1. Settings & Preferences

- Reformat Search: Ctrl + Shift + F   or Command + Shift + F
- Comments: ``` the code is documentation enough ```
- Expand Macro: Ctrl + Shift + E   or Command + Shift + E
- Language: https://splunkinstance/**en-GB**/app/splunk4champions2/lab

Links:

- "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

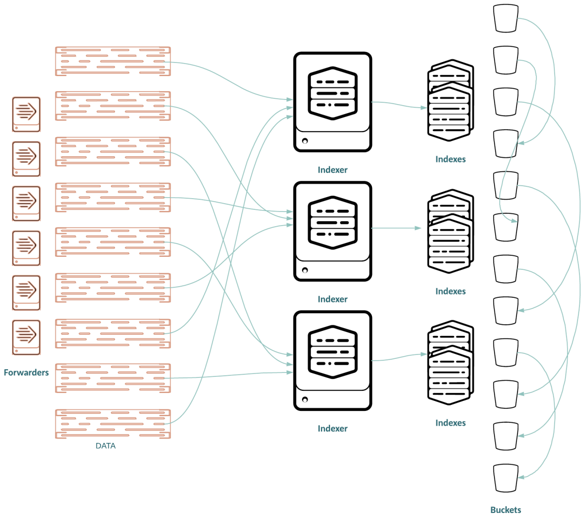
   Details about execution costs and the meaning of the component name.
   https://docs.splunk.com/Documentation/Splunk/9.0.3/Search/ViewsearchjobpropertieswiththeJobInspector#Execution_costs

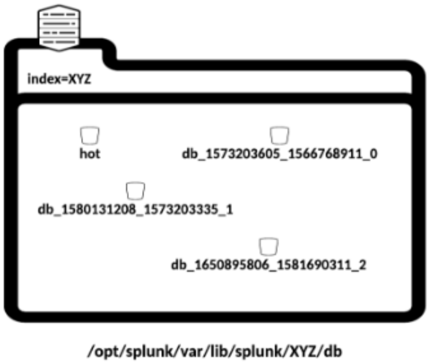
3. Properties: Under lower section "Search job properties"
   - look for the "optimizedSearch" - is it different?
   - diskUsage - how much space the search is using?
4. search.log
   - Alternatively look search for "lispy" in the search log

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:




index=XYZ
hot
db_1573203605_1566768911_0
db_1580131208_1573203335_1
db_1650895806_1581690311_2
/opt/splunk/var/lib/splunk/XYZ/db

- "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

Distributed Architecture

- Splunk Validated Architectures

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
- Tell exactly what you want (before the first pipe)
- 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 "
- Command Types

TERM

TERM directive avoids splitting in minor TERMs. The easiest way to see minor and major breakers in action is to move the mouse over the log terms: whatever you can highlight in one piece contains only minor breakers and can be used with TERM or PREFIX directives:

```
index=_internal 127.0.0.1
```

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

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

```
Major breakers: [ ] < > ( ) | ! ; , ' " * \n \r \s \t & ?
+ %21 %26 %2526 %3B %7C %20 %2B %3D -- %2520 %5D %5B %3A
%0A %2C %28 %29 , `
```

- Event Segmentation in Splunk Docs
- Splunk Docs on TERM
- Major and minor breakers in Splunk Docs

WALKLEX

Walklex command only works on warm and cold buckets, recently indexed data in hot buckets will not be considered.

Users can only run walklex command if their role has following capabilities: "run_walklex" OR "admin_all_objects".

Walklex command does not work if your role has search filters added.

|walklex index=s4c_tutorial type=fieldvalue|stats sum(count) by term

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"

Search Tips:

All Time	● Events are grouped by time ● Reduce searched buckets by being specific about time	● Use a specific time range ● Narrow the time range as much as possible
index=*	● Events are grouped into indexes ● Reduce searched buckets by specifying an index	● Always specify an index in your search

Wildcards	● Wildcards are not compatible with Bloom Filters
	● Wildcard matching of terms in the index takes time
	● Lexicon is structured by common prefixes, so appending an * is best (if you have to do it)
	● Never ever use wildcards to replace minor breakers e.g. autoconfig*bat for autoconfig.bat
		● Varying levels of suck-itude
		`> myterm* → Not great`
		`> my*erm → Bad`
		`> *myterm → Bad`
		`> *myterm* → Death`
		● Use the OR operator
		i.e.: `MyTerm1 OR MyTerm2`

