

Using Datasets

Easier Data Exploration, Preparation and Analysis

Jesse Miller | Staff Sales Engineer
Megumi Hora | Software Engineer

September 2017 | Washington, DC

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.

Agenda

- ▶ What are Datasets?
- ▶ Types of Datasets
- ▶ Using Datasets
- ▶ Datasets: Listing, Viewing, Editing
- ▶ Demo
- ▶ Questions

What Are Datasets?

► Building Blocks

- Source Data
- SPL
- Schema

► Unified Endpoint

- List
- View
- Search
- Edit
- Analyze

splunkbase™

Search App by keyword, technology...



Splunk Datasets Add-on

★★★★★ 17 reviews

Splunk Built

Time	Source	Category	Item	Product ID	Price
2017-01-18T10:10:10.000Z	http://buttercup-shopping.com	Electronics	Smartphone	EST-6	200.00
2017-01-18T10:10:10.000Z	http://buttercup-shopping.com	Electronics	Smartphone	EST-6	200.00
2017-01-18T10:10:10.000Z	http://buttercup-shopping.com	Electronics	Smartphone	EST-6	200.00
2017-01-18T10:10:10.000Z	http://buttercup-shopping.com	Electronics	Smartphone	EST-6	200.00
2017-01-18T10:10:10.000Z	http://buttercup-shopping.com	Electronics	Smartphone	EST-6	200.00

ADMINISTRATOR TOOLS: View App | View Analytics

Overview

Details

8,067

Installs

12,602

Downloads

[Download](#)

The Splunk Datasets Add-on provides an intuitive interface to build, edit and analyze table datasets (tables) without SPL. After you install it, tables become a seamless part of your Splunk user experience.

splunk>

.conf2017

Types Of Datasets

Lookups

- ▶ **What:** Static data (CSV)
Dynamic data (Script)
DBConnect (SQL)
- ▶ **Why:** Enrich search-based datasets by adding fields from external sources
- ▶ **Where:** Lookups
Transforms.conf

Data Model (Objects)

- ▶ **What:** search-based datasets with a hierarchical structure, grouped as "Data Models".
- ▶ **Why:** Establishing hierarchical relationships with domain knowledge. (top-down)
- ▶ **Where:** Data Model Editor
Datasets.conf (JSON)

Tables*

- ▶ **What:** Tabular, search-based dataset (similar to the individual objects in a DM)
- ▶ **Why:** Agile creation and iterative refinement. (bottom-up)
- ▶ **Where:** Table Editor*
Datamodels.conf (JSON)

New!

* Available with the Tables Add-On
(Table Datasets)

Using Datasets

- ▶ Datasets can be **extended**, forming a parent/child model of inheritance
- ▶ Datasets can be **queried**
 - | *from type:"name"* | *eval ...* | *search ...* | *stats ...*
- ▶ Datasets can be **accelerated**
- ▶ Datasets can be **pivoted**
- ▶ Datasets can be **data model objects**

```
130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.10.4740; rv:1.9.1.10 Gecko/20100101 Firefox/35.0"
128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-D5H-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=MX-11-01" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.1.10) Gecko/20100101 Firefox/35.0"
317.27.160.0 - - [07/Jun 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL0FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-11&product_id=FL-SW-01" "Opera/9.80.2013.10.4740; rv:1.9.1.10 Gecko/20100101 Firefox/35.0"
130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.10.4740; rv:1.9.1.10 Gecko/20100101 Firefox/35.0"
128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-D5H-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=MX-11-01" "Mozilla/5.0 (Windows NT 6.0; rv:1.9.1.10) Gecko/20100101 Firefox/35.0"
317.27.160.0 - - [07/Jun 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL0FF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-11&product_id=FL-SW-01" "Opera/9.80.2013.10.4740; rv:1.9.1.10 Gecko/20100101 Firefox/35.0"
```

Datasets: Listing

- ▶ Manage table datasets, data model datasets, and lookups in one place
- ▶ Define acceleration and permissions
- ▶ Search for datasets based on name and contained fields

Datasets

Use the Datasets listing page to view and manage your existing datasets. Click a dataset name to view its contents. Click Pivot to design a visualization-rich report based on the dataset. Click Explore in Search to extend a dataset in Search and save it as a new report, alert, or dashboard panel.

