.conf2013

YOUR DATA
NO LIMITS

Search Language - Beginner

Mitch Fleischman

Senior Instructor

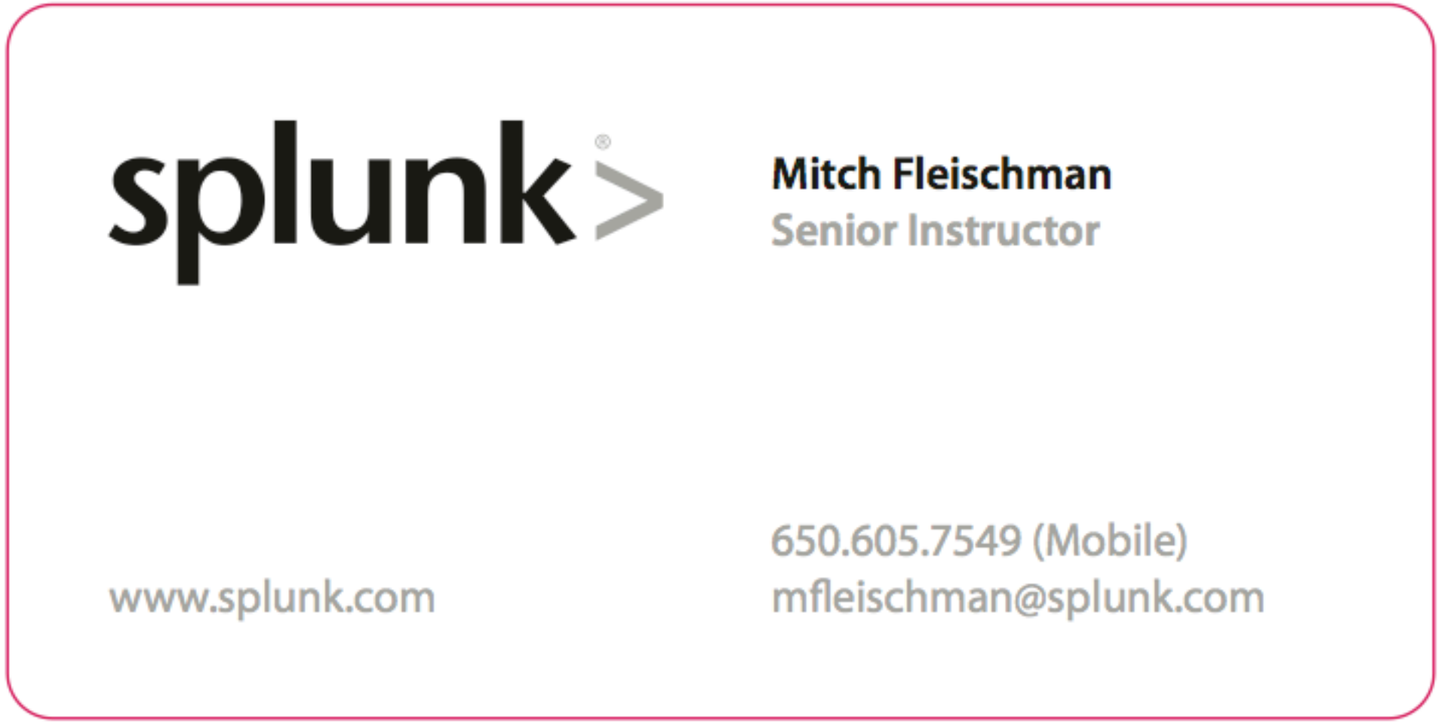
#splunkconf

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.

About Me



- 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

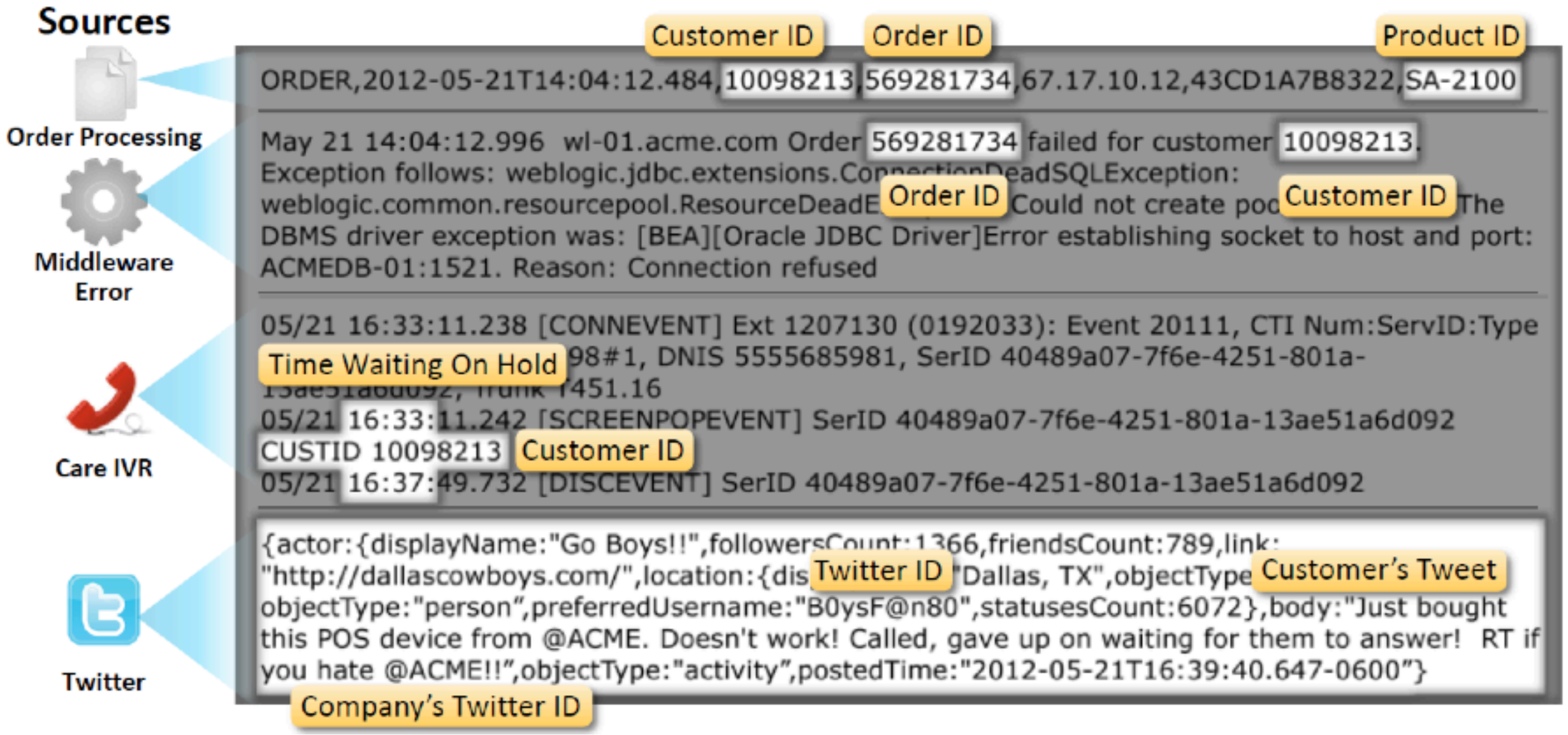
Splunking:

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



What Does Splunk Really Do?

It turns this

```
####<Sep 24, 2009 2:52:38 PM PDT> <Warning> <E
'224' for queue: 'weblogic.kernel.Default (se]
<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: j
primary key '10011968' was not found by 'findE
      at
com.sun.j2ee.blueprints.opc.customerrelations.
alMDB.java:140)
      at weblogic.ejb.container.internal.MDLis
```

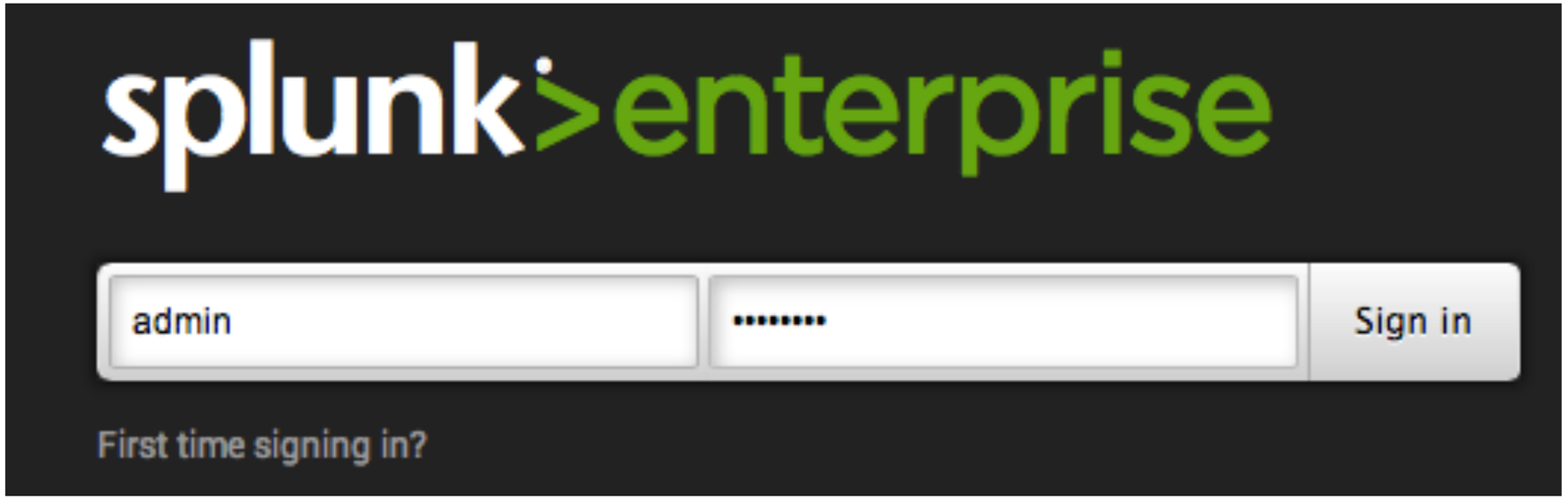
```
[Thu Sep 24 14:57:33 2009] [error] [client 10.
enter_order_information.screen at backend host
'CONNECTION_REFUSED [os error=0, line 1739 of
127.0.0.1:7001', referer: http://10.2.1.223/pe
```

