

Help! I Need To...Where Are...What Is...How Do I... Get Help With All Things Splunk?!

Laura Stewart

Senior Technical Writer, Splunk

Patrick Pablo

Community Content Manager, Splunk

.conf2016

splunk >

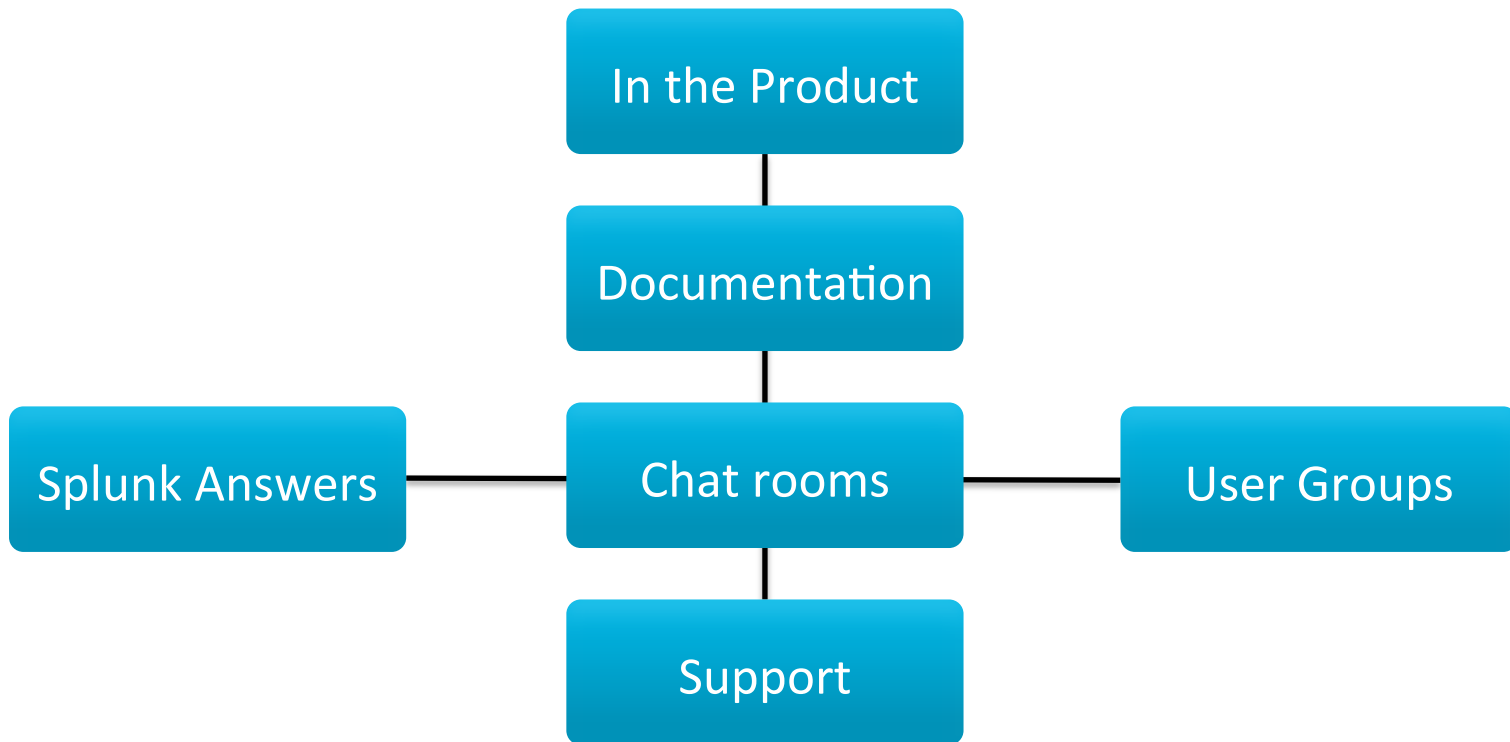
Disclaimer

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 the 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.

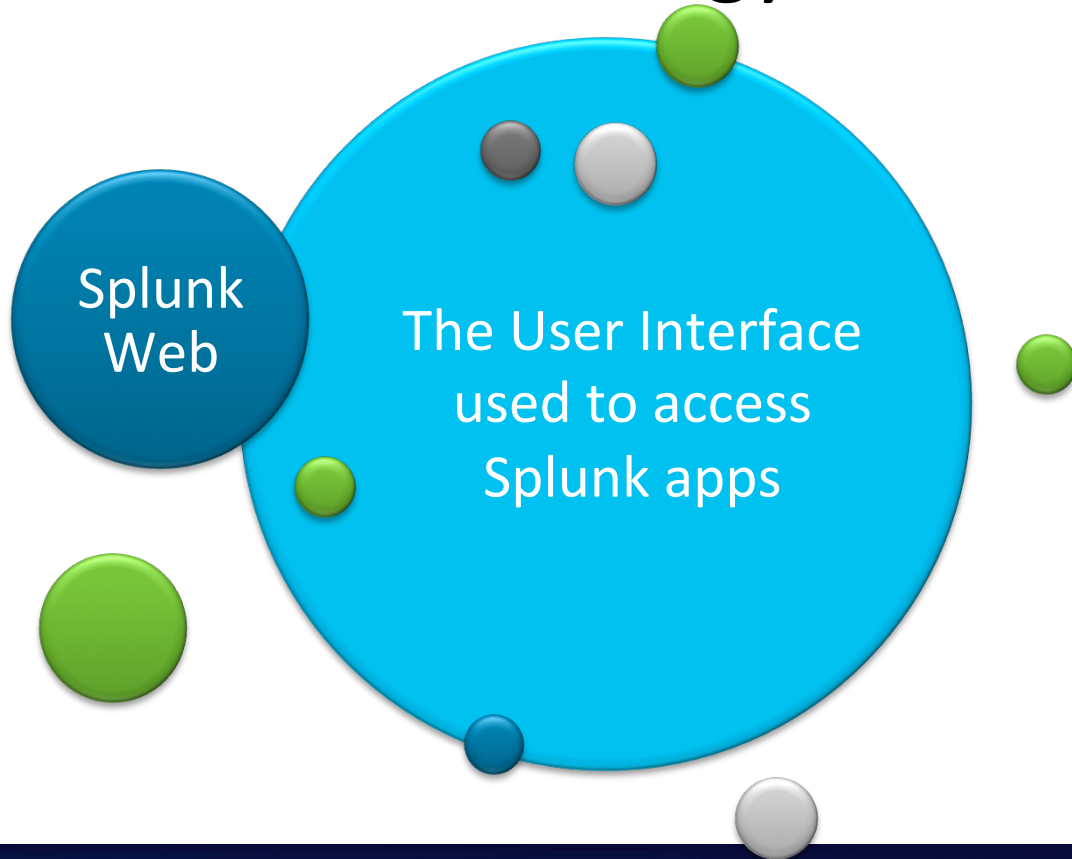
Agenda

- Help in the UI (Splunk Web)
- Help locating info in the docs
- Help with terminology
- Help from the Splunk Community

Where do you start ?



