

.conf2013

**YOUR DATA
NO LIMITS**

**Search Language -
Beginner**

Mitch Fleischman

Senior Instructor

#splunkconf

splunk>

Legal Notices

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>, Splunk Storm, Listen to Your Data, SPL and The Engine for Machine Data 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.

©2013 Splunk Inc. All rights reserved.

About Me



Mitch Fleischman
Senior Instructor

www.splunk.com

650.605.7549 (Mobile)
mfleischman@splunk.com

- Splunker since August 2012
- Background: SFA, Relational Database, Portals, BPM, Platform Management, Big Data

Agenda

- What is Splunk?
- Getting Started
- Basic Searching
- Using Fields
- Saving and Sharing Reports
- Next Steps

.conf2013

**YOUR DATA
NO LIMITS**

What is Splunk?

splunk>

Spelunking:

to explore
underground caves

Splunking:

to explore machine data

What is Machine Data?

- Log files
- Custom applications
- Web servers
- User clickstreams
- Social platforms
- Servers/hypervisors/virtual machines
- Configurations
- Telecom devices
- Storage devices
- Network devices
- Security devices, firewalls, IDS
- Databases
- Web services
- System metrics
- GPS
- DNS, DHCP
- AAA logs
- Proxy servers
- Errors
- Scripts
- Sensors

Machine Data Contains Critical Insights

Sources

Order Processing

Middleware Error

Care IVR

Twitter

```
ORDER,2012-05-21T14:04:12.484, Customer ID 10098213, Order ID 569281734, 67.17.10.12,43CD1A7B8322, Product ID SA-2100
```

```
May 21 14:04:12.996 wl-01.acme.com Order Order ID 569281734 failed for customer Customer ID 10098213.  
Exception follows: weblogic.jdbc.extensions.ConnectionDeadSQLException:  
weblogic.common.resourcepool.ResourceDeadException: Order ID Could not create pool Customer ID The  
DBMS driver exception was: [BEA][Oracle JDBC Driver]Error establishing socket to host and port:  
ACMEDB-01:1521. Reason: Connection refused
```

```
05/21 16:33:11.238 [CONNEVENT] Ext 1207130 (0192033): Event 20111, CTI Num:ServID:Type  
Time Waiting On Hold 98#1, DNIS 5555685981, SerID 40489a07-7f6e-4251-801a-  
13ae51a6d092, trunk 1451.16
```

```
05/21 16:33:11.242 [SCREENPOPEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092  
Customer ID CUSTID 10098213
```

```
05/21 16:37:49.732 [DISCEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092
```

```
{actor:{displayName:"Go Boys!!",followersCount:1366,friendsCount:789,link:  
"http://dallascowboys.com/",location:{dis Twitter ID "Dallas, TX",objectType Customer's Tweet  
objectType:"person",preferredUsername:"B0ysF@n80",statusesCount:6072},body:"Just bought  
this POS device from @ACME. Doesn't work! Called, gave up on waiting for them to answer! RT if  
you hate @ACME!!",objectType:"activity",postedTime:"2012-05-21T16:39:40.647-0600"}
```

Company's Twitter ID

What Does Splunk Really Do?

It turns this



Into this

```
####<Sep 24, 2009 2:52:38 PM PDT> <Warning> <E
'224' for queue: 'weblogic.kernel.Default (sel
<BEA-010065> <MessageDrivenBean threw an Excep
javax.ejb.EJBException: nested exception is:
primary key '10011968' was not found by 'findE
javax.ejb.EJBException: nested exception is:
primary key '10011968' was not found by 'findE
at
com.sun.j2ee.blueprints.opc.customerrelations.
alMDB.java:140)
at weblogic.ejb.container.internal.MDLis
```

```
[Thu Sep 24 14:57:33 2009] [error] [client 10.
enter_order_information.screen at backend host
'CONNECTION_REFUSED [os error=0, line 1739 of
127.0.0.1:7001', referer: http://10.2.1.223/pe
```



.conf2013

**YOUR DATA
NO LIMITS**

Getting Started

splunk>

Splunk Web

- Splunk's dynamic and interactive browser-based interface
- The primary interface for investigating problems, reporting on results, and managing Splunk deployments
- Note: Splunk with a free license does not have access controls, so you will not be prompted for login information



Search & Reporting App – Summary View

The screenshot shows the Splunk Search & Reporting App interface. The top navigation bar includes the Splunk logo, the current app name 'App: Search & Reporting', and user options like 'Administrator', 'Messages', 'Settings', 'Activity', and 'Help'. Below this is a secondary navigation bar with tabs for 'Search', 'Pivot', 'Reports', 'Alerts', and 'Dashboards'. The main content area features a search bar with the placeholder text 'enter search here...', a time range picker set to 'Last 24 hours', and a search button. Below the search bar are two panels: 'How to Search' with links to 'Documentation' and 'Tutorial', and 'What to Search' displaying global statistics such as '5,129,664 Events INDEXED', '2 years ago EARLIEST EVENT', and 'a few seconds ago LATEST EVENT'. A 'Data Summary' button is also present in the 'What to Search' panel.