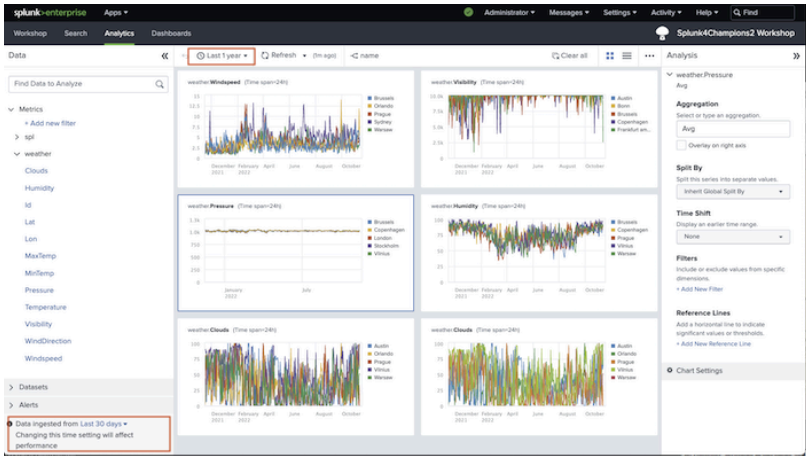
Avoid Transforming before Streaming	● Streaming commands run on indexers in parallel and should be placed first. ● Examples: eval, fields, rename, makemv, rex, spath, where ● Transforming commands run on search heads and require the full set ● Examples: chart, timechart, stats, top, rare, addtotals	

NOT
!=
	● Bloom filters and indexes are designed to quickly locate terms that exist
	● Searching for terms that don't exist takes longer
		● Use the OR/AND operators
		`(host=c OR host=d)`
		`(host=f ANDhost=h)`
		vs.
		`(host!=a host!=b)`
		`NOT host=a host=b`

Verbose Search Mode	● Verbose search mode causes full event data to be sent to the search head, even if it isn't needed	● Use Smart Mode or Fast Mode

<table>
<tr><td>Real-time Searches</td><td>• RT Searches put an increased load on search head and indexers
• The same effect can typically be accomplished with a 1 min. or 5 min. scheduled search or just a quick search with panel refresh in the dashboard.</td><td>• Use a scheduled search that occurs more frequently
• Use Indexed-Realtime searches (Set by Splunk admin)
• Use panel refresh:</td></tr>
<tr><td>Subsearches returning no results</td><td>• running zero-result searches when this might have negative side effects, such as generating false positives or running custom search commands that make costly API calls</td><td>• Use <code>require</code> in your SPL Statements</td></tr>
<tr><td>Transaction</td><td>• Not distributed to indexers
• Typically only needed if using additional parameters (maxSpan, startsWith, etc...)</td><td>• Use the stats command to link events where possible. If you have to use transaction, specify startswith, maxspan, maxpause.</td></tr>
<tr><td>Joins/Subsearches</td><td>• Joins can be used to link events by a common field value, but this is an intensive search command. It has limits for the result number and limits for the duration of the inner search, it also run sequentially.</td><td>• Use the stats (preferred) or transaction command to link events</td></tr>
<tr><td>Prefer <code>loadjob</code> over <code>savedsearch</code></td><td>• The savedsearch command always runs a new search. To reanimate the results of a previously run search, use the loadjob command.</td><td>• Use the loadjob to run a savedsearch.</td></tr>
<tr><td>Search after first |</td><td>• Filtering search results using a second “| search” command in your query is inefficient</td><td>• As much as possible, add all filtering criteria before the first |
i.e.: <code>&gt;index=main foo bar|</code>
vs.
<code>&gt;index=main foo | search bar</code></td></tr>
</table>

5 - Metrics



Select or type an aggregation.

Split this series into separate values.

Display an earlier time range.

Include or exclude values from specific dimensions.

Add a horizontal line to indicate significant values or thresholds.

Data ingested from Last 30 days
Changing this time setting will affect performance

