Splunk4Champions Hand-Out

1. Settings & Preferences

Reformat Search: Ctrl + Shift + F   or Command + Shift + F

Comments: ``` the code is documentation enough ```

- "Using The Search Assistant"
- Searchbar Shortcuts
- "User language and locale"
- "Search Modes"

2. Job Inspector

1. In the first line we see the number of results, scanned events and time. You can calculate events scanned per second from that.

In this example we see something like: "This search has completed and has returned 2,169 results by scanning 1,355,725 events in 6.535 seconds"

2. Execution costs: time to process each component, number of invocation, input and output count
   - "command.search.index" -> time to read the idx files
   - "command.search.rawdata" -> time to read rawdata
   - "command.search.filter" -> time to filter non-matching events
   - "command.search.kv" -> field extractions (analog for lookups, tags)
   - "command.search.typer" -> processing event types

   Details about execution costs and the meaning of the component name.
   https://docs.splunk.com/Documentation/Splunk/9.0.3/Search/ViewsearchjobpropertieswiththeJobInspector#Execution_costs

3. Properties: Under lower section "Search job properties"
   - look for the "optimizedSearch" - is it different?
   - diskUsage - how much space the search is using?
4. search.log
   - Alternatively look search for "lispy" in the search log

Links:

- "Splunk: Clara-fication: Job Inspector"
- "Splunk education, excellent 8m video "
- "Martin Müller's B-Sides Job Inspector talk"
- "Splunk Optimizations Docs"
- "Martin Müller's Lispy talk"
- "TRU1143C - Splunk > Clara-fication: Job Inspector (conf20 session by Martin Müller and Clara Merriman"
- "Splunk > Clara-fication: Search Best Practices"
- "Jacob Brügmann & Martin Müller - "Splunk: Suchen verstehen mit dem Job Inspector"

- "Jacob Brügmann & Martin Müller - "Suchen verstehen mit dem Job Inspector – Episode II: Arbeitsteilung"

3. How is Data Stored:

- "Interactive Bloomfilter-Demo"
- ".conf 2017 - How Splunk Stores Data"
- "Docs: How the indexer stores indexes"
- Data Pipeline in Splunk Docs
- More detailed diagrams of the data pipeline
- "free 1 hour education course on distributed searches:"
- "Splunk Validated Architectures"
- Event Segmentation in Splunk Docs
- "TSIDX in Splexicon"
- "journal.gz in Splexicon"
- "Bloomfilter in Splexicon"

Data Pipeline

- Data Pipeline in Splunk Docs
- More detailed diagrams of the data pipeline

4. Search

Basics

- Specify and limit the index(es) & other meta-fields like host(s), source(s) & sourcetype(s)
- Limit the time range for searching
- Fine-tune your searches to your unique events as much as possible
- Reduce the number of fields being passed SPL pipeline for processing (use fields command)
- Place streaming commands earlier in the pipeline

Links:

- ".conf - Fields, Indexed Tokens and You by Martin Müller"
- ".conf - Clara-Fication: Finding and Improving Expensive Searches PLA1466b by Clara Merriman, Martin Müller"
- ".conf - "TSTATS and PREFIX" by Richard Morgan"
- "Docs: More information on command types"
- "Docs: Write Better Searches"
- "Docs: Search manual: wildcards "

TERM

TERM directive avoids splitting in TERMs

```
index=_internal 127.0.0.1
```

```
index=_internal TERM(127.0.0.1)
```

```
Minor breakers: / : = @ . - $ # % \ _
```

```
Major breakers: \r\n\s\t[] <> () | ! ; , `
```

Event Segmentation in Splunk Docs

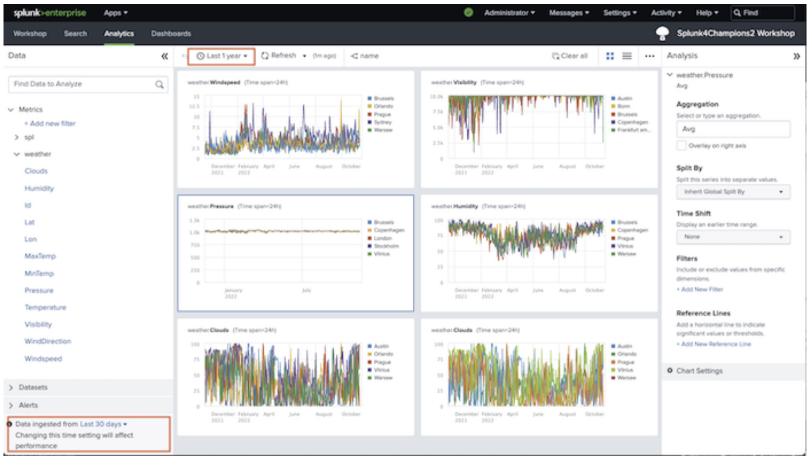
TSTATS

`tstats`` command performs statistical queries on indexed fields in tsidx files. The indexed fields can be from indexed data or accelerated data models.