Terminology



Terminology



Terminology





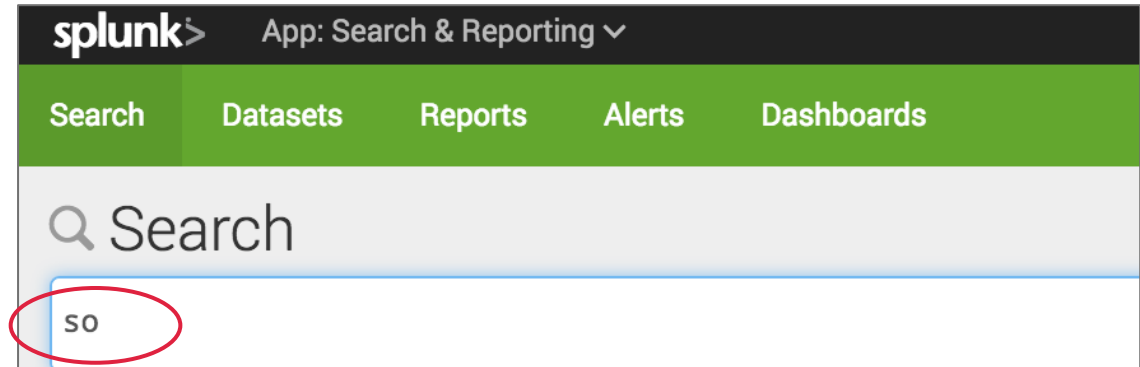
Help in the Search app

- Features to help you build and view searches
 - Search Assistant – Compact (new)
 - Search Assistant - Full
 - Syntax highlighting (new)
 - Shortcuts (new hidden gems)
- Help completing your task
 - Help menu
 - Searching the documentation



Search Assistant (Compact) – search terms

- Type a few letters or a word
- Shows terms in indexed events and search history
- Click term or search to add to the Search bar



Search Assistant (Compact) – command help

The screenshot shows the Splunk Search Assistant interface. At the top, the Splunk logo and navigation tabs (Search, Datasets, Reports, Alerts, Dashboards) are visible. The search bar contains the query `sourcetype=access_* status=200 | top`. Below the search bar, a dropdown menu is open, displaying a list of suggestions for the `top` command, including `top ESXHost`, `top dest_ip`, `top dest_port`, `top limit=100 signature`, and `top user`. A red circle highlights the `top` command description: `top` Displays the most common values of a field. Example: `... | top limit=20 url`. To the right of the dropdown, a 'Learn More' link is circled in red. A red callout box on the left points to the `top` command description, and another red callout box on the right points to the 'Learn More' link.

Command description and an example

Link to command documentation

Search Assistant (Full) – term count

The screenshot shows the Splunk Search Assistant interface. At the top, there's a navigation bar with 'splunk' logo, 'App: Search & Reporting', and user options like 'Administrator', 'Messages', 'Settings', and 'Activity'. Below this is a green navigation bar with 'Search', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The main search bar contains the text 'so'. Below the search bar, there's a section titled 'Matching Searches' with several search queries. To the right, there's a 'How To Search' section with 'Step 1: Retrieve Events' and 'Step 2: Use Search Commands'. At the bottom, there's a 'Matching Terms' section listing search results with their source and count.

Count of indexed events with that term

Matching Terms

Count	Source
9,829	source="tutorialdata.../mailsv/secure.log"
30,244	source="tutorialdata...es/vendor_sales.log"
13,628	source="tutorialdata...p.:/www1/access.log"
10,593	source="tutorialdata...p.:/www1/secure.log"
9,963	source="tutorialdata...p.:/www1/secure.log"
39,532	sourcetype="access_combined_wcookie"
40,088	sourcetype="secure"

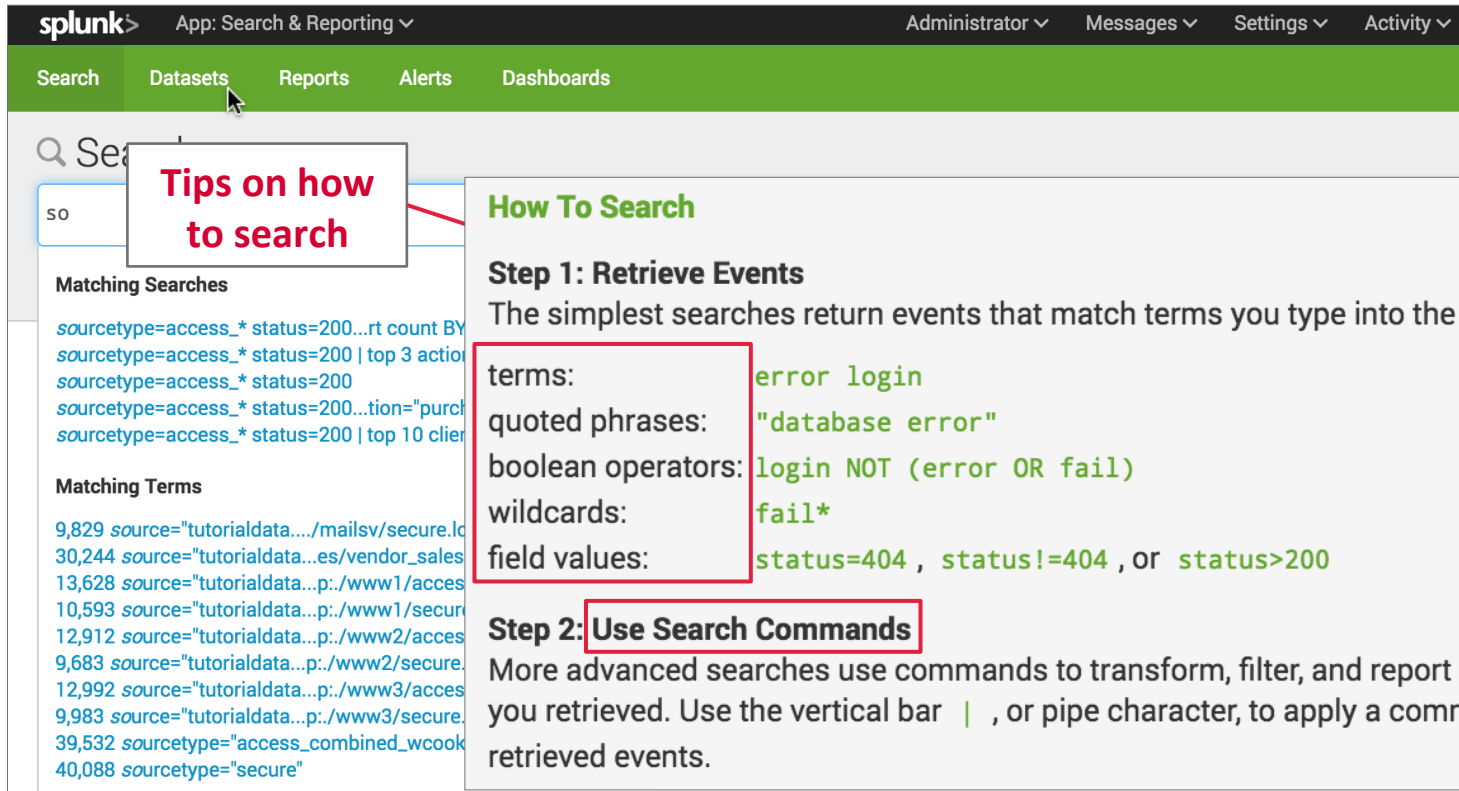
How To Search

Step 1: Retrieve Events
The simplest searches return events that match terms you type into the search bar:

terms: error login
quoted phrases: "database error"
boolean operators: login NOT (error OR fail)
wildcards: fail*
field values: status=404 , status!=404 , or status>200

Step 2: Use Search Commands
More advanced searches use commands to transform, filter, and report on the events you retrieved. Use the vertical bar | , or pipe character, to apply a command to the retrieved events.

