



Splunk, Docs, and You

Making Splunk docs better together

Rich Mahlerwein | Senior Information Systems Security & Database Architect
Forest County Potawatomi Community IT Department

Christopher Gales | Senior Director of Documentation
Splunk

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.

What you will learn today

- ▶ Pros and cons of Splunk docs
- ▶ What sets Splunk documentation apart
- ▶ The different feedback mechanisms
- ▶ How to make the most of them
- ▶ A common path the feedback takes
- ▶ What you should do about it

...and then we will put it into practice



Rich Mahlerwein

- ▶ **Senior Information Systems Security & Database Architect,**
Forest County Potawatomi Community IT Department
- ▶ 3x SplunkTrust member
- ▶ Doc feedback champion
- ▶ “I make things up, you know”



```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=S01SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=S035L7FFGADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K0-CW-01"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=S05$L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=S05$L9FF1ADFF3"
10.55:1871 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=S05$L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
10.55:1871 - - [07/Jan 18:10:55:188] "GET /category.screen?category_id=FLOWERS&JSESSIONID=S05$L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
  
```

Chris Gales

- ▶ Senior Director of Documentation, Splunk
- ▶ Free-roaming community agent
- ▶ “I know where the words are buried”



130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=K9-CB-01"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=K9-CB-01"
10.10.10.10 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-03"
10.10.10.10 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=K9-CB-01"
10.10.10.10 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=K9-CB-01"
10.10.10.10 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-03"
10.10.10.10 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=K9-CB-01"
10.10.10.10 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L7FF6ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=K9-CB-01"

Splunk docs

Two sites for all your Splunking needs

► docs.splunk.com

The screenshot shows the 'Splunk Add-on Builder User Guide' page on docs.splunk.com. The page title is 'Splunk Add-on Builder User Guide' with a version dropdown set to '2.12 (latest release)'. A 'Download manual as PDF' button is visible. The main content area is titled 'Configure data collection using a shell command'. It includes a 'Download topic as PDF' button and a list of instructions: 'Use a REST API call', 'Run a shell command script, described in this topic', and 'Create a modular input from your own Python code'. Below the text is a screenshot of the 'Create Data Input' dialog box in the Splunk interface, showing three options: 'Modular input using a REST API call', 'Modular input using Shell commands', and 'Modular input using my Python code'. A sidebar on the left contains a table of contents with sections like 'Introduction', 'Get started', 'Use the Add-on Builder', 'Advanced', and 'Release Notes'. The top navigation bar includes 'splunk> docs', 'PRODUCTS', 'SOLUTIONS', 'CUSTOMERS', 'COMMUNITY', 'SPLIXICON', 'Support & Services', 'My Account', and a search bar.

► dev.splunk.com

The screenshot shows the 'dev.splunk.com' website. The main navigation bar includes 'splunk> dev', 'Get Started', 'Web Framework', 'REST API', 'SDKs', 'Tools', and 'Developer License'. A search bar and a 'FREE SPLUNK' button are also present. The page content is titled 'Example: Maps using a Simple XML extension'. It features a table of earthquake data with columns for Date, Depth, Lat, Lon, Magnitude, MPT, Region, and Version. Below the table is a map of the Pacific Northwest region showing earthquake locations. To the right of the map is a 'CODE EXAMPLES' sidebar with a list of examples including 'Simple XML extensions', 'Basic dashboard', 'A collection of views', 'Charts', 'Tables with custom renderers', 'Events viewers', 'Maps', 'Drilldown properties', 'Search controls using tokens', 'Search controls using events', 'Search progress events', 'Search results model', 'Token manipulation', 'Token transform and forwarding', '+ HTML dashboards', '+ SplunkJS Stack (outside Splunk Web)', and '+ Same dashboard, different tools'. The main content area includes a 'To use this code:' section with a numbered list of steps and an 'example_map.xml' code block. The code block contains XML for a dashboard script and a map view. The top navigation bar also includes 'Overview', 'Develop Apps', 'Code Examples', 'Tutorials', and 'Component Reference'.

Splunk Docs

They make things easy

Splunk docs are great for a lot of things

- ▶ Are you new to Splunk software?
 - Tutorials
 - Workflow content
 - Conceptual material
 - Simple examples
- ▶ Are you already deep into the Splunk world?
 - Deep reference topics
 - Complex deployment information

