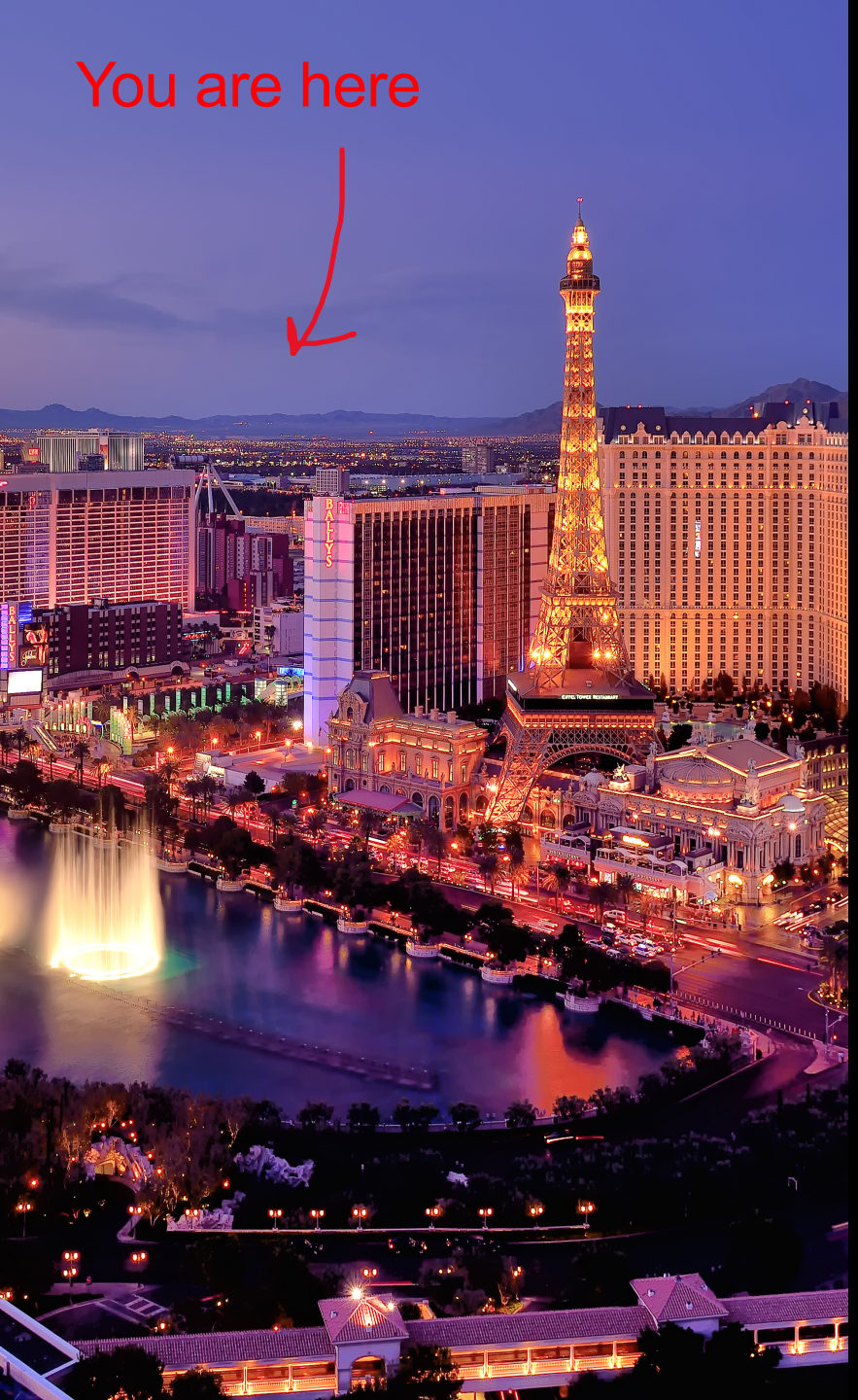
splunk> education

Welcome to *Creating Dashboards* .conf19 *Edition*

splunk> turn data into doing™



splunk> .conf19

.conf19
October 21-24, 2019

Splunk University
October 19-21, 2019

Las Vegas, NV
The Venetian Sands Expo

4 Days of Innovation

350 Education Sessions

20 Hours of Networking

conf.splunk.com


WELCOME
TO Fabulous
Splunkville
NEVADA

Let's Get Ready To Spluuuuuuuuuuuuuunk!>

Mitch Fleischman
Senior Staff Instructor

+1 650.605.7549 m
mitchf@splunk.com
splunk.com

@ Splunk 7 years

Enterprise software experience 25+ years:

- Customer Relationship Management (CRM)
- Relational Database (RDB)
- Portal
- Business Process Management (BPM)
- Endpoint Management
- **Big Data / Data Analytics**

Roles:

- Programmer
- Project Lead
- Consultant
- Course Developer
- **Instructor**

Geography:

- New Jersey
- California
- Vermont
- **Metro DC / Arlington, VA**

Creating Dashboards

1. Creating a Prototype
- Definitions (View, Dashboard, Form)
- Simple XML syntax
- Best practices / Transforming commands
- Panel types (inline / report / pre-built / *clone*)