Search Assistant (Full) – search tips



The image shows a screenshot of the Splunk Search Assistant interface. The top navigation bar includes 'splunk', 'App: Search & Reporting', 'Administrator', 'Messages', 'Settings', and 'Activity'. Below this is a green navigation bar with 'Search', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The 'Search' section is active, showing a search bar with 'so' and a list of 'Matching Searches' and 'Matching Terms'. A red-bordered box highlights the 'Search' tab. A large white box with a red border and red text 'Tips on how to search' is overlaid on the search bar. To the right, a large white box with a red border contains search tips. The tips are organized into two steps: 'Step 1: Retrieve Events' and 'Step 2: Use Search Commands'. The first step explains that the simplest searches return events that match terms typed into the search bar and lists examples for terms, quoted phrases, boolean operators, wildcards, and field values. The second step explains that more advanced searches use commands to transform, filter, and report on the events retrieved, and that the vertical bar (pipe character) is used to apply a command to the retrieved events.

Tips on how to search

How To Search

Step 1: Retrieve Events

The simplest searches return events that match terms you type into the search bar:

terms:	<code>error login</code>
quoted phrases:	<code>"database error"</code>
boolean operators:	<code>login NOT (error OR fail)</code>
wildcards:	<code>fail*</code>
field values:	<code>status=404 , status!=404 , or status>200</code>

Step 2: Use Search Commands

More advanced searches use commands to transform, filter, and report on the events you retrieved. Use the vertical bar `|` , or pipe character, to apply a command to the retrieved events.

Syntax Highlighting

```
Search
sourcetype=access_* status=200 action=purchase | transaction clientip maxspan=10m
```

- Commands
- Command arguments

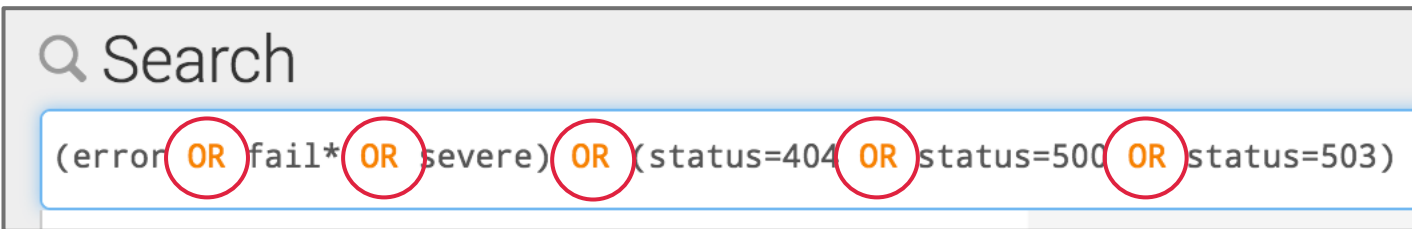
Syntax Highlighting

Q Search

```
sourcetype=access_* status=200 action=purchase | transaction clientip maxspan=10m | chart count
```

- Commands
- Command arguments
- Functions

Syntax Highlighting



- Commands
- Command arguments
- Functions
- Keywords

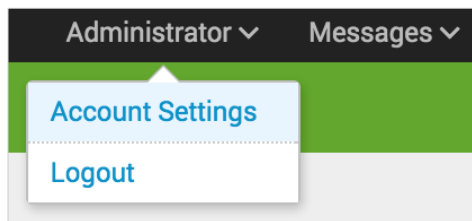
Syntax Highlighting

Search

```
(index=* OR index=_) (((tag=listening tag=port) OR (tag=process tag=report) OR (tag=service tag=report))) | eval nodename =
  "All_Application_State" | eval dest=if(isnull(dest) OR dest="", "unknown", dest), process=if(isnull(process) OR process="", "unknown"
, process) | rex field=process "^\s*(?<process_name>[\s]+)" max_match=1 | eval is_Ports=if(searchmatch("(tag=listening tag=port)"
), 1, 0), is_not_Ports=1-is_Ports, is_Processes=if(searchmatch("(tag=process tag=report)"), 1, 0), is_not_Processes=1-is_Processes,
is_Services=if(searchmatch("(tag=service tag=report)"), 1, 0), is_not_Services=1-is_Services | eval nodename = if(nodename ==
"All_Application_State" AND searchmatch("(tag=listening tag=port)"), mvappend(nodename, "All_Application_State.Ports"), nodename) |
eval dest_port=if(isnum(dest_port), dest_port, 0), transport=if(isnull(transport) OR transport="", "unknown", lower(transport)),
transport_dest_port=if(isnull(transport_dest_port) OR transport_dest_port="", split(replace(mvjoin(mvzip(transport, dest_port), "|"
), "", "/" ), "|"), transport_dest_port) | rename dest_port AS All_Application_State.Ports.dest_port transport AS
All_Application_State.Ports.transport transport_dest_port AS All_Application_State.Ports.transport_dest_port | eval nodename = if
(nodename == "All_Application_State" AND searchmatch("(tag=process tag=report)"), mvappend(nodename, "All_Application_State
.Processes"), nodename) | rename cpu_load_mhz AS All_Application_State.Processes.cpu_load_mhz cpu_load_percent AS
All_Application_State.Processes.cpu_load_percent cpu_time AS All_Application_State.Processes.cpu_time mem_used AS
All_Application_State.Processes.mem_used | eval nodename = if(nodename == "All_Application_State" AND searchmatch("(tag=service
tag=report)"), mvappend(nodename, "All_Application_State.Services"), nodename) | eval service=if(isnull(service) OR service=""
, "unknown", service), service_id=if(isnull(service_id) OR service_id="", "unknown", service_id), start_mode=if(isnull(start_mode) OR
```

Search Help Settings

- Compact and Syntax highlighting are new in 6.5.0. and are the default settings
- Change the settings through Account Settings on the User menu



Search

Use these properties for assistance with command syntax in different colors.

Search assistant

- Compact
- Full
- None

Syntax highlighting

- On
- Off

Shortcuts

Parsing search syntax

Search

```
(index=* OR index=*) (((tag=listening tag=port) OR (tag=process tag=report) OR (tag=service tag=report)) | eval nodename = "All_Application_State" | eval dest=if(isnull(dest) OR dest="", "unknown", dest), process=if(isnull(process) OR process="", "unknown", process) | rex field=process "^\\s*(?<process_name>[\\s]+)" max_match=1 | eval is_Ports=if(searchmatch("(tag=listening tag=port)", 1, 0), is_not_Ports=1-is_Ports, is_Processes=if(searchmatch("(tag=process tag=report)", 1, 0), is_not_Processes=1-is_Processes, is_Services=if(searchmatch("(tag=service tag=report)", 1, 0), is_not_Services=1-is_Services | eval nodename = if(nodename == "All_Application_State" AND searchmatch("(tag=listening tag=port)"), mvappend(nodename, "All_Application_State.Ports"), nodename) | eval dest_port=if(isnum(dest_port), dest_port, 0), transport=if(isnull(transport) OR transport="", "unknown", lower(transport)), transport_dest_port=if(isnull(transport_dest_port) OR transport_dest_port="", split(replace(mvjoin(mvzip(transport, dest_port), "|"), ",", "/"), "|"), transport_dest_port) | rename dest_port AS All_Application_State.Ports.dest_port transport AS All_Application_State.Ports.transport transport_dest_port AS All_Application_State.Ports.transport_dest_port | eval nodename = if(nodename == "All_Application_State" AND searchmatch("(tag=process tag=report)"), mvappend(nodename, "All_Application_State.Processes"), nodename) | rename cpu_load_mhz AS All_Application_State.Processes.cpu_load_mhz cpu_load_percent AS All_Application_State.Processes.cpu_load_percent cpu_time AS All_Application_State.Processes.cpu_time mem_used AS All_Application_State.Processes.mem_used | eval nodename = if(nodename == "All_Application_State" AND searchmatch("(tag=service tag=report)"), mvappend(nodename, "All_Application_State.Services"), nodename) | eval service=if(isnull(service) OR service="", "unknown", service), service_id=if(isnull(service_id) OR service_id="", "unknown", service_id), start_mode=if(isnull(start_mode) OR
```