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
ows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125.17.14.189 "GET /category.screen?category_id=FLOWERS&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&SESSIONID=5D55L9FF1ADFF3"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
ows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125.17.14.189 "GET /category.screen?category_id=FLOWERS&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&SESSIONID=5D55L9FF1ADFF3"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
ows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125.17.14.189 "GET /category.screen?category_id=FLOWERS&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&SESSIONID=5D55L9FF1ADFF3"
```


Splunk docs are great for a lot of things

► Are you new to Splunk software?

- Tutorials

Splunk Enterprise
Search Tutorial
[Download manual as PDF](#)

Documentation / Splunk Enterprise / Search Tutorial / About the Search Tutorial

Search Tutorial

Introduction

About the Search Tutorial

- Part 1: Getting started
- Part 2: Uploading the tutorial data

About the Search Tutorial
[Download topic as PDF](#)

The Search & Reporting application (Search app) is the primary interface for searches, save reports, and create dashboards. This Search Tutorial is for the Search app.

Use this tutorial to learn how to use the Search app. Differences between Search & Reporting and the Search app are specified throughout this tutorial.

How to use this tutorial

Each Part in the Search Tutorial builds on the previous Part. For example, Parts 1 and 5 are used to create reports and charts in Part 7. It is important that you do the following:

- **Part 1: Getting started**
- **Part 2: Uploading the tutorial data**
- **Part 3: Using the Splunk Search app**
- **Part 4: Searching the tutorial data**
- **Part 5: Enriching events with lookups**
- **Part 6: Creating reports and charts**
- **Part 7: Creating dashboards**

Splunk docs are great for a lot of things

► Are you new to Splunk software?

- Workflow content

splunk IT Service Intelligence

User Manual

[Download manual as PDF](#)

☰ Hide Contents ▲
Documentation / Splunk® IT Service Intelligence / User Manual / Notable Event Management Workflow

User Manual

- ▶ Introduction
- ▶ Service Analyzer
- ▶ Notable Events Review
 - Notable Events Review
 - ▶ Notable Event Management Workflow
 - Set up and run notable event actions
 - Ingest third-party alerts as notable events
 - Manage notable event indexes
 - Use the Notable Events Action SDK
 - Notable Events Action SDK reference
- ▶ Aggregation Policies
- ▶ Glass Tables
- ▶ Multi KPI Alerts
- ▶ Correlation Searches
- ▶ ITSI Modules

[Download topic as PDF](#)

Notable Event Management Workflow [\[edit\]](#)

The following sections describe a typical workflow for handling notable events.

Some of this workflow can be automated using aggregation policies. See [Notable Event Aggregation Policies](#) for information.

Initiate the notable event review process [\[edit\]](#)

The Notable Events Review dashboard supports a process through which an analyst or administrator can acknowledge notable events and track actions taken to resolve the issues that triggered the event.

When you identify an event that requires investigation, the first step is to acknowledge the event. Acknowledging an event changes its status from **New** to **In Progress** and assigns the owner to the current ITSI user. An event can only be acknowledged if the status of the event is **New**. If an event with a status of **New** is already assigned to an owner, acknowledging the event changes the owner assignment to the current ITSI user.

A group of events can only be acknowledged if the status of the group is **New**. You can acknowledge multiple events as long as at least one of the events has a status of **New**. Only the new events will be updated to **In Progress** and assigned to the current user.

1. In the notable events list, select one or more new events, or a group with a status of New. The event details sidebar appears on the right.
2. Click the green **Acknowledge** button in the event details sidebar.

If you selected one or more individual events, the status of the event(s) changes from **New** to **In Progress** and the event(s) are assigned to you (the currently logged in ITSI user).
3. If you selected a group of events, the Acknowledge Events dialog displays.
 - Select **Group** to update the group status to **In Progress** and update the owner of the group to you without updating the owner and status of the individual events in the group.

Splunk docs are great for a lot of things

- ▶ Are you new to Splunk software?
 - Conceptual material

The sequence of search-time operations

When you run a search, the Splunk software runs several operations to derive various knowledge objects and apply them to the events returned by the search. These knowledge objects include extracted fields, calculated fields, lookup fields, field aliases, tags, and event types.

The Splunk software performs these operations in a specific sequence. This can cause problems if you configure something at the top of the process order with a definition that references the result of a configuration that is farther down in the process order.

Search-time operations order example

Consider calculated fields. Calculated field operations are in the middle of the search-time operation sequence. The Splunk software performs several other operations ahead of them, and it performs several more operations after them. Calculated fields derive new fields by running the values of fields that already exist in an event through an `eval` formula. This means that a calculated field formula cannot include fields in its formula that are added to your events by operations that follow it in the search-time operation sequence.

For example, when you design an `eval` expression for a calculated field, you can include extracted fields in the expression, because field extractions are processed at the start of the search-time operation sequence. By the time the Splunk software processes calculated fields, the field extractions exist and the calculated field operation can complete correctly.

However, an `eval` expression for a calculated field should never include fields that are added through a lookup operation. The Splunk software always performs calculated field operations ahead of lookup operations. This means that fields added through lookups at search time are unavailable when the Splunk software processes calculated fields. You will get an error message if your calculated field `eval` expression includes fields that are added through lookups.

Splunk docs are great for a lot of things

► Are you new to Splunk software?

- Simple examples

Examples

Example 1: Compute the overall average duration and add 'avgdur' as a new field to each event if the 'duration' field exists

```
... | eventstats avg(duration) AS avgdur
```

Example 2: Same as Example 1 except that averages are calculated for each distinct value of date_hour and then each event gets the average for its particular value of date_hour.

```
... | eventstats avg(duration) AS avgdur BY date_hour
```

Example 3: This searches for spikes in error volume. You can use this search to trigger an alert if the count of errors is higher than average, for example.

```
eventtype="error" | eventstats avg(foo) AS avg | where foo>avg
```

Examples

1. Create a result as an input into the eval command

Sometimes you want to use the `eval` command as the first command in a search. However, the `eval` command expects events as inputs. You can create a dummy event at the beginning of a search by using the `makesresults` command. You can then use the `eval` command in your search.

```
| makesresults | eval newfield="avalue"
```

2. Determine if the modified time of an event is greater than the relative time

For events with the field `scheduled_time` that is in Unix Epoch time, determine if the scheduled time is greater than the relative time. The relative time is 1 minute before now. This search uses a subsearch that starts with the `makesresults` command.

