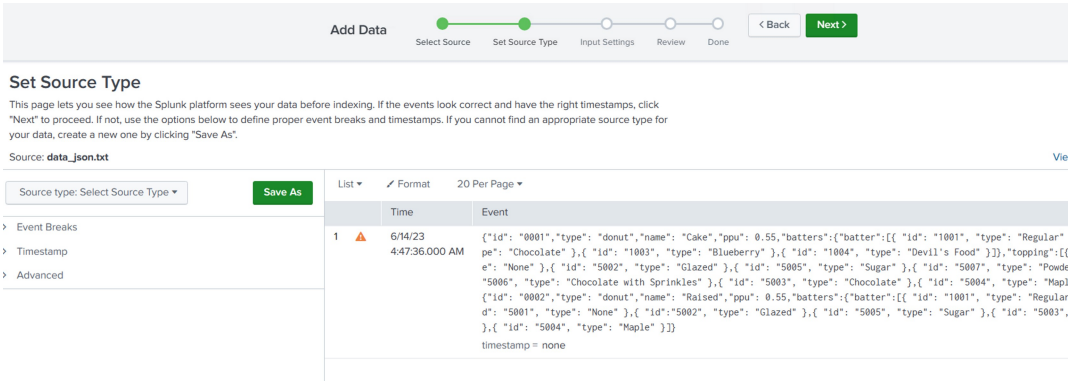
If some events patterns are not clear and if we want to split the event from a particular position, then we use "Event-Line Breaking"

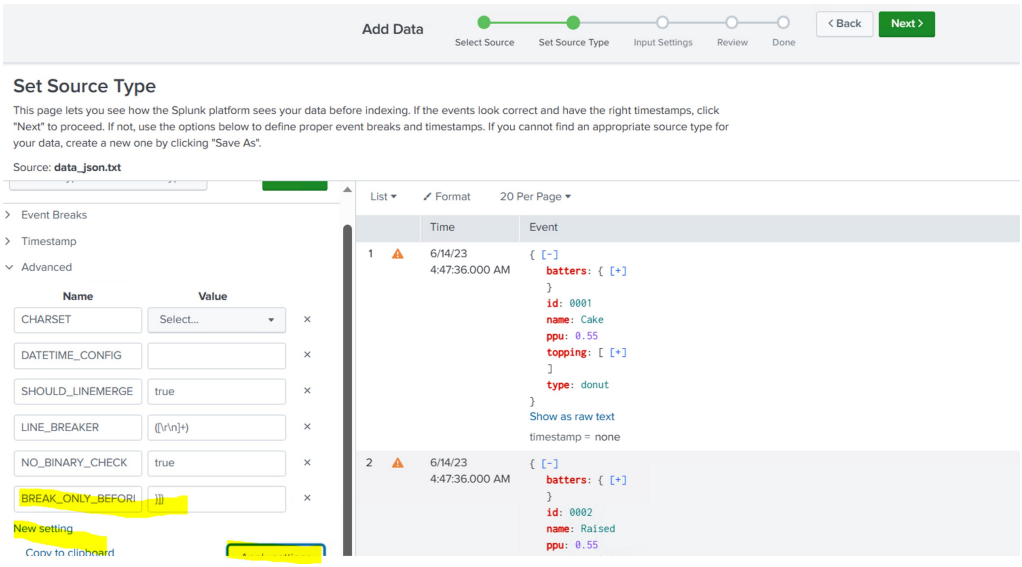
Use **"BREAK_ONLY_BEFORE"** while setting sourcetype.

Props.conf

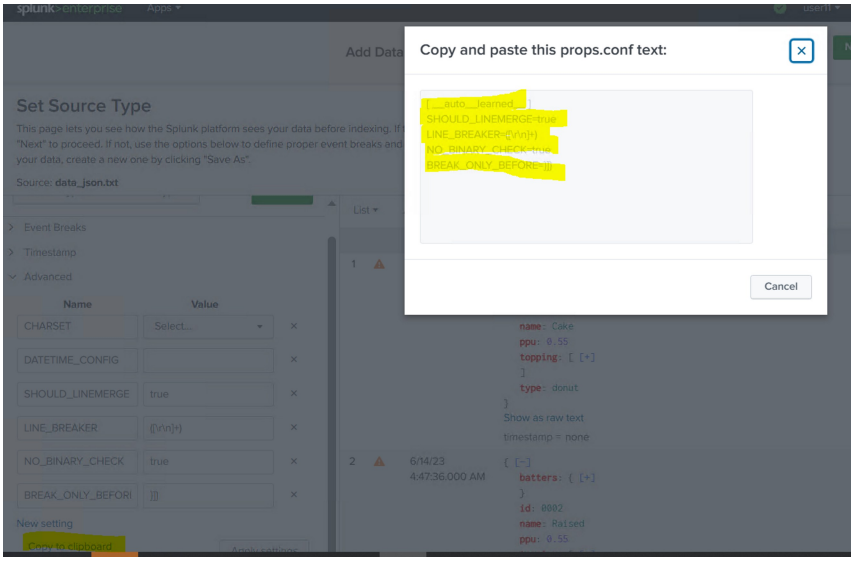
#Event splitting on JSON File:

Settings => Add Data => Upload =>





Copy these line and paste in props.conf



[__auto__learned__]

