Training – Day #5

15 June 2023 04:35

#Data Model & Pivot

Data models drive the **pivot** **tool. Data models enable users of Pivot to create compelling reports and dashboards without designing the searches that generate them. Data models can have other uses, especially for Splunk app developers.**

Splunk knowledge managers design and maintain data models. These knowledge managers understand the format and semantics of their indexed data and are familiar with the Splunk search language.

In building a typical data model, knowledge managers use knowledge object types such as **lookups, transactions, search-time field extractions, and calculated fields.**

https://splunkonbigdata.com/data-model-in-splunk-part-i/

https://docs.splunk.com/Documentation/Splunk/9.0.4/Knowledge/Aboutdatamodels

(1) Data-Model follows **Hierarchal concept** means Root event can have child event -> child will have sub-child

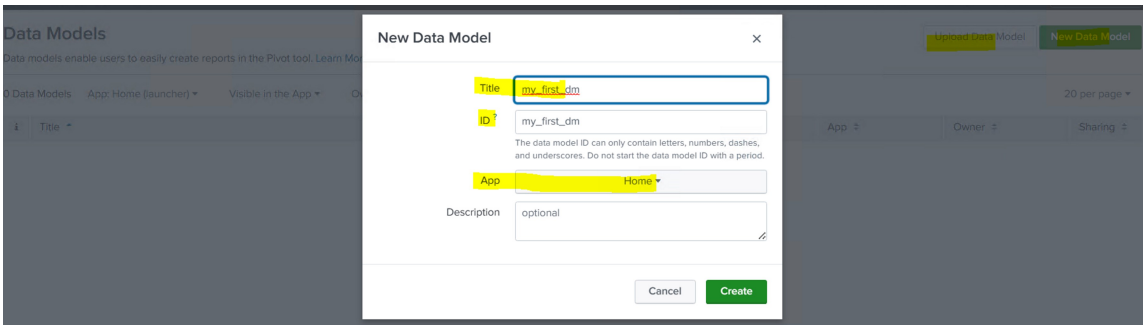
(2) **Define the fields explicitly** (exact needed fields)=> like index="my_indx" will show all events with all fields, BUT Data-model will show advanced specific fields. **So Data-Model will reduce time of result in large result queries.**

(3) **Drawback** is **"Resource Consumption is very High"**

(4) Usually used in Splunk ITSI and Splunk Security

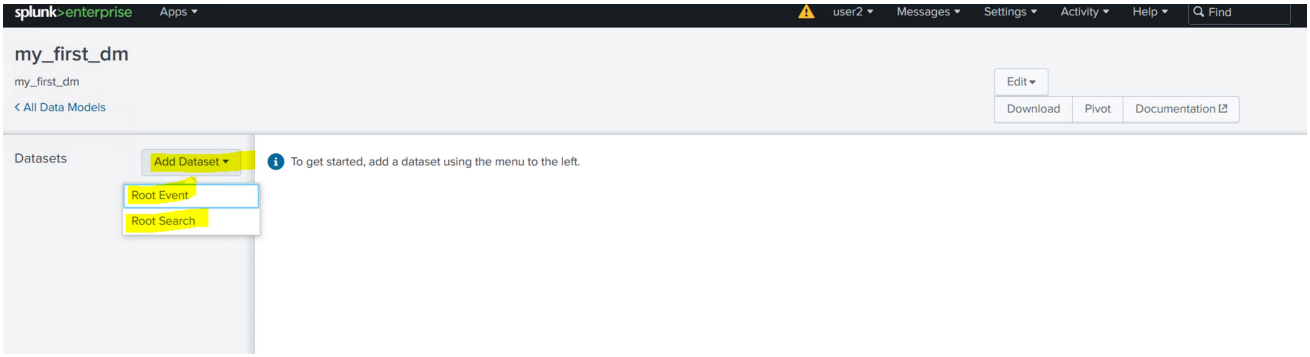
How to create Data-Model ?

Settings => Data models => New Data model (NOTE : we can Upload Data models also)

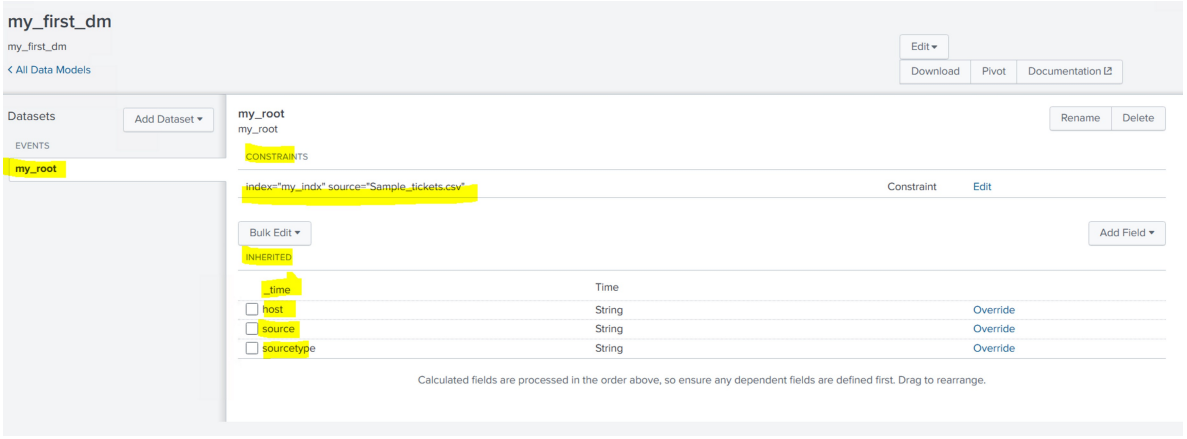


Add Dataset => Root Event

Note : Root Search **faster than** Root Event



Constraints => index="my_indx" source="Sample_tickets.csv"

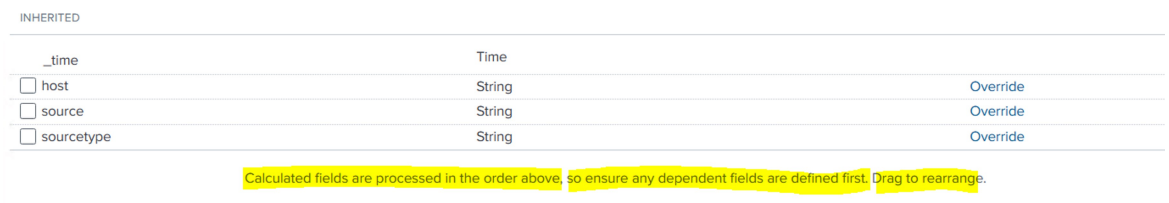


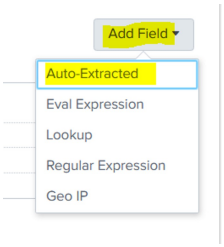
Default **4 inherited fields** are **_time, host, source, sourcetype**

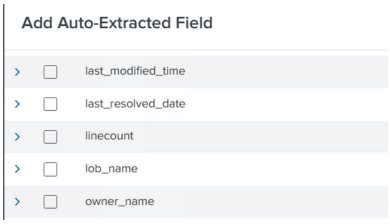
Add Filed by 5 ways :

*"**Auto Extracted**" will be visible in **EXTRACTED fields**,*
Rest 4** will be visible in C**ALCULATED fields

NOTE : **Calculated fields are processed in the order above, so ensure any dependent fields are defined first. Drag to rearrange.**

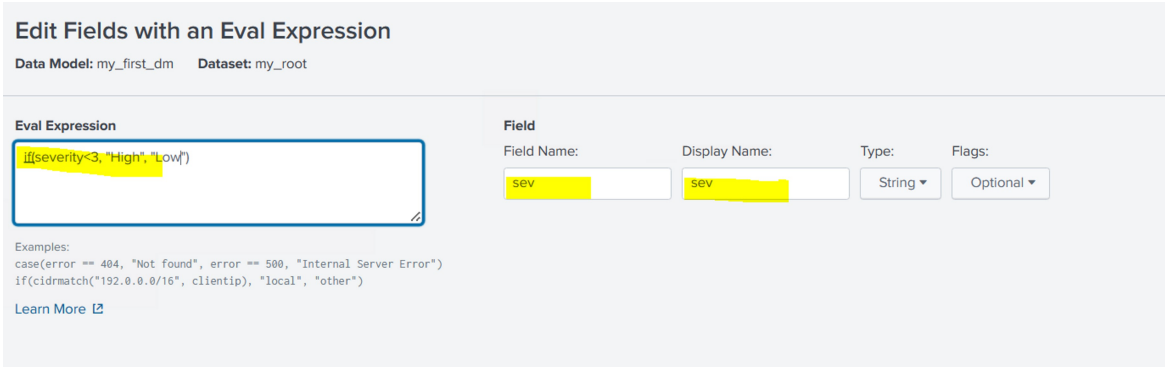




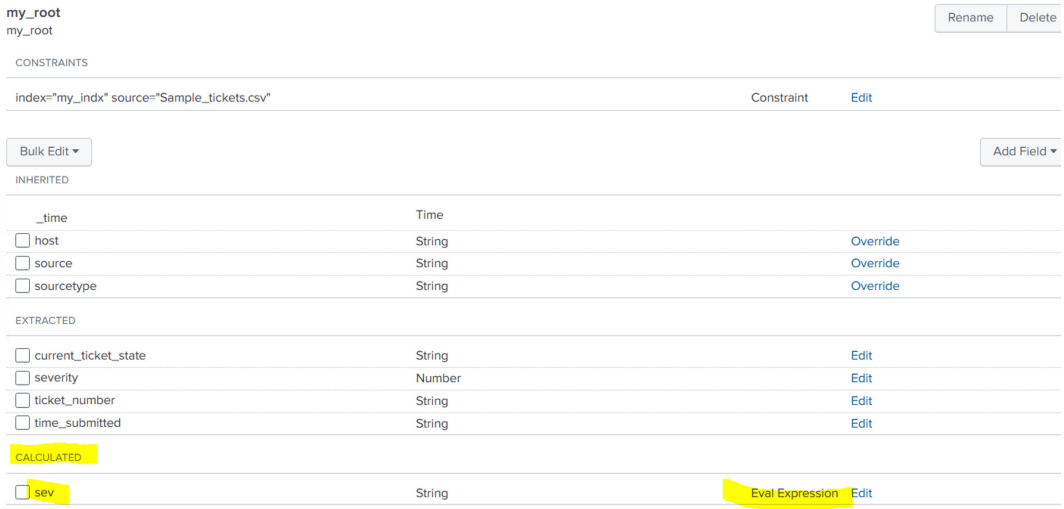


Add Eval field :