```
index=_internal sourcetype=scheduler ( scheduled_time > [ makesresults | eval  
it=relative time(now(), "-m") | return $it ] )
```

Splunk docs are great for a lot of things

- ▶ Are you already deep into the Splunk world?
 - Deep reference topics

walklex

This tool "walks the lexicon" to tell you which terms exist in a given index. For example, with some search commands (like `tstat`), the field is in the index; for other terms it is not. Walklex can be useful for debugging.

Walklex outputs a line with three pieces of information:

- term ID (a unique identifier)
- number of occurrences of the term
- term

Usage:

From `$(SPLUNK_HOME)/bin`, type

```
./splunk cmd walklex </path/to/tsidx_file.tsidx> "<key>::<value>"
```

It recognizes wildcards:

```
./splunk cmd walklex </path/to/tsidx_file.tsidx> ""
```

```
./splunk cmd walklex </path/to/tsidx_file.tsidx> "*::*"
```

Empty quotes return all results, and asterisks return all keys or all values (or both, as in the example above).

Example:

```
./splunk cmd walklex </path/to/tsidx_file.tsidx> "token"
```

Rebuild all buckets

The indexer usually handles crash recovery without your intervention. If an indexer goes down unexpectedly, some recently received data might not be searchable. When you restart the indexer, it will automatically run the `fsck` command in the background. This command diagnoses the health of your buckets and rebuilds search data as necessary.

Caution: It is unlikely that you will need to run `fsck` manually. This is a good thing, because to run it manually you must stop the indexer, and the command can take several hours to complete if your indexes are large. During that time your data will be inaccessible. However, if Splunk Support directs you to run it, the rest of this section tells you how to do so.

To run `fsck` manually, you must first stop the indexer. Then run `fsck` against the affected buckets. To run `fsck` against buckets in all indexes, use this command:

```
splunk fsck repair --all-buckets-all-indexes
```

This will rebuild all types of buckets (hot/warm/cold) in all indexes.

To rebuild all buckets in just a single index, use this version of the command:

```
splunk fsck repair --all-buckets-one-index
```

Note: The `fsck` command only rebuilds buckets created by version 4.2 or later of Splunk Enterprise.

The `fsck repair` command can take several hours to run, depending on the size of your indexes. If you determine that you only need to rebuild a few buckets, you can run the `rebuild` command on just those buckets, as described in the next section, [Rebuild a single bucket](#).

If you just want to diagnose the state of your indexes (without taking any immediate remedial action), run:

```
splunk fsck scan --all-buckets-all-indexes
```

To learn more about the `fsck` command, including a list of all options available, enter:

```
splunk fsck --help
```

Rebuild a single bucket

If the index and metadata files in a bucket (version 4.2 and later) somehow get corrupted, you can rebuild the bucket from the raw data file alone. Use this command:

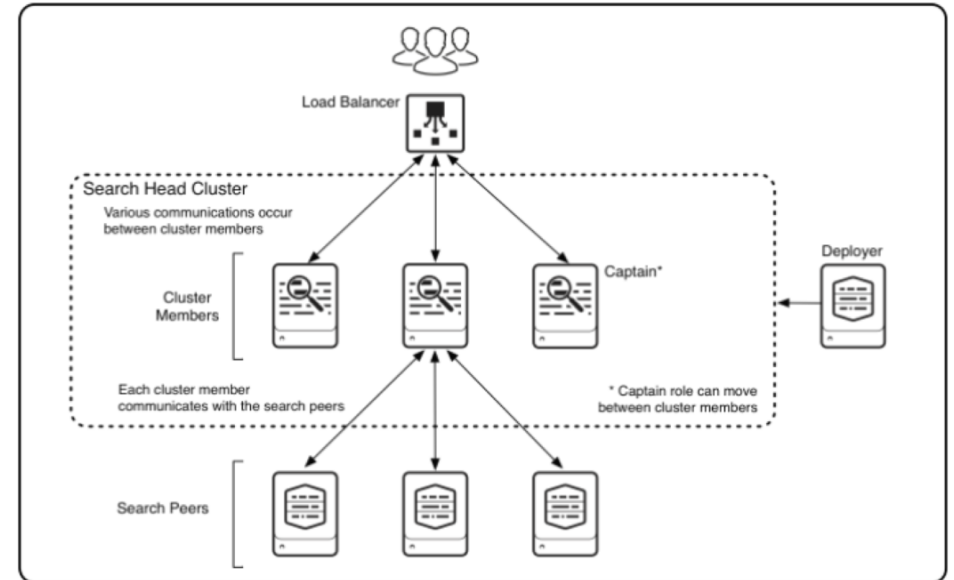
```
splunk rebuild <bucket directory>
```

The indexer automatically deletes the old index and metadata files and rebuilds them. You don't need to delete any files yourself.

Splunk docs are great for a lot of things

- ▶ Are you already deep into the Splunk world?
 - Complex deployment information

here is a diagram of a small search head cluster, consisting of three members.



This diagram shows the key cluster-related components and interactions:

- One member serves as the captain, directing various activities within the cluster.
- The members communicate among themselves to schedule jobs, replicate artifacts, update configurations, and coordinate other activities within the cluster.
- The members communicate with search peers to fulfill search requests.
- Users can optionally access the search heads through a third-party load balancer.
- A deployer sits outside the cluster and distributes updates to the cluster members.

Note: This diagram is a highly simplified representation of a set of complex interactions between components. For example, each cluster member sends search requests directly to the set of search peers. On the other hand, only the captain sends the knowledge bundle to the search peers. Similarly, the diagram does not attempt to illustrate the messaging that occurs between cluster members. Read the text of this topic for the details of all these interactions.

Splunk Docs

They're not perfect

Splunk docs don't always help as much as they should

- ▶ Moving from simple to complex can be hard
 - More complex searches and dashboards
 - Scaling a deployment
 - Using premium solutions
 - Extending the platform

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.189
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CU-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.189
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.189
```