Nice blog article on tstats and PREFIX by Tyler Quinlivan:
https://www.tylerquinlivan.com/posts/exploring_splunk_prefix/

- ".conf - "TSTATS and PREFIX" by Richard Morgan"

5 - Metrics



- "Splunk docs - Get started with Metrics"
- "Splunk blog - Metrics to the Max!"
- "Getting metrics in"
- "Sending metrics with OpenTelemetry Collector"
- "Analytics in the Analytics Workspace"

6 - Dashboards

Use Base Searches:

```
<search id="singleValue_BaseSearch">
   <query>|tstats count WHERE index=* OR index=_* groupby sourcetype source index _time</query>
    <earliest>$time_select.earliest$</earliest>
    <latest>$time_select.latest$</latest>
    <sampleRatio>1</sampleRatio>
</search>
```

And references to the base searches:

```
<search base="singleValue_BaseSearch">
      <query>| timechart  dc(source)</query>
</search>
```

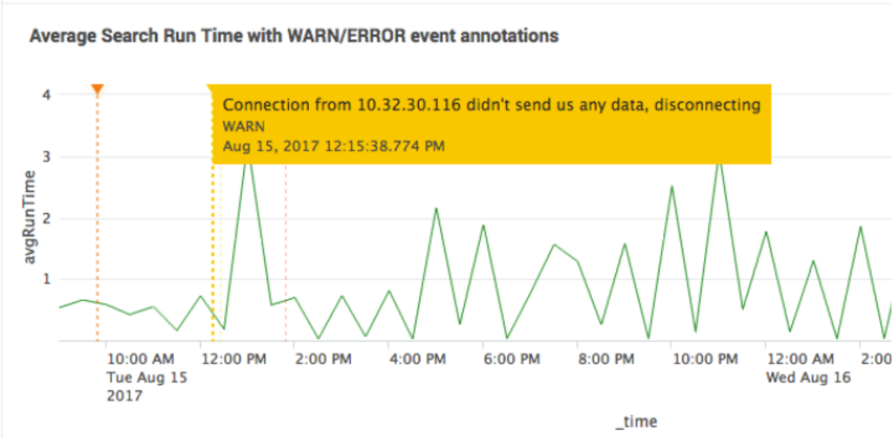
Pan and zoom chart controls (drilldowns)

https://docs.splunk.com/Documentation/Splunk/latest/Viz/Chartcontrols#Pan_and_zoom_chart_controls

Token Switches: <panel depends="$Option1$">

Annotations

https://docs.splunk.com/Documentation/Splunk/9.0.3/Viz/ChartEventAnnotations

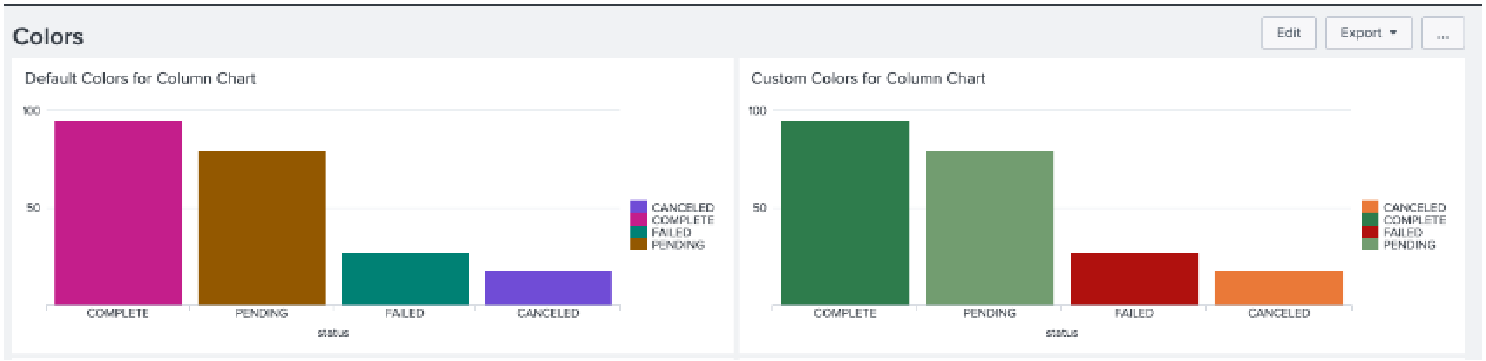


Average Search Run Time with WARN/ERROR event annotations

Connection from 10.32.30.116 didn't send us any data, disconnecting
WARN
Aug 15, 2017 12:15:38.774 PM

Change default colors

```
<option
name="charting.fieldColors">{"COMPLETE":#358856,"CANCELED":#ED8440,"FAILED":#B90E0A,"PENDING":#7
EA77B }</option>
```



Colors

Dashboard Studio

- Edu Courses Dashboarding
- Free Intro Course to Dashboard Studio
- "Dashboard Studio Tutorial"
- "EDU courses: Introduction to Dashboard"
- "Blog: Dashboard Studio: More Maps & More Interactivity"
- "Blogs: All blog articles on Dashboard Studio by Lizzy Li"
- Improving Dashboard Performance