

Training – Day #9

15 June 2023 06:42

#Dashboard

Dashboard = collection of panels

2 Type of Dashboard builder :

(1) **Classic Type** :

- (i) generated on top of **XML**
- (ii) from starting
- (iii) can integrate with HTML, CSS, JS

(A) **Static Classic Dashboard**

- (i) No option of input from user.

(B) **Dynamic Classic Dashboard**

- (i) Option of input from user. User can enter/filter specific value

(2) **Studio Type** :

- (i) generated on top of **JASON**
- (ii) from v8.2.x
- (iii) ITSI **Glass Table** Generation

3 Optimization Process for Dashboard (in both types):

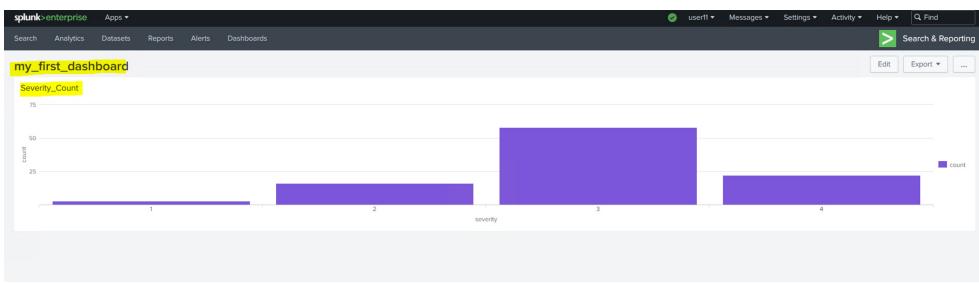
- (1) Base Search
- (2) Saved Search
- (3) Summary Index



How to create a new Dashboard ?

Write a Search query -> save as **New Dashboard** (we can add in an **Existing Dashboard** also)

The screenshot shows the Splunk interface for creating a new dashboard. At the top, there's a search bar with a complex query: `index=_internal _source=*.* _type=stats count | stats count by severity`. Below the search bar, a histogram visualization is displayed, showing the count of events for each severity level (1, 2, 3, 4). The counts are approximately 3, 16, 58, and 22 respectively. To the right of the histogram, a context menu is open, with the 'New Dashboard' option highlighted. Below the histogram, a modal window titled 'Save Panel to New Dashboard' is open. In this modal, the 'Dashboard Title' is set to 'my_first_dashboard'. Under 'Panel Title', the title 'Severity_Count' is entered. Under 'Visualization Type', 'Column Chart' is selected. At the bottom of the modal, there are 'Cancel' and 'Save to Dashboard' buttons.



Add in existing :

source="sample_tickets.csv" host=="ip-172-31-87-147.ec2.internal" | stats count by current_ticket_state

Events Patterns Statistics (6) Visualization

current_ticket_state

current_ticket_state	count
Closed	29
Customer Hold	4
In Progress	15
On Hold	1
Pending	1
Resolved	30

Save Panel to Existing Dashboard

Selected an Existing Dashboard Sort Title (A - Z) ↴

Search By Title

Integrity Check of Installed Files

Job Details Dashboard

jQuery Upgrade

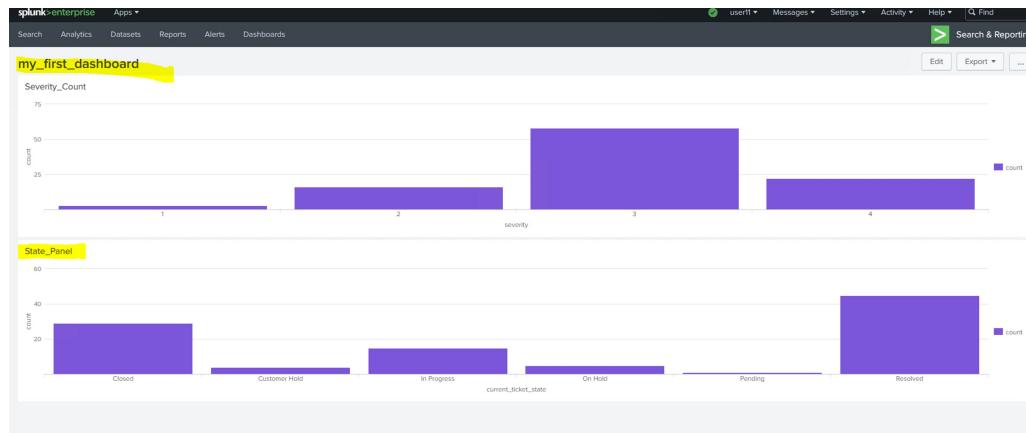
my_first_dashboard

Orphaned Scheduled Searches, Reports, and Alerts

Panel Title **State_Panel**

Visualization Type Column Chart Statistics Table

> Advanced Panel Settings



Options:

my_first_dashboard

Severity_Count

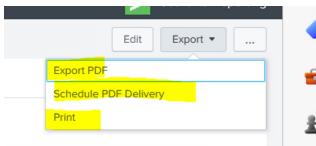
Clone

Clone in Dashboard Studio NEW

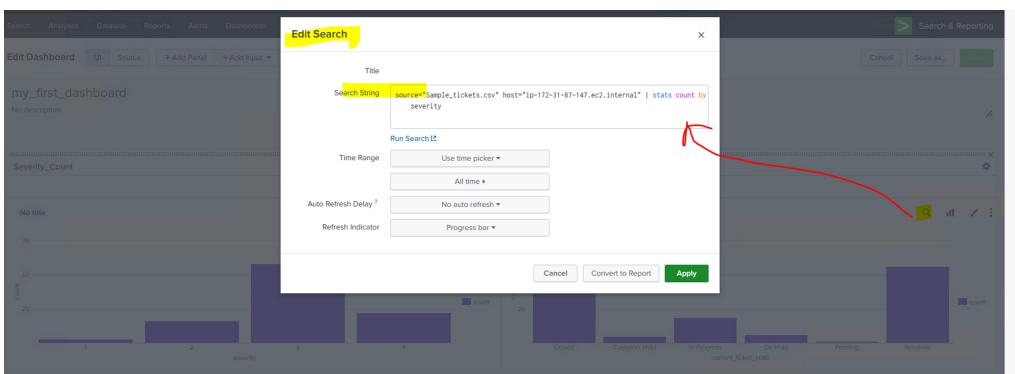
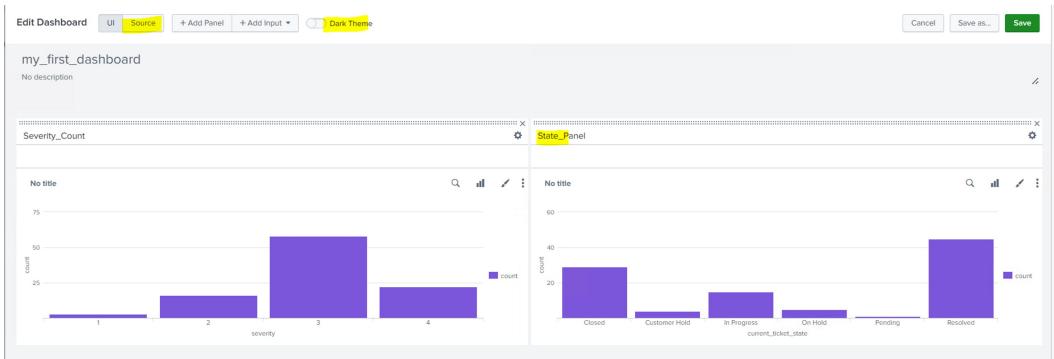
Edit Permissions

Set as Home Dashboard

Delete

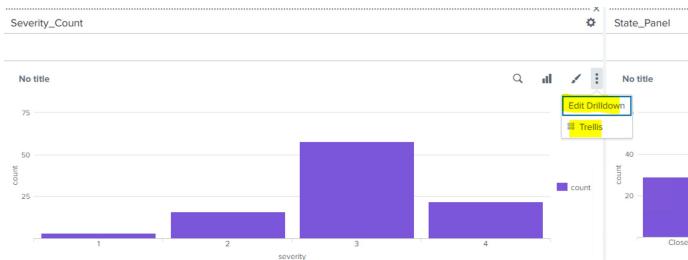


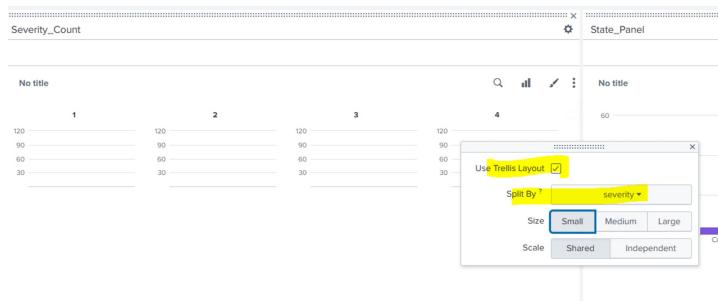
Edit => Drag the Panels to adjust:



Edit Search Dialog Fields:

- Title
- Search String: source="Sample_tickets.csv" host="ip-172-31-87-147.ec2.internal" | stats count by severity
- Run Search
- Time Range: Use time picker ▾
- Auto Refresh Delay: No auto refresh ▾
- Refresh Indicator: Progress bar ▾
- Preview: Background Search with No Progress Bar (checkbox checked)
- Preview and progress bar: Preview Events with Progress Bar (checkbox checked)





Add-Inputs => 8 Types of Inputs

my_first_dashboard
No description

Severity_Count
No title

No title

No title

No title

count

1 2 3 4

count

Closed

Now go to each Panel => and select "Shared Time Picker (time)"

Edit Search

Title

Search String

```
source="Sample_tickets.csv" host="ip-172-31-87-147.ec2.internal" | stats count by severity
```

Run Search

Time Range

Shared Time Picker (time)

Auto Refresh Delay ?