Into this

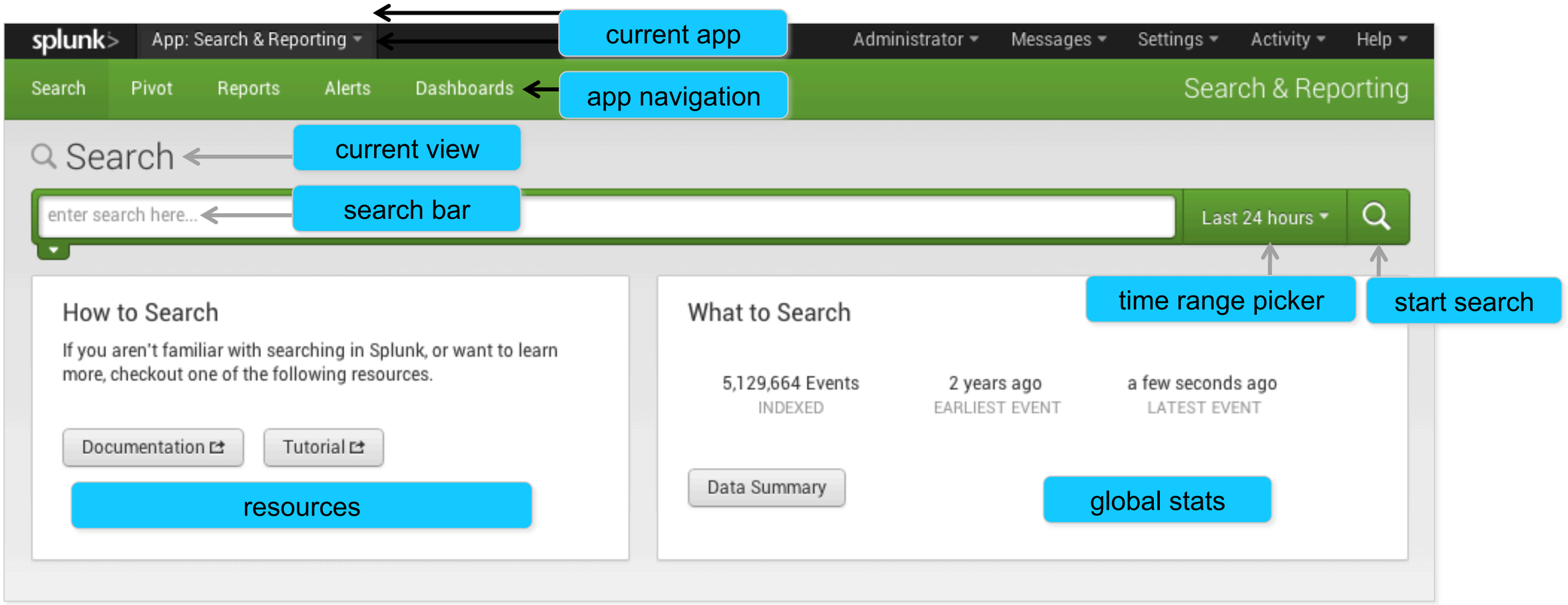

.conf2013
YOUR DATA
NO LIMITS
Getting Started
splunk>

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



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=SDOSL4FF8ADFF4956 HTTP 1.1" 200 883 "http://www.b
uttercupgames.com/oldlink?itemId=EST-26" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like M
ac 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=STRATEG
Y&JSESSIONID=SDOSL4FF8ADFF4956 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 Mobil
e/9B206 Safari/7534.48.3" 292
91.205.40.22 - - [16/Sep/2013:20:19:28] "GET /product.screen?productId=SF-BVS-01
&JSESSIONID=SDOSL4FF8ADFF4956 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=SDOSL4FF8ADFF4956 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=SDOSL4FF8ADFF4956 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=SDOSL4FF8ADFF4956 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