Splunk docs don't always help as much as they should

- ▶ Moving from simple to complex can be hard
 - **More complex searches and dashboards**
 - Scaling a deployment
 - Using premium solutions
 - Extending the platform

Splunk docs don't always help as much as they should

- ▶ Moving from simple to complex can be hard
 - More complex searches and dashboards
 - Scaling a deployment
 - **Using premium solutions**
 - Extending the platform

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D15L9FF1ADFF3 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CB-01"
ows NT 5.1; SV1; .NET CLR 1.1.4322) "GET /oldlink?item_id=EST-26&SESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D18L9FF2ADFF9"
:/buttercup-shopping_id=RP-LI-02" 468 125.17 14.189] "GET /category.screen?category_id=FLOWERS&SESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14"
:/buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CB-01" 468 125.17 14.189] "GET /category.screen?category_id=FLOWERS&SESSIONID=5D55L9FF1ADFF3 HTTP/1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14"
```


Rich's journey

Champions aren't born. They make themselves.

Rich Mahlerwein

A man with a history

- ▶ First real docs experience: doing an upgrade from 4.3 to 6.0 in 2014
 - The docs were well written and generally readable
 - Amazingly, they were **right** and complete.
 - No missing steps!
 - A drop-down for version, so even if I WERE on the wrong version I could change it easily!
 - Feedback section at the bottom.

There's nothing like well written, correct documentation to underscore that the documentation of most companies is terrible.

- Me

Rich Mahlerwein

A man with a history

► First Feedback Experience

- Frustration at a “wall of text” for a set of steps instead of bullet points
 - Ultimately the missed step caused an alert to not work
- Sent in a feedback explaining what frustrated me
- The very next day: Hi Rich

Thanks for your feedback on this topic. I was the original writer for it and I agree that it was a bit confusing. **I've updated the topic** so that it opens with a simple procedure. Hopefully this clears things up a bit. **Let me know if you think there's more that we need to do.**

Kindest regards,
Matt Ness, Splunk Documentation Team

- One hit was all it took.
- “We all just want someone to listen to us!”

Where does the feedback go?

Come take a look inside

It's not too scary. We promise.

“Customer feedback
is the **fuel in our engine.**”

The Splunk doc team

Types of feedback

► Feedback email

Was this topic useful?
Post

Was this documentation topic helpful? Please select ▾

Enter your email address, and someone from the documentation team will r
cgales@splunk.com

Please provide your comments here. Ask a question or make a suggestion.

Send Feedback

► Answers/Slack/IRC

Seeking documentation re: LDAP strategies on a search head cluster in 6.6.1

Hi -

My site has some standalone 6.2 search heads and recently implemented a new cluster of 6.6.1 search heads as well.

I've enabled LDAP authentication, defined a default strategy, and mapped LDAP groups to roles on the cluster, but there are some puzzling differences between 6.2 stand-alone and 6.6.1 clustered that I'm hoping to learn more about. Specifically, there are a number of strategies (settings -> access controls -> authentication method -> LDAP strategies) listed that I didn't create and can't delete/clone/enable but seem to be related to my "default" strategy. Their names are: authentication, cacheTiming,roleMap_default, secrets. And while I can create additional strategies, the only one I can "enable" is "default". I've tried these operations from all cluster members with the same results on all.

I've read lots of docs about 6.6.1 search head clusters and LDAP authentication, but nothing I saw discussed automatically created strategies. Anyone got any pointers that'll help me understand this ?

Thanks,
-Rob

splunk-enterprise search-head-clustering ldap documentation 6.6.1
Question by robgarner Jun 07 at 10:30 AM 26 + 1 + 3
Most Recent Activity: 23,56 + 5 + 13 + 15


Add comment · award points

1 Answer. Add your answer

oldest newest **most voted**


Accepted Answer

If the UI does not clar see : http://docs.splunk.com/Documentation/Splunk/6.6.1/DistSearch/HCarchitecture#Artifact_replication the results are "artifacts"



mdsnmss 1:15 PM


I can't seem to find it in the docs, does a search head cluster replicate search results from scheduled searches?



automine 1:18 PM


yes

http://docs.splunk.com/Documentation/Splunk/6.6.1/DistSearch/HCarchitecture#Artifact_replication



mdsnmss 1:19 PM

Great, thanks!



automine 1:20 PM

np

► Topic comments

Was this topic useful?
Post a Comment

You must be logged into splunk.com in order to post comments. [Log in now.](#)

Please try to keep this discussion focused on the content covered in this documentation topic. If you have a more general question about Splunk functionality or are experiencing a difficulty with Splunk, consider posting a question to [Splunkbase Answers.](#)

0 out of 1000 Characters

Submit Comment

Feedback email

► What happens when you submit feedback?

- The doc team gets an email
- A writer claims it
- We contact you, usually within three days
 - If we can answer your question, we do
 - If we need to do research, we tell you and follow up
 - If we think you should file a support ticket or post your question to Answers, we tell you
 - If we need to change something in the docs, we will
 - If you have encountered a software defect, we file it

Was this topic useful? Post

Was this documentation topic helpful? Please select

Enter your email address, and someone from the documentation team will reach out to you.

Please provide your comments here. Ask a question or make a suggestion.

Send Feedback

Answers/Slack/IRC

- ▶ What if you ask about docs on Answers, or in Slack or IRC?
 - The community can usually help you
 - Doc team members are often lurking as well
 - Writers monitor Answers tags for their areas
 - And, again...
 - If we can answer your question, we do
 - If we need to do research, we tell you and follow up
 - If we think you should file a support ticket, we tell you
 - If we need to change something in the docs, we will
 - If you have encountered a software defect, we file it

Seeking documentation re: LDAP strategies on a search head cluster in 6.6.1

The screenshot shows a question on the Splunk Answers platform. The question asks for documentation regarding LDAP strategies on a search head cluster in version 6.6.1. The user, Rob, mentions they have implemented a new cluster of 6.6.1 search heads and are having trouble with LDAP authentication. They have tried various configurations and operations but are still having issues. They are looking for pointers to help them understand the correct setup.

The thread includes an "Accepted Answer" from user mdsnms, which points to the documentation for authentication configuration and manual LDAP setup. Other users, including automine, provide additional context and confirm the documentation link.

1 Answer · Add your answer

oldest newest most voted

Accepted Answer