SHOULD_LINEMERGE=true

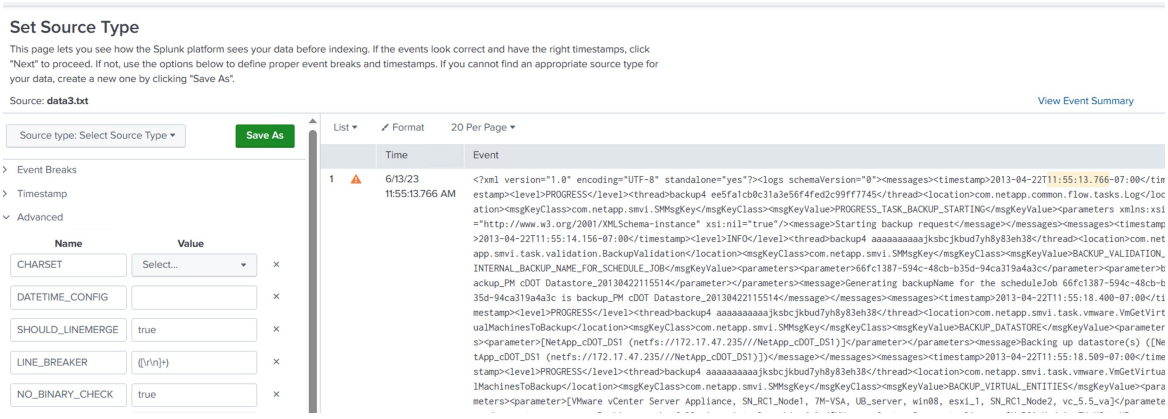
LINE_BREAKER=([\r\n]+)

NO_BINARY_CHECK=true

BREAK_ONLY_BEFORE=}]}

#Event splitting on XML File

Before :

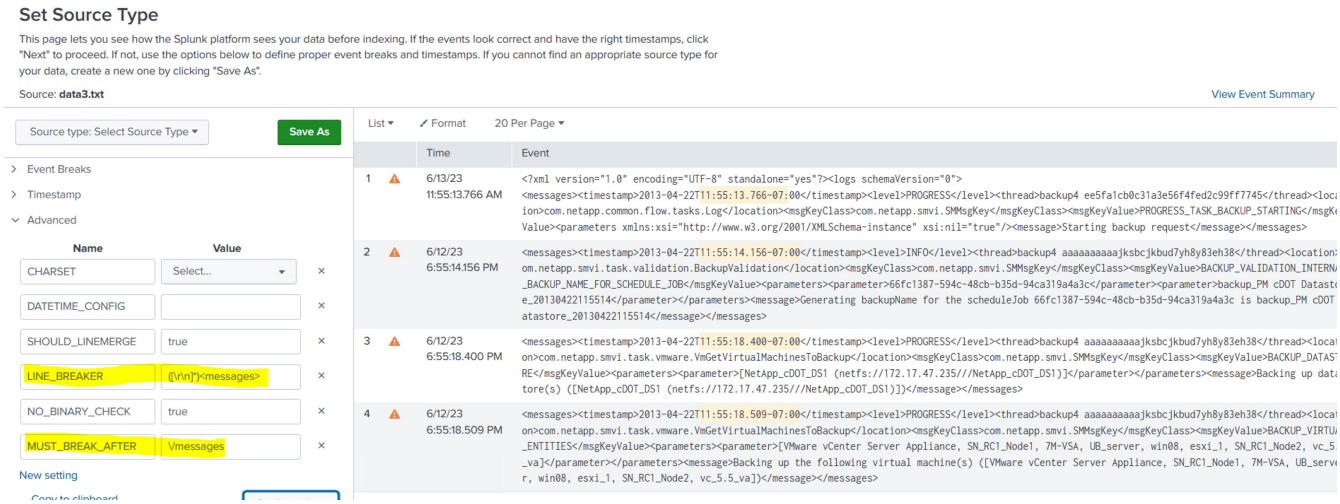


After setting "MUST_BREAK_AFTER" and "LINE_BREAKING"

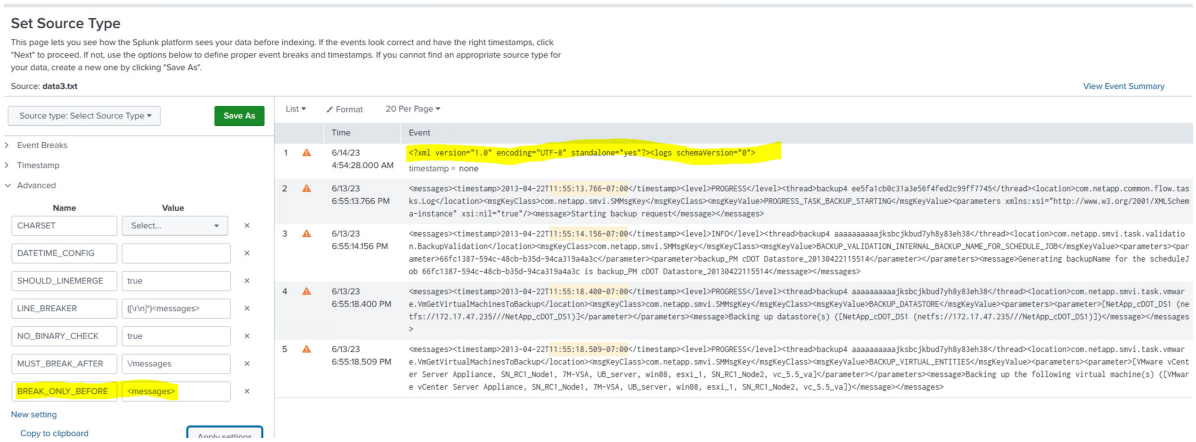
LINE_BREAKER=([\r\n])<messages>*

MUST_BREAK_AFTER=\/messages

Note : here in LINE_BREAKER, it is * sign instead of +.