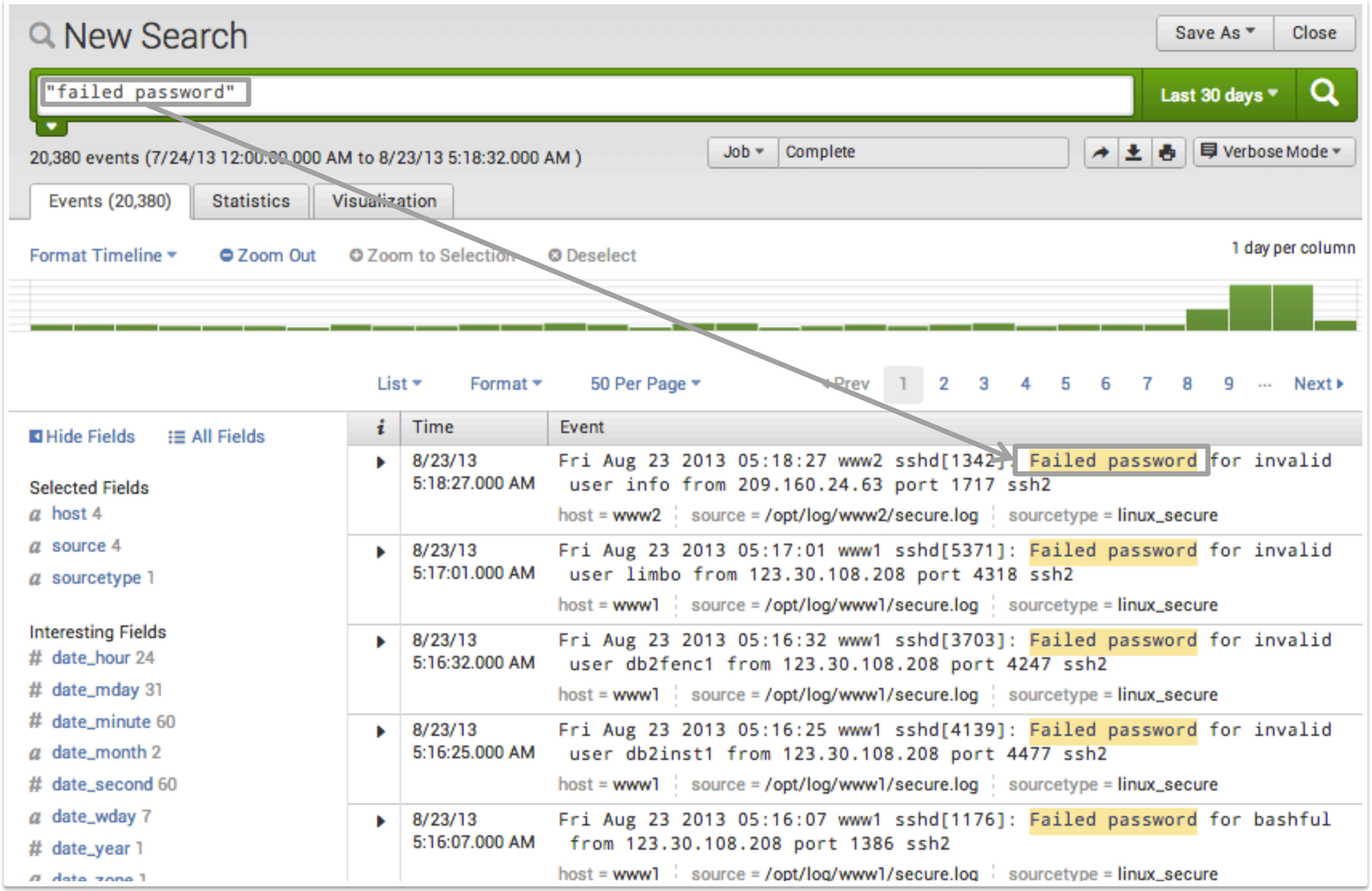
Everything is Searchable

- * 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

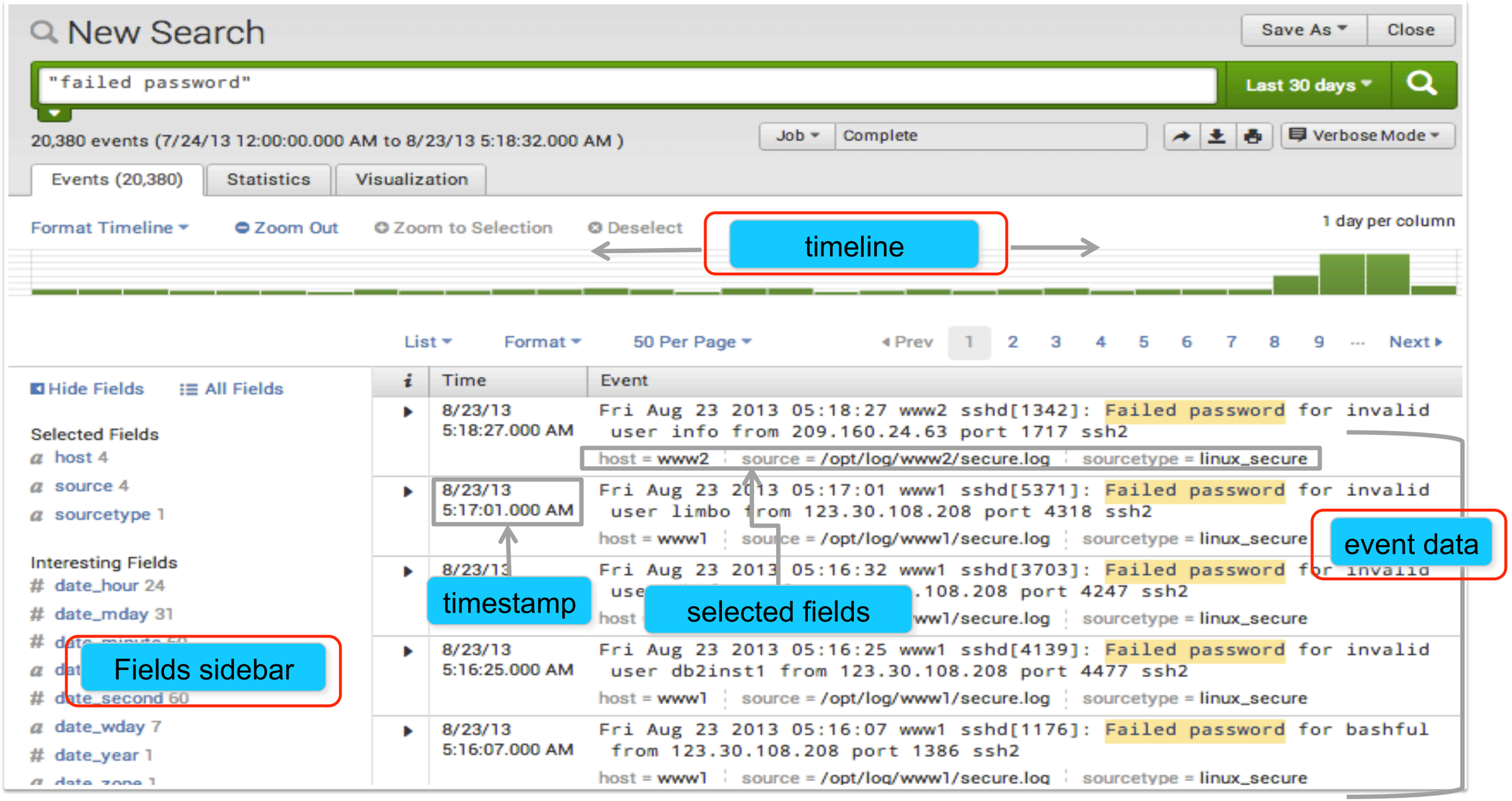

.conf2013
YOUR DATA
NO LIMITS
Basic Searching
splunk>

Search

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

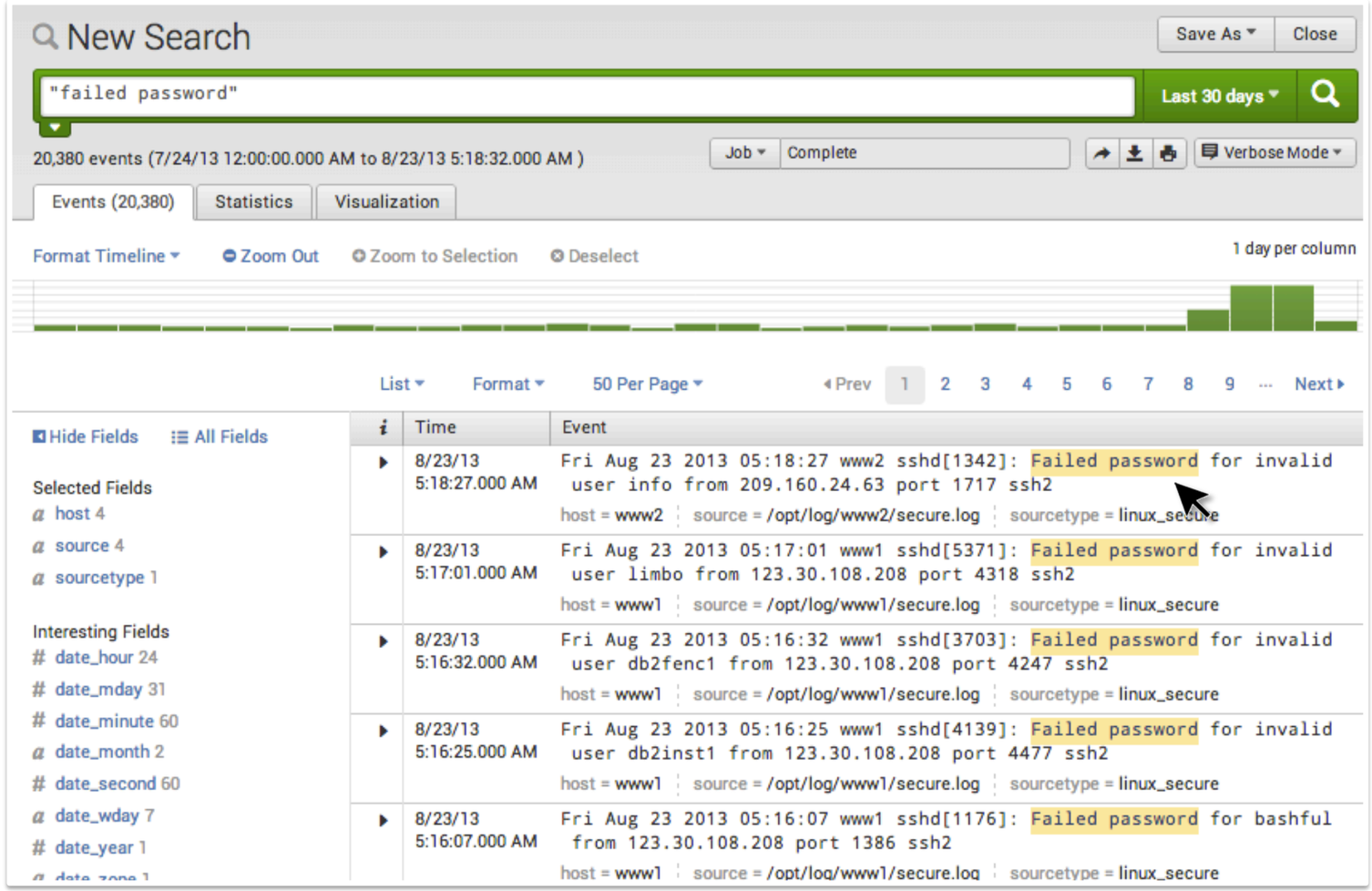


Search Results



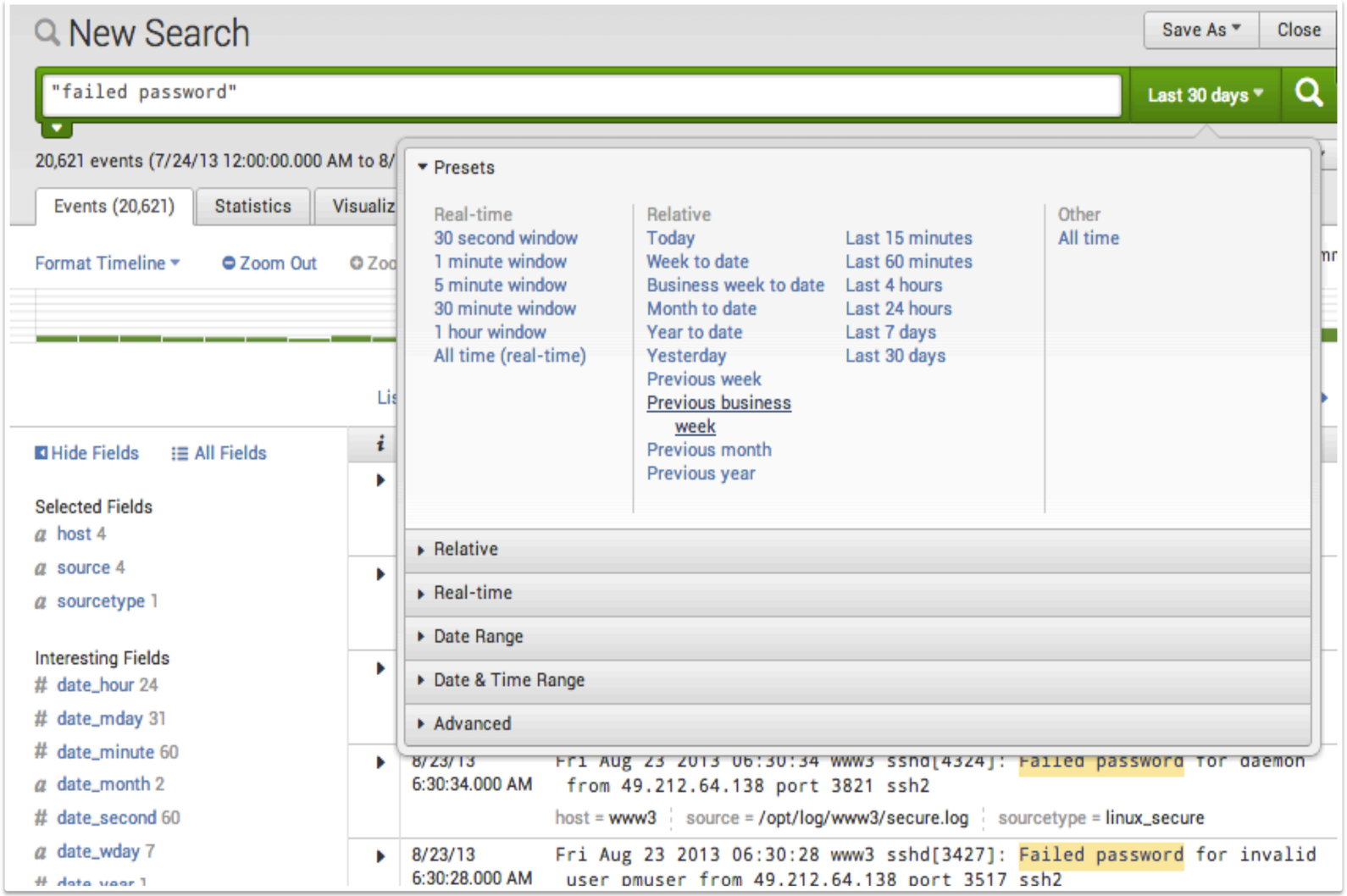
Navigating Search Results

- 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



