

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 **Hierarchical concept** means Root event can have child event -> child will have sub-child

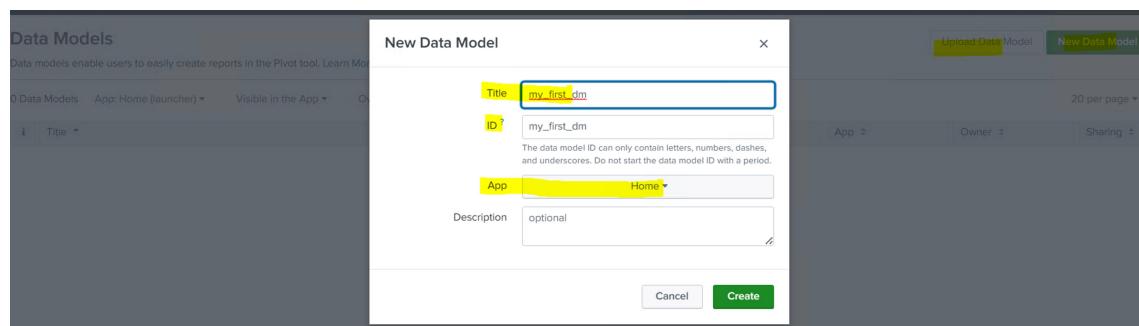
(2) **Define the fields explicitly** (exact needed fields)=> like index="my_indx" will show all events with all fields, BUT Data-model will show advanced specific fields. **So Data-Model will reduce time of result in large result queries.**

(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"`

my_first_dm

my_first_dm

< All Data Models

Datasets Add Dataset ▾ my_root my_root

EVENTS

my_root

CONSTRAINTS

index="my_idx" source="Sample_tickets.csv"

Constraint Edit

Bulk Edit ▾ INHERITED

_time Time
 host String Override
 source String Override
 sourcetype String Override

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

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 **CALCULATED fields**

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

INHERITED

_time Time
 host String Override
 source String Override
 sourcetype String Override

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

Add Field ▾

Auto-Extracted

- Eval Expression
- Lookup
- Regular Expression
- Geo IP

Add Auto-Extracted Field

- > last_modified_time
- > last_resolved_date
- > linecount
- > lob_name
- > owner_name

my_root
my_root

CONSTRAINTS

index="my_idx" source="Sample_tickets.csv"

Ren

Bulk Edit ▾

INHERITED

_time	Time	
<input type="checkbox"/> host	String	Override
<input type="checkbox"/> source	String	Override
<input type="checkbox"/> sourcetype	String	Override

EXTRACTED

<input type="checkbox"/> current_ticket_state	String	Edit
<input type="checkbox"/> severity	Number	Edit
<input type="checkbox"/> ticket_number	String	Edit
<input type="checkbox"/> time_submitted	String	Edit

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.

Edit Fields with an Eval Expression

Data Model: my_first_dm Dataset: my_root

Eval Expression

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

Field

Field Name:	Display Name:	Type:	Flags:
sev	sev	String	Optional

Examples:

```
case(error == 404, "Not found", error == 500, "Internal Server Error")
if(cidrmatch("192.0.0.0/16", clientip), "local", "other")
```

[Learn More](#) ↗

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

my_root
my_root

Rename Delete

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

Add Fields with a Lookup

Data Model: my_first_dm Dataset: my_root

Lookup Table

Field in Lookup:	Field in Dataset:
ticket_number	= raw

Input

Field in Lookup: ticket_number Field in Dataset: ticket_number

Add New

Output

Field in Lookup: ticket_number Field in Dataset: ticket_number Display Name: ticket_number Type: String Flags: Optional

time_taken time_taken String Optional

Buttons: Cancel, Preview, Save

my_root
my_root

CONSTRAINTS

index="my_idx" source="Sample_tickets.csv"

Bulk Edit ▾ **Add Field ▾**

INHERITED

_time	Time	
<input type="checkbox"/> host	String	Override
<input type="checkbox"/> source	String	Override
<input type="checkbox"/> sourcetype	String	Override

EXTRACTED

current_ticket_state	String	Edit
<input type="checkbox"/> severity	Number	Edit
<input type="checkbox"/> ticket_number	String	Edit
<input type="checkbox"/> time_submitted	String	Edit

