



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”



Chris Gales

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



Splunk docs

Two sites for all your Splunking needs

► docs.splunk.com

The screenshot shows the "Splunk Add-on Builder User Guide" page. The main content is titled "Configure data collection using a shell command". It includes a sub-section "Add a data input using shell commands" with three options: "Pass values from data input parameters", "Pass values from setup parameters", and "Learn more". Below this is a screenshot of the "Create Data Input" interface, showing three input methods: "Module input using a REST API", "Module input using Shell command", and "Module input using my Python code". The "Module input using Shell command" option is highlighted. The sidebar on the left contains links for "Introduction", "Get started", "Use the Add-on Builder" (which is selected), "Configure data collection using a shell command", "Configure data collection using your Python code", "Create a setup page", "Add sample data", "Extract fields", "Map to CIM", "Create alert actions", "Validate and package", "Advanced", and "Release Notes".

► dev.splunk.com

The screenshot shows the "Example: Maps using a Simple XML extension" page. It features a map of Washington state with several data points. To the right, there is a "CODE EXAMPLES" sidebar with a list of items such as "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". Below the sidebar is a code block for "example_map.xml" containing the following XML:

```
<dashboard script="example_map.js">
<label>Map view</label>
<row>
<panel>
```

At the bottom right, there is a "Got an idea?" button.

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

Splunk docs are great for a lot of things

- ▶ Are you new to Splunk software?
 - Tutorials

Splunk Enterprise

Search Tutorial

[Download manual as PDF](#)

[Hide Contents ▾](#)

[Documentation](#) / [Splunk® Enterprise](#) / [Search Tutorial](#) / [About the](#)

Search Tutorial

Introduction

About the Search Tutorial

▶ Part 1: Getting started

▶ Part 2: Uploading the tutorial data

[Download topic as PDF](#)