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

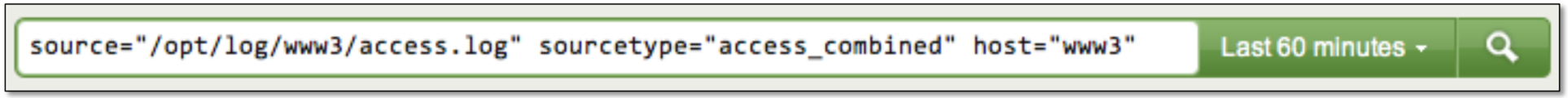



.conf2013
YOUR DATA
NO LIMITS
Using Fields
splunk>

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:

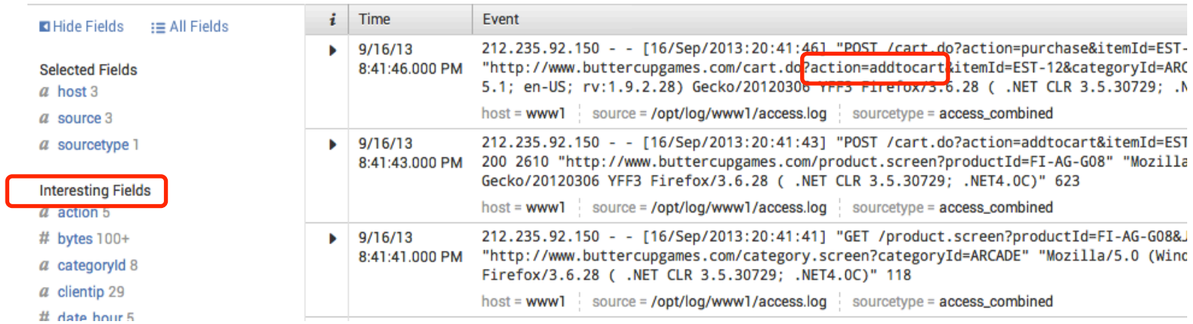
default fields



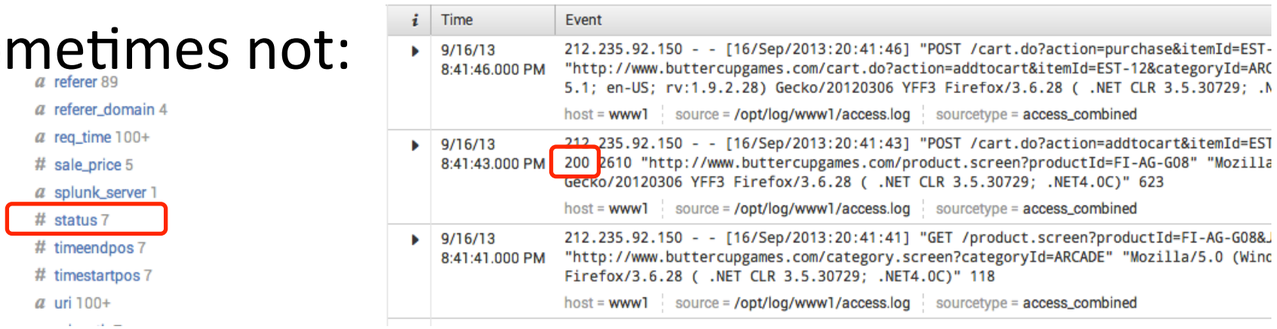
data-specific fields

Identifying Data-specific Fields

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



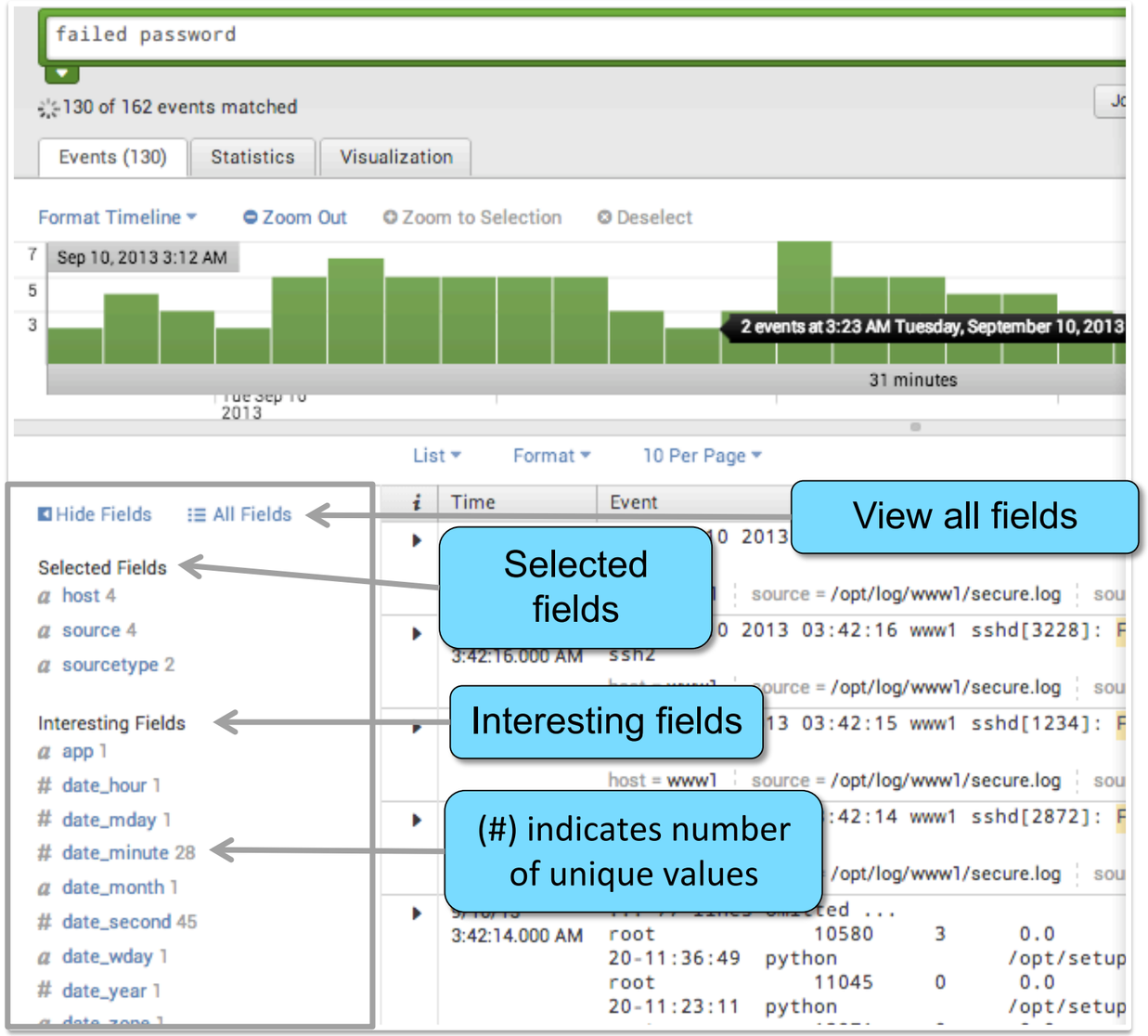
- Sometimes not:



- For more information, please see:
  http://docs.splunk.com/Documentation/Splunk/latest/Data/Listofpretrainedsourcetypes

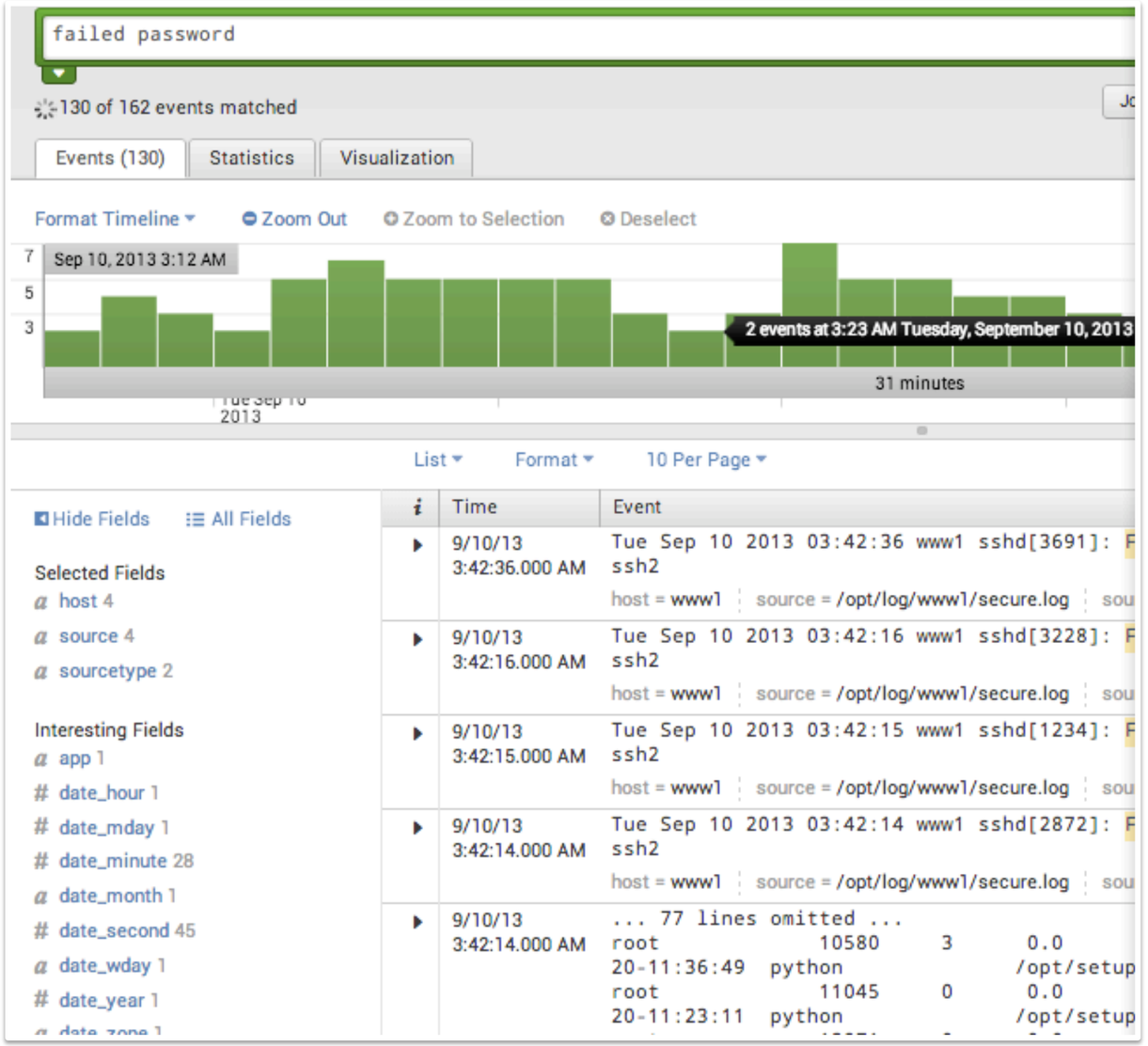
Fields Sidebar

- 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



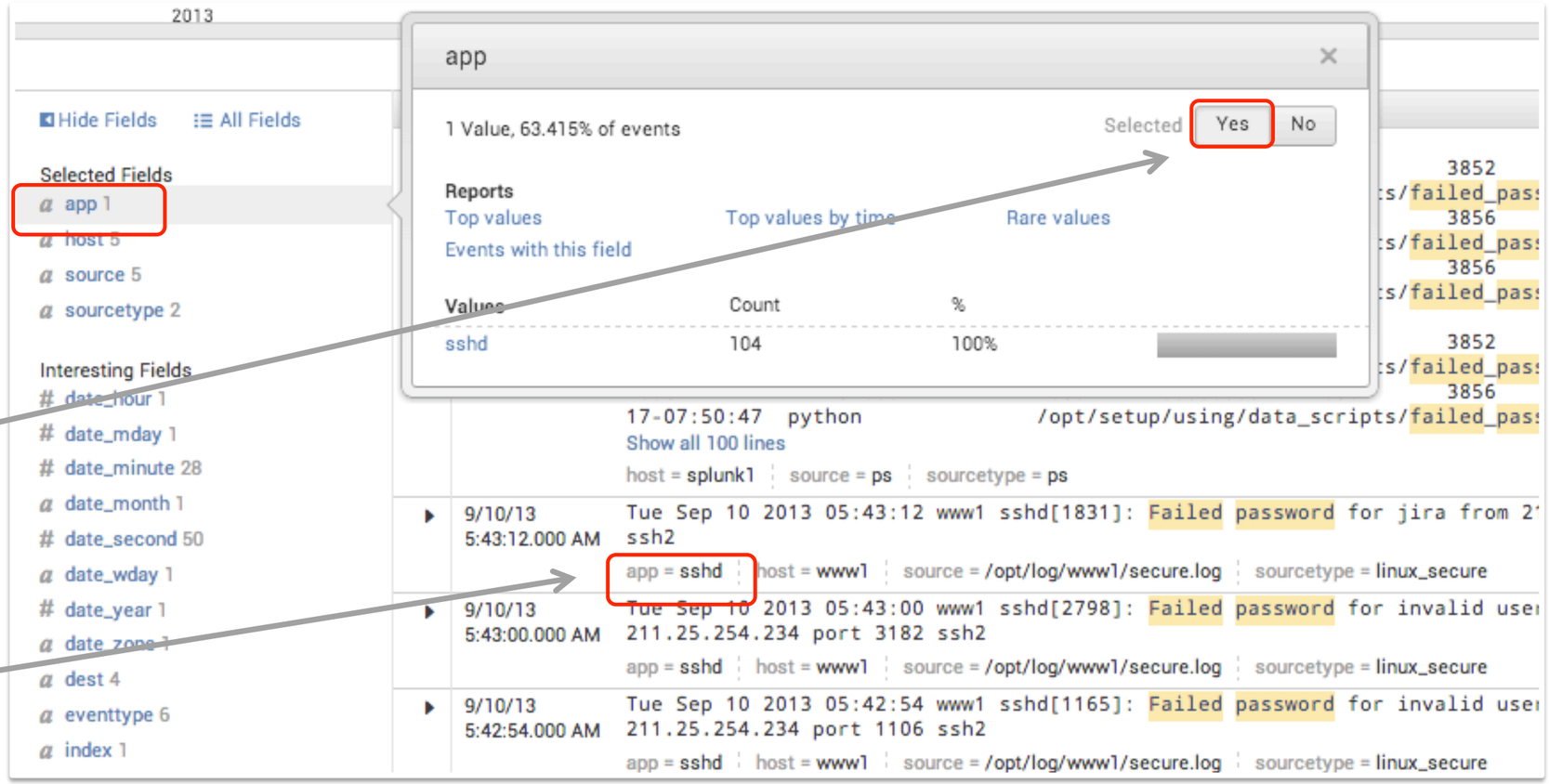
Selected Fields

- 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

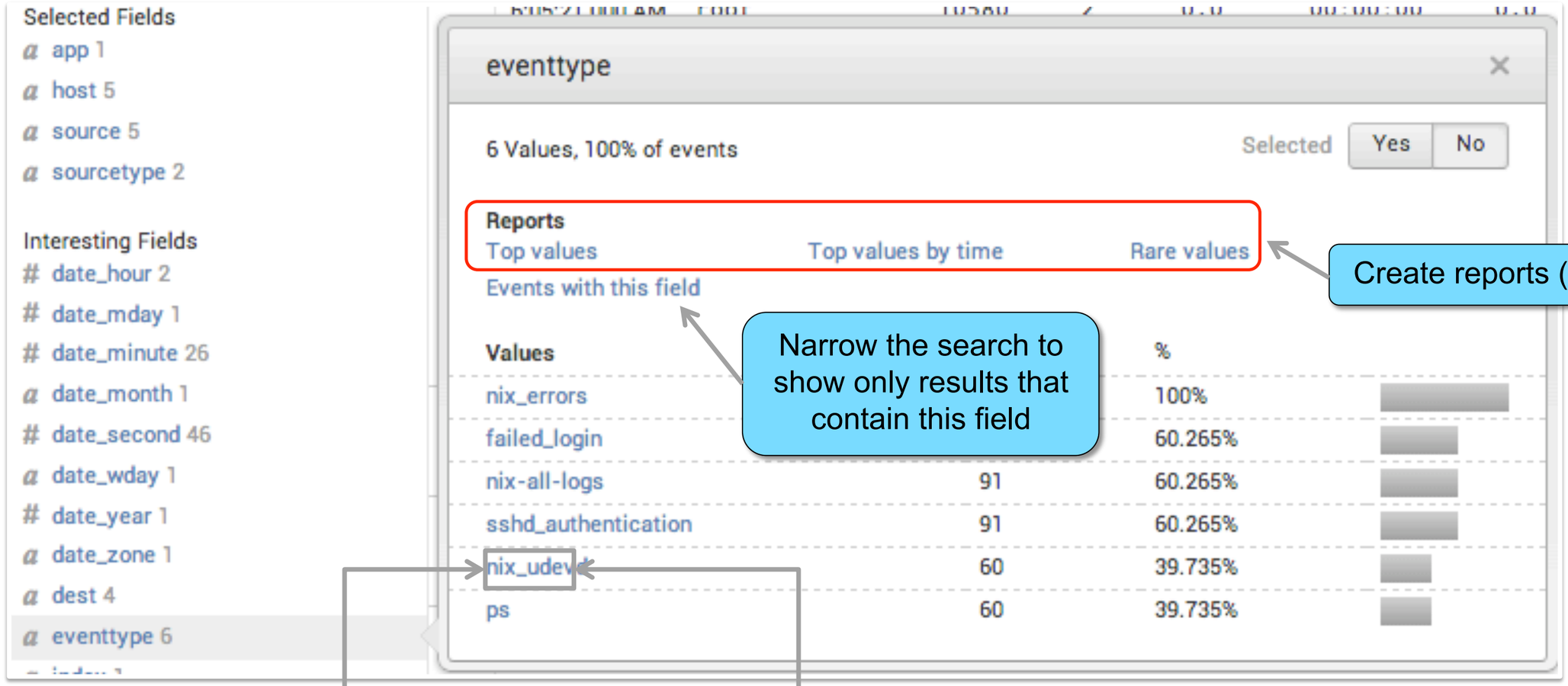


Adding Fields to Selected Fields

- 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



More Ways to Use the Fields Sidebar



Using Fields in Searches

- Efficient way to pinpoint searches and refine results

```
141.146.8.66
```

```
src_ip=141.146.8.66
```