Callouts in the image identify the following elements:

- current app
- app navigation
- current view
- search bar
- time range picker
- start search
- resources
- global stats

Events

- Searches return events
- In Splunk, an event is a single piece of data, such as a record in a log file or other data input
- Splunk breaks up input data into individual events and gives each a timestamp, host, source, and sourcetype

Events (continued)

```
91.205.40.22 - - [16/Sep/2013:20:19:09] "GET /cart.do?action=view&itemId=EST-26&productId=BS-AG-G09&JSESSIONID=SD0SL4FF8ADFF4956 HTTP/1.1" 200 883 "http://www.buttercupgames.com/oldlink?itemId=EST-26" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3" 569
91.205.40.22 - - [16/Sep/2013:20:19:14] "GET /category.screen?categoryId=STRATEGY&JSESSIONID=SD0SL4FF8ADFF4956 HTTP/1.1" 200 2529 "http://www.buttercupgames.com/cart.do?action=view&itemId=EST-27&productId=DB-SG-G01" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3" 292
91.205.40.22 - - [16/Sep/2013:20:19:28] "GET /product.screen?productId=SF-BVS-01&JSESSIONID=SD0SL4FF8ADFF4956 HTTP/1.1" 408 2529 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3" 259
```

i	Time	Event
▶	9/16/13 8:19:28.000 PM	91.205.40.22 - - [16/Sep/2013:20:19:28] "GET /product.screen?productId=SF-BVS-01&JSESSIONID=SD0SL4FF8ADFF4956 HTTP/1.1" 408 2529 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3" 259 host = www2 source = /opt/log/www2/access.log sourcetype = access_combined
▶	9/16/13 8:19:14.000 PM	91.205.40.22 - - [16/Sep/2013:20:19:14] "GET /category.screen?categoryId=STRATEGY&JSESSIONID=SD0SL4FF8ADFF4956 HTTP/1.1" 200 2529 "http://www.buttercupgames.com/cart.do?action=view&itemId=EST-27&productId=DB-SG-G01" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3" 292 host = www2 source = /opt/log/www2/access.log sourcetype = access_combined
▶	9/16/13 8:19:09.000 PM	91.205.40.22 - - [16/Sep/2013:20:19:09] "GET /cart.do?action=view&itemId=EST-26&productId=BS-AG-G09&JSESSIONID=SD0SL4FF8ADFF4956 HTTP/1.1" 200 883 "http://www.buttercupgames.com/oldlink?itemId=EST-26" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3" 569 host = www2 source = /opt/log/www2/access.log sourcetype = access_combined

Everything is Searchable

- * wildcard supported
- Search terms are case insensitive
- Booleans AND, OR, NOT
 - Must be uppercase
 - AND is implied between terms
- Use () for complex searches
- Use quotation marks for phrases

fail*

Last 24 hours



fail* nfs

Last 24 hours



error OR 404

Last 24 hours



error OR failed OR (sourcetype=access* (500 OR 503))

Last 24 hours



login failure"

Last 24 hours



.conf2013

**YOUR DATA
NO LIMITS**

Basic Searching

splunk>



Search

- Matching results are displayed in reverse chronological order (newest first)
- Matching search terms are highlighted

The screenshot shows the Splunk search interface. At the top, the search bar contains the query `"failed password"`. Below the search bar, it indicates 20,380 events were found between 7/24/13 12:00:00.000 AM and 8/23/13 5:18:32.000 AM. The interface includes a timeline visualization and a table of search results. The search term "failed password" is highlighted in yellow in the event descriptions. A red arrow points from the search bar to the highlighted text in the results.

Time	Event
8/23/13 5:18:27.000 AM	Fri Aug 23 2013 05:18:27 www2 sshd[1342]: Failed password for invalid user info from 209.160.24.63 port 1717 ssh2 host = www2 source = /opt/log/www2/secure.log sourcetype = linux_secure
8/23/13 5:17:01.000 AM	Fri Aug 23 2013 05:17:01 www1 sshd[5371]: Failed password for invalid user limbo from 123.30.108.208 port 4318 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
8/23/13 5:16:32.000 AM	Fri Aug 23 2013 05:16:32 www1 sshd[3703]: Failed password for invalid user db2fenc1 from 123.30.108.208 port 4247 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
8/23/13 5:16:25.000 AM	Fri Aug 23 2013 05:16:25 www1 sshd[4139]: Failed password for invalid user db2inst1 from 123.30.108.208 port 4477 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
8/23/13 5:16:07.000 AM	Fri Aug 23 2013 05:16:07 www1 sshd[1176]: Failed password for bashful from 123.30.108.208 port 1386 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure

Search Results

The screenshot shows the Splunk search interface. At the top, the search bar contains the query "failed password" and the time range is set to "Last 30 days". Below the search bar, it indicates "20,380 events (7/24/13 12:00:00.000 AM to 8/23/13 5:18:32.000 AM)". The interface includes tabs for "Events (20,380)", "Statistics", and "Visualization". A timeline visualization is shown at the top, with a blue box labeled "timeline" and arrows pointing to the timeline bars. Below the timeline is a table of search results. The table has columns for "Time" and "Event". The first row shows a failed password attempt on 8/23/13 at 5:18:27 AM from host www2. The second row shows a failed password attempt on 8/23/13 at 5:17:01 AM from host www1. The third row shows a failed password attempt on 8/23/13 at 5:16:32 AM from host www1. The fourth row shows a failed password attempt on 8/23/13 at 5:16:25 AM from host www1. The fifth row shows a failed password attempt on 8/23/13 at 5:16:07 AM from host www1. A blue box labeled "Fields sidebar" is on the left, showing selected fields (host, source, sourcetype) and interesting fields (date_hour, date_mday, date_minute, date_second, date_wday, date_year, date_zone). A blue box labeled "timestamp" points to the time column. A blue box labeled "selected fields" points to the host, source, and sourcetype fields in the event data. A blue box labeled "event data" points to the event column.