Shortcuts

Parsing search syntax

**Command (Ctrl) + **
keyboard shortcut

🔍 Search

```
(index=* OR index=_) ((( )) (tag=listening tag=port) OR (tag=process tag=report) OR (tag=service tag=report))
| eval nodename = "All_Application_State"
| eval dest=if(isnull(dest) OR dest="", "unknown", dest), process=if(isnull(process) OR process="", "unknown", process)
| rex field=process "^\\s*(?<process_name>[\\s]+)" max_match=1
| eval is_Ports=if(searchmatch("(tag=listening tag=port)"),1,0), is_not_Ports=1-is_Ports, is_Processes=if(searchmatch("(tag=process
tag=report)"),1,0), is_not_Processes=1-is_Processes, is_Services=if(searchmatch("(tag=service tag=report)"),1,0), is_not_Services
=1-is_Services
| eval nodename = if(nodename == "All_Application_State" AND searchmatch("(tag=listening tag=port)"), mvappend(nodename,
"All_Application_State.Ports"), nodename)
| eval dest_port=if(isnum(dest_port),dest_port,0), transport=if(isnull(transport) OR transport="", "unknown", lower(transport)),
transport_dest_port=if(isnull(transport_dest_port) OR transport_dest_port="", split(replace(mvjoin(mvzip(transport,dest_port),"|")
),",","/"),"|"),transport_dest_port)
| rename dest_port AS All_Application_State.Ports.dest_port transport AS All_Application_State.Ports.transport transport_dest_port AS
All_Application_State.Ports.transport_dest_port
| eval nodename = if(nodename == "All_Application_State" AND searchmatch("(tag=process tag=report)"), mvappend(nodename,
"All_Application_State.Processes"), nodename)
```

Shortcuts

Locating terms in search strings

Double click
on a term

Search

```
(index=* OR index=_) (((tag=listening tag=port) OR (tag=process tag=report) OR (tag=service tag=report)) | eval nodename =  
"All_Application_State" | eval dest=if(isnull(dest) OR dest="", "unknown", dest), process=if(isnull(process) OR process="", "unknown"  
, process) | rex field=process "\s*(?<process_name>[\s]+)" max_match=1 | eval is_Ports=if(searchmatch("(tag=listening tag=port  
)", 1, 0), is_not_Ports=1-is_Ports, is_Processes=if(searchmatch("(tag=process tag=report)", 1, 0), is_not_Processes=1-is_Processes,  
is_Services=if(searchmatch("(tag=service tag=report)", 1, 0), is_not_Services=1-is_Services | eval nodename = if(nodename =  
"All_Application_State" AND searchmatch("(tag=listening tag=port)", mvappend(nodename, "All_Application_State.Ports", nodename)  
| eval dest_port=if(isnum(dest_port), dest_port, 0), transport=if(isnull(transport) OR transport="", "unknown", lower(transport)),  
transport_dest_port=if(isnull(transport_dest_port) OR transport_dest_port="", split(replace(mvjoin(mvzip(transport, dest_port), "|"  
) , "", "/"), "|"), transport_dest_port) | rename dest_port AS All_Application_State.Ports.dest_port transport AS  
All_Application_State.Ports.transport transport_dest_port AS All_Application_State.Ports.transport_dest_port | eval nodename = if  
(nodename = "All_Application_State" AND searchmatch("(tag=process tag=report)", mvappend(nodename, "All_Application_State  
.Processes", nodename), rename cpu_load_mhz AS All_Application_State.Processes.cpu_load_mhz cpu_load_percent AS  
All_Application_State.Processes.cpu_load_percent cpu_time AS All_Application_State.Processes.cpu_time mem_used AS  
All_Application_State.Processes.mem_used | eval nodename = if(nodename = "All_Application_State" AND searchmatch("(tag=service  
tag=report)", mvappend(nodename, "All_Application_State.Services", nodename), eval service=if(isnull(service) OR service=""  
, "unknown", service), service_id=if(isnull(service_id) OR service_id="", "unknown", service_id), start_mode=if(isnull(start_mode) OR
```

Shortcuts

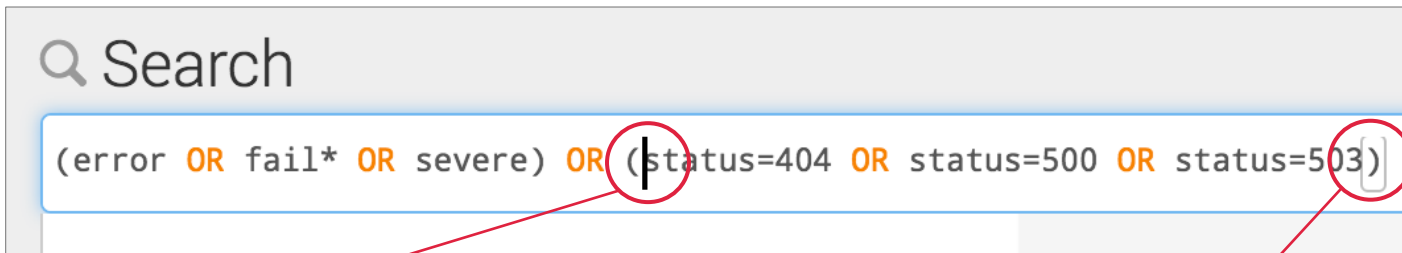
Locating matching parenthesis

Q Search

```
(error OR fail* OR severe) OR (status=404 OR status=500 OR status=503)
```

Shortcuts

Locating matching parenthesis



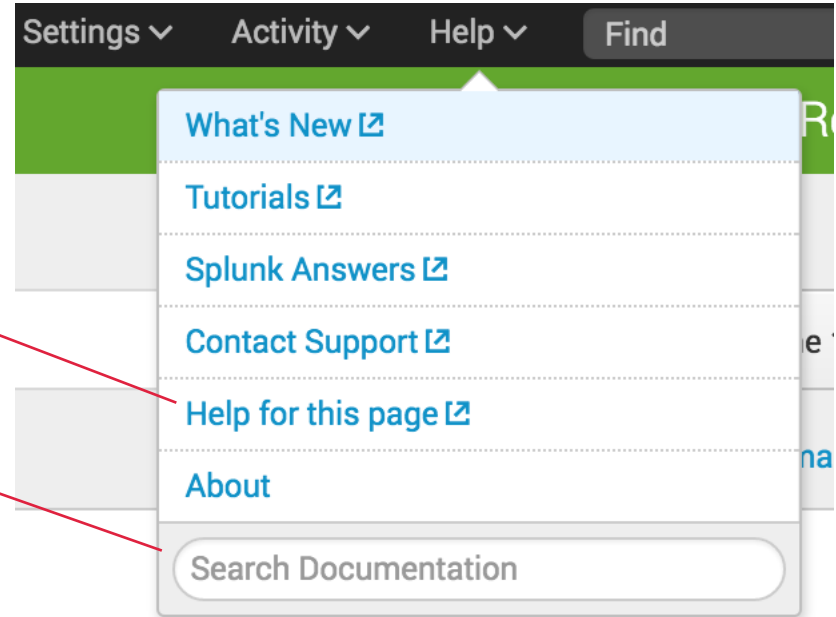
**Position the cursor immediately
after the parenthesis**