- "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>
```

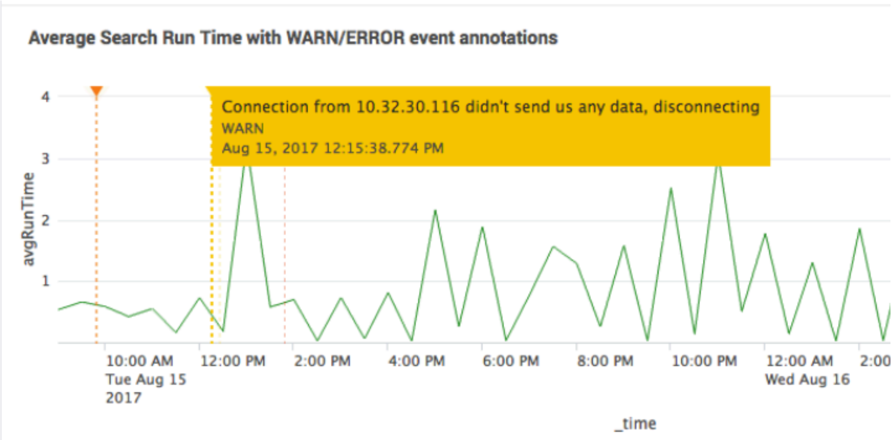
Pan and zoom chart controls (drilldowns)

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

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

Annotations

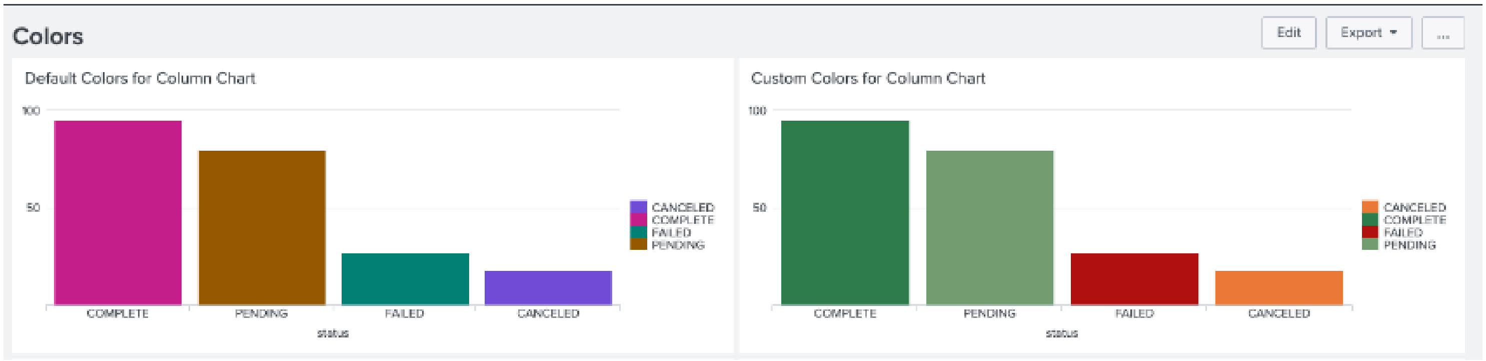
https://docs.splunk.com/Documentation/Splunk/9.0.3/Viz/ChartEventAnnotations



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>
```



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

Splunk Mobile and AR

Setup the Gateway and add your device

How to setup Splunk Mobile & Augmented Reality

1. Download Splunk Mobile

Download Splunk Mobile for the device you're using:

Download Splunk Mobile for iOS https://apps.apple.com/us/app/splunk-mobile/id1420299852

Download Splunk Mobile for Android https://play.google.com/store/apps/details?id=com.splunk.android.alerts&hl=en_US&gl=US&pli=1

Download Splunk Mobile for iPad https://apps.apple.com/us/app/splunk-for-ipad/id1568523145

2. Set up Splunk Secure Gateway

Splunk Secure Gateway (SSG) is included with Splunk Enterprise version 8.1 and higher and Splunk Cloud Platform version 8.1.2103 and higher. SSG provides a secure method for connecting authorized mobile devices to your Splunk platform instance. See the following links in the Administer Splunk Secure Gateway manual to get started and learn more:

Get started with Splunk Secure Gateway https://docs.splunk.com/Documentation/SecureGateway/3.4.251/Admin/Requirements

About the Splunk Secure Gateway security process https://docs.splunk.com/Documentation/SecureGateway/3.4.251/Admin/Security

Set up SAML authentication for Splunk Secure Gateway
https://docs.splunk.com/Documentation/SecureGateway/3.4.251/Admin/SAMLauth

3. Log your device in to your Splunk platform instance

After setting up SSG, you can log your device into the Splunk platform instance using several methods. See Log in to a Splunk platform instance in a Connected Experiences app in the Use Splunk Secure Gateway manual to learn how.
https://docs.splunk.com/Documentation/SecureGateway/3.4.251/User/RegisterorUnregisteraDevice

4. Start using Splunk Mobile

After logging into a Splunk platform instance from your device, you can start using Splunk Mobile. Here are some ways you can get started:

Splunk Mobile for iOS features https://docs.splunk.com/Documentation/Alerts/2.36.0/Alerts/About Send alerts and dashboards to Splunk Mobile users https://docs.splunk.com/Documentation/Alerts/2.36.0/Alerts/SendAlerts

Setup for AR

- "Splunk App for Edge Hub and AR"
- (Opens new window)
- is required on Splunk search head to create and manage AR deployments.
- On the phone here is the documentation on "Splunk AR for iOS App "
- (Opens new window)
-
- There is also the Splunk AR app for Android: "Splunk AR for Android App "
- (Opens new window)
- and here is the download link (in some environments this link only works in incognito mode)