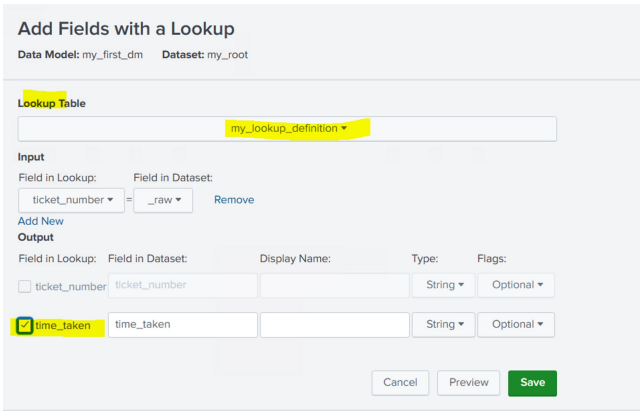
NOTE : CALCULATED fields like eval expression should be based on EXTRACTED fields only.

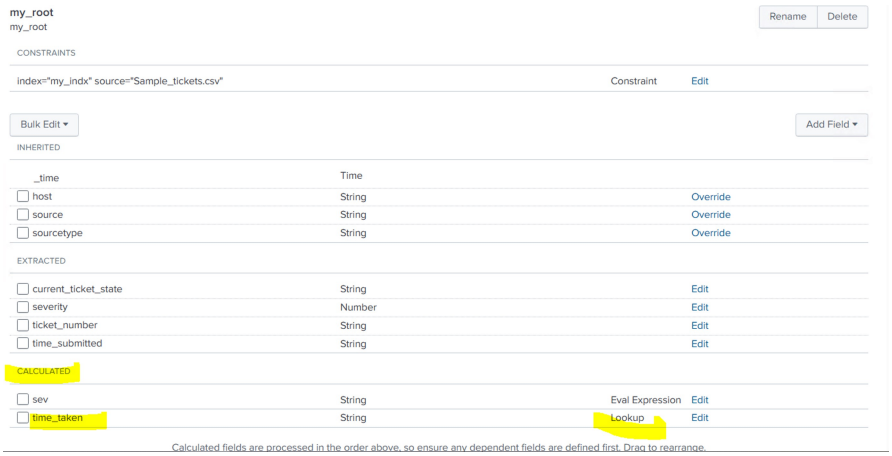


if(severity<3, "High", "Low")

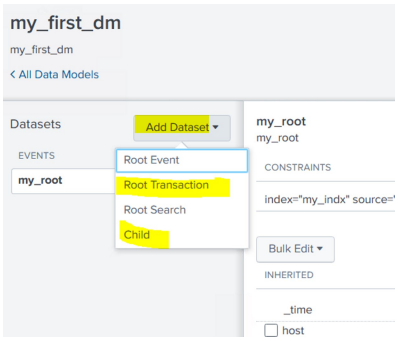


To add Lookup , **make sure your Lookup is shared with this application in "Lookup Definition" Because Data model is in "Home" App.**

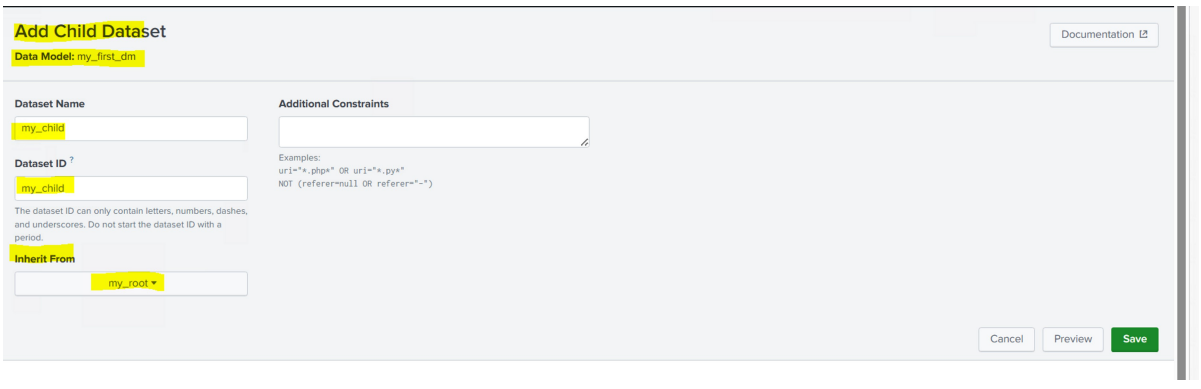




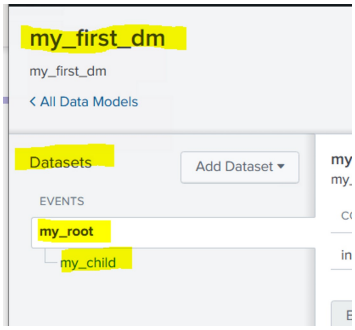
Add Adding one data set, we are getting 2 more options :

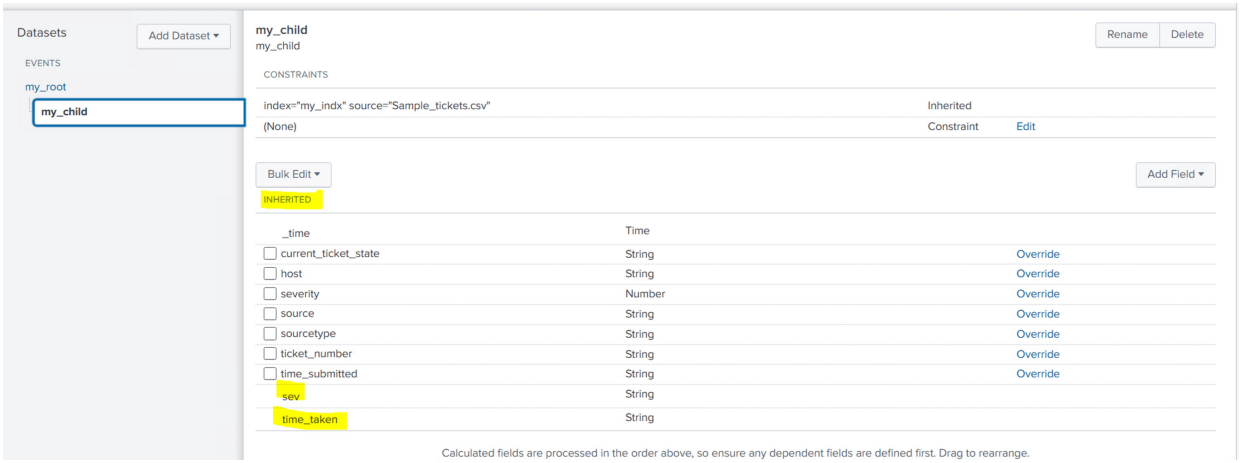


Add Dataset as "Child"

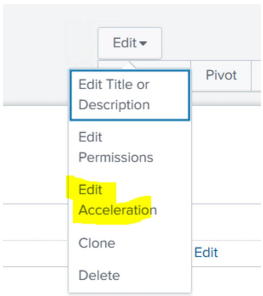


It will in Hierarchy to Root dataset :





Datamodel "Edit" Option :

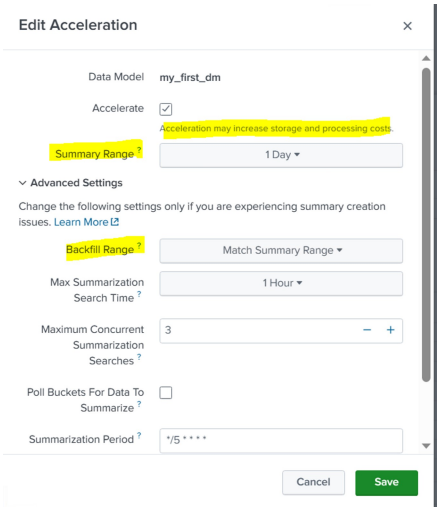


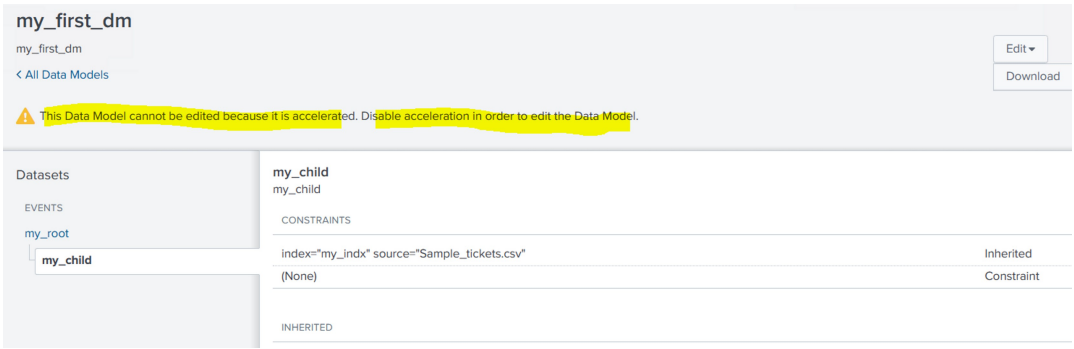
Notes:

(1) Data-model all parent-child hierarchy data will be save backend in JSON format. We can use this JSON and UPLOAD it to create similar data-model.