[Learn more about Datasets.](#)

Create New Table Dataset

452 Datasets

All

Yours

This App's

Filter by title, description, fields

< Prev

1

2

3

4

5

Next >

i	Title ^	Dataset Type		Actions	Owner	App	Sharing
>	_weekday.csv	lookup table file		Manage Explore	nobody	splunk_6.1_overview	Global
>	Alerts > Alerts	data model		Explore	nobody	Splunk_SA_CIM	Global
>	Application State > All Application State	data model		Explore	nobody	Splunk_SA_CIM	Global
>	Application State > All Application State > Ports	data model		Explore	nobody	Splunk_SA_CIM	Global
>	Application State > All Application State > Processes	data model		Explore	nobody	Splunk_SA_CIM	Global
>	Application State > All Application State > Services	data model		Explore	nobody	Splunk_SA_CIM	Global
>	Authentication > Authentication	data model		Explore	nobody	Splunk_SA_CIM	Global
>	Authentication > Authentication > Default Authentication	data model		Explore	nobody	Splunk_SA_CIM	Global
>	Authentication > Authentication > Default Authentication > Failed D...	data model		Explore	nobody	Splunk_SA_CIM	Global
>	Authentication > Authentication > Default Authentication > Succes...	data model		Explore	nobody	Splunk_SA_CIM	Global
>	Authentication > Authentication > Failed Authentication	data model		Explore	nobody	Splunk_SA_CIM	Global
>	Authentication > Authentication > Insecure Authentication	data model		Explore	nobody	Splunk_SA_CIM	Global
>	Authentication > Authentication > Privileged Authentication	data model		Explore	nobody	Splunk_SA_CIM	Global
>	Authentication > Authentication > Privileged Authentication > Faile...	data model		Explore	nobody	Splunk_SA_CIM	Global
>	Authentication > Authentication > Privileged Authentication > Succ...	data model		Explore	nobody	Splunk_SA_CIM	Global
>	Authentication > Authentication > Successful Authentication	data model		Explore	nobody	Splunk_SA_CIM	Global
>	Business Analytics > Business Transactions	data model		Manage Explore	nobody	oidemo	Global
>	Business Analytics > Business Transactions > Purchases	data model		Manage Explore	nobody	oidemo	Global
>	Business Analytics > Business Transactions > Purchases > Failed ...	data model		Manage Explore	nobody	oidemo	Global
>	Business Analytics > Business Transactions > Purchases > Succes...	data model		Manage Explore	nobody	oidemo	Global

Datasets: Viewing

- ▶ Explore existing dataset
- ▶ Two views (read only):
 - Preview Rows (table)
 - Summarize Fields (field stats)
- ▶ Filter data by time range
- ▶ Manage dataset search jobs

Business Analytics > Business Transactions ⚡

View Results Summarize Fields

Manage More Info Explore

All time

✓ 71,957 events (before 8/7/17 3:08:08.000 PM)

Job

20 per page

< Prev 1 2 3 4 5 6 7 8 9 ... Next >

*	@ _time	a host	a source	a sourcetype	a action	a address	# bytes	a category
1	2017-08-07T15:08:06.224-05:00	webserver-01	/opt/apache/log/access_combined.log	access_combined	addtocart	50303 Truax Crossing	3509	Misc
2	2017-08-07T15:08:04.224-05:00	webserver-03	/opt/apache/log/access_combined.log	access_combined	changequantity	3020 Mitchell Drive	2323	Misc
3	2017-08-07T15:08:01.014-05:00	webserver-01	/opt/apache/log/access_combined.log	access_combined	view	64 Melby Hill	3058	Misc
4	2017-08-07T15:08:00.138-05:00	webserver-02	/opt/apache/log/access_combined.log	access_combined	purchase	819 Manitowish Avenue	3773	Misc
5	2017-08-07T15:08:00.107-05:00	webserver-01	/opt/apache/log/access_combined.log	access_combined	changequantity	2468 Laurel Hill	551	Misc