To remove <?xml version> as separate line, user setting "BREAK_ONLY_BEFORE"



[__auto__learned__]

SHOULD_LINEMERGE=true

LINE_BREAKER=([\r\n])<messages>*

NO_BINARY_CHECK=true

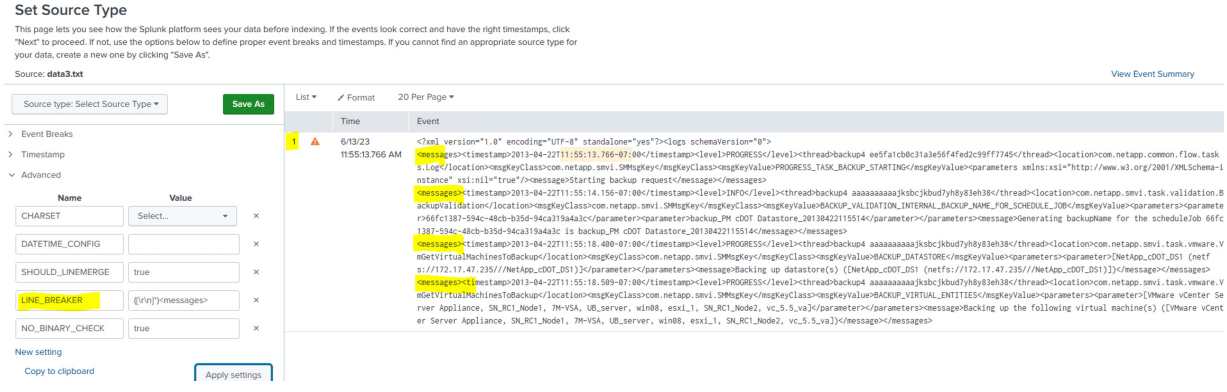
MUST_BREAK_AFTER=\/messages

BREAK_ONLY_BEFORE=<messages>

Difference between LINE_BREAKER and MUST_BREAK_AFTER ?

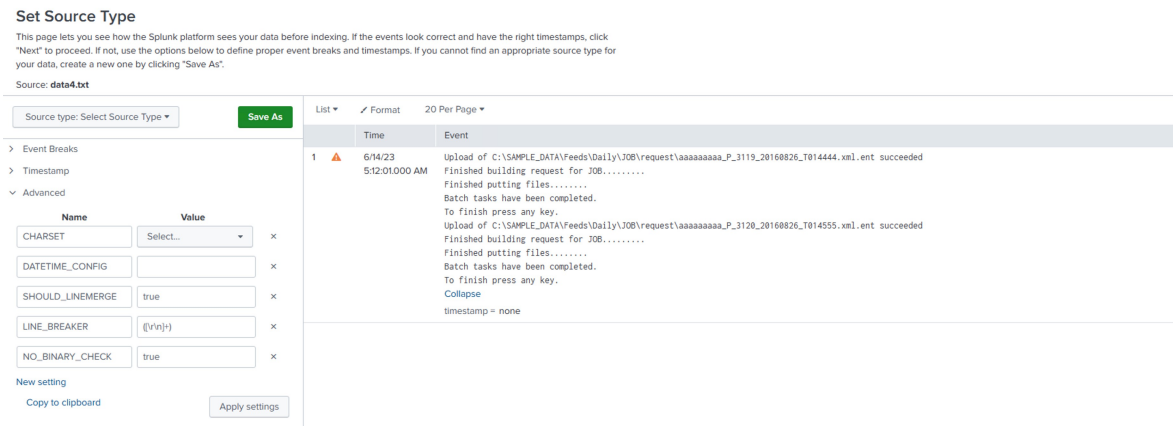
LINE_BREAKER => will break the event's line in multiple lines but in same the event. It will not create new event.

MUST_BREAK_AFTER => will convert each break into **new events**.