CALCULATED

sev	String	Eval Expression	Edit
<input checked="" type="checkbox"/> time_taken	String	Lookup	Edit

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

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

my_first_dm

my_first_dm

Datasets **Add Dataset ▾**

EVENTS

my_root	Root Event
	Root Transaction
	Root Search
<input checked="" type="checkbox"/> Child	

my_root

Root Event

CONSTRAINTS

index="my_idx" source="

Bulk Edit ▾

INHERITED

_time	
<input type="checkbox"/> host	

Add Dataset as "Child"

Add Child Dataset

Data Model: my_first_dm

Dataset Name my_child

Additional Constraints

Examples:
uri="*.php*" OR uri="*.py*"
NOT (referer=null OR referer="-")

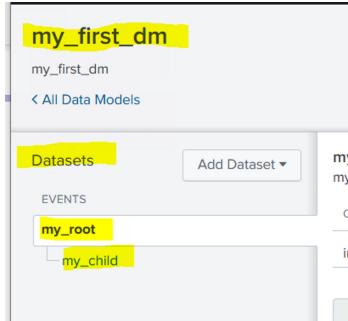
Dataset ID my_child

The dataset ID can only contain letters, numbers, dashes, and underscores. Do not start the dataset ID with a period.

Inherit From my_root

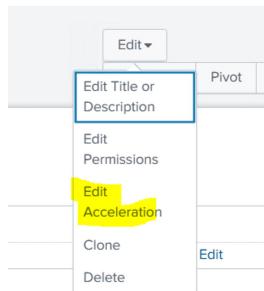
Buttons: Documentation, Cancel, Preview, Save

It will in Hierarchy to Root dataset :



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

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.

Edit Acceleration

Data Model my_first_dm

Accelerate Acceleration may increase storage and processing costs.

Summary Range? 1 Day ▾

Advanced Settings

Change the following settings only if you are experiencing summary creation issues. Learn More ↗

Backfill Range? Match Summary Range ▾

Max Summarization Search Time? 1 Hour ▾

Maximum Concurrent Summarization Searches? 3 - +

Poll Buckets For Data To Summarize?

Summarization Period? */5 * * * *

Cancel **Save**

my_first_dm

my_first_dm

< All Data Models

⚠ This Data Model cannot be edited because it is accelerated. Disable acceleration in order to edit the Data Model.

Datasets

EVENTS

my_root

- my_child

my_child

CONSTRAINTS

index="my_idx" source="Sample_tickets.csv" (None)

Inherited Constraint

INHERITED

Edit **Download**

#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.

my_first_dm

my_first_dm

< All Data Models

Edit **Download** **Pivot** **Documentation**

Select a Dataset

i 2 Objects in my_first_dm

> my_root

> my_child

New Pivot

✓ 99 events (before 6/9/23 4:57:30.000 AM)