No auto refresh

Refresh Indicator

Progress bar

Cancel Convert to Report Apply

Creating Dropdown input:

T Text

Radio

Dropdown

Checkbox

Multiselect

Link List

Time

General

Label: my_dropdown

Search on Change

Token Options

Token: sev_token

Default?

Clear Selection

Initial Value?

Clear Selection

Token Prefix?

Static Options

Dynamic Options

Cancel **Apply**

T Text

Radio

Dropdown

Checkbox

Multiselect

Link List

Time

General

Token Options

Static Options

Dynamic Options

Content Type

Search String

Run Search

All time

Field For Label?

Field For Value?

Cancel **Apply**

my_dropdown

Select...

1
2
3
4

T Text

Radio

Dropdown

Checkbox

Multiselect

Link List

Time

General

Token Options

Clear Selection

Token Prefix?

Token Suffix?

Static Options

Name	Value
All	t

+Add New +

Dynamic Options

Content Type

Search String

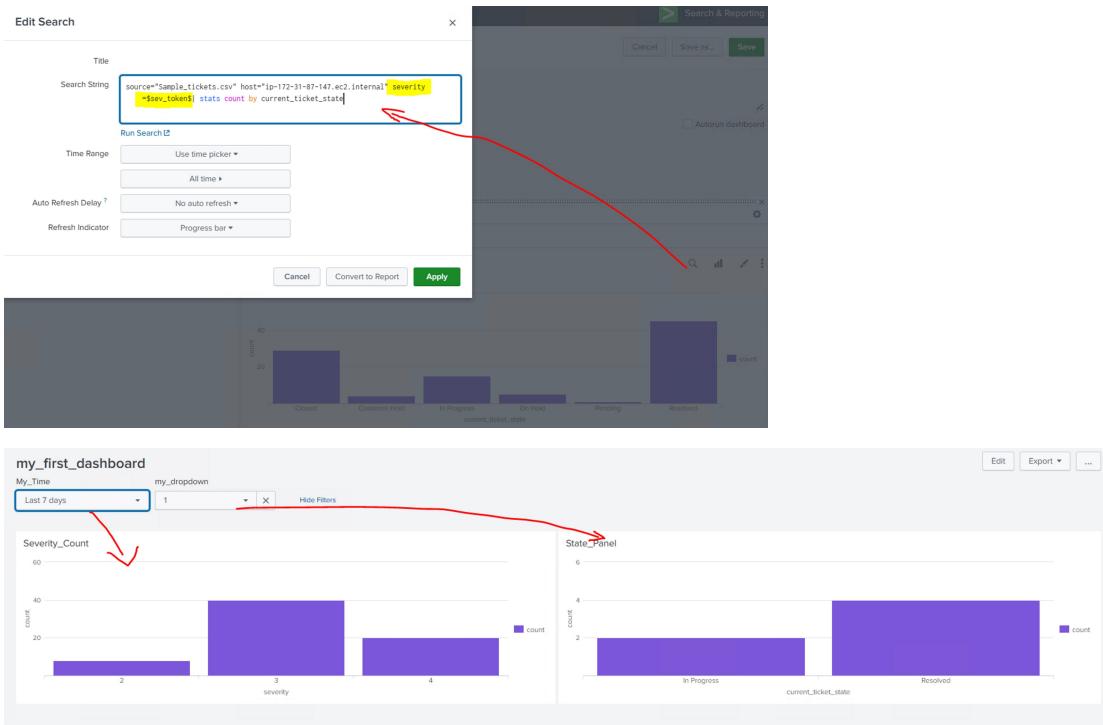
Cancel **Apply**

my_dropdown

Select...

All
1
2
3
4

Mapping dropdown token to dashboard panel :



Creating Multiselect Input:

The figure shows the configuration dialog for a Multiselect input field.