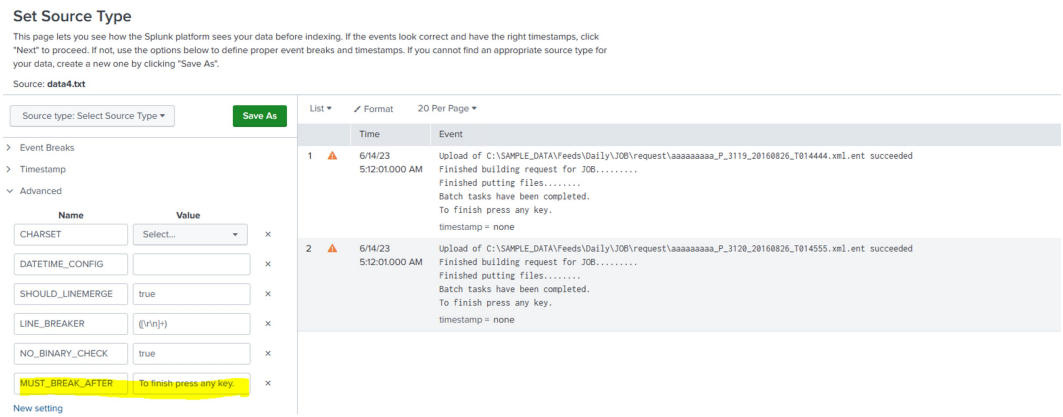


#Event splitting on Random File

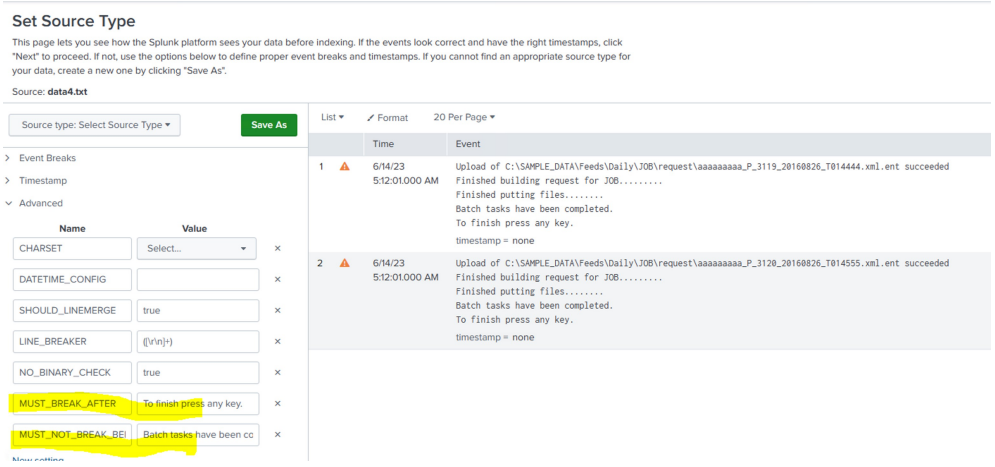
Before:



After using "MUST_BREAK_AFTER"



Property "MUST_NOT_BREAK_BEFORE"



[__auto__learned__]

SHOULD_LINEMERGE=true

LINE_BREAKER=([\r\n]+)

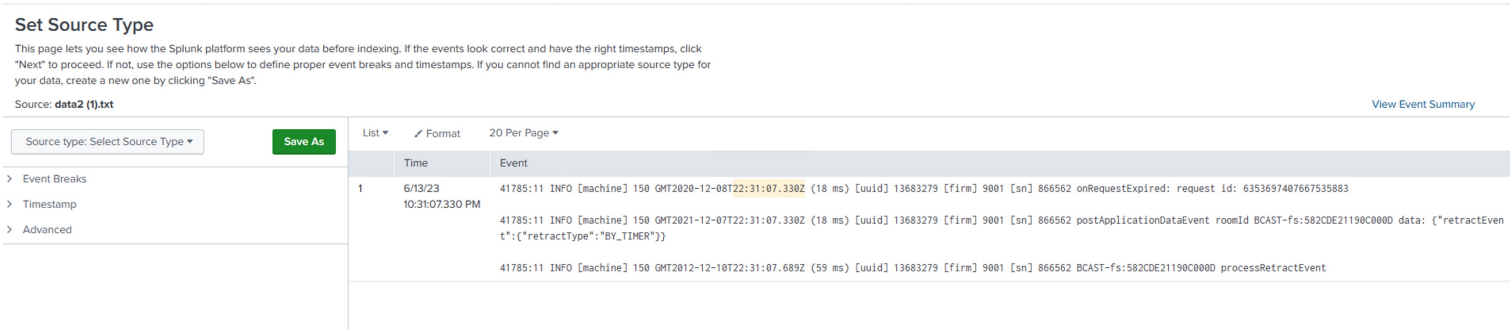
NO_BINARY_CHECK=true

MUST_BREAK_AFTER=To finish press any key.

MUST_NOT_BREAK_BEFORE=Batch tasks have been completed

#Timestamp Customization

Before :



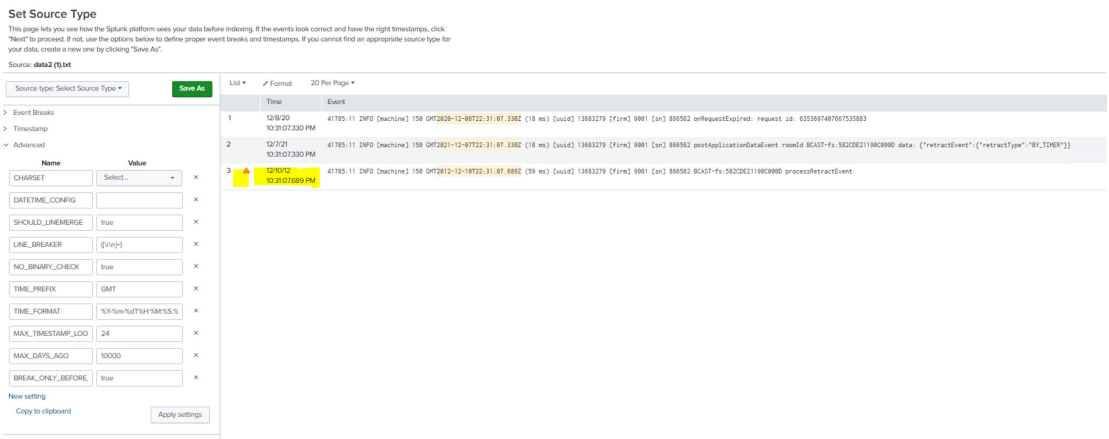
After using "BREAK_ONLY_BEFORE_DATE" and "TIME_PREFIX" and "TIME_FORMAT" settings