Filters All time +

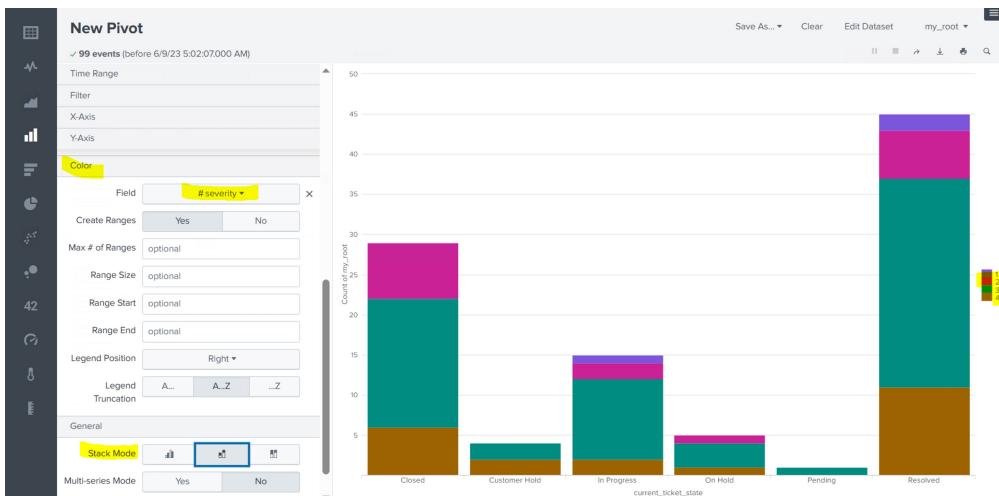
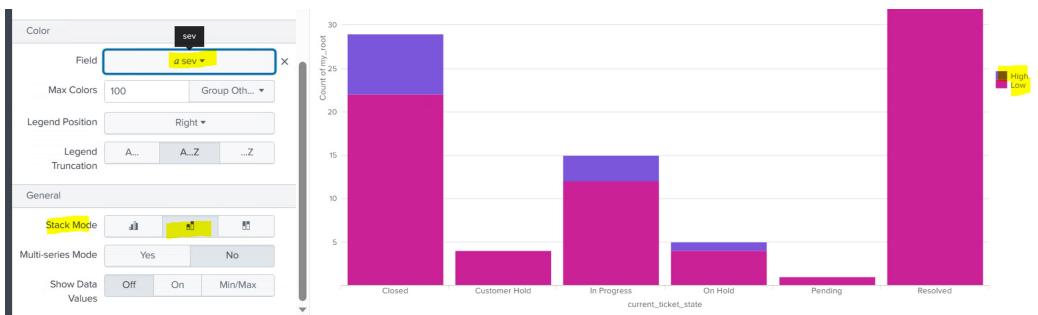
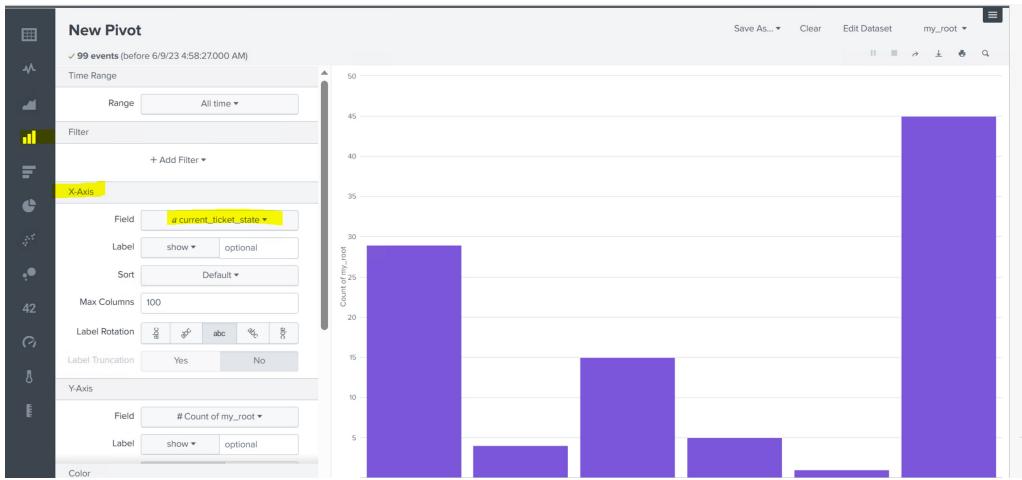
Split Rows +