General:

- Label: my_multiselect
- Search on Change: checked

Token Options:

- Token: my_multiselect_token1
- Default: (empty)
- Initial Value: (empty)
- Token Prefix: (empty)
- Token Suffix: (empty)

Dynamic Options:

Content Type:

```
source="Sample_tickets.csv" host="ip-172-31-87-147.ec2.internal" | stats count by current_ticket_state
```

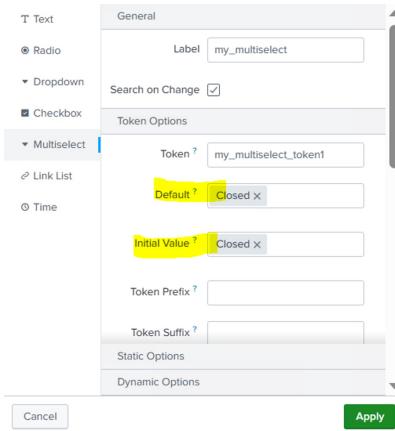
Run Search: All time

Field For Label: current_ticket_state

Field For Value: current_ticket_state

The figure shows the dropdown menu for the 'my_multiselect' field, listing ticket states: Closed, In Progress, Customer Hold, On Hold, Pending, and Resolved.

Again edit and select Default/Initial Value



Map with Panel :

No result as values are not separate

To fix this => Use token_prefix, token suffix, and delimiter :

Note : check the Space in Preview and adjust Space before after "Delimiter"

Modify the search query on panel :

Before :

```
source="Sample_tickets.csv" host="ip-172-31-87-147.ec2.internal"
current_ticket_state="$my_multiselect_token1$" | stats count by current_ticket_state
```

After Modification :

```
source="Sample_tickets.csv" host="ip-172-31-87-147.ec2.internal" "$my_multiselect_token1$"
stats count by current_ticket_state
```

Edit Search

Title

Search String

```
source="sample_tickets.csv" host="ip-172-31-87-147.ec2.internal"
| my_multiselect_tokens | stats count by current_ticket_state
```

Run Search

Time Range

- Use time picker
- All time

Auto Refresh Delay

- No auto refresh

Refresh Indicator

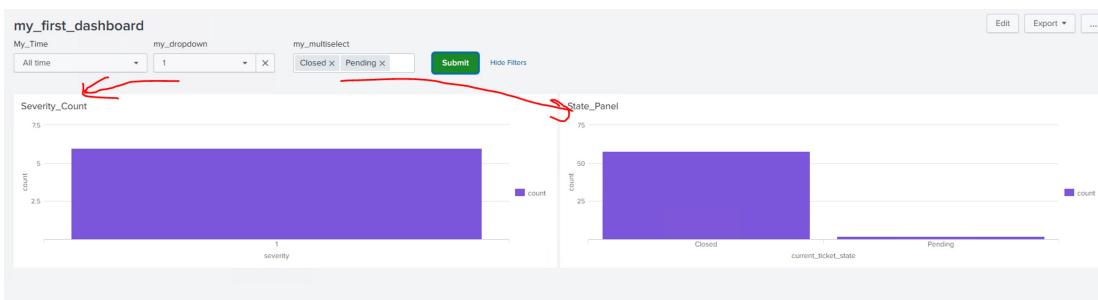
- Progress bar



"SUBMIT" button :

It is used to pass values to panel searches all at a time instead of every change.

Unset all the input "Search on change" and Add a **Submit** button in last:



#Dashboard Optimization :

(1) Base Search :

Base search **create a Virtual table** and from this virtual table we can extract/pull the data in the respective panels/dropdown.

Step #1 : Go to "Source" and add below XML to create base search

```
<search id="base_search1">
<query>
    index=main Sample_tickets.csv" host="ip-172-31-87-147.ec2.internal" | table severity,
    current_ticket_state
</query>
<earliest>0</earliest>
<latest>now</latest>
</search>
```

Step #2 : Edit the <search> and <query> in panel

NOTE :

- (1) base search query should be transformational
 - (2) base search will generate virtual table at each refresh of dashboard

(1) *Saved Search* :

Saved search will also create a Virtual table, but it will not be created every refresh of dashboard but we have to define a time-interval like every 15 min or 30 min and virtual table will be created at that time-interval.

After 7.x Splunk has merged the Saved Search with Report generation

Step #1 : Create a Report let's name "**my_savedsearch_report_name**" and schedule its time interval.

Edit Schedule

Scheduling this report results in removal of the time picker from the report display.