NOTE :

(1)There is certain limit that Splunk can handle older data. We can change this by using property "MAX_DAYS_AGO"

(2) 2016 = %Y

16 = %y



For 2102 event => warning will be "**Accepted time is suspiciously far away from previous event time but still accepted as it is extracted by same pattern**"

[__auto__learned__]

SHOULD_LINEMERGE=true

LINE_BREAKER=([\r\n]+)

NO_BINARY_CHECK=true

TIME_PREFIX=GMT

TIME_FORMAT=%Y-%m-%dT%H:%M:%S.3N%

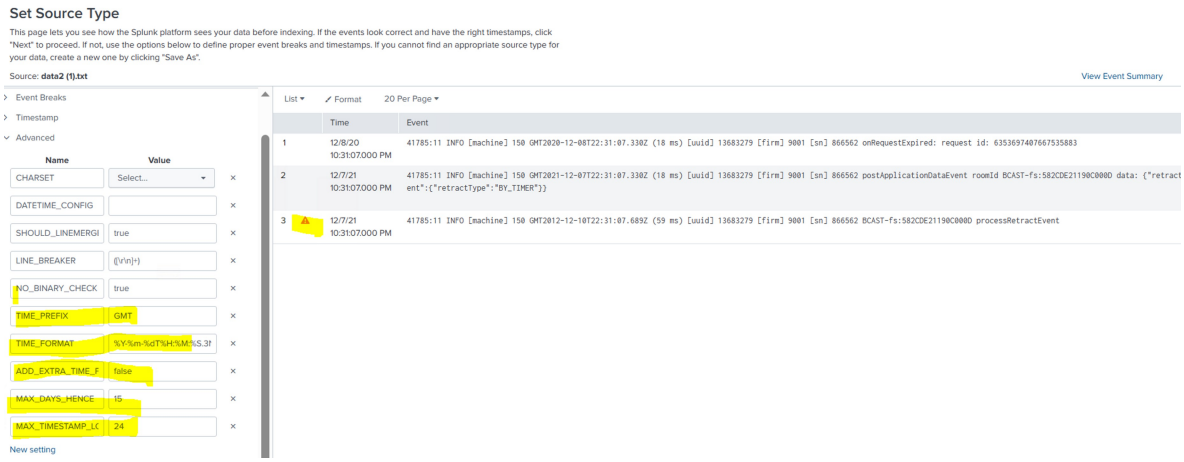
MAX_DAYS_AGO=10000

MAX_TIMESTAMP_LOOKAHEAD=24

BREAK_ONLY_BEFORE_DATE=true

NOTE :

(1) If setting "**ADD_EXTRA_TIME_FIELDS**" is set to **false** -> then it will **not add any extra timestamp filed** after processing.



[__auto__learned__]

SHOULD_LINEMERGE=true

LINE_BREAKER=([\r\n]+)

NO_BINARY_CHECK=true

TIME_PREFIX=GMT

TIME_FORMAT=%Y-%m-%dT%H:%M:%S.3N%

ADD_EXTRA_TIME_FIELDS=false

MAX_DAYS_HENCE=15

MAX_TIMESTAMP_LOOKAHEAD=24

#User and Roles

(1) Capabilities => Features like :

(i) feature to add data

(ii) feature to create Alert/Report/Dashboard

(iii) Create/Modify/Customize Index

(iv) Resource consumption user-wise

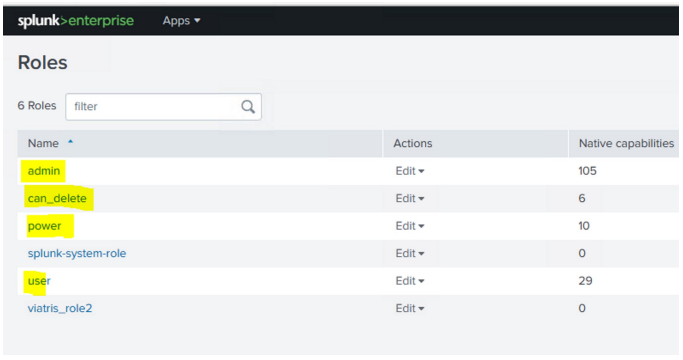
(v) to remove real-time search

(vi) Access to License

NOTE :Users' activities get saved on disk. We can customize the max space used by an user.

(2) Role => Combination of features/Access

(1) **4 defaul**t roles => admin, can_delete, power, user



(2) admin don't have "can_delete" role by default.

?

Question : How to delete data ?