If the UI does not clarify the settings, you can check the configuration specifications, in particular the authentication.conf see : <http://docs.splunk.com/Documentation/Splunk/latest/Admin/authenticationconf> and the manual LDAP setup on the config file.

mdsnms 1:15 PM
I can't seem to find it in the docs, does a search head cluster replicate search results from scheduled searches?

automine 1:18 PM
yes
http://docs.splunk.com/Documentation/Splunk/6.6.1/DistSearch/S/HArchitecture#Artifact_replication
the results are "artifacts"

mdsnms 1:19 PM
Great, thanks!

automine 1:20 PM
np

Topic comments

- ▶ What happens if you post a comment?
 - Your comment is visible to everyone
 - The doc managers monitor for new comments
 - A writer claims it
 - We respond on the page and in an email to you
 - And (repeat after me)...
 - If we can answer your question, we do
 - If we need to do research, we tell you and follow up
 - If we think you should file a Support ticket or post your question to Answers, we tell you
 - If we need to change something in the docs, we will
 - If you have encountered a software defect, we file it

Was this topic useful?

Post a Comment

You must be logged into splunk.com in order to post comments. [Log in now.](#)

Please try to keep this discussion focused on the content covered in this documentation topic. If you have a more general question about Splunk functionality or are experiencing a difficulty with Splunk, consider posting a question to [Splunkbase Answers](#).

0 out of 1000 Characters

Submit Comment

PREVIOUS
Cluster maps

NEXT
Dashboard overview

This documentation applies to the following versions of Splunk® Enterprise: 6.6.0, 6.6.1

Comments

The sort command issue is SPL-142769

Robinson splunk, Splunker
June 28, 2017

After looking into the issue, our engineering team has filed a bug for the sort command issue you are reporting. It is listed in our known issues page for the 6.6.0 release. Please check there for further updates.

Robinson splunk, Splunker
June 28, 2017

Hi Ehartvm,
I'll follow up with you via email.

Robinson splunk, Splunker
June 23, 2017

This is my code right now:
index=dummy priority=2 OR priority=10
| stats count by host
| sort 6 -count

This gives me a table with two rows: the top 6 hosts and the event count for each host.
The column and bar charts will be sorted in descending order, based on the count.
The same doesn't work if I'm using the Trellis Feature and "Single Value" or "Radial Gauge".

Should you care?

Well, actually...




130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CR-01"
192.168.1.1 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 189 "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=RP-LI-02"
192.168.1.1 - - [07/Jan 18:10:57:187] "GET /category.screen?category_id=EST-1&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=RP-LI-02"
192.168.1.1 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 189 "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=RP-LI-02"
192.168.1.1 - - [07/Jan 18:10:57:187] "GET /category.screen?category_id=EST-1&JSESSIONID=SD5L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=RP-LI-02"

“Not only does the docs team produce great docs, they also respond to feedback helpfully and in almost no time.”

– *A Splunk customer*

“I have never before experienced this kind of ‘improve as you go’ collaboration across a company boundary with one of our vendors...before Splunk! I always tell my team to post comments and feedback on your documentation because you guys always listen and improve things. I have found it to be very true and it is really a wonderful attribute of your product offering.”

– *Another Splunk customer*

An underwater scene with a blue color palette. In the foreground, a diver is swimming towards the right. In the background, two other divers are visible. The water is filled with a stream of white text, resembling a data stream or log output, which flows from the left towards the right. The text includes various technical details like IP addresses, HTTP methods, and user agents. A large, dark circular graphic is overlaid on the right side of the image, containing white and green text.

Your **comments and suggestions** make Splunk documentation great, so that **the community and your future self** are successful and confident using Splunk software.

Let's look at some examples

First things first

Is your feedback really about Splunk docs?

- ▶ “Hi, I have a Belkin WPN824v2 Range Max Wireless Router that was misbehaving and now defunct. Three questions: 1) will Splunk tell me if the router has gone bad? 2) Can it distinguish between a firmware issue and a bad circuit issue? 3) Does the router have to be functional (good working order) prior to diagnosis? I am using this router in my home for up to four computers and several devices like my Sony Blue Ray Player with Netflix, etc. So can Splunk help me with this.”

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"
 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=K0-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"
 10.0.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D15L4FF10ADFF10 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"
 10.0.0.0 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"
 10.0.0.0 - - [07/Jan 18:10:55:188] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"

First things first

Make sure you are sending feedback that is really about Splunk docs

- ▶ “I some what understand but I am a homewindows7 64 bit and I want to build the greatest CLASSIC ROCK list anyone could have. Am I ion the right place or barking up the wrong tree your system sounds great just dont know where to start.”

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" "Mozilla/5.0 (Windows NT 6.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 6.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0"
137.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3" "Mozilla/5.0 (Windows NT 6.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0"
137.27.160.0 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14" "Mozilla/5.0 (Windows NT 6.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0"
137.27.160.0 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14" "Mozilla/5.0 (Windows NT 6.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0"

First things first

Make sure you are sending feedback that is really about Splunk docs

► “please help me”

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_0; rv:52.0) Gecko/20100801 Firefox/52.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_0; rv:52.0) Gecko/20100801 Firefox/52.0"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D5L9FF1ADFF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_0; rv:52.0) Gecko/20100801 Firefox/52.0"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_0; rv:52.0) Gecko/20100801 Firefox/52.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_0; rv:52.0) Gecko/20100801 Firefox/52.0"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_0; rv:52.0) Gecko/20100801 Firefox/52.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_0; rv:52.0) Gecko/20100801 Firefox/52.0"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_0; rv:52.0) Gecko/20100801 Firefox/52.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_0; rv:52.0) Gecko/20100801 Firefox/52.0"
```