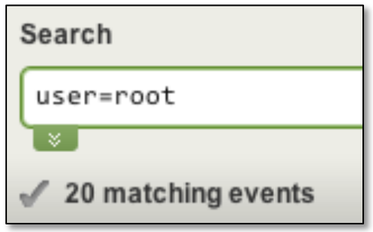
```
status=404
```

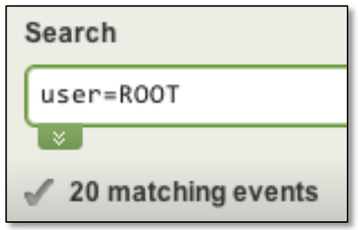
```
area_code=404
```

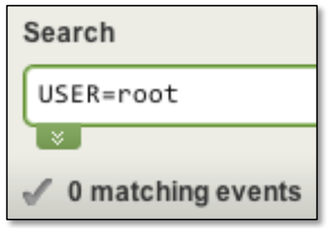
- Use wildcards

```
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:

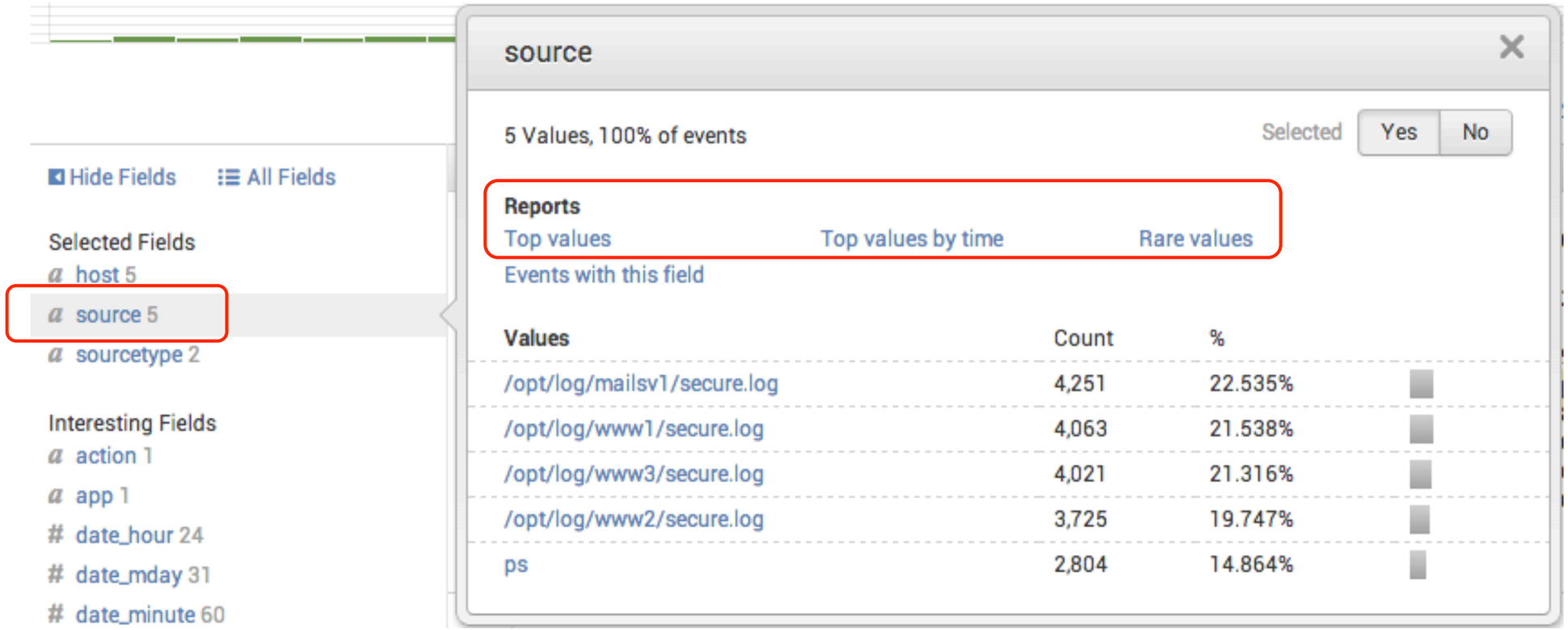




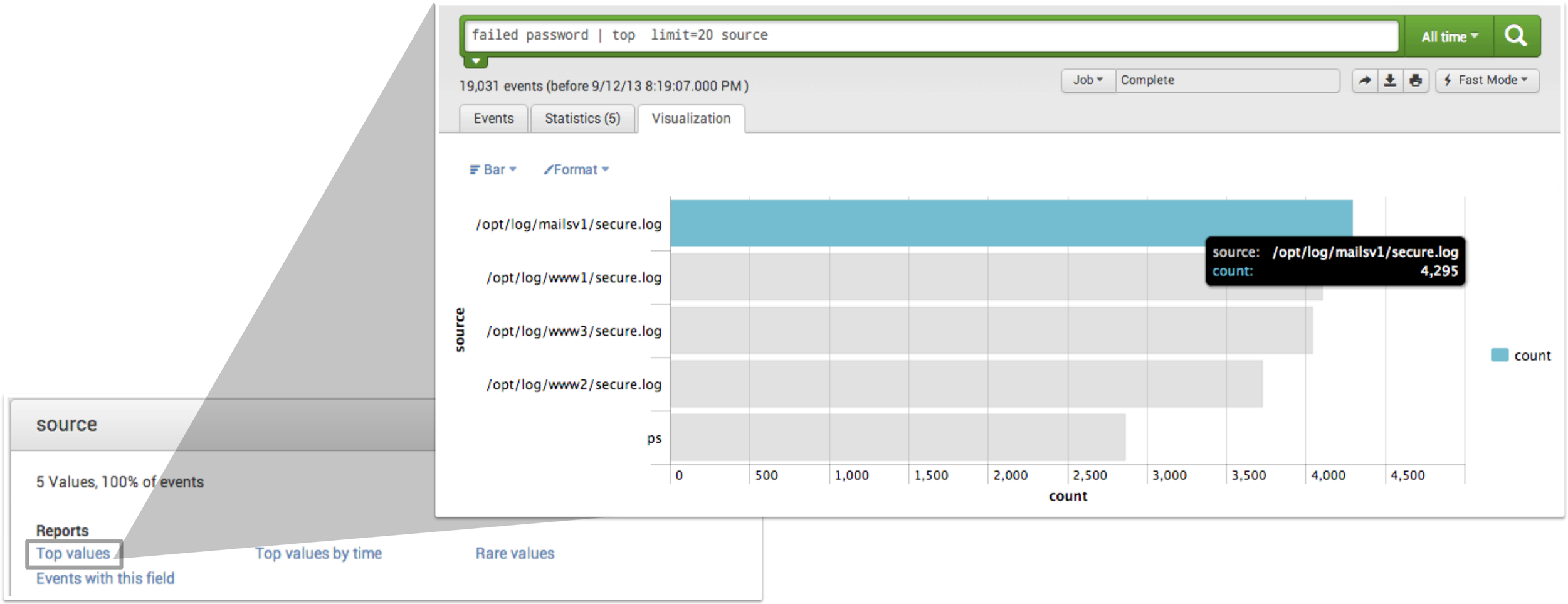


Create Reports from Fields Sidebar

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



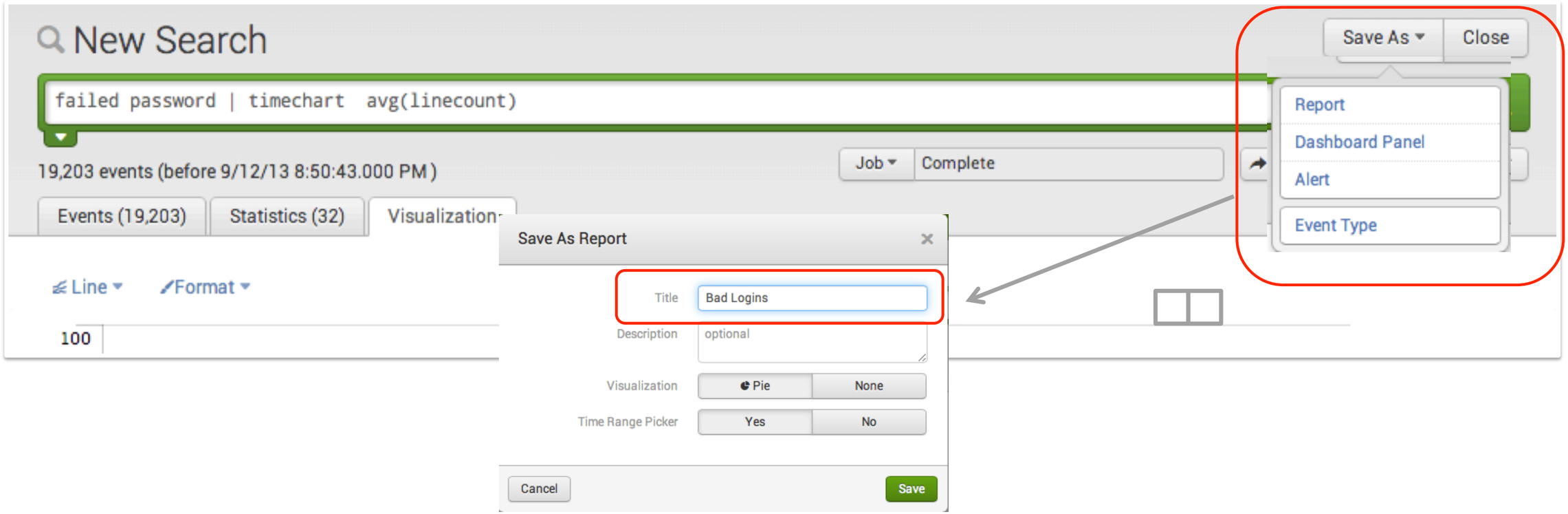
Create a ‘Top Values’ Report



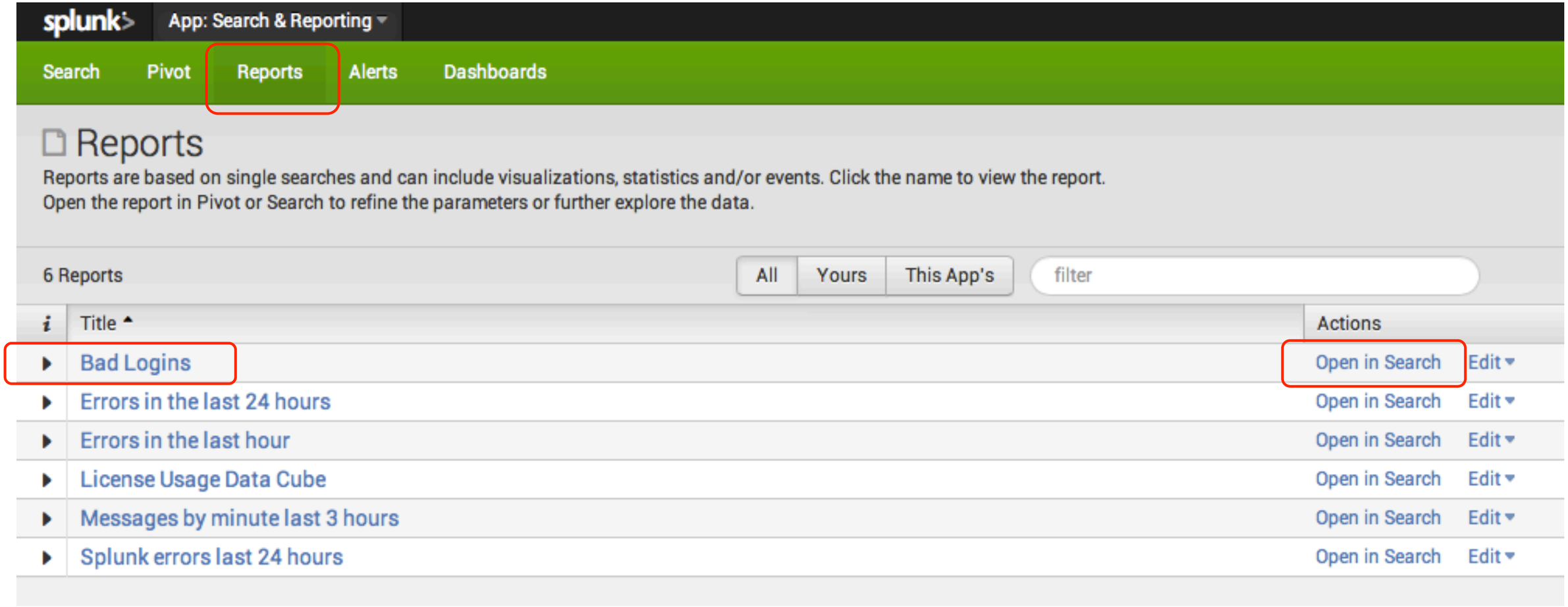

.conf2013
YOUR DATA