Answer : *Search the data and then* "***| delete***"

(3) Native Capabilities => capabilities which we **add manually** to that particular role only

Inherited Capabilities => capabilities which we **get automatically by assigning an existing Role.**

Capabilities => C1, C2,C3…..C10

Roles => R1, R2, R3

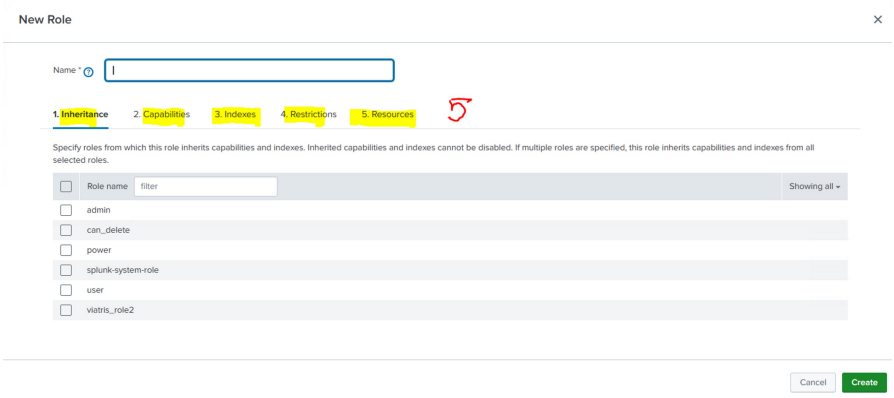
R1 = C1 + C2 + C3

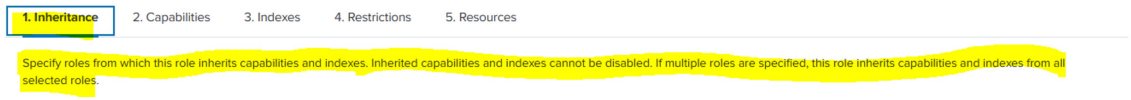
R2 = R1 + C4 + C5

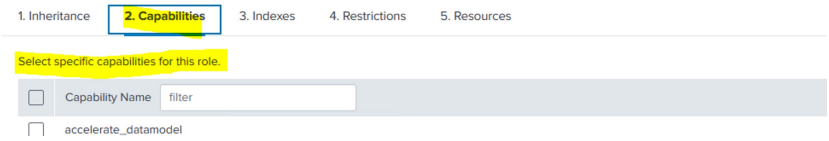
= inherited capabilities will be C1,C2,C3 + Native Capabilities will be C4,C5

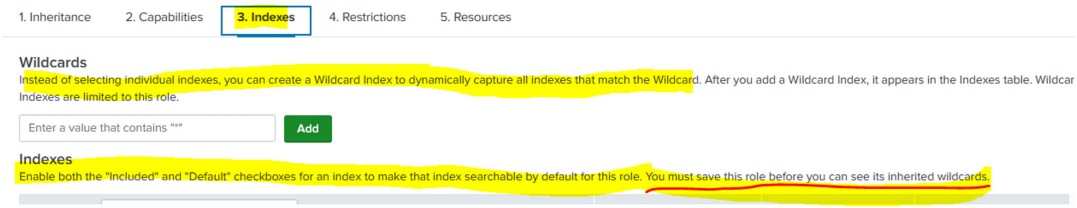
R3 = R2 + C9 + C10

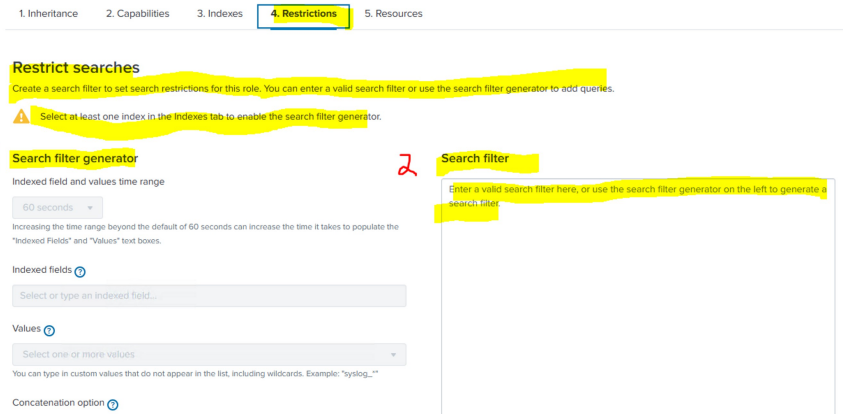
= inherited capabilities will be C1,C2,C3,C4,C5 + Native Capabilities will be C9,C10