About the Search Tutorial

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

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

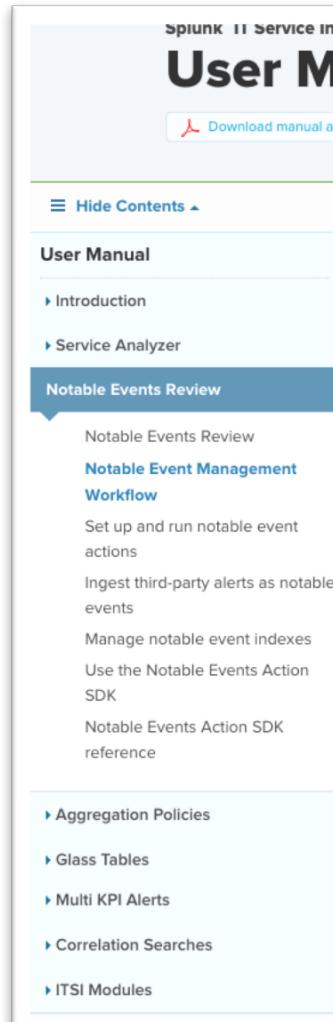
How to use this tutorial

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

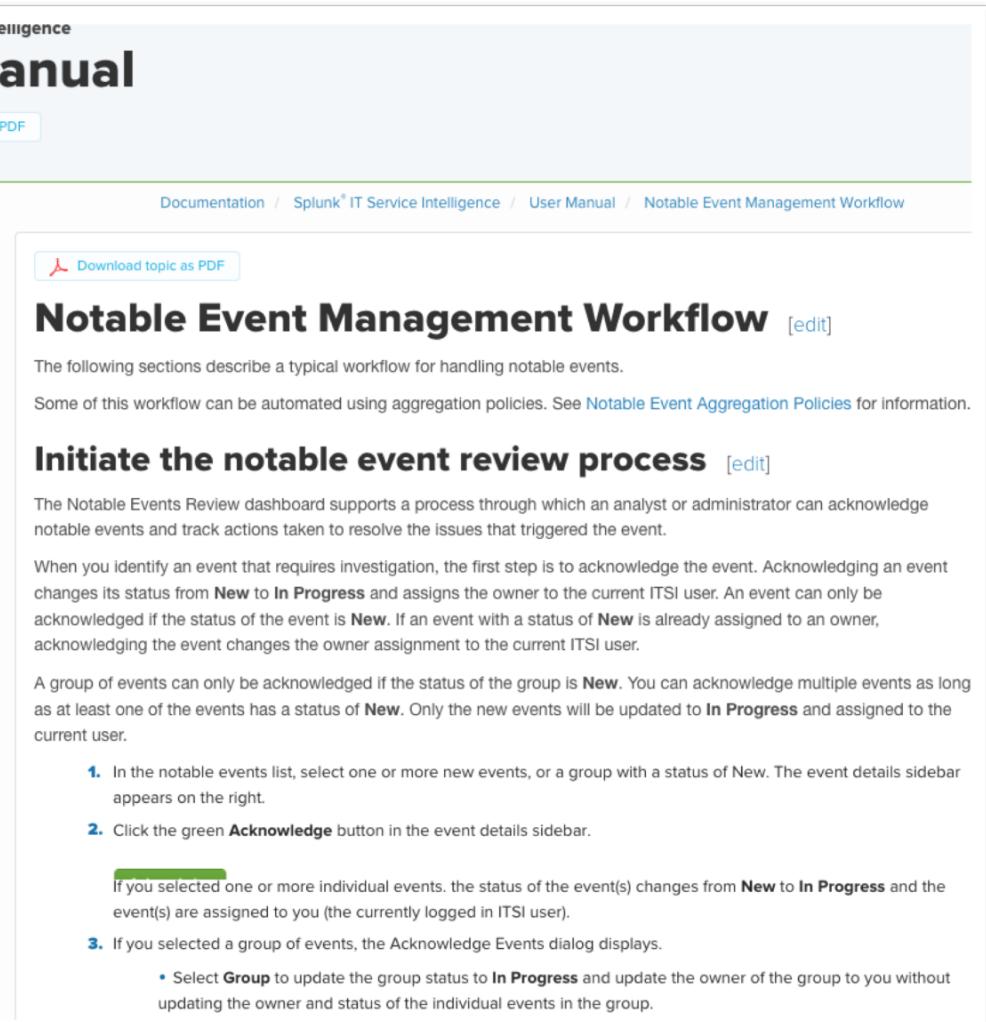
- [Part 1: Getting started](#)
- [Part 2: Uploading the tutorial data](#)
- [Part 3: Using the Splunk Search app](#)
- [Part 4: Searching the tutorial data](#)
- [Part 5: Enriching events with lookups](#)
- [Part 6: Creating reports and charts](#)
- [Part 7: Creating dashboards](#)

Splunk docs are great for a lot of things

- ▶ Are you new to Splunk software?
 - Workflow content



The screenshot shows a navigation sidebar on the left with sections like 'User Manual', 'Introduction', 'Service Analyzer', and 'Notable Events Review' (which is highlighted). Below the sidebar, there's a main content area for 'Notable Event Management Workflow' with sub-sections for 'Initiate the notable event review process' and 'Acknowledge events'.



The main content area contains a heading 'Notable Event Management Workflow' with a sub-section titled 'Initiate the notable event review process'. It includes a list of steps for acknowledging events and a note about updating group status.

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 '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 `makeresults` command. You can then use the `eval` command in your search.

```
| makeresults | 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 `makeresults` command.