2. Using Forms
- Form inputs / Cascading inputs

3. Improving Performance
- Scheduled Reports / Accelerations
- tstats
- Global search / post-processing

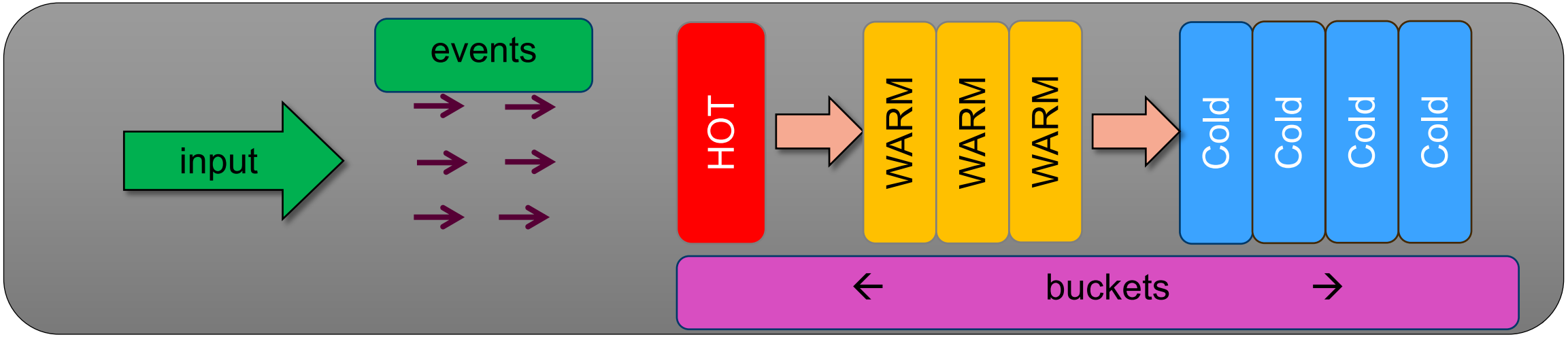
4. Customizing Dashboards
- Modify chart and panel colors
- Set panel refresh and delay times
- Enable / disable search controls (panel links)

5. Using Drilldowns
- Dynamic vs contextual
- Pre-defined tokens for drilldowns

6. Adding Advanced Visualizations & Behaviors
- Event handlers
- Simple XML extensions for JavaScript and CSS
- Custom visualizations

How Splunk Indexes Data

- Inputs (file / network port, etc) come into Splunk and are broken up into events with these attributes:
  - host: The machine where the data originated
  - source: For example, path to the file
  - sourcetype: Classification / categorization, for example web log: access_combined
  - timestamp: Epoch (Unix) time, UTC offset
  - index (main by default)
- A bucket (directory) has the raw data (compressed), a time-series index (.tsidx files), [bloomfilter]
  - Each bucket has an earliest and latest time for the events it contains
  - There are also metadata (.data) files that track `source`, `sourcetype`, and `host`



Acceleration Overview

Summary Indexing	• Store search results (typically a small subset of raw events) in indexes separate from the main indexes • The original acceleration technique - to speed up dashboard loading, panels load from a smaller index • Premium apps such as ES and ITSI use as repositories for app components such as notable events • Summary indexes reside on the Search Head! "Events" stored in the normal fashion – no additional metering (Admins configure Search Head Forwarding to the Indexer tier) • Can persist after "parent" events have been frozen Summary indexes have their own settings for controlling retention period and index size
Report Acceleration	• Store results of statistical (reporting) searches in indexes separate from the main indexes • Qualifying searches must use a reporting command (stats, top, etc) • All matching events from the search have to be "streaming" into the reporting command (no dedup, no transaction) • If these criteria can't be met, fallback is Summary Indexing - given a choice, use Report Acceleration • RA indexes reside on the Indexer, alongside the main index buckets. "Events" stored in the normal fashion – no additional license metering • Configurable retention window – but data always ages out with the corresponding main index buckets
Data Model Acceleration	• Store metadata (statistics), **not** search results, for the fields defined in the datamodel • Storage format is time-series index (tsidx) files, which are created on the Indexer – no additional metering • Perform searches directly against the metadata (tstats command) without opening the raw data • Huge performance gain ("cost" is maintenance processing and storage space) • Data ages out when the corresponding main index buckets ages out

