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

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.
Types Of Datasets

- **Lookups**
  - **What:** Static data (CSV) Dynamic data (Script) DBCConnect (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)

* 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
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: Viewing

▶ Explore existing dataset

▶ Two views (read only):
  • Preview Rows (table)
  • Summarize Fields (field stats)

▶ Filter data by time range

▶ Manage dataset search jobs
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
Demo
Thank You!
Thank You

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