Count of my_root 99

Save As... Clear Edit Dataset my_root Documentation

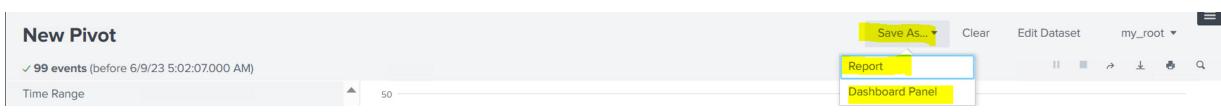
Split Columns +

Column Values Count of my_root +



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

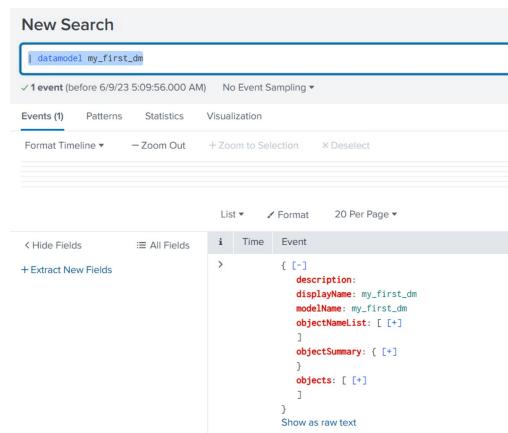


```
| pivot my_first_dm my_root count(my_root) AS "Count of my_root" SPLITROW current_ticket_state
AS current_ticket_state SPLITCOL severity SORT 100 current_ticket_state ROWSUMMARY 0
COLSUMMARY 0 NUMCOLUMNS 1000 SHOWOTHER 0
```



#Datamodel command :

```
| datamodel my_first_dm
| datamodel <datamodel name>
```



| datamodel my_first_dm my_root

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

New Search

| datamodel my_first_dm my_root

✓ 1 event (before 6/9/23 5:10:44.000 AM) No Event Sampling ▾

Events (1) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect

List ▾ Format 20 Per Page ▾

< Hide Fields	All Fields	i Time	Event
+ Extract New Fields		>	<pre>{ autoextractSearch: search (index=< OR index=_) (index="my_idx" source="Sample_tickets.csv") calculations: [[+]] comment: constraints: [[+]] displayName: my_root fields: [[+]] indexScopeWarning: false lineage: my_root objectAccelerationSearch: search (index=< OR index=_) (index="my_idx" source="Sample_tickets.csv") eval nodename = "my_root" eval sev;if(severi "High" "Low") lookup my_lookup_definition ticket_number AS _raw OUTPUT time_taken AS time_taken eval is_my_child;if(searchmatch("0"))1,0, is_not_my_child=1-is_my_child eval nodename = if(nodename == "my_root" AND searchmatch("0"), mvappend(nodename, "my_root.my_child"), nodename) renam</pre>

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

New Search

| datamodel my_first_dm my_root search

✓ 99 events (before 6/9/23 5:11:41.000 AM) No Event Sampling ▾

Events (99) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect

1 month per column

List ▾ Format 20 Per Page ▾

< Hide Fields	All Fields	i Time	Event
SELECTED FIELDS		> 6/6/23 5:41:00.000 AM	Project 1,Org_1,,MSTR,Access,16-01-17 5:41,In Progress,3618,Not Defined,240,10,16-01-17 5:41,15-01-17 5:17,BI Reports,owner_name3272,PROD MACHINE 1a q9ndwpr01: Error Code: 510 Job dat-inh-rdm-q9n558_rdm550sqppsmdf.s is running longer,Not Defined,13-01-17 4:16,Not Defined,15-01-17 5:17,3,Met,Met,BI Data,INC000020793170,Remedy,Incident,13-01-17 4:16,SRVCAM-AM BI-Data host = ip-172-31-84-138.ec2.internal source = Sample_tickets.csv sourcetype = csv
INTERESTING FIELDS		> 6/6/23 5:17:00.000 AM	Project 1,Org_1,,MSTR,Training / How to,15-01-17 5:17,In Progress,650,Not Defined,150,10,15-01-17 5:17,15-01-17 5:17,BI Reports,owner_name2398,PROD M ACHINE vwhemstrp05: Error Code: 510 Job rpt-inh-mst-lcl711_s1v0003.f is running longer than t,Not Defined,13-01-17 5:00,Not Defined,14-01-17 5:11,2, Met,Met,BI Reports,INC000020793217,Remedy,Incident,13-01-17 5:00,SRVCAM-AM BI-Reports host = ip-172-31-84-138.ec2.internal source = Sample_tickets.csv sourcetype = csv
		> 6/6/23 5:17:00.000 AM	Project 1,Org_1,,MSTR,Configuration,15-01-17 5:17,In Progress,1198924,Not Defined,Not Defined,10,15-01-17 5:17,14-01-17 5:11,BI Reports,owner_name138 7,Access enabled. Confirmed from user.,Not Defined,30-01-16 3:44,30-01-16 3:44,13-02-16 12:46,3,Met,Met,BI Reports,INC000019343584,Remedy,Incident,30

