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
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

▶ dev.splunk.com
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 docs are great for a lot of things

- Are you new to Splunk software?
  - Workflow content
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

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.

   ```bash
   | makeresults | eval newfield="a value"
   ```

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.

   ```bash
   index=internal sourcetype=scheduler ( scheduled_time > [ makeresults | eval it=relative_time(now(), "-m") | return it ] )
   ```

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

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

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

   ```bash
   ... | 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.

   ```bash
   eventtype="error" | eventstats avg(foo) AS avg | where foo > avg
   ```
Splunk docs are great for a lot of things

- Are you already deep into the Splunk world?
  - Deep reference topics
Splunk docs are great for a lot of things

- Are you already deep into the Splunk world?
  - Complex deployment information
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
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
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 documentation topic helpful? Please select 1

Enter your email address, and someone from the documentation team will reply:
cgates@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

- My site has two active directories. I search through them on head clusters for search clusters.
- I've tested LDAP authentication with a single strategy and multiple LDAP groups to make the difference. There are some missing options between 6.6.0 and 6.6.1. Although I'm having trouble to learn more about authentication, there seems to be a number of strategies setting up a search cluster with automatic indexers. I'm not sure how to find a specific strategy that isn't in this discussion. Does anyone have a similar strategy that isn't in there? I'm looking for a solution.

Add comment • award points

1 Answer

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

animate 1:15 PM
Yes

http://docs.splunk.com/Documentation/Splunk/6.6.1/DistSearch/S
HCarchitecture#Artifact_replication
the results are "artifacts"

Madhulagna 1:19 PM
Great, thanks!

animate 1:20 PM

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
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
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
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 somewhat 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
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______@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!
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!
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/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

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. Which is it? Should the app go on the indexers or just the add-on?
User: 64.XXX.XXX.XXX
Email: m______@a________.edu
Result: NO

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.
User: 64.XXX.XXX.XXX
Email: m______@a________.edu
Result: NO
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

The text in the "Description" ...

the text in the "Example 1" section

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.

Thank you

Provided email

Tells us where they got confused, why they got confused, and what specific information would help. And so polite.
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://kittybloger.files.wordpress.com/2012/05/cute-kittens-20-great-pictures-1.jpg
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.

Have a kitten,

http://kittybloger.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

Additional comments: Contents of docs on eval function "match" is incomplete, at least. 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.
```
| stats count |
| eval direction = "in out out 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
Rich’s feedback

The result – additional clarity
In the course of that endeavor I began to review and formulate a reply to this particular question:


"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 much surprise I find myself transported in an instant 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 the most clear and easy to follow pieces.  Perhaps this is because the source material Docs is documenting does itself still involve sacrifices to the great gods of Geek.  Perhaps it's simply a holdover from an earlier age where all the children were smarter and could read fluent Geek.  In any case I am not aware of the reasons, but do feel upon myself the chilling effect of unadulterated Geek and must leave for a short while with only half an answer done.

I may - oh horrors! - only post a partial answer, with much hand-waviness 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 in my brain, but I beg of you kind folks, 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 statement trảnt by corresponding geospatial lookups.

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