New Search

"failed password" Last 30 days

20,380 events (7/24/13 12:00:00.000 AM to 8/23/13 5:18:32.000 AM)

Events (20,380) Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect timeline 1 day per column

List Format 50 Per Page Prev 1 2 3 4 5 6 7 8 9 ... Next

Time	Event
8/23/13 5:18:27.000 AM	Fri Aug 23 2013 05:18:27 www2 sshd[1342]: Failed password for invalid user info from 209.160.24.63 port 1717 ssh2 host = www2 source = /opt/log/www2/secure.log sourcetype = linux_secure
8/23/13 5:17:01.000 AM	Fri Aug 23 2013 05:17:01 www1 sshd[5371]: Failed password for invalid user limbo from 123.30.108.208 port 4318 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
8/23/13 5:16:32.000 AM	Fri Aug 23 2013 05:16:32 www1 sshd[3703]: Failed password for invalid user .108.208 port 4247 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
8/23/13 5:16:25.000 AM	Fri Aug 23 2013 05:16:25 www1 sshd[4139]: Failed password for invalid user db2inst1 from 123.30.108.208 port 4477 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
8/23/13 5:16:07.000 AM	Fri Aug 23 2013 05:16:07 www1 sshd[1176]: Failed password for bashful from 123.30.108.208 port 1386 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure

Fields sidebar

Selected Fields: host, source, sourcetype

Interesting Fields: date_hour, date_mday, date_minute, date_second, date_wday, date_year, date_zone

timestamp

selected fields

event data

Navigating Search Results

- Mouse over search results
 - Keywords and parts of keywords are highlighted
- To add a term to the search, click it
 - AND is implied
 - To remove, click again
- To exclude a term from a search, alt+click it
 - Adds NOT [term] to search

The screenshot shows the Splunk search interface. At the top, the search bar contains the query "failed password" and the time range is set to "Last 30 days". Below the search bar, it indicates "20,380 events (7/24/13 12:00:00.000 AM to 8/23/13 5:18:32.000 AM)". The interface includes tabs for "Events (20,380)", "Statistics", and "Visualization". A timeline visualization is shown above the event list, with a zoom level of "1 day per column". The event list is displayed in a table format with columns for "Time" and "Event". The "Event" column contains log entries with the phrase "Failed password" highlighted in yellow. A mouse cursor is pointing at the first highlighted entry.

i	Time	Event
▶	8/23/13 5:18:27.000 AM	Fri Aug 23 2013 05:18:27 www2 sshd[1342]: Failed password for invalid user info from 209.160.24.63 port 1717 ssh2 host = www2 source = /opt/log/www2/secure.log sourcetype = linux_secure
▶	8/23/13 5:17:01.000 AM	Fri Aug 23 2013 05:17:01 www1 sshd[5371]: Failed password for invalid user limbo from 123.30.108.208 port 4318 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
▶	8/23/13 5:16:32.000 AM	Fri Aug 23 2013 05:16:32 www1 sshd[3703]: Failed password for invalid user db2fenc1 from 123.30.108.208 port 4247 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
▶	8/23/13 5:16:25.000 AM	Fri Aug 23 2013 05:16:25 www1 sshd[4139]: Failed password for invalid user db2inst1 from 123.30.108.208 port 4477 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
▶	8/23/13 5:16:07.000 AM	Fri Aug 23 2013 05:16:07 www1 sshd[1176]: Failed password for bashful from 123.30.108.208 port 1386 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure

Selecting Search Time Range

- By default, search is “all time”
 - Can consume a great deal of resources
 - Ideal for looking at long term patterns, such as, advanced persistent threat
- To narrow your search, use the time range picker

The screenshot shows the Splunk search interface with a search query "failed password" and a time range picker menu open. The menu is divided into several sections: Presets, Relative, Real-time, Date Range, Date & Time Range, and Advanced. The Presets section is further divided into Real-time, Relative, and Other. The search results show two events related to failed password attempts.

Search Query: "failed password"

Time Range: Last 30 days

Results: 20,621 events (7/24/13 12:00:00.000 AM to 8/23/13 12:00:00.000 AM)

Fields: host 4, source 4, sourcetype 1

Interesting Fields: date_hour 24, date_mday 31, date_minute 60, date_month 2, date_second 60, date_wday 7, date_year 1

Presets:

- Real-time
 - 30 second window
 - 1 minute window
 - 5 minute window
 - 30 minute window
 - 1 hour window
 - All time (real-time)
- Relative
 - Today
 - Week to date
 - Business week to date
 - Month to date
 - Year to date
 - Yesterday
 - Previous week
 - Previous business week
 - Previous month
 - Previous year
- Other
 - Last 15 minutes
 - Last 60 minutes
 - Last 4 hours
 - Last 24 hours
 - Last 7 days
 - Last 30 days
 - All time

Search Results:

- 8/23/13 Fri Aug 23 2013 06:30:34 www3 sshd[4324]: Failed password for daemon 6:30:34.000 AM from 49.212.64.138 port 3821 ssh2
- 8/23/13 Fri Aug 23 2013 06:30:28 www3 sshd[3427]: Failed password for invalid user dmuser from 49.212.64.138 port 3517 ssh2

.conf2013

**YOUR DATA
NO LIMITS**

Using Fields

splunk>

What are Fields?