Bad feedback 1

User: 173.XX.XXX.XXX

Email:

Result: NO

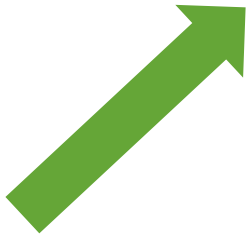


Not logged in, didn't leave email – no way to follow up

URL: <http://docs.splunk.com/Documentation/Splunk/6.6.0/DMC/Searchusagestatistics>

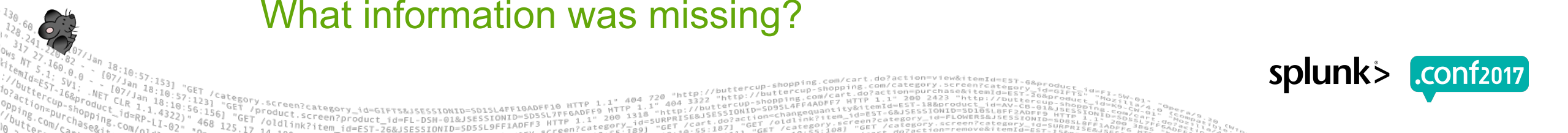
Additional comments:

Topic Not Helpful Reason: The topic did not answer my question(s)



What was the question?

What information was missing?



Bad feedback 3

User: B _____

Email:

Result: NO

URL: <http://docs.splunk.com/Documentation/Splunk/6.6.1/Alert/Reviewtriggeredalerts>

Additional comments: Something better

Topic Not Helpful Reason: The topic did not answer my question(s)

Didn't give us much to go on, but at least we have a way to follow up

Better feedback?

Sent on Friday at 10:04 PM...

User: J _____

Email: j_____@gmail.com

Result: NO

URL:

<http://docs.splunk.com/Documentation/SplunkLight/latest/Installation/Runasnonrootuser>

Additional comments: I know my login and pswd but the system identifies it as incorrect and does not give me an option to create a new one??? Why...how am I suppose to get started. I am looking for the start up screen for splunk light. Please update me asap...I have to turn in something for school by Sunday!

Better feedback?

Sent on Friday at 10:04 PM....

Provided email

User: J _____

Email: j _____@gmail.com

Result: NO

URL:

<http://docs.splunk.com/Documentation/SplunkLight/latest/Installation/Runasnonrootuser>

Doc feedback is not 24/7 customer support.

Additional comments: I know my login and pswd but the system identifies it as incorrect and does not give me an option to create a new one??? Why...how am I suppose to get started. I am looking for the start up screen for splunk light. Please update me asap...**I have to turn in something for school by Sunday!**

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.10.10.10

Definitely better feedback

User: 130.XXX.XX.XXX

Email: t@.edu

Result: NO

URL: <http://docs.splunk.com/Documentation/UnixApp/5.2.2/>

User/DeploytheSplunkAppforUnixandLinuxinadistributedSplunkenvironment

Additional comments: This documentation seems to have conflicting advice. In the top of this page there is a table called "Recommended Splunk App for Unix and Linux Component Installation Locations" where it shows you should only install the app on search heads and the add-on everywhere. However, later on it says after you've installed the app on both the searchhead and indexers "Once you have installed the Splunk App for Unix and Linux onto the indexers and search heads in the central Splunk App for Unix and Linux instance". Also on the other page called "What a Splunk App for Unix and Linux deployment looks like" there is an image that looks like the app is supposed to go on both the indexer and searchhead. http://docs.splunk.com/File:Unix_50_typicallayout.png

Which is it? Should the app go on the indexers or just the add-on?