Resources

Splunkbase: Splunk Dashboard Examples

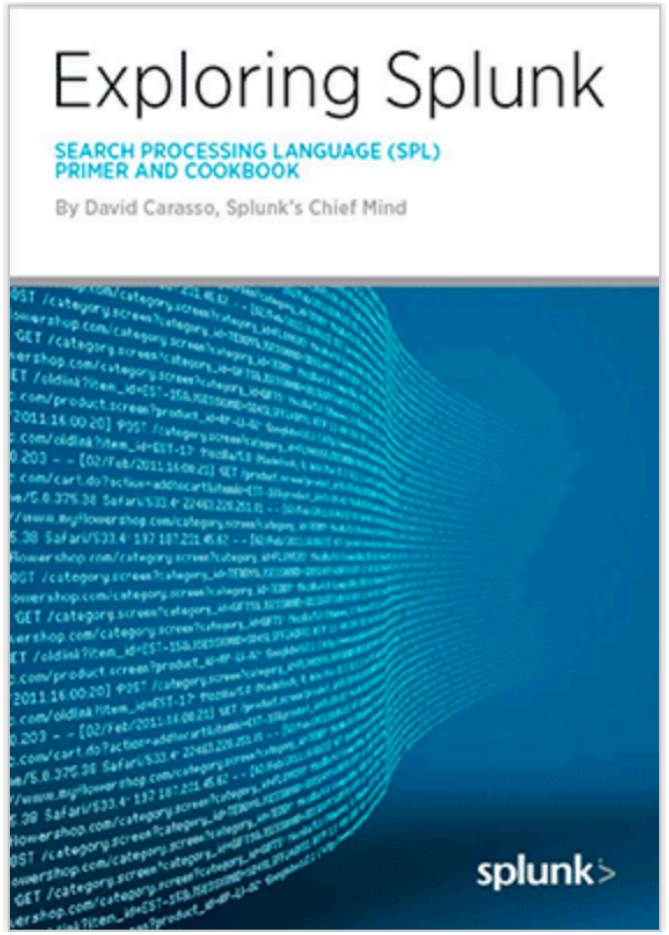
Dashboards Quick Reference Guide
https://www.splunk.com/pdfs/solution-guides/splunk-dashboards-quick-reference-guide.pdf

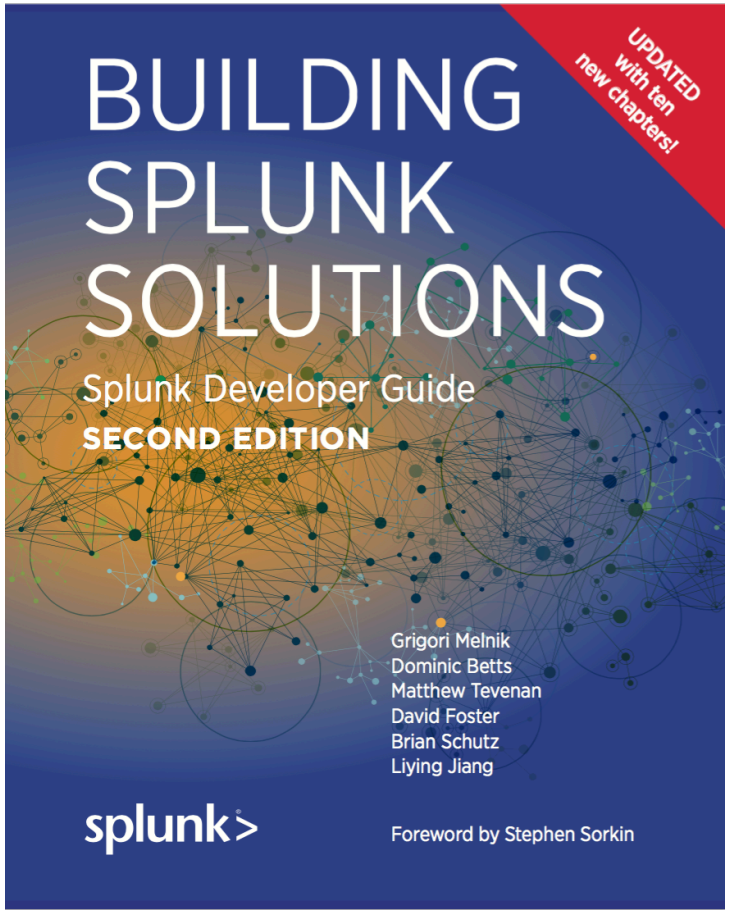
Simple XML Reference
docs.splunk.com/Documentation/Splunk/latest/Viz/PanelreferenceforSimplifiedXML

Event Handler Reference
http://docs.splunk.com/Documentation/Splunk/latest/Viz/EventHandlerReference

Developer resources and courses
dev.splunk.com
splunk.com/view/SP-CAAAH9P

Books





Get the PDF: splunk.com/goto/book

dev.splunk.com/view/dev-guide/SP-CAAAE2R

Splunk Training + Certification

1. Course **Certificate of Completion** Perform the labs!
2. **Splunk Certification** Program
   - Tracks
     https://www.splunk.com/en_us/training/faq-training.html

     Splunk Core Certified User
     Splunk Core Certified Power User
     Splunk Enterprise Certified Admin
     Splunk Enterprise Certified Architect
     Splunk Certified Developer
   - Program information handbook
     https://www.splunk.com/pdfs/training/Splunk-Certification-Candidate-Handbook.pdf
   - Exam registration
     https://www.splunk.com/pdfs/training/Exam-Registration-Tutorial.pdf
   - If you have further questions, send an email to certification@splunk.com

splunk>

Making machine data accessible, usable, and valuable to everyone.