- Fields are searchable key/value pairs in your event data
 - Example: `host=www1, status=503`
- All fields have names and can be searched with those names
 - Example: Separating an http status code of 404 from Atlanta's area code
- There are 2 types of fields:

default fields

```
source="/opt/log/www3/access.log" sourcetype="access_combined" host="www3"
```

Last 60 minutes ▾



data-specific fields

```
action="purchase" status="503"
```

Last 60 minutes ▾



Identifying Data-specific Fields

- Data-specific field values come from your data
- Sometimes indicated by obvious key=value pairs:

i	Time	Event
▶	9/16/13 8:41:46.000 PM	212.235.92.150 - - [16/Sep/2013:20:41:46] "POST /cart.do?action=purchase&itemId=EST- "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-12&categoryId=ARC 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .N host = www1 source = /opt/log/www1/access.log sourcetype = access_combined
▶	9/16/13 8:41:43.000 PM	212.235.92.150 - - [16/Sep/2013:20:41:43] "POST /cart.do?action=addtocart&itemId=EST 200 2610 "http://www.buttercupgames.com/product.screen?productId=FI-AG-G08" "Mozilla Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 623 host = www1 source = /opt/log/www1/access.log sourcetype = access_combined
▶	9/16/13 8:41:41.000 PM	212.235.92.150 - - [16/Sep/2013:20:41:41] "GET /product.screen?productId=FI-AG-G08&J "http://www.buttercupgames.com/category.screen?categoryId=ARCADE" "Mozilla/5.0 (Winc Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 118 host = www1 source = /opt/log/www1/access.log sourcetype = access_combined

- Sometimes not:

Selected Fields
a host 3
a source 3
a sourcetype 1
Interesting Fields
a action 5
bytes 100+
a categoryId 8
a clientip 29
date hour 5

i	Time	Event
▶	9/16/13 8:41:46.000 PM	212.235.92.150 - - [16/Sep/2013:20:41:46] "POST /cart.do?action=purchase&itemId=EST- "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-12&categoryId=ARC 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .N host = www1 source = /opt/log/www1/access.log sourcetype = access_combined
▶	9/16/13 8:41:43.000 PM	212.235.92.150 - - [16/Sep/2013:20:41:43] "POST /cart.do?action=addtocart&itemId=EST 200 2610 "http://www.buttercupgames.com/product.screen?productId=FI-AG-G08" "Mozilla Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 623 host = www1 source = /opt/log/www1/access.log sourcetype = access_combined
▶	9/16/13 8:41:41.000 PM	212.235.92.150 - - [16/Sep/2013:20:41:41] "GET /product.screen?productId=FI-AG-G08&J "http://www.buttercupgames.com/category.screen?categoryId=ARCADE" "Mozilla/5.0 (Winc Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 118 host = www1 source = /opt/log/www1/access.log sourcetype = access_combined

- For more information, please see:

<http://docs.splunk.com/Documentation/Splunk/latest/Data/Listofpretrainedsourcetypes>

Fields Sidebar

- For the current search, shows
 - Selected fields
 - Interesting fields
 - Link to view all fields
- Fields returned are those Splunk recognized from your search results
- Interesting fields are fields that have values in at least 50% of events

The screenshot displays a Splunk search interface for the query "failed password". It shows a timeline visualization with a bar chart and a table of search results. The fields sidebar is visible on the left, listing fields categorized into "Selected Fields" and "Interesting Fields".

Selected Fields:

- host 4
- source 4
- sourcetype 2

Interesting Fields:

- app 1
- date_hour 1
- date_mday 1
- date_minute 28
- date_month 1
- date_second 45
- date_wday 1
- date_year 1

Callouts in the image:

- "View all fields" points to the "All Fields" link in the sidebar.
- "Selected fields" points to the "Selected Fields" section.
- "Interesting fields" points to the "Interesting Fields" section.
- "(#) indicates number of unique values" points to the counts in the "Interesting Fields" list.

Selected Fields

- Selected fields and their values display under every event when a value is available
- By default, host, source, and sourcetype are selected fields
- Fields sidebar is interactive

The screenshot shows a Splunk search interface for the query "failed password". It displays 130 of 162 events. A timeline visualization shows event density over a 31-minute period, with a callout for "2 events at 3:23 AM Tuesday, September 10, 2013". Below the timeline is a list of events with selected fields (host, source, sourcetype) displayed under each event.