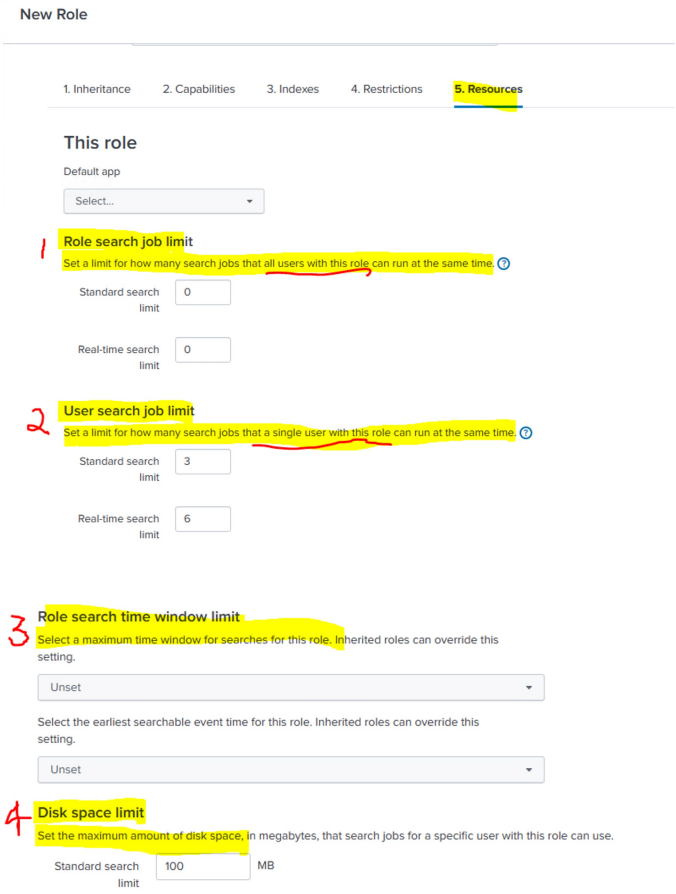




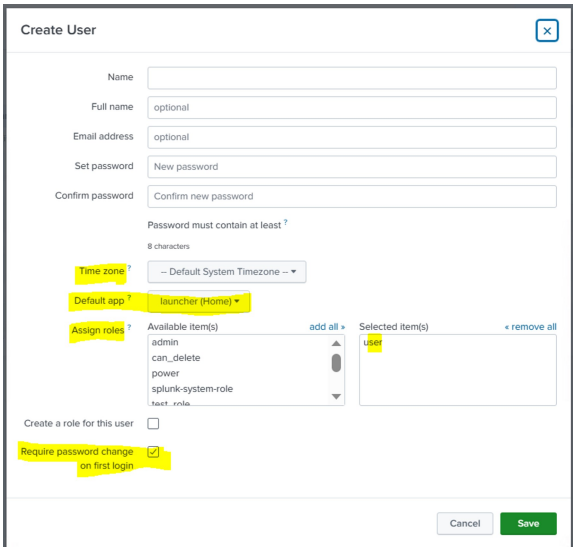




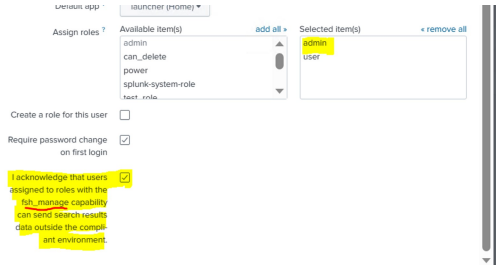




(3) User =>End User



If giving "***admin***" role, it will ask to acknowledge a message "***I acknowledge that users assigned to roles with the fsh_manage capability can send search results data outside the compliant environment.***"



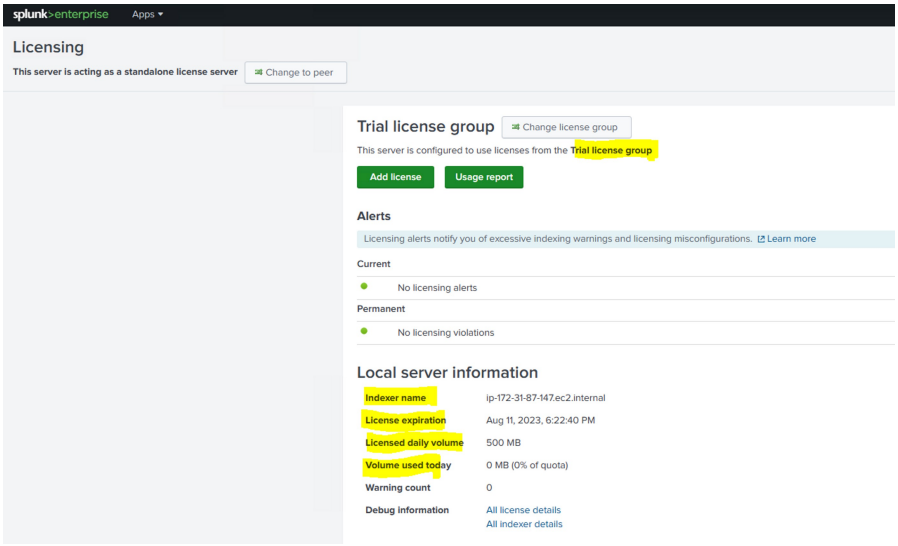
Note:

(1) Once LDAP is set we cannot use local account.

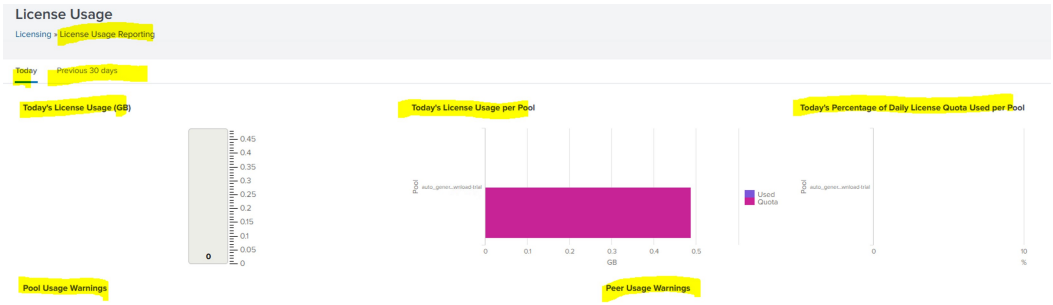
(2) **Roles mapping** of Splunk with LDAP (using ***authorization.conf***)