**To see the matching
parenthesis highlighted**



Task Help

- Help specific to the window you are on
- Search the specific product and version of the documentation





Searching the docs

Searching within the documentation

All Splunk doc pages have a link to the Splexicon

Type your search terms here

The screenshot shows the Splunk documentation search interface. At the top, a dark navigation bar contains the Splunk logo, 'docs', and several menu items: 'PRODUCTS', 'SOLUTIONS', 'CUSTOMERS', 'COMMUNITY', 'SPLEXICON', 'Support & Services', and 'My Account'. A search box labeled 'Search Docs' is on the right. Below the navigation bar, the main content area features 'Splunk® Enterprise' and 'Search Manual' in large text. A 'Download manual as PDF' button is visible. On the right side of the main content area, there is a 'Version' dropdown menu currently set to '6.5.0'. Red circles and lines highlight the 'SPLEXICON' menu item, the 'Splunk® Enterprise' text, the 'Version' dropdown, and the search box. Red text boxes with arrows provide instructions: 'All Splunk doc pages have a link to the Splexicon' points to the Splexicon menu item; 'Type your search terms here' points to the search box; and 'Searches only the product and version for your terms' points to the 'Splunk® Enterprise' text.

Searches only the product and version for your terms



Searching the docs

Uses the Google Search Appliance

Results in different locations

Search Results

Documentation - (387)

Splunk.com - (458)

Community Wiki - (109)

Results 1 - 10 of approximately 387 total for "source type" on Splunk.com

Why source types matter - Splunk Knowledgebase | Docs

... *sourcetype* is the name of the **source type** search field. You can use the *sourcetype* field to find similar **types** of data from any **source type**. ...

<http://docs.splunk.com/Documentation/Splunk/6.4.2/Data/Whysourcetypesmatter>

Manage source types - Splunk Knowledgebase | Docs

... *whose names contain a certain string, type that string in ... Only source types*

Related Answers

- Discard Source type
- remove source type
- Source type to use for postgresql log
- Combine Multiple Source Types with Rename Function
- Can't find the right source type
- remove source and source types
- Source types and field tagging
- use multiple sources of the same type in



Searching the entire doc site

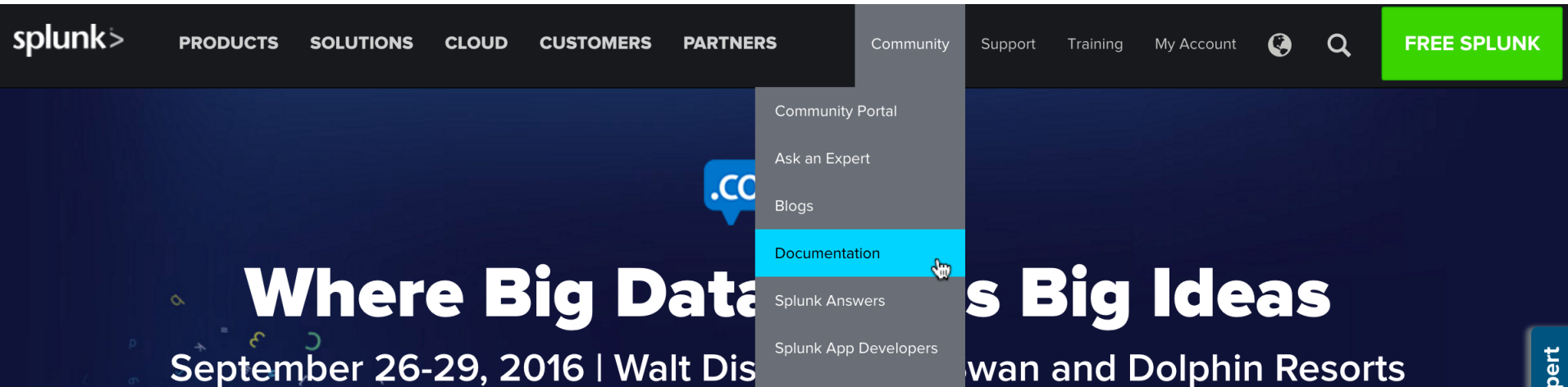


site:docs.splunk.com security





How do I find the Splunk documentation?

- From inside Splunk Web
- docs.splunk.com
- dev.splunk.com
- From the splunk.com web site
 - Under Community
 - Under Support



The screenshot shows the Splunk website's navigation bar. The 'Community' menu is open, and the 'Documentation' option is highlighted in blue. The background features a banner for 'Where Big Data Meets Big Ideas' with the dates 'September 26-29, 2016 | Walt Disney World Swan and Dolphin Resorts'.

splunk > PRODUCTS SOLUTIONS CLOUD CUSTOMERS PARTNERS Community Support Training My Account   FREE SPLUNK

Community Portal
Ask an Expert
Blogs
Documentation
Splunk Answers
Splunk App Developers

Where Big Data Meets Big Ideas
September 26-29, 2016 | Walt Disney World Swan and Dolphin Resorts

What docs are available?



Core products

[Splunk® Enterprise](#)

[Splunk® Light](#)

[Splunk Cloud™](#)

[Hunk®](#)

[Splunk® Universal Forwarder](#)



Premium solutions

[Splunk® Enterprise Security](#)



Apps and add-ons

[Splunk® Supported Add-ons](#)



Developer tools

[Splunk® Add-on Builder](#)

[Splunk® SDKs](#)

[Splunk® Web Framework](#)

[Get started](#)

[Search and report](#)

[Administer](#)

[Alerting Manual](#)

How to create and dispatch alerts that are triggered when specific conditions are met.

[Dashboards and Visualizations](#)

Create and edit dashboards by using Splunk Enterprise interactive editors and simple XML source code. Includes information about visualizations that you can use to show search results. Also includes a reference to simple

[Pivot Manual](#)

How to use Pivot to create tables and charts without the use of the Splunk Search Processing Language (SPL).

[Reporting Manual](#)

How to save and manage searches and pivots as a report. Includes report acceleration, report scheduling, and printing reports as PDFs.

Splunk Dev Portal

dev.splunk.com

splunk > dev

Splunk.com | Comm

Search

[Get Started](#) [Web Framework](#) [REST API](#) [SDKs](#) [Tools](#) [Developer License](#)

FREE SPLUNK

[Overview](#) [Developer Guidance](#) [Integrate and Extend](#) [App Certification](#)

CUSTOM
THE PO
Integrate
Build real

Splunk Developer Guidance

Overview

The Splunk developer platform enables developers to take advantage of their web development skills and the same underlying technologies that power the core Splunk Enterprise product to build exciting new apps and solutions that address your specific use cases and technologies.

Splunk Developer Guidance includes two reference apps and associated applied engineering guidance to help you become productive, competent and successful in building, testing and deploying comprehensive Splunk solutions. The reference apps are complete, end-to-end real-world apps build together with our partners which are meant to showcase various underlying technologies as well as good and proven practices and patterns.