Time	Event
9/10/13 3:42:36.000 AM	Tue Sep 10 2013 03:42:36 www1 sshd[3691]: F ssh2 host = www1 source = /opt/log/www1/secure.log sou
9/10/13 3:42:16.000 AM	Tue Sep 10 2013 03:42:16 www1 sshd[3228]: F ssh2 host = www1 source = /opt/log/www1/secure.log sou
9/10/13 3:42:15.000 AM	Tue Sep 10 2013 03:42:15 www1 sshd[1234]: F ssh2 host = www1 source = /opt/log/www1/secure.log sou
9/10/13 3:42:14.000 AM	Tue Sep 10 2013 03:42:14 www1 sshd[2872]: F ssh2 host = www1 source = /opt/log/www1/secure.log sou
9/10/13 3:42:14.000 AM	... 77 lines omitted ... root 10580 3 0.0 20-11:36:49 python /opt/setup root 11045 0 0.0 20-11:23:11 python /opt/setup

Adding Fields to Selected Fields

- Alt-click any field to see a window of options for that field

- Click Yes to the right of Selected
 - The field will appear in the selected fields list and in the search results

The screenshot shows the Splunk interface with a search results view. On the left, the 'Selected Fields' list includes 'app 1', 'host 5', 'source 5', and 'sourcetype 2'. A modal window titled 'app' is open, displaying '1 Value, 63.415% of events' and a 'Selected' status with 'Yes' and 'No' buttons. The 'Yes' button is highlighted with a red box. Below the modal, the search results show the 'app' field added to the event data, with 'app = sshd' highlighted in a red box. The search results also show the 'Failed password' message for jira from 211.25.254.234 port 3182 ssh2.

Values	Count	%
sshd	104	100%

```
17-07:50:47 python /opt/setup/using/data_scripts/failed_pas
Show all 100 lines
host = splunk1 | source = ps | sourcetype = ps
9/10/13 5:43:12.000 AM Tue Sep 10 2013 05:43:12 www1 sshd[1831]: Failed password for jira from 211.25.254.234 port 3182 ssh2
app = sshd | host = www1 | source = /opt/log/www1/secure.log | sourcetype = linux_secure
9/10/13 5:43:00.000 AM Tue Sep 10 2013 05:43:00 www1 sshd[2798]: Failed password for invalid user from 211.25.254.234 port 1106 ssh2
app = sshd | host = www1 | source = /opt/log/www1/secure.log | sourcetype = linux_secure
9/10/13 5:42:54.000 AM Tue Sep 10 2013 05:42:54 www1 sshd[1165]: Failed password for invalid user from 211.25.254.234 port 1106 ssh2
app = sshd | host = www1 | source = /opt/log/www1/secure.log | sourcetype = linux_secure
```

More Ways to Use the Fields Sidebar

The image shows a screenshot of the Splunk interface. On the left is the 'Fields Sidebar' with 'Selected Fields' (app 1, host 5, source 5, sourcetype 2) and 'Interesting Fields' (date_hour 2, date_mday 1, date_minute 26, date_month 1, date_second 46, date_wday 1, date_year 1, date_zone 1, dest 4, eventtype 6). On the right is the 'eventtype' dialog box showing '6 Values, 100% of events' and a 'Selected' checkbox. The dialog has three tabs: 'Reports', 'Top values by time', and 'Rare values'. The 'Reports' tab is active and shows a table of values with their counts and percentages. A red box highlights the 'Reports' tab, and a blue callout box points to it with the text 'Create reports (charts)'. A blue callout box points to the 'nix_errors' row with the text 'Narrow the search to show only results that contain this field'. A blue callout box points to the 'nix_udev' row with the text 'Click a value to add to a search'. Another blue callout box points to the 'ps' row with the text 'ALT + click a value to remove from a search'.

Values		%	
nix_errors		100%	
failed_login		60.265%	
nix-all-logs	91	60.265%	
sshd_authentication	91	60.265%	
nix_udev	60	39.735%	
ps	60	39.735%	

Selected Fields

- @ app 1
- @ host 5
- @ source 5
- @ sourcetype 2

Interesting Fields

- # date_hour 2
- # date_mday 1
- # date_minute 26
- @ date_month 1
- # date_second 46
- @ date_wday 1
- # date_year 1
- @ date_zone 1
- @ dest 4
- @ eventtype 6

eventtype

6 Values, 100% of events Selected Yes No

Reports Top values Top values by time Rare values

Events with this field

Narrow the search to show only results that contain this field

Create reports (charts)

Click a value to add to a search

ALT + click a value to remove from a search

Using Fields in Searches

- Efficient way to pinpoint searches and refine results

```
141.146.8.66
```

```
src_ip=141.146.8.66
```

```
status=404
```

```
area_code=404
```

- Use wildcards

```
src_ip="10.5.6.*"
```

- Field names ARE case sensitive, field values are NOT
 - Example: Splunk extracts a field in linux_secure data named user
 - These two searches return results: This one does not:

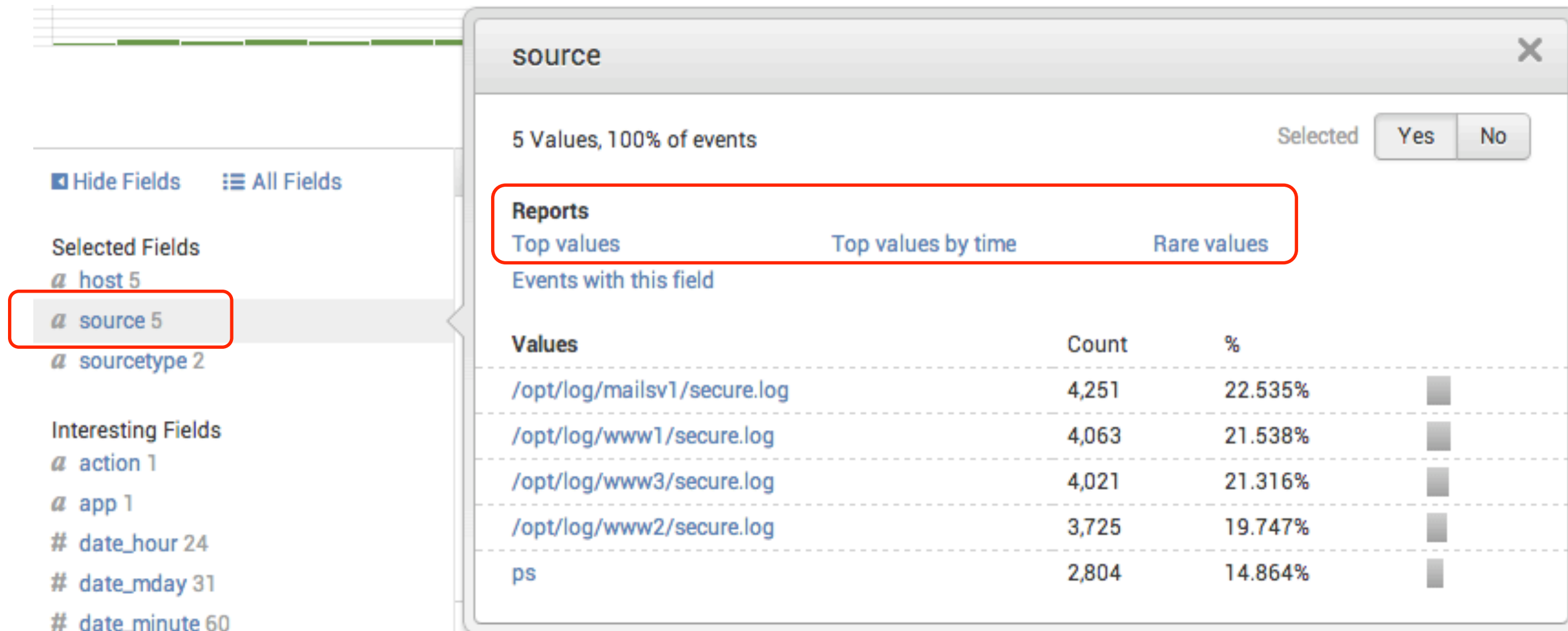
```
Search
user=root
20 matching events
```

```
Search
user=ROOT
20 matching events
```

```
Search
USER=root
0 matching events
```

Create Reports from Fields Sidebar

- From the fields sidebar, select a field and a report definition (Top values, Top values by time, or Rare values)



The screenshot shows the Splunk interface. On the left is the 'Fields Sidebar' with sections for 'Selected Fields' (host 5, source 5, sourcetype 2) and 'Interesting Fields' (action 1, app 1, date_hour 24, date_mday 31, date_minute 60). The 'source' field is highlighted in red. On the right is a 'source' dialog box. It shows '5 Values, 100% of events' and 'Selected' buttons for 'Yes' and 'No'. A red box highlights the 'Reports' section with options: 'Top values', 'Top values by time', and 'Rare values'. Below this is a table of values for the 'source' field.

Values	Count	%
/opt/log/mailsv1/secure.log	4,251	22.535%
/opt/log/www1/secure.log	4,063	21.538%
/opt/log/www3/secure.log	4,021	21.316%
/opt/log/www2/secure.log	3,725	19.747%
ps	2,804	14.864%

Create a 'Top Values' Report

failed password | top limit=20 source

All time

19,031 events (before 9/12/13 8:19:07.000 PM)

Job Complete

Events Statistics (5) Visualization

Bar Format

source	count
/opt/log/mailsv1/secure.log	4,295
/opt/log/www1/secure.log	~3,900
/opt/log/www3/secure.log	~3,800
/opt/log/www2/secure.log	~3,500
ps	~2,700

source

5 Values, 100% of events

Reports

Top values

Events with this field

Top values by time

Rare values

.conf2013

**YOUR DATA
NO LIMITS**

Saving and Sharing Reports

splunk>

Saving Reports

- Save search criteria and time range, but not results, to re-run at any point in the future
- Click the Save As button, select Report, enter a title

The screenshot shows the Splunk search interface. At the top, there is a search bar with the query `failed password | timechart avg(linecount)`. Below the search bar, it indicates `19,203 events (before 9/12/13 8:50:43.000 PM)`. The interface includes tabs for `Events (19,203)`, `Statistics (32)`, and `Visualization`. A `Save As` dropdown menu is open, showing options: `Report`, `Dashboard Panel`, `Alert`, and `Event Type`. A red box highlights this menu. Below the main interface, a `Save As Report` dialog box is open. It has a `Title` field containing `Bad Logins`, a `Description` field with `optional`, a `Visualization` section with `Pie` and `None` options, and a `Time Range Picker` section with `Yes` and `No` options. A red box highlights the `Title` field. The dialog box has `Cancel` and `Save` buttons at the bottom.

Running Saved Reports

splunk> App: Search & Reporting ▾

Search Pivot **Reports** Alerts Dashboards

Reports

Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Pivot or Search to refine the parameters or further explore the data.