Definitely better feedback

User: 130.XXX.XX.XXX

Provided email

Email: t @ .edu

Result: NO

Clear background and a specific question

URL: <http://docs.splunk.com/Documentation/UnixApp/5.2.2/>

User/DeploytheSplunkAppforUnixandLinuxinadistributedSplunkenvironment

Additional comments: This documentation seems **conflicting advice**. In the top of this page there is a table called "Recommended Splunk App for Unix and Linux Component" **it shows you should only** install the app on search heads and the add-on everywhere. However, later on it

However, later on it says ... says after you've installed the app on both the searchhead and indexers "Once you deploy the Splunk App for Unix and Linux onto the indexers and search heads in the central Splunk App for Unix and Linux instance". Also on the other page called "What a Splunk App for Unix and Linux deployment looks like" there is an image that looks like the app is supposed to go on both the indexer and searchhead. http://docs.splunk.com/File:Unix_50_typicallayout.png

Which one should the app go on the indexers or just the add-on?

130.60.4 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-03"
 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CU-01"
 317 27.160.0.0 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D15L9FF2ADFF3"
 10.0.0.1 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=FI-5W-03"
 10.0.0.1 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 468 125.17 14.0.0 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CU-01"
 10.0.0.1 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 468 125.17 14.0.0 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CU-01"
 10.0.0.1 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 468 125.17 14.0.0 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CU-01"

Really good feedback

User: 64.XXX.XXX.XXX

Email: m@.edu

Result: NO

URL: <http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Cofilter>

Additional comments: Greetings! I think that the text in the "Description" section of this search command's reference page actually belongs in the "Example 1" section. The generalized description of the command seems to be missing. It isn't clear that the command counts events in which both specified fields occur, and simply outputs a number. It would also be worth investigating and documenting the conditions under which records are counted or excluded. For example, is a record with a zero, an empty string, or a null (if the concept exists in Splunk) in the specified field counted as having a value in that field? Thank you for considering these suggestions.

Really good feedback

Provided email

User: 64.XXX.XXX.XXX

Email: m @ a .edu

Result: NO

URL: <http://docs.splunk.com/Documentation/Splunk/Latest/SearchReference/Commands/GeneralizedDescription>

the text in the "Description" ...

Additional comments: Greetings! I think that the text in the belongs in the "Example 1" section

The generalized description of the comma *generalized description ... seems to be missing* events in which both specified fields occur, and simply outputs a

number. It would also be worth investigating and documenting the conditions under which records are *It isn't clear that ...* example, is a record with a zero, an empty string, or a null (if the concept exists in Splunk) in the specified field counted as *having a value in* that field? Thank you for considering these suggestions. *Thank you*

Tells us where they got confused, why they got confused, and what specific information would help. And so polite.



Really good feedback 2

Bonjour, I was browsing your exceptional documentation when I did happen across a small inconsistency. Once I regained my composure, following my surprise at such a revelation, I sought to make you aware as soon as possible.

Lacking any fully grown carrier pigeons this early into the season I have resorted to submitting this comment.

In the section that starts;

TRANSFORMS- = , ,...*

Used for creating indexed fields (index-time field extractions).

You start referring to the transforms stanza as the transform stanza, you also in the example use TRANSFORM-blah for the yellow example. It may work but it doesn't match up with the example at the bottom of the page nor the terminology used throughout the page. Otherwise, very helpful whilst on-site!

Have a kitten,

<http://kittyblogger.files.wordpress.com/2012/05/cute-kittens-20-great-pictures-1.jpg>



Really good feedback 2

Bonjour, I was browsing *your exceptional documentation* as a small inconsistency. Once I regained my composure, following my surprise at such a revelation, I sought to make you aware as soon as possible.

Lacking any fully grown carrier pigeons this early into the season I have resorted to submitting this comment.

In the section *that starts:* ***In the section that starts; TRANSFORMS-***
TRANSFORMS- =

Used for creating indexed fields (index-time field extractions).

You *start referring to ... as the transform stanza* so in the example use TRANSFORM blank for the yellow example. It may work but it doesn't match up with the example at the bottom of the page nor the terminology used throughout the page.
but it doesn't match up with the example

Have a kitten,

<http://kittyblogger.files.wordpress.com/2012/05/cute-kittens-20-great-pictures-1.jpg>

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CW-01"
ows NT 27.160.0.0 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02"
10 - - [07/Jan 18:10:57:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CW-01"
10 - - [07/Jan 18:10:57:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CW-01"
10 - - [07/Jan 18:10:57:156] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CW-01"
10 - - [07/Jan 18:10:57:156] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CW-01"
10 - - [07/Jan 18:10:57:156] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CW-01"
10 - - [07/Jan 18:10:57:156] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CW-01"

Recap new knowledge

- ▶ For good feedback the minimum you should provide is...
 - Your email or be logged in
 - What confused you?
- ▶ For even **BETTER** feedback
 - What do the docs say to do?
 - What exactly did you do?
 - What result did you expect?
 - What incorrect result did you get?
 - Are there any errors, messages or other information?
 - What do you think would improve the doc content?
 - (It never hurts to include lots of praise on how awesome the docs team is.)