NO LIMITS
Saving and Sharing Reports
splunk>

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

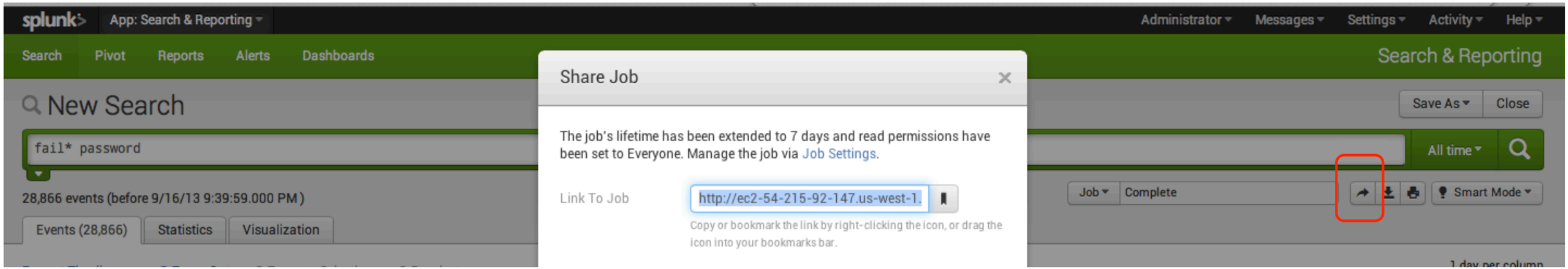


Running Saved Reports



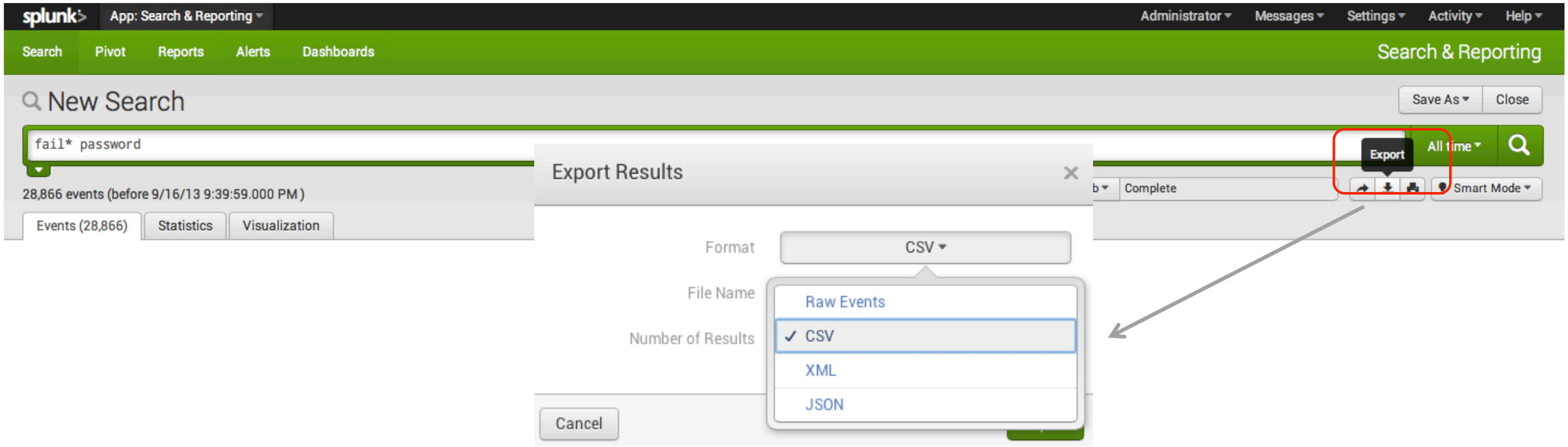
Sharing Reports (Jobs)

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



Saving Results

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




.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.

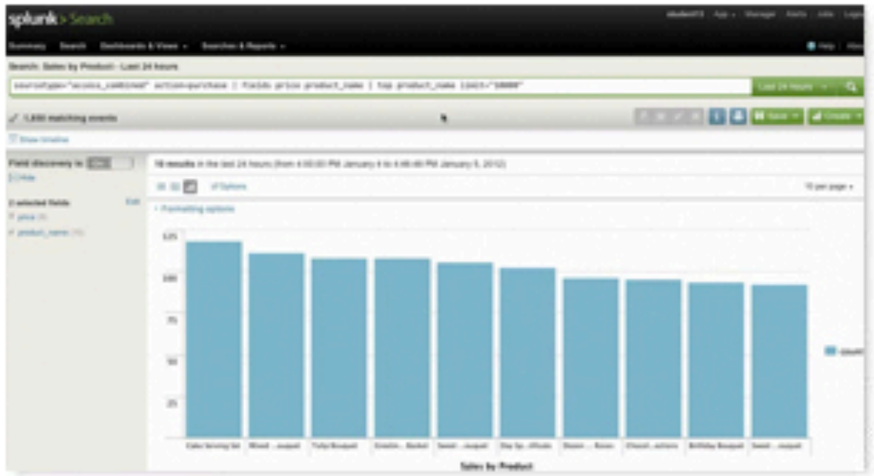
	User	Administrator	Architect	Developer	Support Engineer
Splunk Architecture Overview (eLearning)»	✓	✓	✓	✓	✓