6 Reports All Yours This App's

i	Title ▲	Actions
▶	Bad Logins	Open in Search Edit ▾
▶	Errors in the last 24 hours	Open in Search Edit ▾
▶	Errors in the last hour	Open in Search Edit ▾
▶	License Usage Data Cube	Open in Search Edit ▾
▶	Messages by minute last 3 hours	Open in Search Edit ▾
▶	Splunk errors last 24 hours	Open in Search Edit ▾

Sharing Reports (Jobs)

- Save report results and generate a link to it – good for 7 days
- Use Share button or Job dropdown
- Distribute link as appropriate

The screenshot displays the Splunk Search & Reporting interface. A search for 'fail* password' has been performed, resulting in 28,866 events. A 'Share Job' dialog box is open in the center, displaying the message: 'The job's lifetime has been extended to 7 days and read permissions have been set to Everyone. Manage the job via Job Settings.' Below this message, a 'Link To Job' field contains the URL 'http://ec2-54-215-92-147.us-west-1.'. A red box highlights the share icon (a right-pointing arrow) in the job controls area on the right side of the interface.

Saving Results

- Capture the search output at a point in time – “freeze” results
- Click Export
- Choose a format

The screenshot displays the Splunk Search & Reporting interface. At the top, the navigation bar includes 'splunk>', 'App: Search & Reporting', and user options like 'Administrator', 'Messages', 'Settings', 'Activity', and 'Help'. Below this, a secondary navigation bar contains 'Search', 'Pivot', 'Reports', 'Alerts', and 'Dashboards'. The main search area shows a search bar with the query 'fail* password' and a search button. Below the search bar, it indicates '28,866 events (before 9/16/13 9:39:59.000 PM)'. A modal dialog titled 'Export Results' is open, showing options for 'Format' (set to CSV), 'File Name' (with a dropdown menu open showing 'Raw Events', 'CSV', 'XML', and 'JSON'), and 'Number of Results'. The 'Export' button in the search bar is highlighted with a red box, and an arrow points from it to the 'Export Results' dialog. The dialog also has a 'Cancel' button at the bottom left.

.conf2013

**YOUR DATA
NO LIMITS**

Next Steps

splunk>

Beyond the Basics

- Splunk has many powerful features and search commands that allow you to:
 - Pivot - quickly build queries and display results through an easy to use interface
 - Create alerts
 - Capture and share knowledge
 - Calculate statistics
 - Format and organize values within search results
 - Create compelling data visualizations and reports
 - And more!
 - Learn about these features in other Using Splunk track sessions

Get Yourself Educated!

www.splunk.com > Services > Education

Splunk Education

Splunk classes are designed for specific roles such as Splunk Administrator, Developer, User, or Architect. Please read the descriptions below to find the best class and delivery method for you.

Splunk Classes

The table below lists available Instructor-led courses along with suggested learning tracks by student type. Click on a course name to view the full course description and schedule.

	User	Administrator	Architect	Developer	Support Engineer
Splunk Architecture Overview (eLearning)»	✓	✓	✓	✓	✓
Using Splunk »	✓	✓	✓	✓	✓
Using Splunk (eLearning with live labs) »	✓	✓	✓	✓	✓
Splunk Tutorial (eLearning) »	✓	✓	✓	✓	✓



Catch a Flick!

Education Videos

Our education videos provide valuable how-tos and tutorials. Whether you've just installed Splunk or are a seasoned user looking for a quick refresher, these videos will have you Splunking in no time!