INTERESTING FIELDS

a my_root.current_ticket_state 6
my_root.is_my_child 1
my_root.is_not_my_child 1
a my_root.sev 2
my_root.severity 4
a my_root.ticket_number 99
a my_root.time_submitted 94

+ Extract New Fields

Edit Permission:

Data Models

Data models enable users to easily create reports in the Pivot tool. Learn More [Learn More](#)

Upload Data Model New Data Model

1 Data Models	App: Search & Reporting (search) ▾	Visible in the App ▾	Owner: (user2) ▾	filter	Actions	Type ▾	App ▾	Owner ▾	Sharing ▾
i Title ▾						data model	launcher	user2	Global
> my_first_d									

20 per page ▾

Edit Datasets
Edit Title or Description
Edit Permissions
Edit Acceleration
Clone

#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

splunk>enterprise Apps ▾

Searches, Reports, and Alerts

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

New Report New Alert

Name ▾	Actions	Type	Next Scheduled Time ▾	Display View ▾	Owner ▾	App ▾	Alerts ▾	Sharing ▾	Status ▾
0 Searches, Reports, and Alerts	Type: All ▾	App: Search & Reporting (search) ▾	Owner: (user2) ▾	filter					10 per page ▾

Hour < Day < Week < Month < Cron

Create Alert

Settings

Title: my_alert
Description: index="my_index"
Search: enter search here...
App: Search & Reporting (search)
Permissions: Private Shared in App
Alert type: Scheduled Real-time
Run every week ▾
On: Monday ▾ a Run every hour
Expires: 24 Run every day
Trigger Conditions: Run every week
Trigger alert when: Run on Cron Schedule

Cancel Save

<https://crontab.guru/>

```
index="my_idx" source="sample_tickets.csv"
| stats count by severity
```

Create Alert

Settings

Title: my_alert

Description: Optional

Search: index="my_idx" source="sample_tickets.csv" | stats count by severity

App: Search & Reporting (search)

Permissions: Private Shared in App

Alert type: Scheduled Real-time

Run on Cron Schedule

Time Range: All time

Cron Expression: 0/2 * * * *

e.g. 00 18 *** (every day at 6PM). Learn More

Expires: 24 hour(s)

Run on Cron Schedule

Last 15 minutes

Cron Expression: */15 * * * *

e.g. 00 18 *** (every day at 6PM). Learn More

Expires: 24 hour(s)

Trigger Conditions

Trigger alert when: Number of Results

is greater than: 0

Trigger: Once For each result

Throttle?

Trigger Actions

+ Add Actions

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

Throttle?

- Suppress triggering for: 60 second(s)

Action=> 8 type of Actions

Trigger:

- Add to Triggered Alerts
- Add this alert to Triggered Alerts list

Trigger:

- Log Event
- Send log event to Splunk receiver endpoint

Output results to lookup

Output the results of the search to a CSV lookup file

Output results to telemetry endpoint

Custom action to output results to telemetry endpoint

Suppress:

- Run a script
- Invoke a custom script

T Send email

+ Add Actions

Send email

Send an email notification to specified recipients

Send to Splunk Mobile

Send a notification to Splunk Mobile recipients

Webhook

Generic HTTP POST to a specified URL

Manage Actions

Manage available actions and browse more 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.

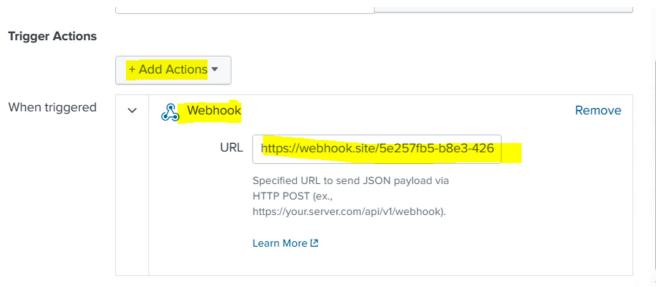
Use-Case #1 : If expression is to run every 2 hours and Time range is Last 3 hours => It may create duplicate Alert if event is between 2nd to 3rd hour.