(2) **Acceleration** : we can define time-range to save data so backend query can run **faster**. It will **consume more storage and CPU**.

(3) If Data-model in Acceleration mode, it **cannot** be edited further. First disable the acceleration and then edit the data-model.



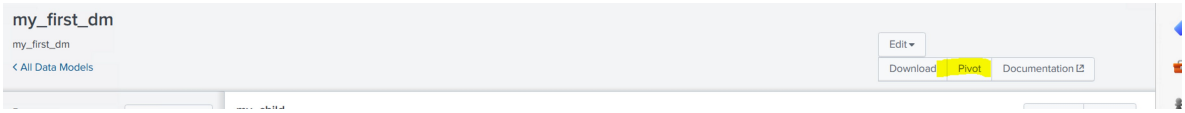


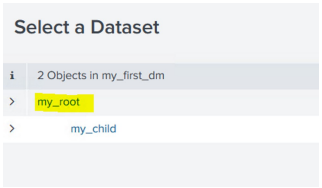
#PIVOT

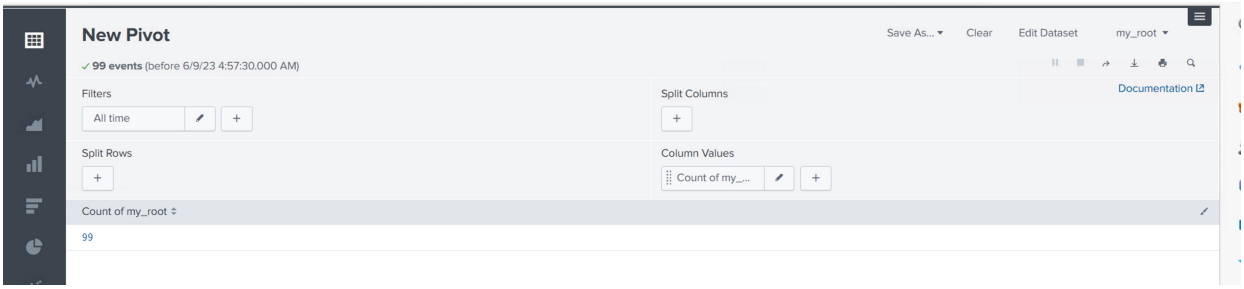
1. Pivot is for **Graphical/Visualization representation**.
2. Chart/timechart command refer to index, **BUT Pivot refer to data-model**.

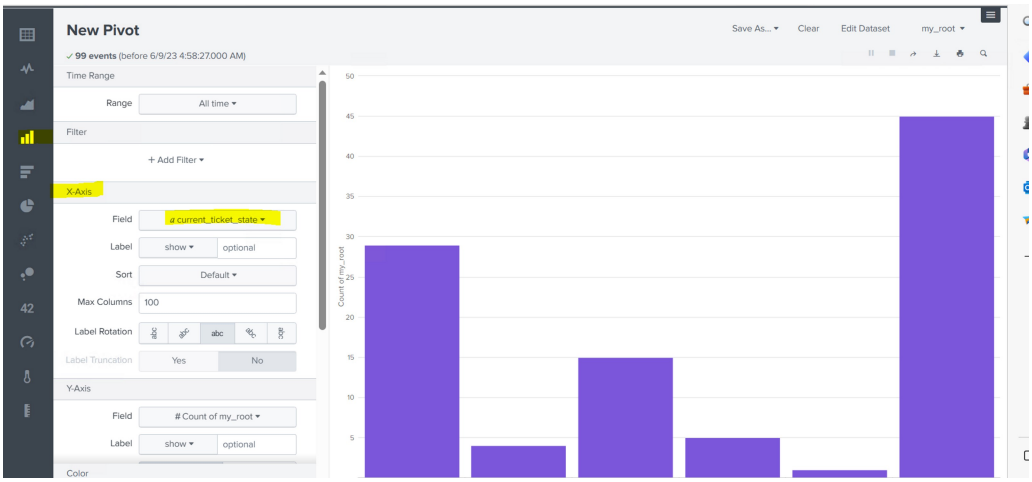
(3) Since the source is data-model, hence visualization will be **very fast.**

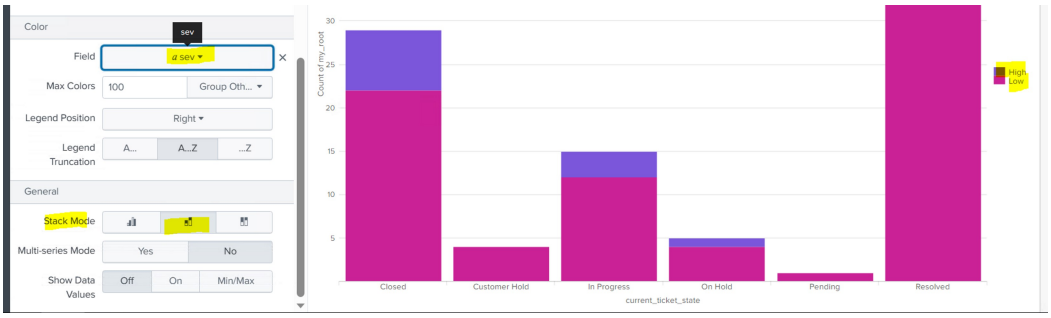
(4) "**Click and Go**" option. It will fast to create/modify.