```
index=_internal sourcetype=scheduler ( scheduled_time > [ makeresults | 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:

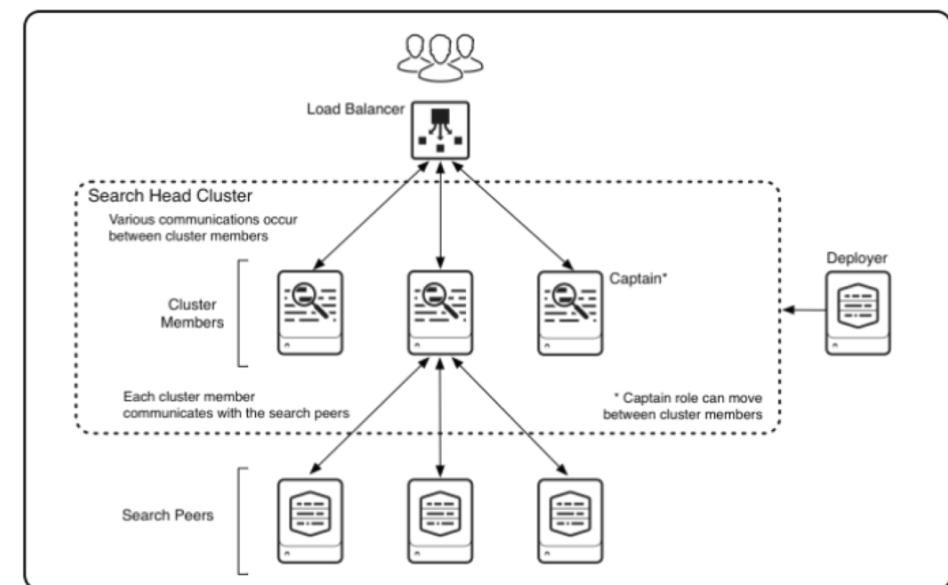
```
splunk rebuild <bucket directory>
```

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

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

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

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

138 60 4
128 241 220 82 ~ [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_6&product_id=EST_5&category_id=EST_5&sw=0"
317 27 160 0 0 ~ [07/Jan 18:10:57:153] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=process&itemId=EST_26&product_id=EST_26&category_id=EST_26&sw=0"
ows NT 5.1: SV1: .NET CLR 1.1.4322 [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=process&itemId=EST_26&product_id=EST_26&category_id=EST_26&sw=0"
kitemid=EST_16&product_id=EST_16&category_id=EST_16&sw=0" [07/Jan 18:10:57:153] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD85LBF2ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=process&itemId=EST_26&product_id=EST_26&category_id=EST_26&sw=0"
102&action=purchase&it [07/Jan 18:10:57:153] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD85LBF2ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=process&itemId=EST_26&product_id=EST_26&category_id=EST_26&sw=0"
opping.com/purchase&it [07/Jan 18:10:57:153] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD85LBF2ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=process&itemId=EST_26&product_id=EST_26&category_id=EST_26&sw=0"
128 241 220 82 ~ [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_6&product_id=EST_5&category_id=EST_5&sw=0"
317 27 160 0 0 ~ [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=process&itemId=EST_26&product_id=EST_26&category_id=EST_26&sw=0"
ows NT 5.1: SV1: .NET CLR 1.1.4322 [07/Jan 18:10:57:153] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=process&itemId=EST_26&product_id=EST_26&category_id=EST_26&sw=0"
kitemid=EST_16&product_id=EST_16&category_id=EST_16&sw=0" [07/Jan 18:10:57:153] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD85LBF2ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=process&itemId=EST_26&product_id=EST_26&category_id=EST_26&sw=0"
102&action=purchase&it [07/Jan 18:10:57:153] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD85LBF2ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=process&itemId=EST_26&product_id=EST_26&category_id=EST_26&sw=0"
opping.com/purchase&it [07/Jan 18:10:57:153] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD85LBF2ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=process&itemId=EST_26&product_id=EST_26&category_id=EST_26&sw=0"

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 contact you.