Datasets: Table Editor

- ▶ Refine dataset with SPL commands using selections, menus, and forms

- ▶ Two views:

- Preview Rows (table)
- Summarize Fields (field stats)

- ▶ Command history

- ▶ Field types

splunk> App: Search & Reporting ▾ Administrator ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Datasets Reports Alerts Dashboards Search & Reporting

New Table Dataset Preview Rows Summarize Fields Pivot Save Save As

Commands SPL Edit ▾ Sort ▾ Filter ▾ Clean ▾ Summarize ▾ Add New ▾

Initial Data ✓ 6,406 events (before 8/11/16 11:30:33.000 AM) Event Limiting: ~100,000 All time ▾ || ■ ↺

product	salesforce_id	AccountName	AccountTheater	version
<div> <div>Matched type.....99.98%</div> <div>Mismatched type.....0.00%</div> <div>Null values.....0.02%</div> </div> <div> <div>Single value.....6405</div> <div>Multivalue.....0</div> <div>Unique values.....5</div> </div>	<div> <div>Matched type.....100.00%</div> <div>Mismatched type.....0.00%</div> <div>Null values.....0.00%</div> </div> <div> <div>Single value.....6405</div> <div>Multivalue.....0</div> <div>Unique values.....3406</div> </div>	<div> <div>Matched type.....20.29%</div> <div>Mismatched type.....0.00%</div> <div>Null values.....79.71%</div> </div> <div> <div>Single value.....1300</div> <div>Multivalue.....0</div> <div>Unique values.....657</div> </div>	<div> <div>Matched type.....20.29%</div> <div>Mismatched type.....0.00%</div> <div>Null values.....79.71%</div> </div> <div> <div>Single value.....1300</div> <div>Multivalue.....0</div> <div>Unique values.....3</div> </div>	<div> <div>Matched type.....100.00%</div> <div>Mismatched type.....0.00%</div> <div>Null values.....0.00%</div> </div> <div> <div>Single value.....6405</div> <div>Multivalue.....0</div> <div>Unique values.....3</div> </div>
splunk 58.75%	00Q40000016iteAEQ 0.58%	carapace 1.77%	AMER 65.15%	6.2.2 99.44%
universalforwarder 24.54%	0034000001d0kphAAA 0.45%	destroyers 1.38%	EMEA 23.54%	2.0.1 0.53%
splunk_light 15.57%	0034000000bIXGr 0.44%	cribber 1.15%	APAC 11.31%	6.2.1 0.03%
hunk 0.61%	00Q40000016iojEAA 0.44%	gemstone 0.92%		
mobile_access_server 0.53%	0034000001UtBNWAA3 0.36%	susses 0.92%		
	00Q40000016jE88EAE 0.34%	svelte 0.92%		
	0034000001byGnJAAU 0.28%	vignettes 0.85%		
	00Q40000016jCmaEAE 0.27%	sogginess 0.77%		
	00Q4000000QZnHMEA1 0.25%	plagued 0.69%		
	00Q40000010j6IAEAQ 0.25%	rebids 0.69%		
	0034000000cmCKKAA2 0.23%	smilingly 0.69%		
	00Q4000000mf3xxEAA 0.22%	tidied 0.69%		
	00Q4000000ohP7VEAU 0.22%	walloping 0.69%		
	00Q40000016DEH8EAO 0.22%	internationalism 0.69%		



Demo

Q&A

Thank You!

Thank You

Don't forget to **rate this session** in the
.conf2017 mobile app

splunk> .conf2017