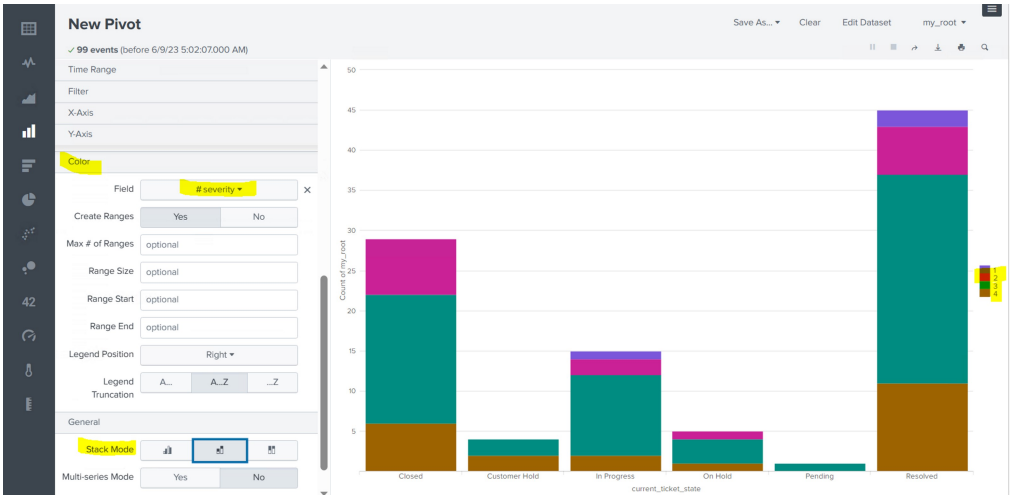








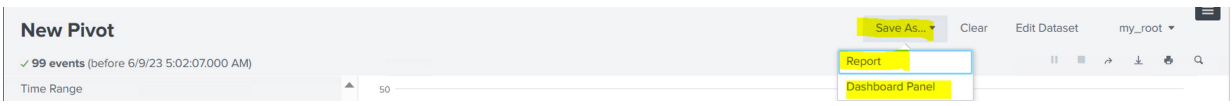




Pivot can be saved as **2 ways :**

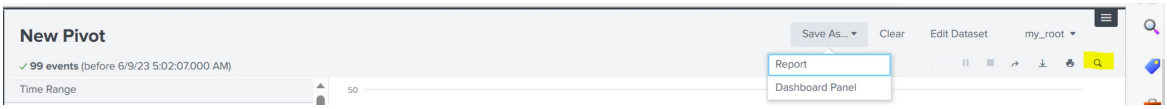
(1) Report

(2) Dashboard Panel

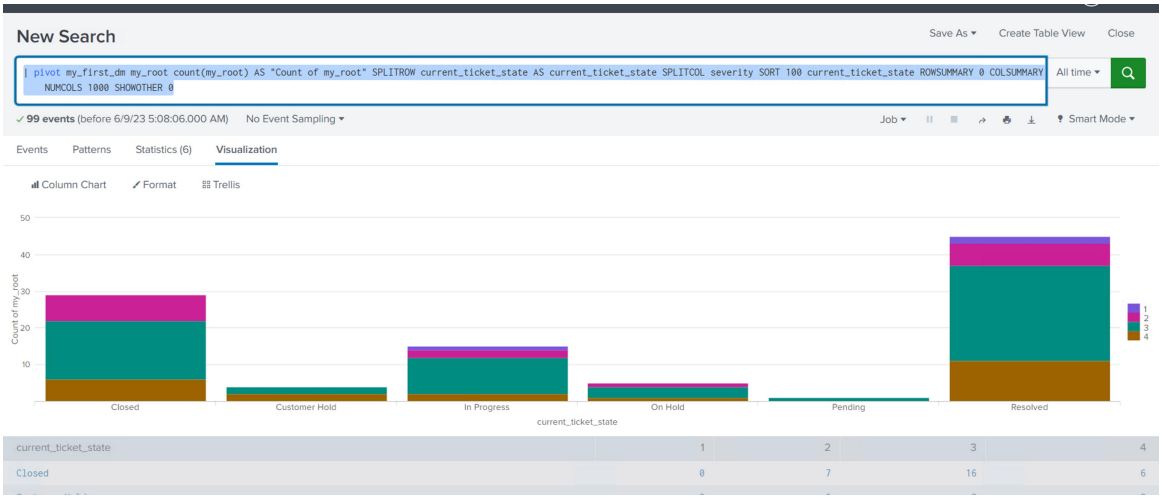


Question : How to check backend query of pivot ?

Answer : click "open in search" icon



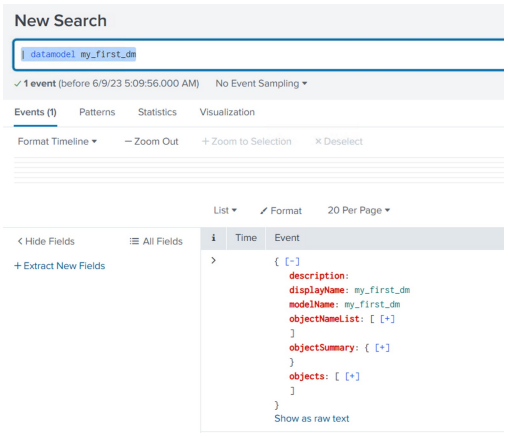
| pivot my_first_dm my_root count(my_root) AS "Count of my_root" SPLITROW current_ticket_state AS current_ticket_state SPLITCOL severity SORT 100 current_ticket_state ROWSUMMARY 0 COLSUMMARY 0 NUMCOLS 1000 SHOWOTHER 0



#Datamodel command :

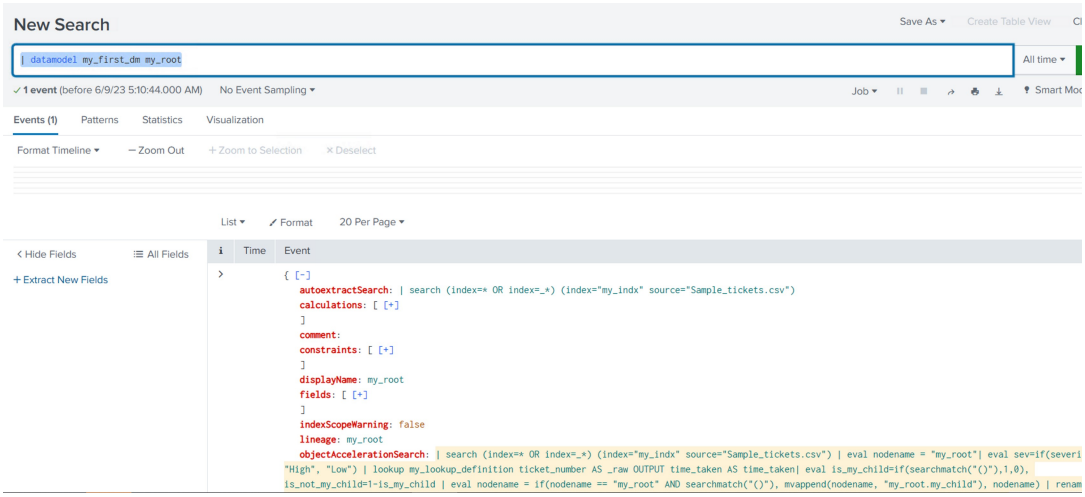
| datamodel my_first_dm

| datamodel <datamodel name>



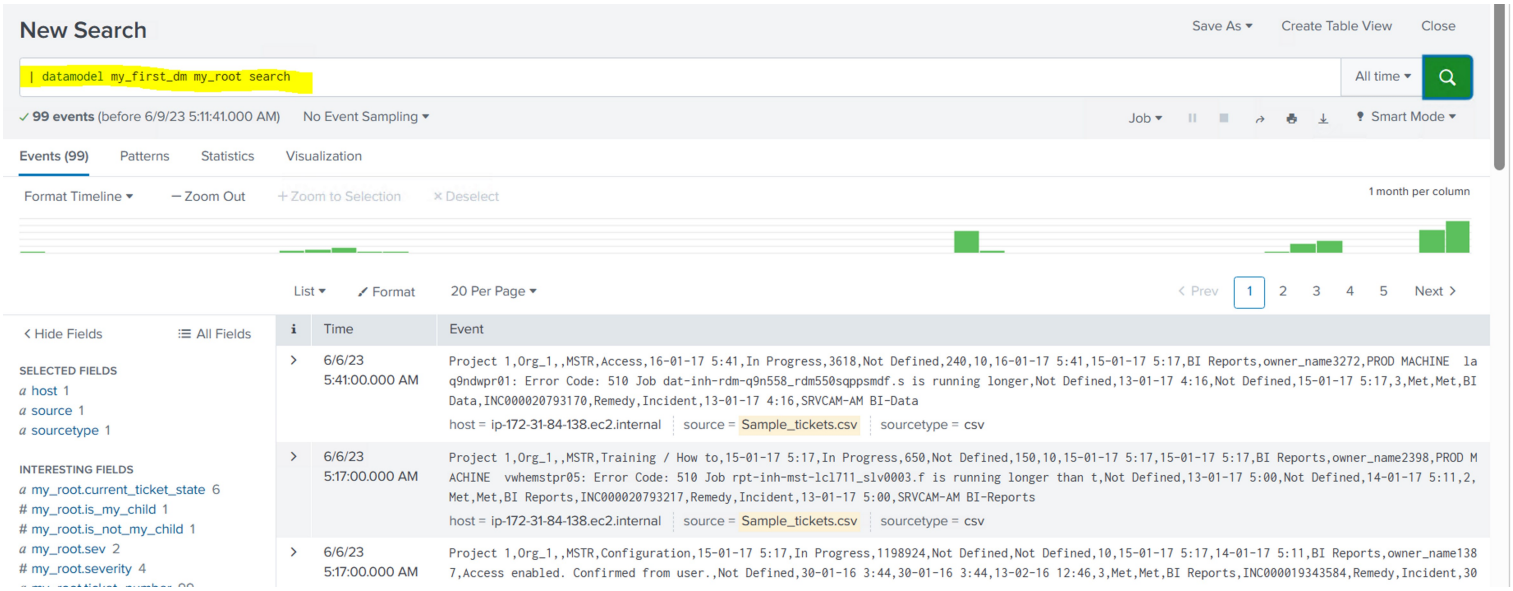
| datamodel my_first_dm my_root

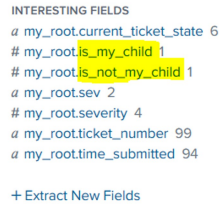
| datamodel <data model name> <root dataset name>



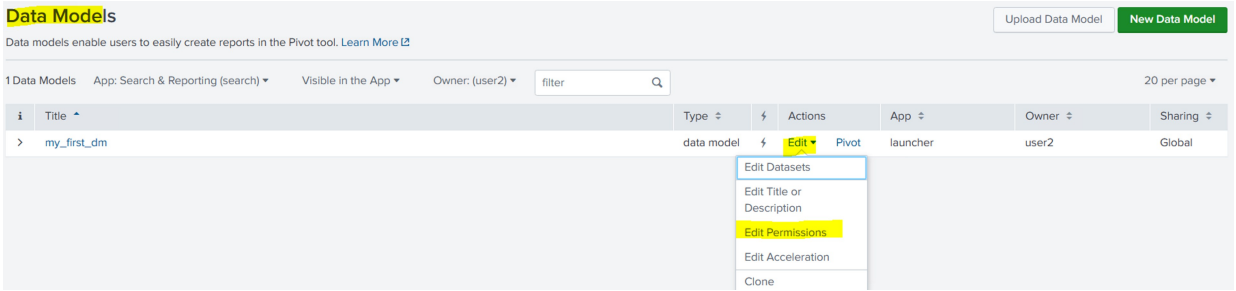
To show all events of data-model, use search command,. Events will have only those fields mentioned in data-set with **2 extra fields** "**is_my_child**" and "**is_not_my_child**".

| datamodel my_first_dm my_root search





Edit Permission:



#Alert

(1) Define **search query**

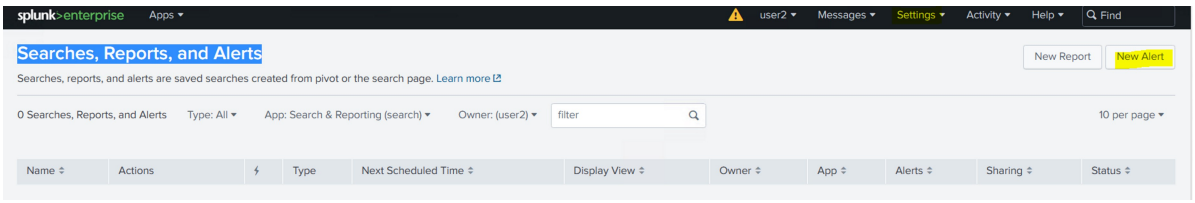
(2) Define **Condition** (like count > 5)

(3) Define **Frequency** (like every 15 minute, on weekend)

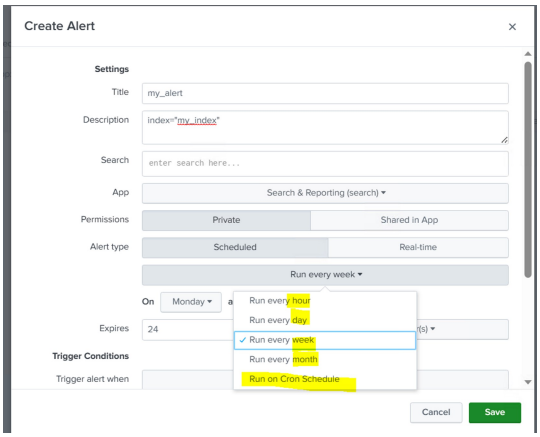
(4) Define **Data-length /Time-Filer**

(5) Define **Trigger Action** (send email/webhook/lookup/Triggered Alert/Script/Mobile/Otel, ***reindex the data as separate event***)

Settings => Searches, Reports, and Alerts => New Alert



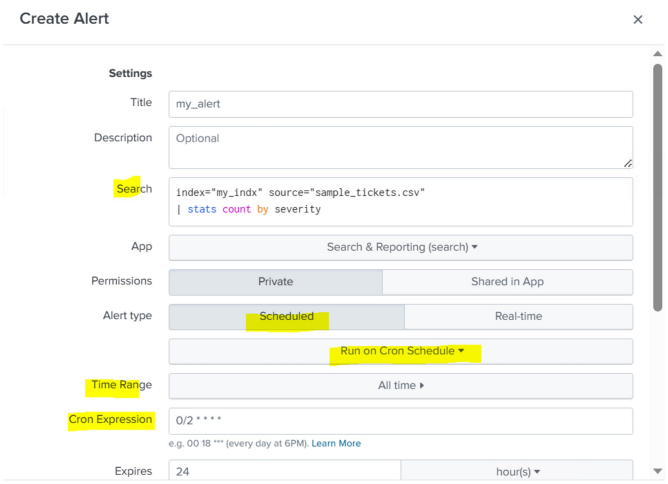
Hour < Day < Week < Month < Cron

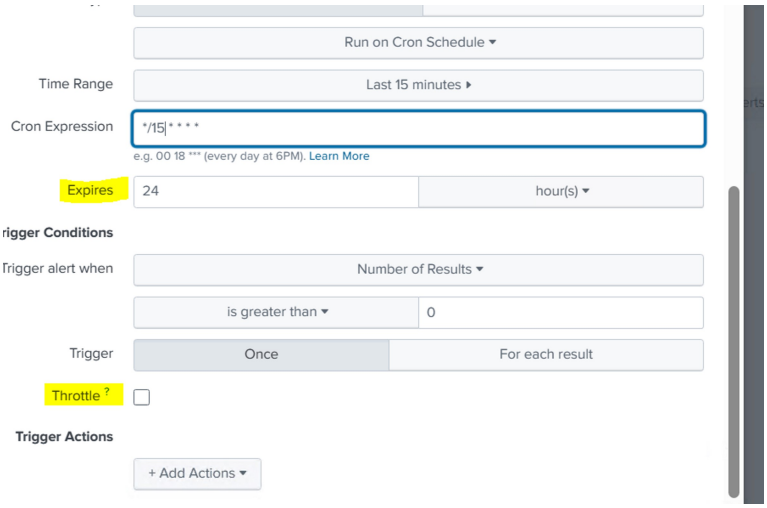


https://crontab.guru/

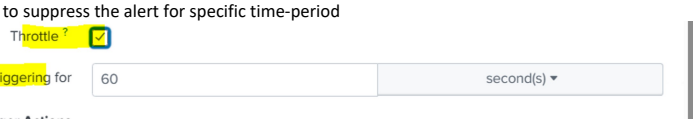
index="my_indx" source="sample_tickets.csv"

| stats count by severity

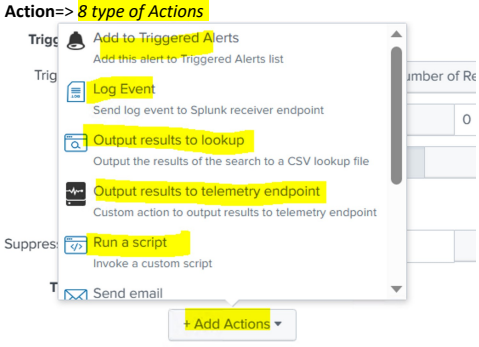


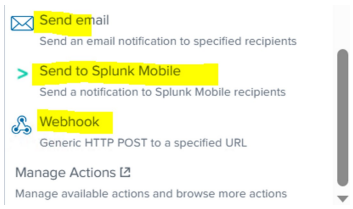


- **Expire** => will expire the Alert search job
- **Throttle** => to suppress the alert for specific time-period



- **Action**=> *8 type of Actions*





Difference between webhook and API :

API => call happens at interval of time when Receiver asks data and Sender sends the data.

Webhook => whenever source get the data, Sender sends data to Receiver.

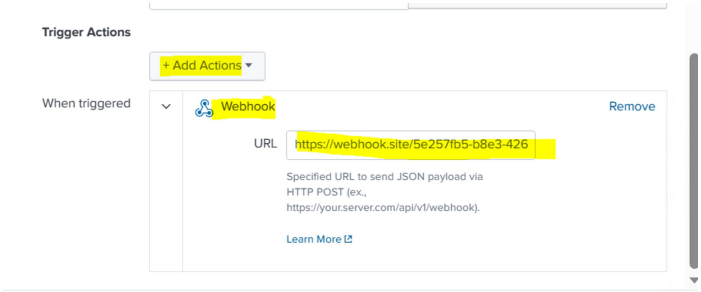
Use-Case #1 : If **expression is to run every 2 hours and Time range is Last 3 hours** => It **may create duplicate Alert if event is between 2nd to 3rd hour.**

Solution: **Expression run time and time-range should be same.**

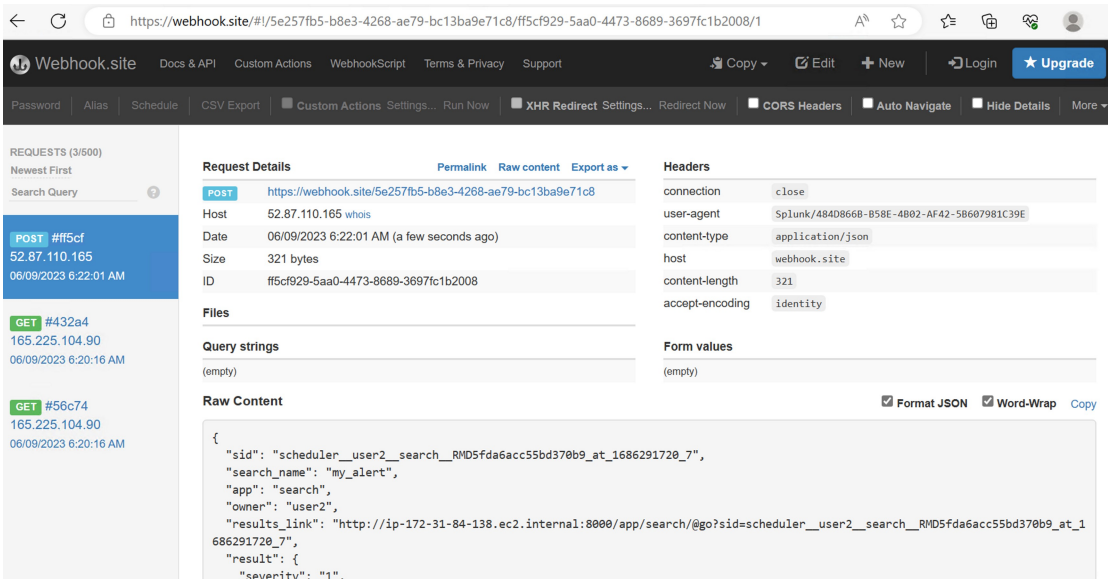
Use-Case #2: To check License Utilization data and **expression is to run every 1 hours and Time range is Last 1 hours** => then **license consumption in Alert will be incorrect.**

Solution: **Use Time-Rage as "Today"**

https://webhook.site/#!/5e257fb5-b8e3-4268-ae79-bc13ba9e71c8



Received at webhook:



#Report

Same as Alert , except Condition

(1) Define **search query**

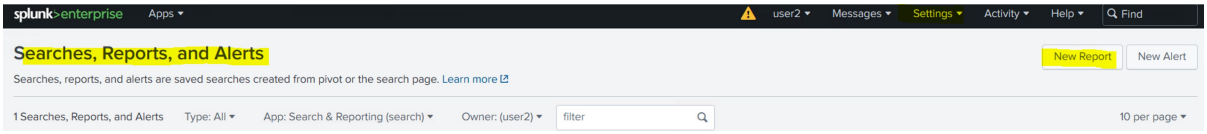
~~(2) Define **Condition** (like count > 5)~~