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:

A screenshot of the Splunk Webhook site interface. On the left, a sidebar shows recent requests: a POST from '52.87.110.165' at 06/09/2023 6:22:01 AM, a GET from '165.225.104.90' at 06/09/2023 6:20:16 AM, and a GET from '165.225.104.90' at 06/09/2023 6:20:16 AM. The main area displays a detailed view of a POST request from '52.87.110.165' at 06/09/2023 6:22:01 AM. The request details show the URL as 'https://webhook.site/5e257fb5-b8e3-4268-ae79-bc13ba9e71c8'. The raw content is a JSON object with fields like 'sid', 'search_name', 'app', 'owner', 'results_link', and 'result'. The headers include 'connection: close', 'user-agent: Splunk/48408668-B58E-4B02-AF42-5B607981C39E', 'content-type: application/json', 'host: webhook.site', 'content-length: 321', and 'accept-encoding: identity'. The form values section is empty.

#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_index" source="sample_tickets.csv" | stats count by severity

Earliest time: optional

Latest time: optional

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

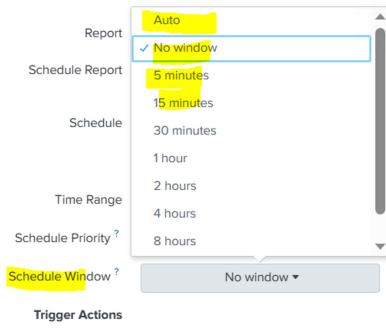
To: Remove

Schedule Priority: Default

Schedule Window: Default

Trigger Actions

+ Add 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_idx" source="data.txt"

Extract New Field

The screenshot shows the 'Extract Fields' wizard with the first step, 'Select Sample', completed. The progress bar has a green dot at 'Select Sample'. The 'Next >' button is visible. The 'Source type' is set to 'my_txt' and the 'Time Range' is 'Last 90 days'. A note says 'Choose a source or source type, select a sample event, and click Next to go to the next step. The field extractor will use the event to extract fields. Learn more'.

The 'Events' section displays a log entry: 'Mon Mar 19 20:16:27 2018 Info: Bounced: DCID 8413617 MID 19338947 From: <MariaDubois@example.com> To: <zecora@buttercupgames.com> RID 0 - 5.4.7 - Delivery expired (message too old) ('000', ['timeout'])'. The 'Events' tab is selected.

The 'Select Method' step is shown with two options: 'Regular Expression' and 'Delimiters'. The 'Regular Expression' option is highlighted with a blue box. It shows a placeholder '(.*?)' and a note: 'Splunk Enterprise will extract fields using a Regular Expression.' The 'Delimiters' option shows a placeholder 'x|y|z' and a note: 'Splunk Enterprise will extract fields using a delimiter (such as commas, spaces, or characters). Use this method for delimited data like comma separated values (CSV files).' The progress bar has a green dot at 'Select Method'. The 'Next >' button is visible.

The 'Select Fields' step is shown. A log entry is displayed: 'Mon Mar 19 20:16:27 2018 Info: Bounced: DCID 8413617 MID 19338947 From: <MariaDubois@example.com> To: <zecora@buttercupgames.com> RID 0 - 5.4.7 - Delivery expired (message too old) ('000', ['timeout'])'. A specific word in the 'From' field is highlighted with a yellow box. A modal window titled 'Extract' is open, showing 'Field Name' as 'emailid' and 'Sample Value' as 'MariaDubois@example.com'. The 'Add Extraction' button is visible. The progress bar has a green dot at 'Select Fields'. The 'Next >' button is visible.



Select Fields

Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in an event for the regular expression to match. Click on highlighted values in the them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. Learn more [↳](#)

Mon Mar 19 20:16:27 2018 Info: Bounced: DCID 8413617 MID 19338947 From: <MariaDubois@example.com> To: <zechora@buttercupgames.com> RID 0 - 5.4.7 - Delivery expired (message too old)

Show Regular Expression >

Preview

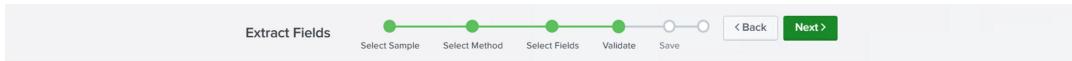
If you see incorrect results below, click an additional event to add it to the set of sample events. Highlight its values to improve the extraction. You can remove incorrect values in the next step.