Report **my_savedsearch_report_name**

Schedule Report [Learn More ↗](#)

Schedule: **Run on Cron Scheduler** [Change](#) [Run Now](#)

Cron Expression: **/10 * * * *** e.g. 00 08 *** (every day at 8PM) [Learn More](#)

Time Range

Schedule Priority? **Default** [Change](#)

Schedule Window? **No window** [Change](#)

Trigger Actions

[+ Add Actions ▾](#)

[Cancel](#) [Save](#)

Step #2 : In Dashboard add in xm

```
<search id="saved search" ref="my savedsearch report name"></search>
```

```
1 //UI Variables defined
2
3 <form version="1.1">
4   <label>My First Dashboard</label>
5
6   <search id="base_search1">
7     <query>
8       index=main Sample_tickets.csv host="ip-172-31-87-147.ec2.internal" | table severity, current_ticket_state
9     </query>
10    <earliest>@{@earliest}
11    <latest>now@{@latest}
12  </search>
13
14  <search id="saved_search" ref="My_savedsearch_report_name"></search>
15
16  <submit submitButton="true" autoRun="false">
17    <input type="time" token="time" searchWhenChanged="false">
18      <label>My_Time</label>
19
20      <earliest>7d@{@earliest}
21      <latest>now@{@latest}
22    </default>
23  </input>
24
25  <input type="dropdown" token="sev_token" searchWhenChanged="false">
26    <label>My_Dropdown</label>
27    <choice value="">All</choice>
```

(3) Summary Index :

It will writes the output of a search query into a **separate index**.

Downside : more resource consumption but will not cost license as sourcetype as "stash"

We can manually push the data
Or we can use automatic one.

(1) Manual creation of Summary-Index:

Step #1 : create an index

Step #2 : prepare search query and add " | collect index=<new index name> "testmode=true"

testmode=true => it will only show the data but will not push the data into index
testmode = false => it will push the data into index

New Search

```
source="Sample_tickets.csv" host="ip-172-31-87-147.ec2.internal" severity=1 | stats count by current_ticket_state | collect index="my_summary" testmode=true
```

Events (6) Patterns Statistics (2) Visualization

Time	Event
12/16/22 12:38:00:000 PM	Project 1,Org_1,Directory,MSTR,Password Reset,24-11-16 8:23,Resolved,176637,Not Defined,270,28,24-11-16 8:23,24-11-16 8:23,BI Reports,owner_name1638,SAP BI report -16 7:19,22-11-16 7:19,24-11-16 8:23,1,Met,Net,RI Reports,INC200820614689,Remedy,RTC Work Request,22-11-16 7:19,SRVCAH-M BI-Reports host= ip-172-31-87-147.ec2.internal source = Sample_tickets.csv sourcetype = csv
12/16/22	Project 1,Org_1,Directory,MSTR,Password Reset,24-11-16 8:23,Resolved,176637,Not Defined,270,28,24-11-16 8:23,24-11-16 8:23,BI Reports,owner_name1638,SAP BI report

Step #3 : prepare search query and add " | collect index=<new index name> "testmode=false"

```
source="Sample_tickets.csv" host="ip-172-31-87-147.ec2.internal" severity=1 | stats count by current_ticket_state | collect index="my_summary" testmode=false
```

Data will get saved into index with sourcetype as "stash"

New Search

```
Index="my_summary"
```

Events (2) Patterns Statistics Visualization

Time	Event
6/15/23 06:25:13:000 AM	06/15/2023 06:25:13 +0000, info_search_time=1686810313.126, count=4, current_ticket_state=Resolved host = ip-172-31-87-147.ec2.internal source = /home/ec2-user/splunk/var/spool/splunk/c414c36d8caa306b_748d05730eb... sourcetype = stash
6/15/23 06:25:13:000 AM	06/15/2023 06:25:13 +0000, info_search_time=1686810313.126, count=2, current_ticket_state="In Progress" host = ip-172-31-87-147.ec2.internal source = /home/ec2-user/splunk/var/spool/splunk/c414c36d8caa306b_748d05730eb... sourcetype = stash

(2) Automated creation of Summary-Index:

Step #1 : Create a Report Settings=> Report => Edit Report

Step #2 : Enable Summary Indexing by "Edit Summary Index" and give details

Searches, Reports, and Alerts

Searches, reports, and alerts are saved searches created from pivot or the search page. Learn more [? help](#)

1 Searches, Reports, and Alerts Type: All ▾ App: Search & Reporting (search) ▾ Owner: (user1) ▾ filter

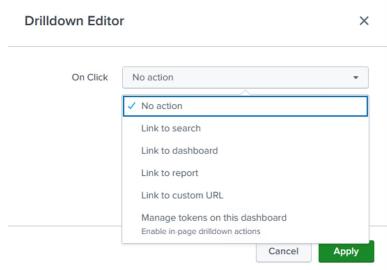
Name	Actions	Type
my_savedsearch_report_name	Edit ▾ Run View Recent Report	

my_savedsearch_report_name

- [Edit Search](#)
- [Edit Permissions](#)
- [Edit Schedule](#)
- [Edit Acceleration](#)
- [Edit Summary Indexing](#)
- [Disable](#)
- [Advanced Edit](#)
- [Clone](#)
- [Embed](#)
- [Move](#)
- [Delete](#)