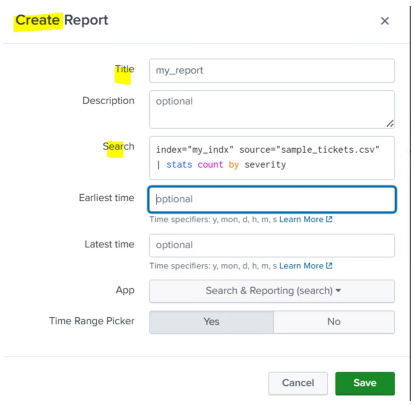
(2) Define **Frequency** (like every 15 minute, on weekend)

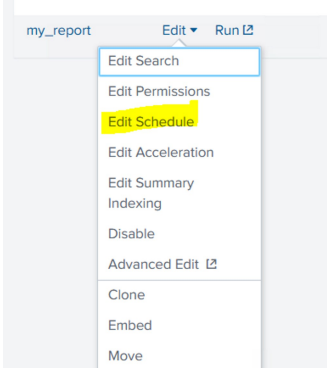
(3) Define **Data-length /Time-Filer**

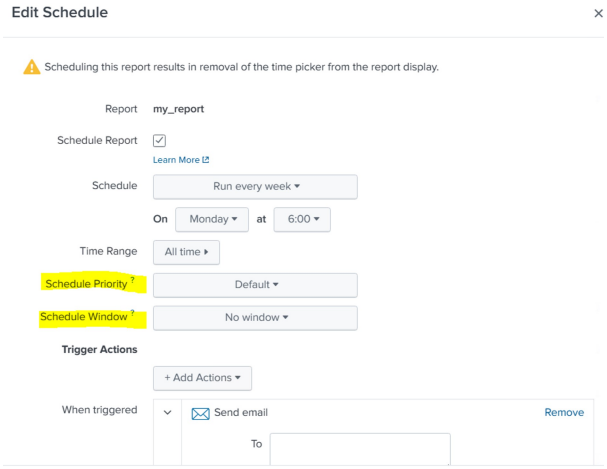
(4) Define **Trigger Action** (send email/webhook/lookup/Triggered Alert/Script/Mobile/Otel, ***reindex the data as separate event***)

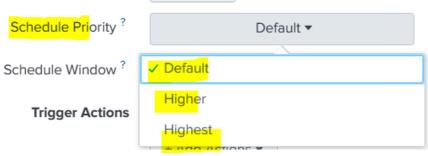
Settings => Searches, Reports, and Alerts => New Report

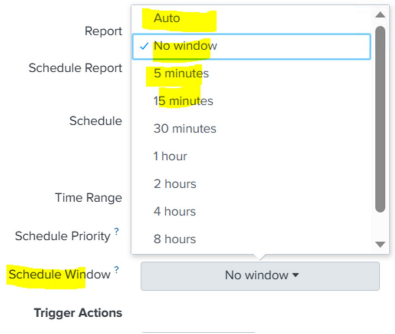

splunk>enterprise
Apps
user2
Messages
Settings
Activity
Help
Find
Searches, Reports, and Alerts
Searches, reports, and alerts are saved searches created from pivot or the search page. Learn more
New Report
New Alert
1 Searches, Reports, and Alerts
Type: All
App: Search & Reporting (search)
Owner: (user2)
filter
10 per page


Create Report
Title
my_report
Description
optional
Search
index="my_indx" source="sample_tickets.csv"
| stats count by severity
Earliest time
optional
Time specifiers: y, mon, d, h, m, s Learn More
Latest time
optional
Time specifiers: y, mon, d, h, m, s Learn More
App
Search & Reporting (search)
Time Range Picker
Yes
No
Cancel
Save


my_report
Edit
Run
Edit Search
Edit Permissions
Edit Schedule
Edit Acceleration
Edit Summary Indexing
Disable
Advanced Edit
Clone
Embed
Move


Edit Schedule
Scheduling this report results in removal of the time picker from the report display.
Report
my_report
Schedule Report
Learn More
Schedule
Run every week
On
Monday
at
6:00
Time Range
All time
Schedule Priority
Default
Schedule Window
No window
Trigger Actions
+ Add Actions
When triggered
Send email
Remove
To


Schedule Priority
Default
Schedule Window
Default
Higher
Highest
Trigger Actions



#Field Alias

Alias = nick name

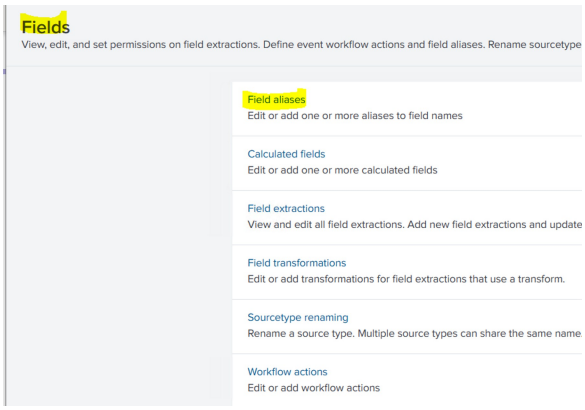
If there are 3 indexes which are having same data but with different field-name

Index1 has UserName as Ankit

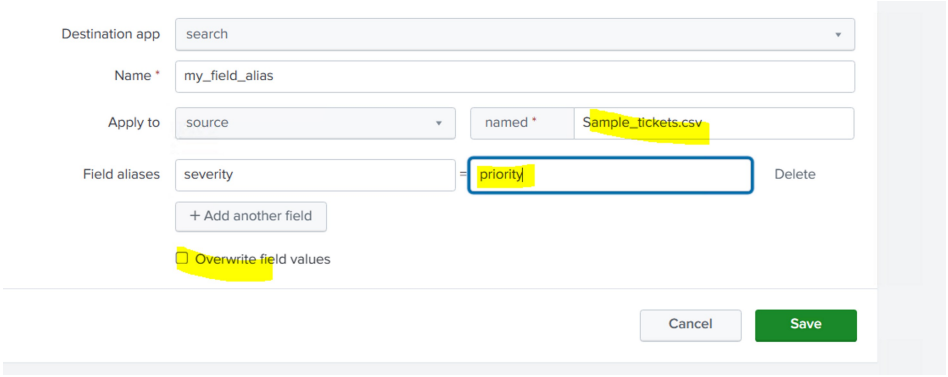
Index2 has EmployeeName as Ankit

Index3 has User_id as Ankit

FieldAlias **add new filed in Dataset.**



Override field value if there is already a field with name of alias



#Field Expression

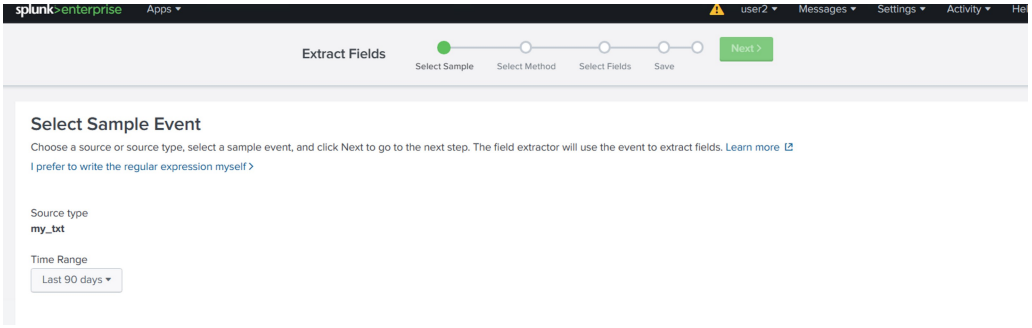
2 Type of Field Expression :

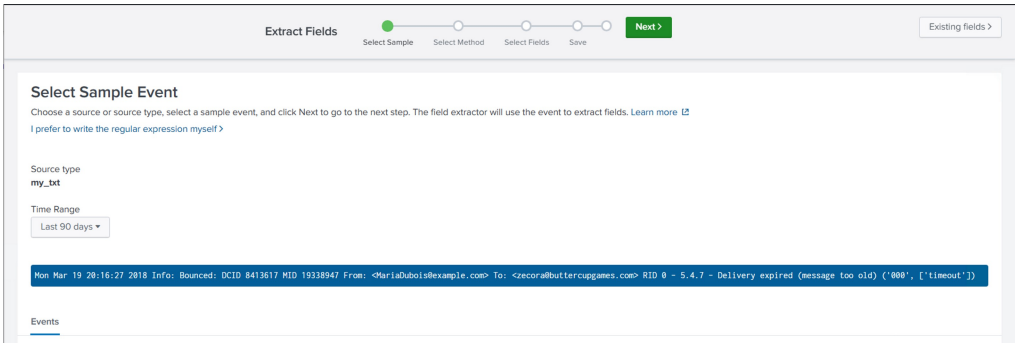
(1) **Regular Expression** : Splunk will write the expression