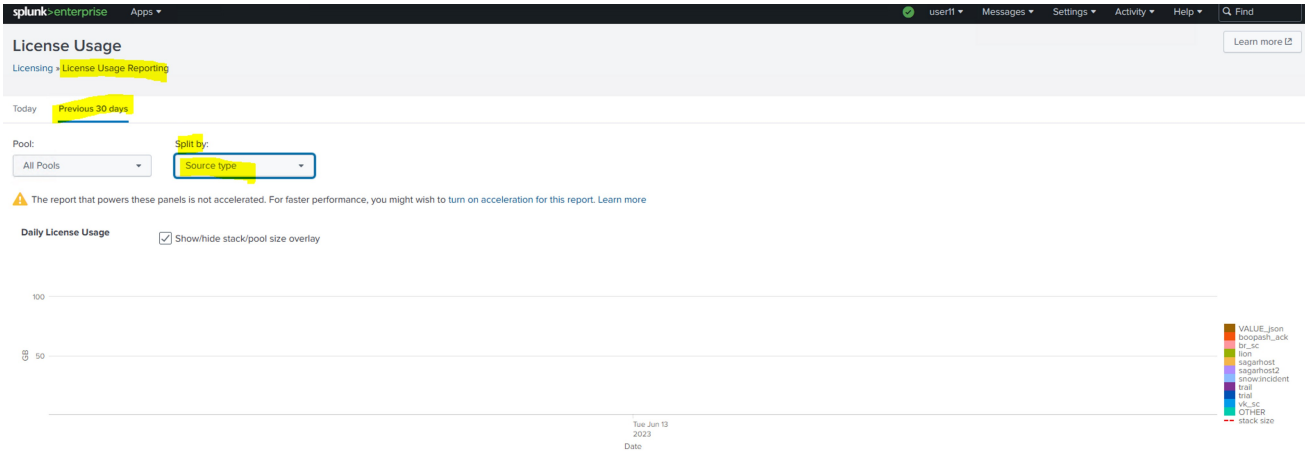
#License Management

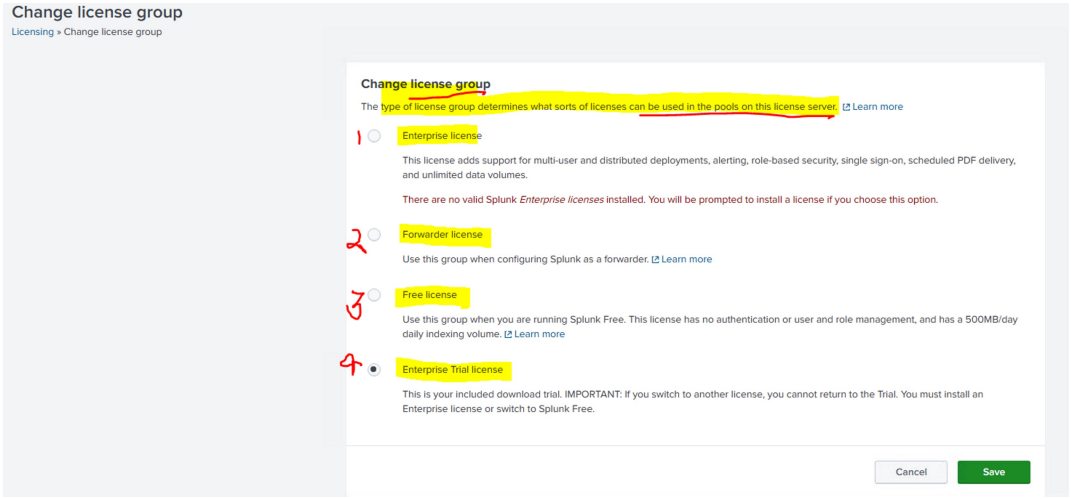
Settings => Licensing



License file of splunk **looks like an XML file.**




splunk>enterprise
Apps
user11
Messages
Settings
Activity
Help
Find
License Usage
Licensing » License Usage Reporting
Learn more
Today
Previous 30 days
Pool:
All Pools
Split by:
Source type
The report that powers these panels is not accelerated. For faster performance, you might wish to turn on acceleration for this report. Learn more
Daily License Usage
Show/hide stack/pool size overlay
100
GB
50
Tue Jun 13
2023
Date
VALUE_json
boopash_ack
br_sc
lion
sagarhost
sagarhost2
snow:incident
trail
trial
vk_sc
OTHER
stack size


Change license group
Licensing » Change license group
Change license group
The type of license group determines what sorts of licenses can be used in the pools on this license server. Learn more
1
Enterprise license
This license adds support for multi-user and distributed deployments, alerting, role-based security, single sign-on, scheduled PDF delivery, and unlimited data volumes.
There are no valid Splunk Enterprise licenses installed. You will be prompted to install a license if you choose this option.
2
Forwarder license
Use this group when configuring Splunk as a forwarder. Learn more
3
Free license
Use this group when you are running Splunk Free. This license has no authentication or user and role management, and has a 500MB/day daily indexing volume. Learn more
4
Enterprise Trial license
This is your included download trial. IMPORTANT: If you switch to another license, you cannot return to the Trial. You must install an Enterprise license or switch to Splunk Free.
Cancel
Save