Featured Videos



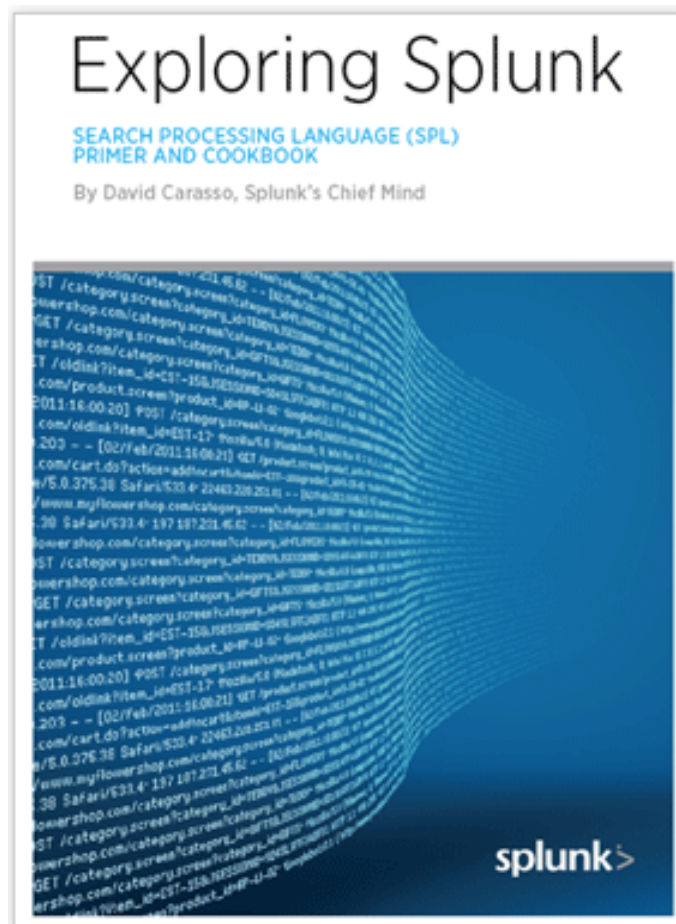
Reports and Dashboards

The screenshot shows the "Getting Data In" configuration page in Splunk. The main heading is "Get your data into Splunk from this machine or any other machine in your network". Below this, there's a section "To get started, choose your data type from this list, OR choose a collection method from the second list below." The data type list includes: "A file or directory of files", "Syslog", "Windows event logs", "Windows Registry", "Windows performance metrics", "Unix/Linux logs and metrics", "File integrity monitoring", "Configuration files", "OPSEC LEA", "Cisco device logs", "IIS logs", "Apache logs", "WebSphere logs, metrics and other data", and "Any other data...". The collection method section is titled "Choose how you want Splunk to consume your data." and includes options: "From files and directories", "From a TCP port", "From a UDP port", and "Run and collect the output of a script". At the bottom, there's a note: "Is your data on another machine, besides this Splunk server? Install Splunk's universal forwarder on that machine and tell it to send the data to this Splunk server."

Getting Data In - Linux

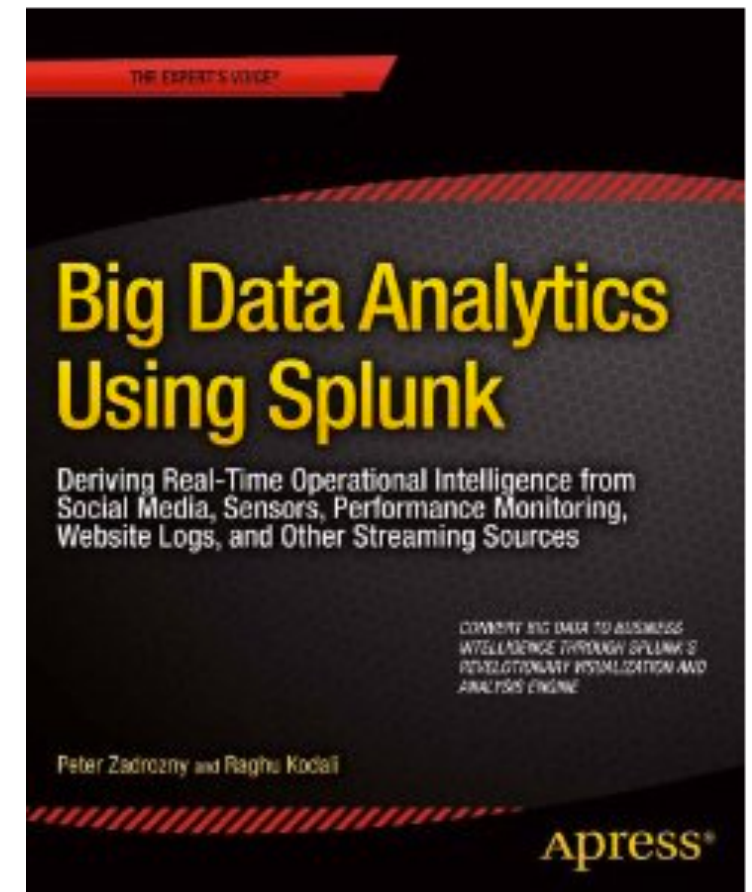
Read Any Good Books Lately?

splunk.com/goto/book



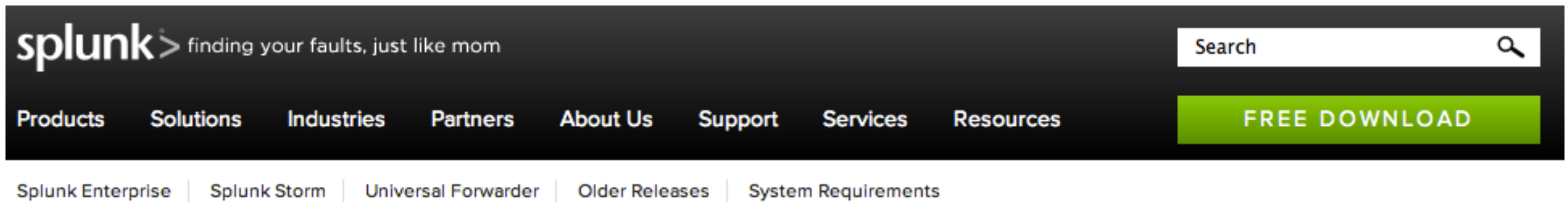
Download the Book: [ePub](#) | [pdf](#) | [Kindle](#)

Purchase the hardcopy at [Amazon](#)



Take a Test Drive!

- Download Splunk Enterprise - build your own sandbox
- Free! www.splunk.com/download
- Pick your platform
- Installs in minutes



Next Steps

1 Download the .conf2013 Mobile App

If not iPhone, iPad or Android, use the Web App

2 Take the survey & **WIN A PASS FOR .CONF2014...** Or one of these bags!

3 Go to “Splunk for Operational Intelligence”

Room: Nolita 1, Level 4

Today, 1:45-2:45pm



.conf2013

**YOUR DATA
NO LIMITS**

Thank You!

splunk>