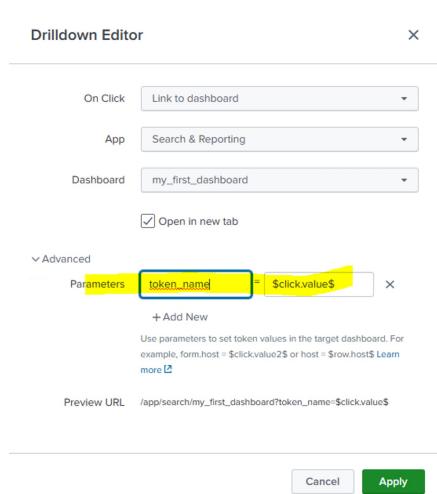
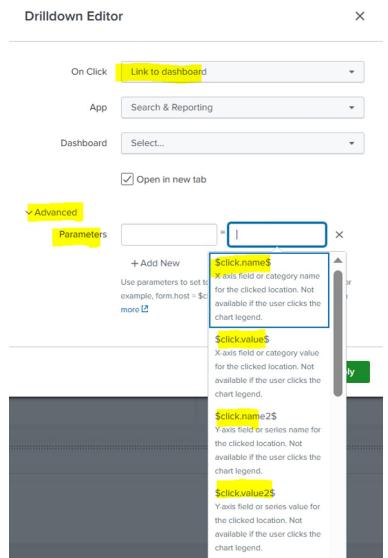
(1) Drilldown in Dashboard :

If I will click any graph/column then it will show the backend events in separate page.



Question : How to pass the value from One dashboard to other ?
 Answer : Use drilldown => "Link to dashboard"

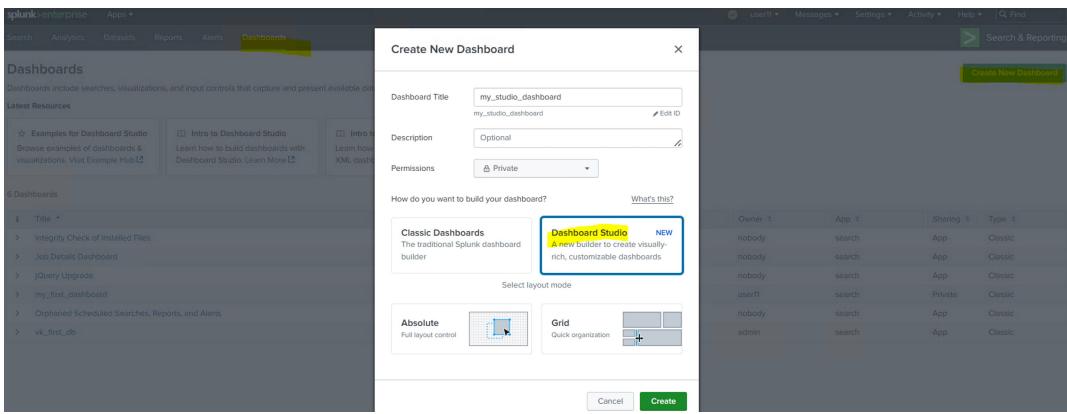
Click on Name
 Click on Value



(2) STUDIO Dashboard:

1. Backend query is in JSON
2. Can add Background Image (**those images are get stored in KV store**)
3. **Integration not possible** with HTML, CSS

How to create a Studio Dashboard ?



Splunk enterprise Apps ▾

Search Analytics Datasets Reports Alerts Dashboards

Gridlines 119% Light View Save

my_studio_dashboard

This is for the dashboard description.

Global Time Range

Configuration

Canvas

Display Mode

Canvas Width Canvas Height

Background Color

Background Image
Drop your file here or browse...

Note: Uploaded image files can be accessed and deleted by others in your organization

Preferences Show Title & Description

View Options Show Edit Button

Splunk enterprise Apps ▾

Search Analytics Datasets Reports Alerts Dashboards

Gridlines 119% Light View Save

my_studio_dashboard

This is for the dashboard description.

Global Time Range

Search & Reporting

Search

Saved Search

Chain Search

Data Overview

Difference between Search and Chain Search ??

Settings Background via Canvas :

Search Analytics Datasets Reports Alerts Dashboards

Gridlines 119% Light View Save

my_studio_dashboard

This is for the dashboard description.