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/enable but seem to be related to my "default" strategy. Their names are: authenticaon, 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

Add comment · award points

Question by robgarner Jun 07 at 10:30 AM
26 ▪ 1 ▪ 3

Most Recent Activity:
Answered by yannK [Splunk] 33.5k ▪ 5 ▪ 13 ▪ 15

1 Answer.

Add your answer

oldest newest most voted

If the UI does not clarify see : http://docs.splunk.com/Documentation/Splunk/6.6.1/DistSearch/SHCarchitecture#Artifact_replication and the manual LDAP

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/SHCarchitecture#Artifact_replication
the results are "artifacts"

mdsnmss 1:19 PM
Great, thanks!

automine 1:20 PM
np

► Topic comments

<p>Was this topic useful?</p> <hr/>	<p>Post a Comment</p>  <hr/> <p>You must be logged into splunk.com in order to post comments. Log in now.</p> <p>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.</p> <p>0 out of 1000 Characters</p> <div style="border: 1px solid #ccc; height: 100px; margin-top: 10px;"></div> <p>Submit Comment</p>
--	---

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 respond.

cgales@splunk.com

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

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 robgermer Jun 07 at 10:30 AM
26 • 1 • 3
Most Recent Activity: Answered by yannk (Splunk)
33.5k ▾ 5 ▾ 13 ▾ 15

Add comment · award points Add your answer

1 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.

 **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/HArchitecture#Artifact_replication

the results are "artifacts"

 **mdsnmss** 1:19 PM

Great, thanks!

 **automine** 1:20 PM

np

 **mdsnmss** 4:59 PM

AnswersAllDay

splunk> .conf2017

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

Frob Robinson, 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.

Frob Robinson, Splunker
June 28, 2017

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

Frob Robinson, Splunker
June 23, 2017

This is my code right now:
`index=dummy priority=2 OR priority=10
I stats count by host
I 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...



“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*



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.”

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.”

First things first

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

- ## ► “please help me”

Bad feedback 1

User: 173.xx.xxx.xxx

Email:

Result: NO

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 2

User: 198. xx.xxx.xxx

Email: no@no.com

Result: NO

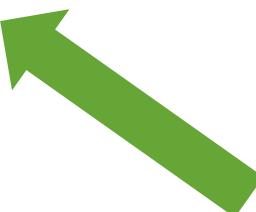
URL: <http://docs.splunk.com/Documentation/Splunk/6.2.2/Data/UploaddataRaw>

Additional comments: Just no

Not logged in, left fake email— no way to follow up



Okay, you're mad, but we would like to help



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

Recap what we've learned so far

- ▶ For good feedback the minimum you should provide is...
 - Your email or be logged in.
 - Either works – we just need a way to contact you.
 - This is the essential piece.
 - What's wrong with which portion of the doc?
 - Not good: “This didn't work!”
 - Better: “What logs are powering the data model?”
 - Pointing us in a direction saves us and yourself some time.

Better feedback?

Sent on Friday at 10:04 PM...

User: J

Email: j@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!**

Definitely better feedback

User: 130.XXX.XX.XXX

Email: t @m .edu

Result: NO

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

User/Deploy the Splunk App for Unix and Linux in a distributed Splunk environment

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%2050%20typicallayout.png>

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

Definitely better feedback

User: 130.XXX.XX.XXX

Email: t @m .edu

Provided email

Result: NO

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

User/Deploy the Splunk App for Unix and Linux in a distributed Splunk environment

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". 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've 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_typicallylayout.png

Which is it?

Whichever one is correct, does the app go on the indexers or just the add-on?

Really good feedback

User: 64.XXX.XXX.XXX

Email: m_____@a_____.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>

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

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

Thank you

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://kittibloger.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; ***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. Otherwise, very helpful.

Have a kitten.

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



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>

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 ...**

Here's a run anywhere example:

Here's a run anywhere example

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

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>

So often my answers were a sugary coating around a nugget of a Doc link

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 scoured out the first part of the answer relatively easily with some regex and a bit of squinting.

Then with 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

a land where the documentation is convoluted and full of gibberish

of all the great documentation Splunk has produced...this isn't one of them

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 beg of you kind folks

please examine this documentation friendly to regular people.

I will, of course and as is usual, provide more feedback later about exactly what may be the best colour to make this topic more understandable. At this point, honestly, I 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 "hot" the data generated by corresponding geospatial lookups.

This would break up into counties.

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



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

splunk> .conf2017