Using Splunk »	✓	✓	✓	✓	✓
Using Splunk (eLearning with live labs) »	✓	✓	✓	✓	✓
Splunk Tutorial (eLearning) »	✓	✓	✓	✓	✓

Catch a Flick!

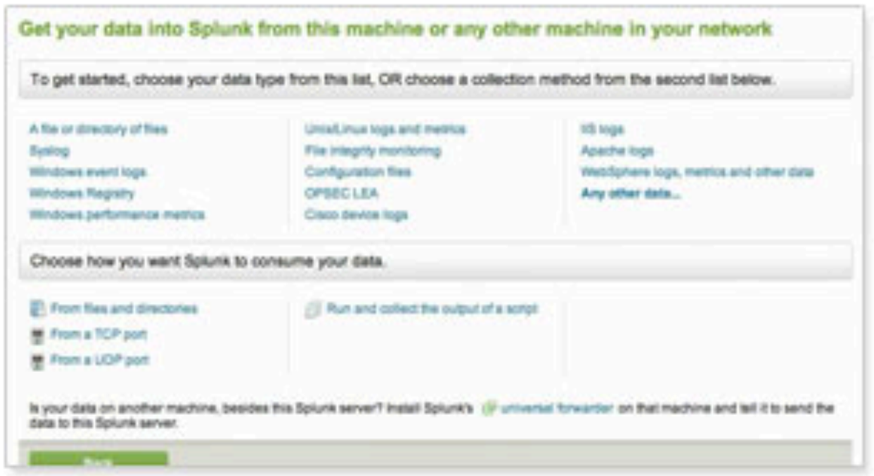
Education Videos

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



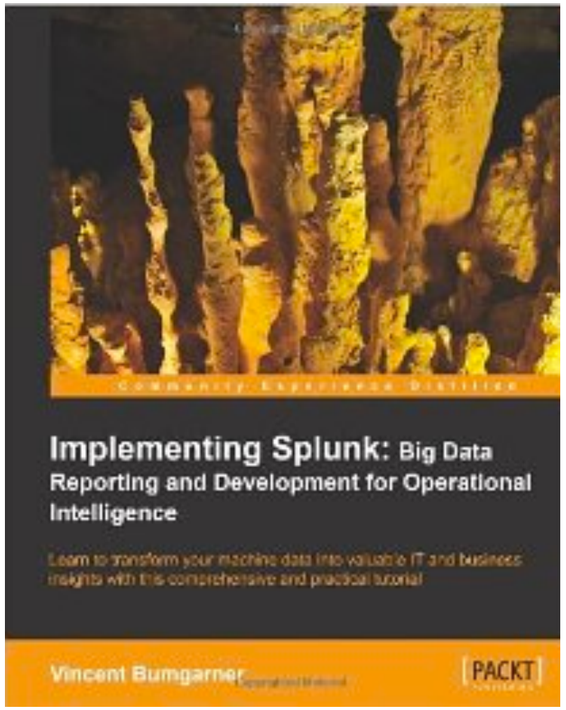
Reports and Dashboards

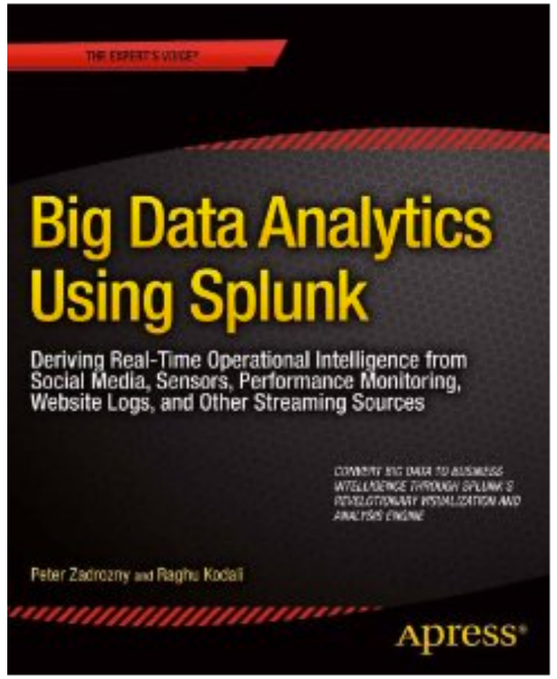


Getting Data in - Linux

Read Any Good Books Lately?

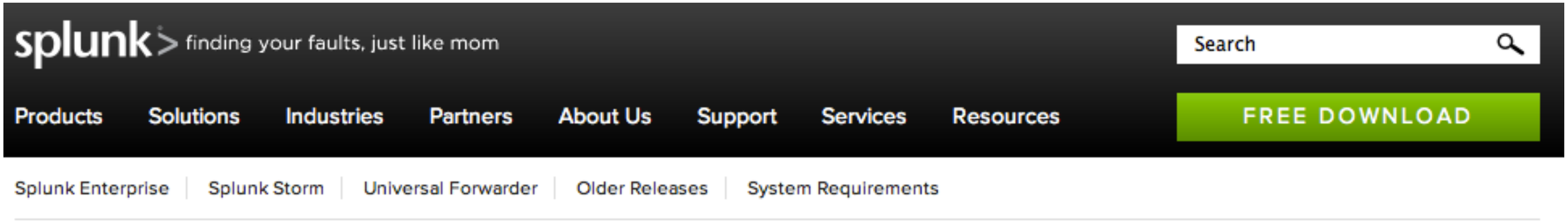
splunk.com/goto/book





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>