[Order paperback](#)
[Order ebook](#)

DEVELOPER GUIDANCE

Part I: The Journey

[Planning a journey](#)

[Platform and tools](#)

[UI and visualizations](#)

[Working with data](#)

[Adding code](#)

[Packaging and deployment](#)

[Updating our equipment and OAuth](#)

Accelerate
Better code, faster

- Deliver improved proactive alerts
- Gain new insights into business transactions
- Improve DevOps

Can I get a PDF of the docs?

PDF of the manual

Splunk® Enterprise

Dashboards and Visualizations

 Download manual as PDF

Hide Contents

Dashboards and Visualizations

Introduction

Getting started

- ▶ Visualization options
- ▶ Dashboards: An overview
- ▶ Build dashboards in Splunk Web
- ▶ Export dashboards

Documentation / Splunk® Enterprise

PDF of the topic

Dashboards and Visualizations / Getting started

 Download topic as PDF

Getting started

Learn how to share insights with data visualizations and dashboards.

Failed Logins

Edit More Info  

66,506

Failed attempts

48,022

Invalid accounts

18,484

Valid accounts

Top 5 hackers

109.169.32.135 targeted accounts

Hacker	Failed Logins	username	count
87.194.216.51	1896	109	284

Related information

Installation Manual

[Download topic as PDF](#)

Migrate a Splunk Enterprise instance [\[edit\]](#)

These migration instructions are for on-premises Splunk Enterprise instances only.

If you are a Splunk Cloud customer or want to migrate your data from Splunk Enterprise to Splunk Cloud, do not use these instructions. See [Splunk Cloud Migration](#) for assistance.

Related Answers

- [Migrate from Splunk Storm to Enterprise](#)
- [How to migrate data from a 6.2.0 Splunk instance to a new instance on 6.4.1?](#)
- [Migrating Splunk instance from Windows to Linux](#)
- [Migrate All Alerts from one instance to other instance](#)
- [Migrating Splunk Enterprise instances to new servers, what steps do I need to follow with a deployment server?](#)

Migrate a Splunk Enterprise instance

- [When to migrate](#)
 - [What to consider when migrating](#)
 - [How to migrate](#)
 - [How to move index buckets from one host to another](#)

Upgrade or migrate Splunk Enterprise

- [How to upgrade Splunk Enterprise](#)
- [About upgrading to 6.4 READ THIS FIRST](#)
- [How Splunk Web procedures have changed](#)

Callout 1: Scroll down the manual TOC to see related information

Callout 2: Related Answers

Help with terminology

Splexicon

Documentation / Splexicon * A B C D E **E** G H I J K

The Splexicon defines technical terms that are specific to Splunk. Definitions include links to rel

* *nix

splunk > docs PRODUCTS SOLUTIONS CUSTOMERS COMMUNITY **SPLEXICON**

alert
alert action

App Key value Store
archiving

- Link to the Splexicon at the top of every documentation page

Topic links to Splexicon entries

When Splunk Enterprise extracts fields

Splunk Enterprise extracts fields first at [index time](#), and again at [search time](#). After you run a search, fields extracted for that search are listed in the fields sidebar.

**Splexicon links
are bold**

Field extraction at index time

At index time, Splunk Enterprise extracts a small set of [default fields](#) for each event, including `host`, `source`, and `sourcetype`. Default fields are common to all events. See [Use default fields](#).

Normal links to other topics

People say no one reads documentation

- Over 1.3 million unique page views each month
- More than 3500 pages of content



“Reading the utterances that other companies pass off as their documentation always makes me appreciate Splunk's docs.”

- *Rich Mahlerwein,
Forest County Potawatomi
IT Department*

And we get fan mail ...

“Splunk's documentation is excellent... Good docs make a huge difference ... most companies and open-source projects can barely be bothered to document anything at all. Your team's hard work in this area is one of the reasons that Splunk is a joy to use.”

- Matt Perry, Lawrence Livermore National Laboratory

Why are Splunk Docs so good?

- Besides our awesome team of writers and editors?
- Because users take the time to send us feedback:
 - Suggestions for improvements
 - Corrections
 - Examples
 - Requests for more info
- An average of 150 doc feedback emails each month.
- We always follow up!



How do I send doc feedback?

(and what happens to it)

- Two methods for providing doc feedback
 - Feedback and Comments
- Feedback > the fastest way to communicate with the doc team

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

- Johannes Effland, Consist Software Solutions

Feedback form

Was this topic useful

Post a Comment

Was this documentation topic helpful?

If you'd like to hear back from us, please provide your email address:

We'd love to hear what you think about this topic or the documentation as a whole
Feedback you enter here will be delivered to the documentation team

Send Feedback



Feedback examples

This feedback
is helpful

User: [REDACTED]
Email: [REDACTED]
Result: YES
URL: <http://docs.splunk.com/Documentation/Splunk/latest/Search/Exportsearchresults>
Additional comments: Hi, the documentation is all in all helpful but contains unfortunately some mistakes, point 2 under python SDK contains the following code:

```
rr = results.ResultsReader(service.jobs.export("search index=_internal | earliest= -1h"))
```

this code is wrong, first you don't use a pipe in this kind of search, second there is a quotation mark on the end missing. Here the corrected version:

```
rr = results.ResultsReader(service.jobs.export("search index=_internal earliest= -1h"))
```

Without comments or
an email address, we
can't help this user

User: 173.36.[REDACTED]
Email:
Result: NO
URL: <http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Stats>
Additional comments:

Comment form

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

Comments

Cgardiner

Thank you for the examples!

I have added them to the documentation.

Lstewart splunk, Splunker

July 1, 2016

**The doc team
responds with a
comment**

For reference on alternate timezone formats:

%z - hour and minute (e.g. +0500)

:%z - hour and minute separated with a colon (e.g. +05:00)

%::z - hour minute and second separated with colons (e.g. +05:00:00)

%:::z - hour only (e.g. +05)

Cgardiner

June 29, 2016

**Comments are
posted at the bottom
of the topic**

Customer examples in the docs

Example: Use a sudo event to locate the user logins

This example illustrates how to find a sudo event and then use the map command to trace back to the computer and the time that users logged on before the sudo event. Start with the following search for the sudo event:

```
sourcetype=syslog sudo | stats count by user host
```



Which returns a table of results, such as:

User	Host	Count
userA	serverA	1

userB

userA

When you pipe

```
sourcetype=syslog  
username=$user
```

_time	computername	computertime	username	usertime
10/12/15 8:31:35.00 AM	Workstation\$	10/12/2015 08:25:42	userA	10/12/2015 08:31:35 AM

(Thanks to Splunk user [Alacercogitatus](#) for this example.)

It takes each of the three results from the previous search and searches in the `ad_summary` index for the user's logon event. The results are returned as a table, such as:

_time	computername	computertime	username	usertime
10/12/15 8:31:35.00 AM	Workstation\$	10/12/2015 08:25:42	userA	10/12/2015 08:31:35 AM

(Thanks to Splunk user [Alacercogitatus](#) for this example.)



Splunk Community

“It comes back to the fact that [the competitors] don’t have the same user community base or following...

Even if they had like functionality, they wouldn’t have the same large community that I can work with...

The people are open. In a nutshell, that's the major difference between Splunk and the other guys.”