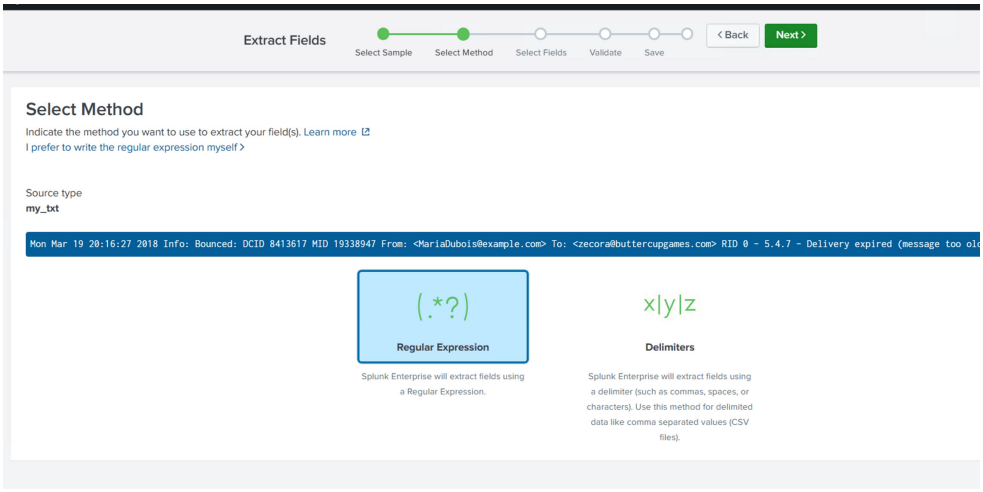
(2) **Delimiter** : symbol-wise splitting of event

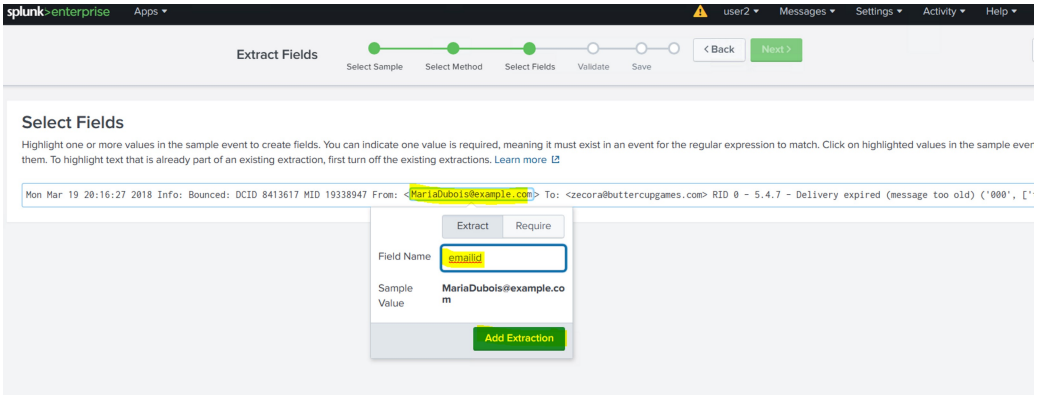
index="my_indx" source="data.txt"