Global Time Range

Configuration

Canvas

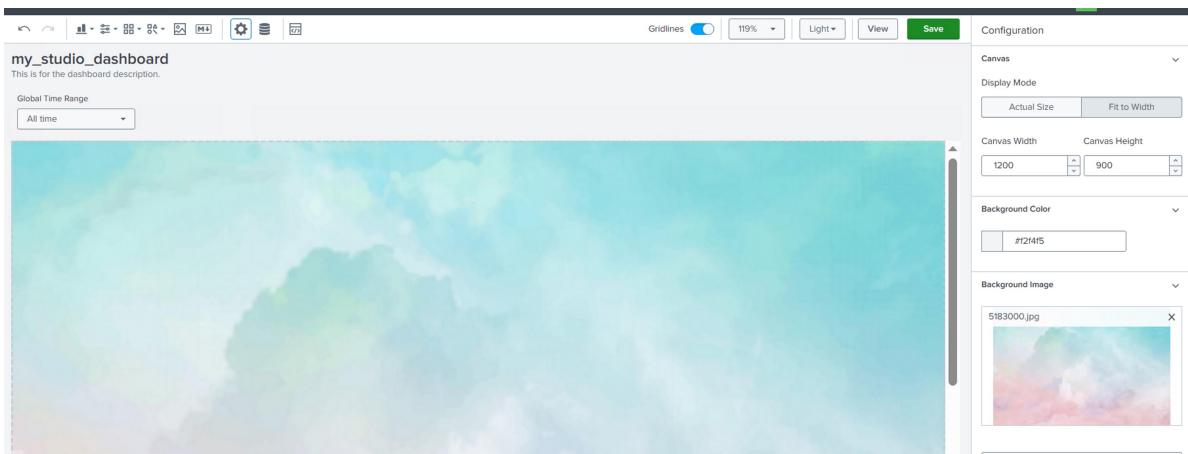
Display Mode

Canvas Width Canvas Height

Background Color

Background Image
Drop your file here or browse...

Note: Uploaded image files can be accessed and deleted by others in your organization



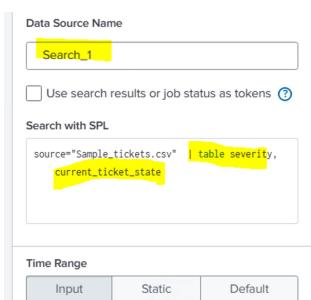
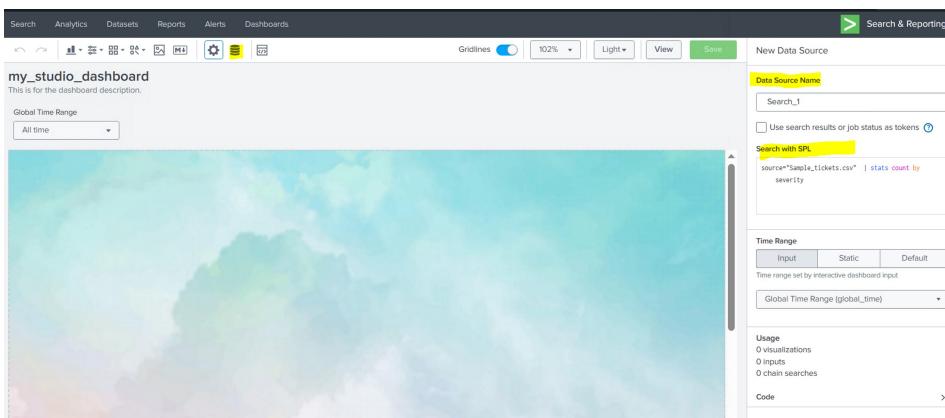
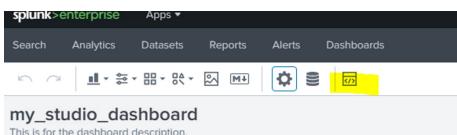
Background image is getting stored in kvstore:

```

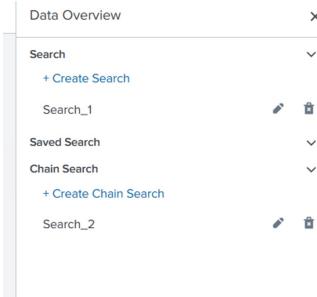
5 },
6   "layout": {
7     "type": "absolute",
8     "options": [
9       "display": "auto-scale",
10      "backgroundImage": {
11        "sizeType": "contain",
12        "x": 0,
13        "y": 0,
14        "src": "splunk-enterprise-kvstore://648ab5eeecb5f9b051f2a7a65"
15      }
16    },
17    "structure": [],
18    "globalInputs": [
19      "input_global_trp"
20    ]
21  }

```

Check the JSON :



Search should be like base search => table command



Select a Graph => click Cancel => then select "Data Configuration"

The screenshot shows the Splunk dashboard configuration interface. A histogram visualization is selected, showing a distribution of 'severity' levels (1, 2, 3, 4) with counts of approximately 10, 30, 110, and 50 respectively. To the right, the 'Configuration' panel is open, showing the 'Data Configurations' section with 'Search_1' selected. Other sections include 'Visualization Options' (set to 'Column'), 'Position & Size' (X: 0, Y: 0, Width: 300, Height: 300), and 'General'.