Behind the scenes

The story of an actual doc feedback

Rich's feedback

URL:

<http://docs.splunk.com/Documentation/Splunk/6.5.0/SearchReference/CommonEvalFunctions>

Additional comments: ***docs on eval function "match" is incomplete***

Martin M and I were chatting in Slack about an Answers post, and I don't think he initially believed me that you can use something like "match(myfield,anotherfield)" and it works. ***When [it] isn't quoted, it's treated as ...*** name and the contents of the field are used to match on or not.

Here's a run anywhere example.

Here's a run anywhere example out out in in in in lol" | makemv direction | mvexpand direction | eval test="out" | where not match(direction,test)

Regardless if that's correct behavior or not, it's CERTAINLY not documented anywhere I can find. :)



Rich's feedback – What happened?

- ▶ Laura S got the feedback
- ▶ She responded to Rich to let him know she was investigating
- ▶ Laura tried it herself, then talked to the developers to ask
 - if the behavior was correct, and
 - if it should be documented.
- ▶ Laura and the developers worked through the implementation
- ▶ Laura updated the docs and replied to Rich to let him know

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" "Mozilla/5.0 (Windows NT 6.0; rv:15.0) Gecko/15.0 Firefox/15.0"

128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CB-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322) " 468 125.17.14.189 "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" "0"

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=FI-SW-01" "Mozilla/5.0 (Windows NT 6.0; rv:15.0) Gecko/15.0 Firefox/15.0"

128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CB-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322) " 468 125.17.14.189 "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" "0"

Rich's feedback

- ▶ The result – additional clarity

Evaluation functions

Commands

You can use these functions with the `eval`, `fieldformat`, and `where` commands, and as part of evaluation expressions.

Usage

- All functions that accept strings can accept literal strings or any field.
- All functions that accept numbers can accept literal numbers or any numeric field.

String arguments

For most evaluation functions, when a string argument is expected, you can specify either an explicit string or a field name. The explicit string is denoted by double quotation marks. In other words, when the function syntax specifies a string you can specify any expression that results in a string. For example, `name + "server"`.

Nested functions

Just so you know it's not a fluke

URL: <http://docs.splunk.com/Documentation/SplunkCloud/6.6.0/Knowledge/Configuregeospatiallookups>

Additional comments: *So often my answers were a sugary coating around a nugget of a Doc link.* I was much enjoying this relaxing endeavor

In the course of that endeavor I began to review and formulate a reply to this particular question:

<https://answers.splunk.com/answers/557590/extracting-countries-from-sourcetype-without-longi.html>

"Intriguing," I thought. I do so love those questions that make me think.

I scouted out the first part of the answer relatively easily with some rex and a bit of squinting.

Then with *I find myself transported to a land where the documentation is convoluted and full of gibberish.* I did check my browser for an accidental switching of locales, but I found none. No, the words "XPath" and "feature_id_element" are in fact of my own language, or perhaps there's no known translation of same and thus I get them in their original Geek instead of regular-people English.

Regardless of how I arrived at this page of arcane symbols and statements, I am here and it is a confusing place to be in. I must find my way out, and I fear this will involve a lengthy struggle involving cryptic, tightly-scrawled notes made in the margins and much head-scratching and interpretation.

I am of a thought that *of all the great documentation Splunk has produced... this isn't one of them* still involve sacrifices to the great gods of Geek and must leave for a short while with only nair an answer done. The chilling effect of unadulterated Geek and must leave for a short while with only nair an answer done.

I may - oh horrors - only post a partial answer, with much hand-wringing involving the final touches. I would of course get back to the final touches later after much thinking and staring at these examples.

I *am* sure it is able to be made sensible to my brain, but I beg of you kindly please examine this documentation with an eye toward making it less Geek and more friendly to regular people.

I will, of course and as is usual, provide more feedback later about exactly what it may be that could help make this topic more understandable. At this point I honestly don't know how to fix it.



Just so you know it's not a fluke

- ▶ After some discussion:
 - Really was a different look, feel and style
 - Provided no clear indication when you needed this doc...
 - vs. one of several others which you probably DID need.
- ▶ Resulting in ...

Configure geospatial lookups

Use geospatial lookups to create queries that return results that Splunk software can use to generate a choropleth map visualization. Choropleth maps cannot be rendered without the data generated by corresponding geospatial lookups.

This world, divided up into countries.

This topic shows you how to create additional geospatial lookups that break up choropleth maps into other types of regions (counties, provinces, timezones, and so on).

For more information about choropleth maps and geographic data visualizations, see [Mapping data](#), in the *Dashboards and Visualizations* manual.

For information on using an existing kmz file as a lookup, see the `geom` command in the *Search Reference* manual.

For more information on creating a choropleth map, see [Generate a Choropleth map](#) in the *Dashboards and Visualizations* manual.

Resounding conclusion

Now you know...

- ▶ The Docs team thrives on feedback
- ▶ How feedback is processed
- ▶ To include your contact information
- ▶ To be specific
- ▶ That you can make the docs better for yourself and the entire community



```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5SLAFF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.0 (Windows NT 6.0; U; en) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF1ADFF9 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 189 "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5SLAFF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.2013.0 (Windows NT 6.0; U; en) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF1ADFF9 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 189 "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
```

Going live

We are all in this together

Feedback exercise

LET'S DO THIS!

1. Think of a doc page you were recently using, especially one where you were confused or thought something was missing.
2. Log in to docs.splunk.com.
3. Go to that doc page.
4. Refresh your memory about what the issue was.
5. Scroll to the bottom.
6. Compose excellent doc feedback.
7. Click **Send Feedback**.



Thank You

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