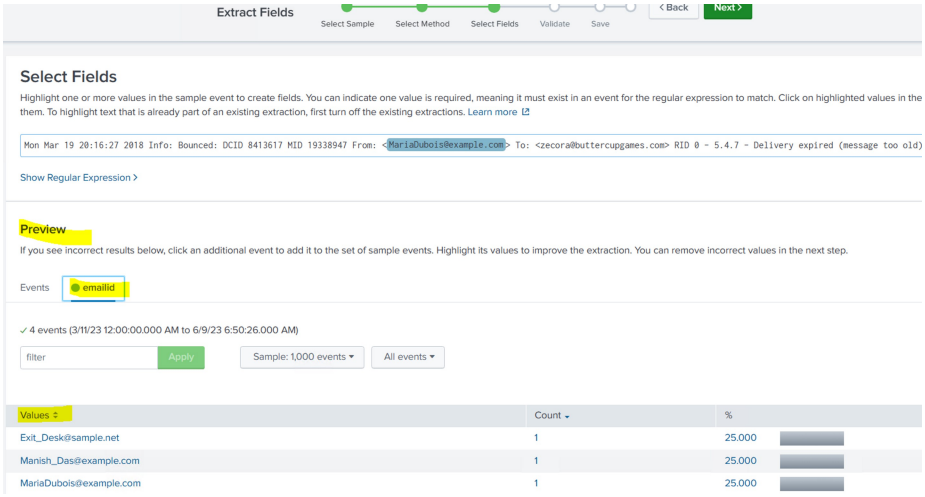
Extarct New Field

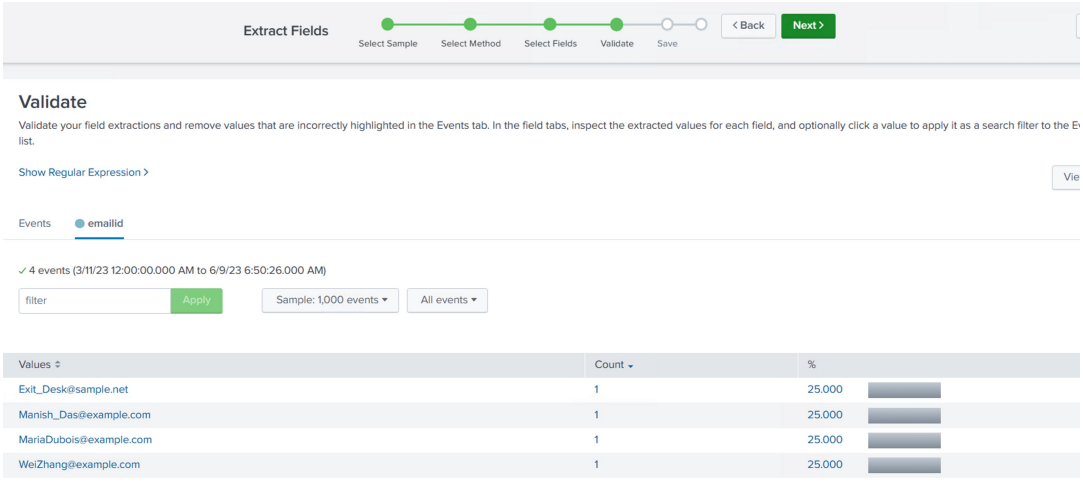


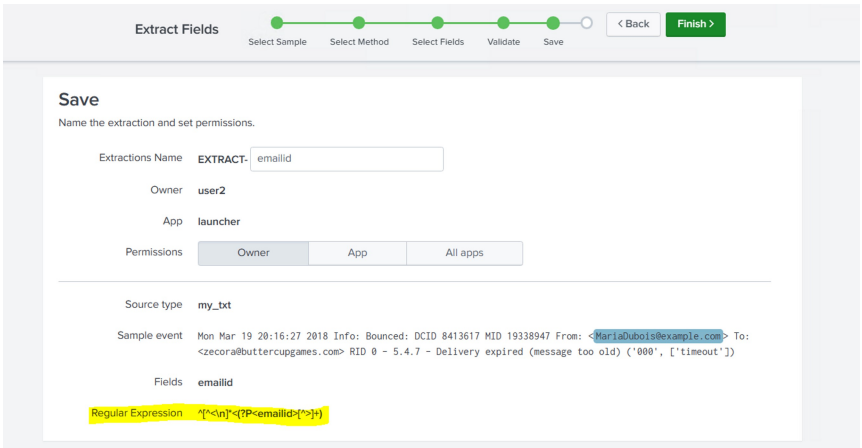




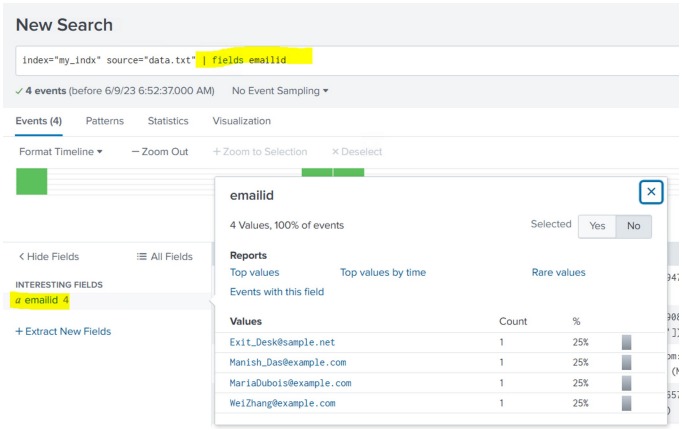




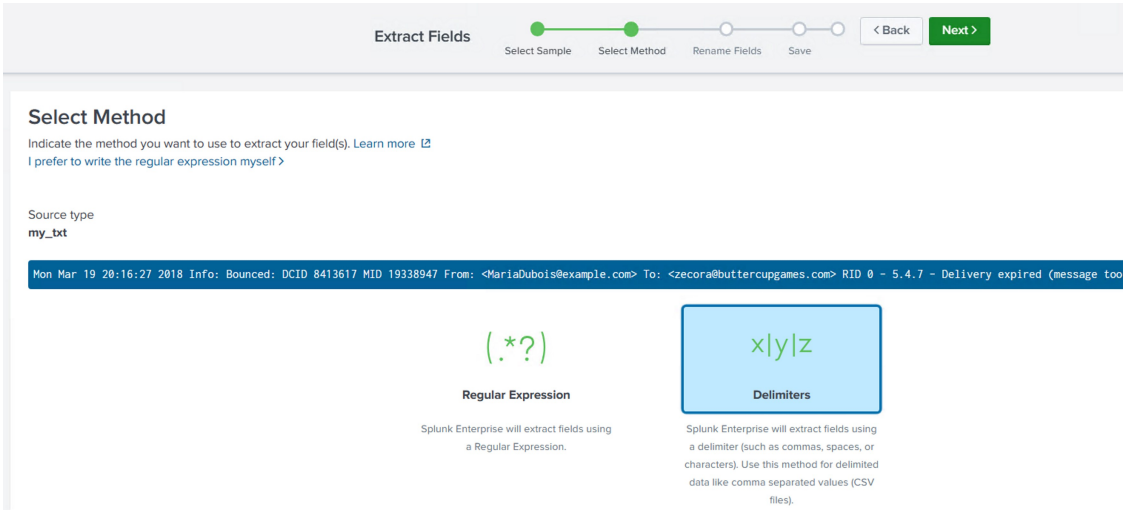


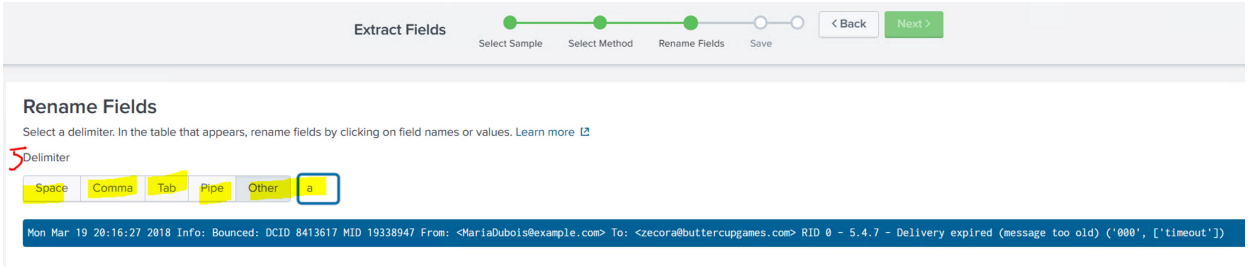


index="my_indx" source="data.txt" | fields emailid

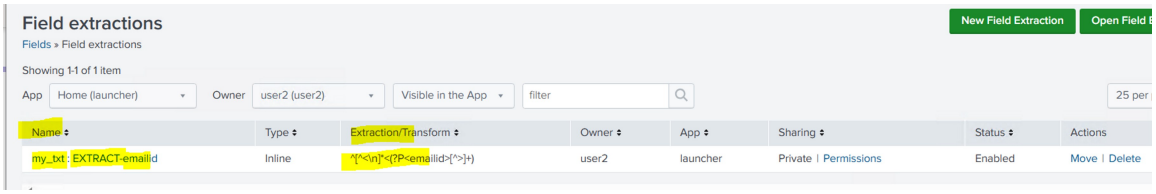


#Delimiter:



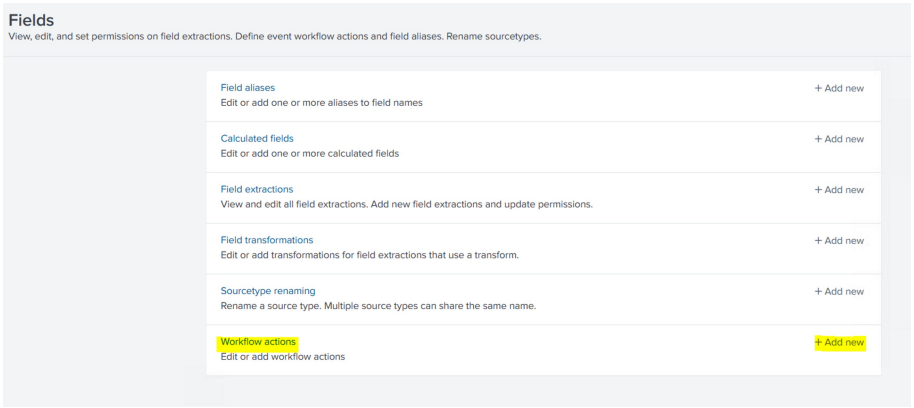


Name of Filed Extraction:

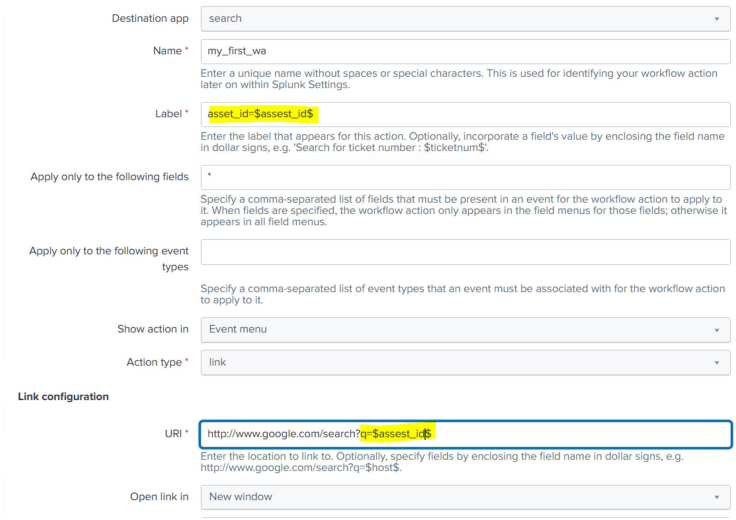


#Workflow Action

Settings => Field =>

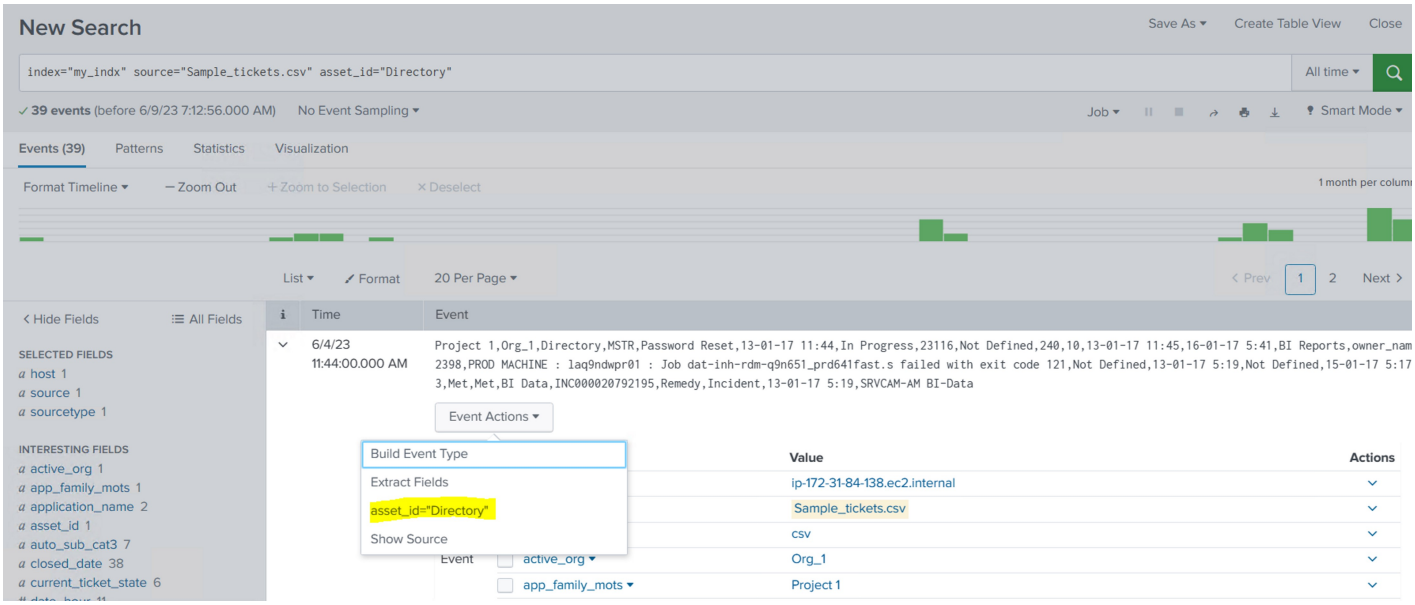


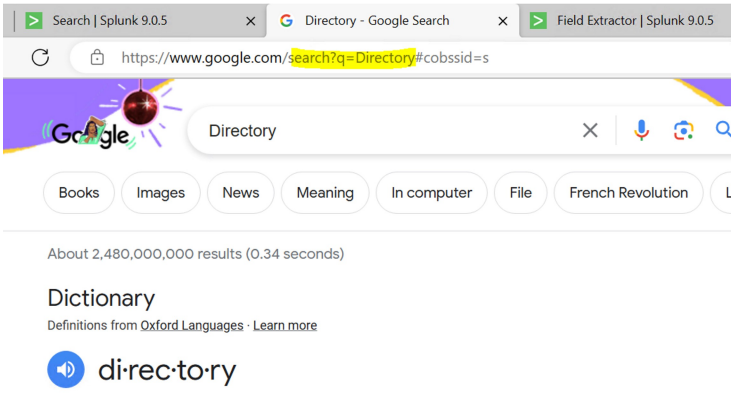
index="my_indx" source="Sample_tickets.csv" asset_id="Directory"



Workflow_action will be visible in "Event Menu" option.

It can be also be visible in "Event menu", "Filed menus" or Both.





Action type = 2kinds

(1) link

(2) search