JSON:

```
my_studio_dashboard
1  {
2     "visualizations": [
3         "viz_1031088h": {
4             "type": "splunk.column",
5             "options": {},
6             "dataSources": [
7                 {
8                     "primary": "ds_ofaRSNE"
9                 }
10            ]
11        },
12        "ds_ofaRSNE": {
13            "type": "ds-search",
14            "options": {
15                "query": "sources\\\"Sample_tickets.csv\\\" | stats count by severity",
16                "queryParameters": [
17                    "earliest": "$global_time.earliest$",
18                    "latest": "$global_time.latest$"
19                ],
20            },
21            "name": "Search_1"
22        },
23        "ds_ykxk8Ht": {
24            "type": "ds-chain",
25            "options": {
26                "extend": "ds_ofaRSNE"
27            },
28            "name": "Search_2"
29        }
30    },
31    "defaults": {
32        "dataSources": [
33            "ds.search": {
34                "options": {

```

Note : There is no save button. If any modification is done, it will not allow us to go back until we remove that modification from JSON

#Scripted Input

Data ingestion will done through an script.

TMDB website for movie details => create account and get API key

[The Movie Database \(TMDB\) \(themoviedb.org\)](http://The Movie Database (TMDB) (themoviedb.org))

Script						New Local Script		
Data inputs > Script								
Showing 1-25 of 25 items						25 per page		
Command	Interval	Source type	App	Status	Actions			
\$SPLUNK_HOME/etc/apps/Splunk_TA_snow/bin/migrate_existing_filter_parameter.py	-1	script	Splunk_TA_snow	Enabled Disable	Clone			
\$SPLUNK_HOME/etc/apps/python_upgrade_readiness_app/bin/era_email_notification_switch_scripted_input.py	0 */4 * * *	script	python_upgrade_readiness_app	Enabled Disable	Clone			
\$SPLUNK_HOME/etc/apps/python_upgrade_readiness_app/bin/era_remote_latest_report.py	0 7:19 */1 * *	script	python_upgrade_readiness_app	Enabled Disable	Clone			

Note :

(1) script can be anywhere but it must be in **/bin** folder (if SaaS, then store the script in Heavy Forwarder)

Add Data < Back Next >

Select Source Input Settings Review Done

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Scripts
Get data from any API, service, or database with a script.

Splunk Assist Instance Identifier
Assigns a random identifier to every node

Systemd Journal Input for Splunk
This is the input that gets data from journal (systemd's logging component) into Splunk.

Splunk Secure Gateway
Initializes the Splunk Secure Gateway application to talk to mobile clients over websockets

Configure this instance to execute a script or command and to capture its output as event data.
Scripted inputs are useful when the data that you want to index is not available in a file to monitor.

Learn More ↗

Script Path : \$SPLUNK_HOME/bin/scripts
\$SPLUNK_HOME/etc/apps/Splunk_TA_snow/bin

Command : \$SPLUNK_HOME/etc/apps/python_upgrade_readiness_app/bin/era_email_notification_switch_scripted_input.py

Interval Input : \$SPLUNK_HOME/etc/apps/search/bin

Interval : \$SPLUNK_HOME/etc/apps/splunk_essentials_9_0/bin

Source name override : \$SPLUNK_HOME/etc/apps/splunk_instrumentation/bin

\$SPLUNK_HOME/etc/apps/splunk_metrics_workspace/bin

FAQ

> What kind of scripts can I run?
> How do I control when scripts run?

Add Data < Back Next >

Select Source Input Settings Review Done

Configure this instance to execute a script or command and to capture its output as event data.
Scripted inputs are useful when the data that you want to index is not available in a file to monitor.

Learn More ↗

Script Path : \$SPLUNK_HOME/etc/apps/search/bin

Script Name : xmilkv.py

Command : \$SPLUNK_HOME/etc/apps/search/bin/xmilkv.py

Interval Input : In Seconds

Interval : 60.0

Source name override : optional

Add Data < Back Review >

Select Source Input Settings Review Done

Source type

The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Select New Select Source Type ↗

App context

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. Learn More ↗

App Context : Search & Reporting (search)

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More ↗

Host field value : ip-172-31-87-147.ec2.internal

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can

Index : Default Create a new index

#Index Time Field Extraction

Pull the event at the time of insertion into index