Events emailid

✓ 4 events (3/1/23 12:00:00.000 AM to 6/9/23 6:50:26.000 AM)

filter Sample: 1000 events

Values	Count	%
Exit_Desk@example.net	1	25.00
Manish_Das@example.com	1	25.00
MariaDubois@example.com	1	25.00



Validate

Validate your field extractions and remove values that are incorrectly highlighted in the Events tab. In the field tabs, inspect the extracted values for each field, and optionally click a value to apply it as a search filter to the Events list.

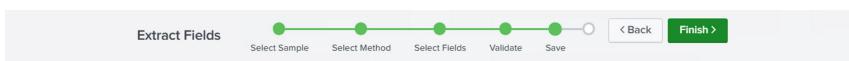
Show Regular Expression >

Events emailid

✓ 4 events (3/1/23 12:00:00.000 AM to 6/9/23 6:50:26.000 AM)

filter Sample: 1,000 events

Values	Count	%
Exit_Desk@example.net	1	25.00
Manish_Das@example.com	1	25.00
MariaDubois@example.com	1	25.00
WeiZhang@example.com	1	25.00



Save

Name the extraction and set permissions.

Extractions Name

Owner

App

Permissions

Source type

Sample event Mon Mar 19 20:16:27 2018 Info: Bounced: DCID 8413617 MID 19338947 From: <MariaDubois@example.com> To: <zechora@buttercupgames.com> RID 0 - 5.4.7 - Delivery expired (message too old) ('000', ['timeout'])

Fields

Regular Expression

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

New Search

```
index="my_idx" source="data.txt" | fields emailid
```

✓ 4 events (before 6/9/23 6:52:37:000 AM) No Event Sampling ▾

Events (4) Patterns Statistics Visualization

Format Timeline ▾ Zoom Out + Zoom to Selection × Deselect

emailid

4 Values, 100% of events Selected Yes No

Reports Top values Top values by time Rare values

INTERESTING FIELDS ↗ emailid 4 Events with this field

+ Extract New Fields

Values	Count	%
Exit_Desk@example.net	1	25%
Manish_Das@example.com	1	25%
MariaDubois@example.com	1	25%
Weizhang@example.com	1	25%

#Delimiter:

Extract Fields

Select Sample Select Method Rename Fields Save < Back Next >

Select Method

Indicate the method you want to use to extract your field(s). Learn more ⓘ

I prefer to write the regular expression myself >

Source type
my_txt

```
Mon Mar 19 20:16:27 2018 Info: Bounced: DCID 8413617 MID 19338947 From: <MariaDubois@example.com> To: <zecora@buttercupgames.com> RID 0 - 5.4.7 - Delivery expired (message too old)
```

(.*?)

Regular Expression

Splunk Enterprise will extract fields using a Regular Expression.

x|y|z

Delimiters

Splunk Enterprise will extract fields using a delimiter (such as commas, spaces, or characters). Use this method for delimited data like comma separated values (CSV files).

Extract Fields Select Sample Select Method Rename Fields Save < Back Next >

Rename Fields

Select a delimiter. In the table that appears, rename fields by clicking on field names or values. Learn more ⓘ

Delimiter

Space Comma Tab Pipe Other : ; ,

```
Mon Mar 19 20:16:27 2018 Info: Bounced: DCID 8413617 MID 19338947 From: <MariaDubois@example.com> To: <zecora@buttercupgames.com> RID 0 - 5.4.7 - Delivery expired (message too old) ('000', ['timeout'])
```

Rename Fields

Select a delimiter. In the table that appears, rename fields by clicking on field names or values. Learn more ⓘ

Delimiter

Space Comma Tab Pipe Other : ; ,

field1	field2	field3	field4	field5	field6	field7
Mon Mar 19 2018	16	27 2018	Bounced	DCID 8413617 MID 19338947	<MariaDubois@example.com>	<zecora@buttercupgames.com> RID 0 - 5.4.7 - Delivery expired (message too old) ('000', ['timeout'])

Name of Filed Extraction:

Field extractions

Fields > Field extractions

New Field Extraction Open Field Extraction

Showing 1 of 1 item

App Home (launcher) Owner user2 (user2) Visible in the App filter 25 per page

Name	Type	Extraction/Transform	Owner	App	Sharing	Status	Actions
my_txt_EXTRACT_emailid	Inline	{"<in>": {"P": "emailid", ">": ""}}	user2	launcher	Private Permissions	Enabled	Move Delete

#Workflow Action

Settings => Field =>

Fields
View, edit, and set permissions on field extractions. Define event workflow actions and field aliases. Rename sourcetypes.