– Golan Ben-Oni, CSO/SVP Network Architecture, IDT

Splunk Answers

<https://answers.splunk.com>



- Q&A forum for the Splunk community
- Find solutions before filing a support case
- Contributors are Splunkers, partners, and customers
- Learn from other users' hands-on experience



Photo of SplunkTrust Community MVPs 2015-2016

Splunk Answers

<https://answers.splunk.com>

- 75-85% of content contributed by non-employees
- Time to Answer metrics:
 - 25% of questions answered within 1 hour
 - 50% within 12 hours
- Currently 62,000+ Questions and 75,000+ Answers
- 2000+ followers on Twitter @splunkanswers

Splunk Answers

How do I increase my chances of getting my questions answered?

- Question title should clearly state your issue
- In the question content, provide all relevant details of your environment and issue:
 - Splunk products and versions
 - Exact Splunk product names and terminology
 - Type of Splunk deployment
 - Types of forwarders

Splunk Answers

How do I increase my chances of getting my questions answered?

- Provide all details about your environment and issue:
 - Error messages and in which logs
 - Anonymized sample data
 - Attempted searches or regular expressions
 - Configuration file names
 - Prior research you have done
 - Expected results

Help with Splunk Answers

The screenshot shows the Splunk Answers interface. At the top, there is a navigation bar with links for Documentation, Splunkbase, Answers, Wiki, Blogs, and Developers. A user profile for 'ppablo_splunk' is visible with 5,494 points, 4 questions, 10 answers, and 8 badges. A search bar is present with the text 'Search Splunk Answers'. A green arrow points to the search bar with the text 'Search first!'. Below the navigation bar, there is a banner for a competition: 'Get ready to compete for one of 3 .conf passes between July 15th and August 15th!'. The main content area is titled 'All Questions' and features a filter menu with options: hottest, newest (selected), most voted, unanswered, and double points. A green arrow points to the 'newest' filter with the text 'Question title'. Below the filter menu, there are three question cards. The first card is titled 'How to set the x-axis limits of a line chart?' and has tags: timechart, timerange, limit, x-axis, linechart. A green arrow points to the 'x-axis' tag with the text 'Question tags'. The second card is titled 'Why is our universal forwarder not forwarding all logs on DHCP servers?' and has tags: universal-forwarder, monitor, windows-event-logs, dhcp. The third card is titled 'How to add a column of averages to a timechart?' and has tags: splunk-enterprise, timechart, average, column. On the right side of the page, there is a summary box showing '61,523 Questions' and '74,104 Answers', along with buttons for 'Follow us on Twitter' and 'Follow our RSS Feed'. Below this is a 'Most Used Tags' section with a grid of tags including splunk-enterprise, search, dashboard, regex, field-extraction, index, forwarder, splunk, universal-forwarder, indexing, windows, props.conf, time, chart, stats, timechart, lookup, and alert. Two red circles highlight the 'ask a question' buttons in the top navigation bar and in the main content area.

Splunk User Groups

<https://usergroups.splunk.com>


- Learn and network with Splunk users in your local region
- 215 members joined between 2010 – 2014
- 1000+ new members since 2014
- 60+ groups worldwide
- Users meet monthly, every other month, or quarterly
- Each group decides on own meeting topics and structure

Help with Splunk User Groups


splunk>usergroups FIND MORE GROUPS Splunk.com Support & Services My Account

Find a Splunk User Group

Connect with like-minded people who are passionate about Splunk technology



Join a user group near [Washington, DC](#)



[Washington DC Splunk User Group](#) 89 Members

📍 Vienna, VA

DC-Area Splunk enthusiasts, this is your spot!


[Learn More](#)

Help with Splunk User Groups


splunk > usergroups FIND MORE GROUPS Splunk.com Support & Services My Account

Find a Splunk User Group

Connect with like-minded people who are passionate about Splunk technology



Join a user group near [London, United Kingdom](#)



[Splunk User Group London](#) 102 Members

📍 London, United Kingdom

Splunk, we're all in

[Learn More](#)

Help with Splunk User Groups

The screenshot shows the Splunk User Groups website interface. At the top, there is a navigation bar with the Splunk logo and the text 'splunk>usergroups'. To the right of the logo is a search bar labeled 'FIND MORE GROUPS' with the placeholder text 'Enter city or postal code'. Further right are links for 'Splunk.com', 'Support & Services', and 'My Account'. Below the navigation bar, the breadcrumb trail reads 'User Groups > Splunk User Group London'. The main heading is 'Splunk User Group London' in a large, bold font. Below the heading is the tagline 'Splunk, we're all in'. To the right of the heading, it says '102 Members' and a green button labeled 'Join This Group' is circled in red. Below the main content area, there are sections for 'Upcoming Events (0)' and 'Past Events (4)'. The 'Past Events' section features a map of London with a red pin at 3 Sheldon Square, and a card for an event titled 'An evening with Splunk CTO, Snehal Antani' which took place on June 13, 2016, at 10:15 AM. The card also indicates that 12 people attended and provides a brief description of the event.

splunk>usergroups FIND MORE GROUPS Enter city or postal code Splunk.com Support & Services My Account

User Groups > Splunk User Group London

Splunk User Group London


Splunk, we're all in

102 Members

[Join This Group](#)

Upcoming Events (0)

Past Events (4)

 **An evening with Splunk CTO, Snehal Antani** 12 Attended

June 13, 2016 10:15 AM

Splunk, 3 Sheldon Square, London, United Kingdom

On Monday June 13th at 6:15pm, Splunk CTO, Snehal Antani will be joining the London community for a very special evening. This is an amazing opportunity to get...

Slack & Internet Relay Chat (IRC)

- Chat with fellow customers, partners, and Splunkers worldwide
- Opportunity to network outside of in-person events
- Ask for help with issues and learn from other users in real time
- Experience Splunk community culture daily!

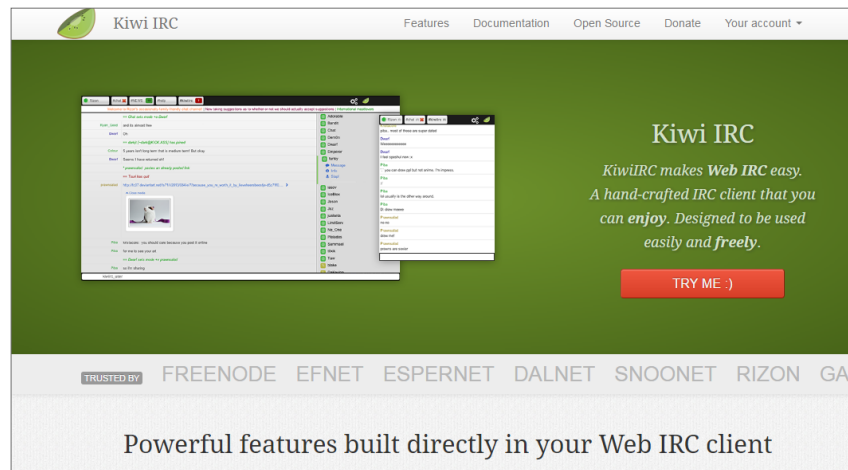


Join us on Slack!