Field aliases Edit or add one or more aliases to field names	+ Add new
Calculated fields Edit or add one or more calculated fields	+ Add new
Field extractions View and edit all field extractions. Add new field extractions and update permissions.	+ Add new
Field transformations Edit or add transformations for field extractions that use a transform.	+ Add new
Sourcetype renaming Rename a source type. Multiple source types can share the same name.	+ Add new
Workflow actions Edit or add workflow actions	+ Add new

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

Destination app

Name *
Enter a unique name without spaces or special characters. This is used for identifying your workflow action later on within Splunk Settings.

Label *
Enter the label that appears for this action. Optionally, incorporate a field's value by enclosing the field name in dollar signs, e.g. 'Search for ticket number: \$ticketnum\$'.

Apply only to the following fields
Specify a comma-separated list of fields that must be present in an event for the workflow action to apply to it. When fields are specified, the workflow action only appears in the field menus for those fields; otherwise it appears in all field menus.

Apply only to the following event types
Specify a comma-separated list of event types that an event must be associated with for the workflow action to apply to it.

Show action in

Action type *

Link configuration

URI *
Enter the location to link to. Optionally, specify fields by enclosing the field name in dollar signs, e.g. http://www.google.com/search?q=\$host\$.

Open link in

Label *
Enter the label that appears for this action. Optionally, incorporate a field's value by enclosing the field name in dollar signs, e.g. 'Search for ticket number: \$ticketnum\$'.

Apply only to the following fields
Specify a comma-separated list of fields that must be present in an event for the workflow action to apply to it. When fields are specified, the workflow action only appears in the field menus for those fields; otherwise it appears in all field menus.

Apply only to the following event types
Specify a comma-separated list of event types that an event must be associated with for the workflow action to apply to it.

Show action in

Action type *

Link configuration

URI *
Enter the location to link to. Optionally, specify fields by enclosing the field name in dollar signs, e.g. http://www.google.com/search?q=\$host\$.

Open link in

Link method

Workflow_action will be visible in "Event Menu" option.

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

New Search

index="my_idx" source="Sample_tickets.csv" asset_id="Directory" All time

✓ 39 events (before 6/9/23 7:12:56.000 AM) No Event Sampling Job

Events (39) Patterns Statistics Visualization Format Timeline 1 month per column

List 20 Per Page 1 2 Next >

< Hide Fields Time Event

SELECTED FIELDS
`a host 1`
`a source 1`
`a sourcetype 1`

INTERESTING FIELDS
`a active_org 1`
`a app_family_mots 1`
`a application_name 2`
`a asset_id 1`
`a auto_sub_cat3 7`
`a closed_date 38`
`a current_ticket_state 6`
`# data below 44`

Event Actions

Value	Actions
ip-172-31-84-138.ec.internal	
Sample_tickets.csv	
csv	
Org_1	
Project 1	

Search | Splunk 9.0.5 Google Search Field Extractor | Splunk 9.0.5

https://www.google.com/search?q=Directory#cobssid=

About 2,480,000,000 results (0.34 seconds)

Dictionary

Definitions from Oxford Languages · Learn more



Action type = 2kinds

(1) link

(2) search

Action type *

Action type *

Search configuration

Search string `index="my_idx" source="Sample_tickets.csv" asset_id="Directory"`
 Enter the search for this action. Optionally, specify fields as \$fieldname\$, e.g. sourcetype=rails controller=\$controller\$ error=\$

Run in app `search`
 Choose an app for the search to run in. Defaults to the current app.

Open in view
 Enter the name of a view for the search to open in. Defaults to the current view.

Run search in `New window`

Time range

Earliest time `0`
 Latest time `now`

Use the same time range as the search that created the field listing