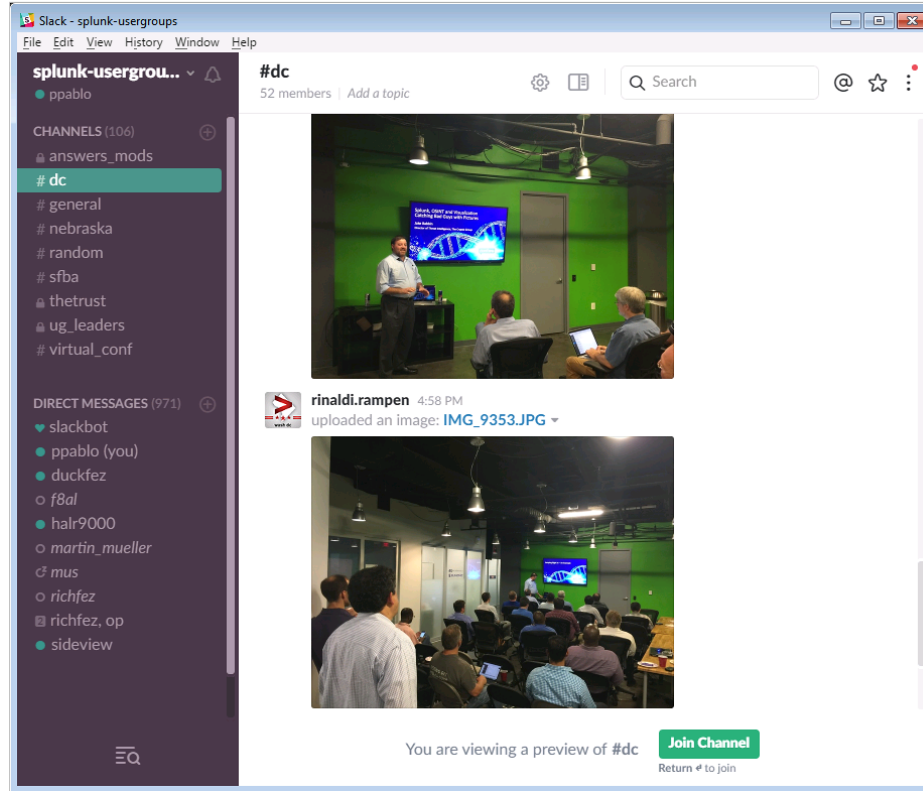
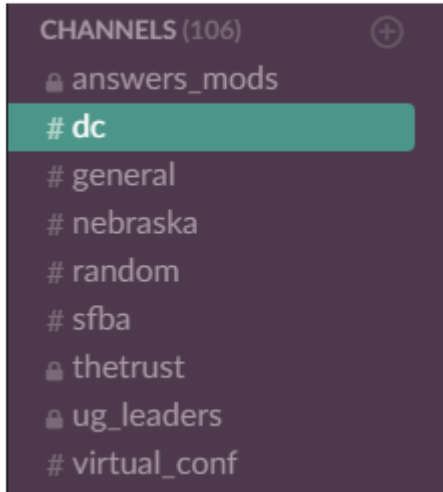
- Submit a request through <http://splunk402.com/chat>
- Request will be reviewed for approval by someone on the Community team
- Access the web or free Slack client from <http://slack.com>

Join us on IRC!

- Download an IRC client or use a web client like <https://kiwiirc.com>
- Network: Efnet
- Server: Find one here!
<http://www.efnet.org/?module=servers>
- Channel: #splunk



Help with Slack



Slack #general channel

CHANNELS (106)

- answers_mods
- # general
- # nebraska
- # random
- # sfba
- thetrust
- ug_leaders
- ug_leaders
- # virtual_conf

DIRECT MESSAGES (977)

- slackbot
- ppablo (you)
- duckfez
 - f8al
 - halr9000
- martin_mueller
 - mus
- richfez
 - richfez, op
 - sideview

Slack - splunk-usergroups

#general
974 members | 6.4.2 smells like bulgogi | all topics... Search

mattymo 8:28 AM
this works but feels hackish

```
index=n00blab sourcetype=syslog | extract pairdelim=")", kvdelim=","
```

yah that doest work fully

automine 8:32 AM
what would you like an example field and value to be?


```
[my_kv_maker]  
REGEX = \s(<_KEY_1>[a-z]+)='(<_VAL_1>[^\s]+)'
```

(edited)

```
\s(<_KEY_1>[a-z]+)='[^']*(<_VAL_1>[^\s]+)'
```

that actually looks a little nicer

<https://regex101.com/r/IW5hB2/1>

 **Regex101 - online regex editor and debugger**
Regex101 allows you to create, debug, test and have your expressions explained for PHP, PCRE, JavaScript and Python. The website also features a community where you can share useful expressions.

gonna have to adjust that first capture to decide on what the field names should be

Slack #office_hours channel

CHANNELS (106)

- answers_mods
- # general
- # nebraska
- # office_hours**
- # random
- # sfba
- thetrust
- ug_leaders
- virtual_conf

Slack - splunk-usergroups

File Edit View History Window Help

splunk-usergrou... | ppablo

CHANNELS (106)

- answers_mods
- # general
- # nebraska
- # office_hours**
- # random
- # sfba
- thetrust
- ug_leaders
- virtual_conf

DIRECT MESSAGES (977)

- slackbot
- ppablo (you)
- duckfez
- f8al
- halr9000
- martin_mueller
- mus
- richfez
- richfez, op
- sideview

#office_hours
152 members | next office hours: Friday, August 5...

Search

jeffland 11:30 PM
@ghendrey @cpride sorry I couldn't be there for any feedback, but your effort to answer nevertheless is much appreciated. For the moment, I'm happy to hear that the lookup is not naive, and log(n) gives me a better feeling about adding more and more shapes. I must admit I hadn't fully analyzed the situation before asking this question (e.g. it could well be that I looked at the first-time runtime of a search as "this is how long it takes with 10 shapes, this is how long with 20, whoa" and so on), asking was based more on a feeling that I maybe I should know more things before doing geoshapes in serious numbers. I would have followed up with a question about how to ideally create shapes (e.g. more shapes is worse than more points per shape or stuff like that), but now I'll just go ahead until I run into real problems. Thanks a ton!

July 19th

teddybfez 9:40 AM
So next one of these is 5 August ?

martin_mueller 10:01 AM
that'd be the regular schedule

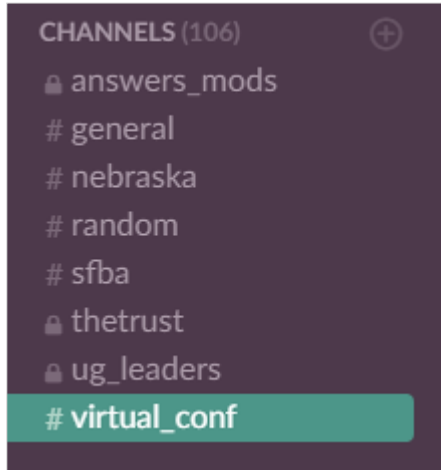
rachel 5:43 PM
oh yeah, although i will be at defcon, i think

rachel 5:44 PM
set the channel topic: next office hours: Friday, August 5th at 11am Pacific.

You are viewing a preview of #office_hours [Join Channel](#)
Return # to join

Slack #virtual_conf channel

www.meetup.com/splunk-meetups



- Channel for SplunkTrust Virtual .conf Series - what is that?
- Monthly series of live talks by SplunkTrust members with Q&A
- Anyone worldwide can watch, listen, and learn!
- Stay updated on upcoming sessions through the Splunk Meetup page

Other Resources

- Splunk Community Portal: www.splunk.com/en_us/community.html
- Splunk Education & Training: www.splunk.com/view/SP-CAAAAH9
- Splunk Blogs: <http://blogs.splunk.com>
- Sizing Tool: <https://splunk-sizing.appspot.com>
- Search Examples:
 - www.bbosearch.com
 - www.gosplunk.com

Questions?



THANK YOU

Visit us at the booths!

- Patrick at Splunk Answers
- Laura at Documentation

.conf2016