

.conf2013

**YOUR DATA
NO LIMITS**

**Unleashing the Power of Splunk
with Knowledge Objects**

Lincoln Bowser

Sr. Technical Instructor, Splunk

#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

- Home office in the metropolis of Tracy, CA
- Deliver all core Splunk classes
- SPL enthusiast



Agenda

- Tags
- Event Types
- Alerts

.conf2013

**YOUR DATA
NO LIMITS**

Tags

splunk>



Splunk as a “Search Engine”

Type in keywords, hit return, get results ...

The screenshot shows the Splunk search interface. At the top, there is a search bar with the query `sourcetype=linux_secure error OR fail*` and a search button. Below the search bar, it indicates 495 events were found for the time range 9/15/13 12:36:00.000 PM to 9/15/13 4:36:53.000 PM. The interface includes navigation options like 'Events (495)', 'Statistics', and 'Visualization'. A table of results is displayed with columns for Time and Event. The event descriptions include 'Failed password for invalid user' for various users like 'sys', 'local', 'administrator', and 'games'.

Time	Event
9/15/13 4:36:45.000 PM	Sun Sep 15 2013 16:36:45 www2 sshd[4726]: Failed password for invalid user sys from 192.162.19.179 port 1294 ssh2 user = sys
9/15/13 4:36:30.000 PM	Sun Sep 15 2013 16:36:30 www2 sshd[4348]: Failed password for invalid user local from 192.162.19.179 port 2118 ssh2 user = local
9/15/13 4:35:59.000 PM	Sun Sep 15 2013 16:35:59 www2 sshd[5374]: Failed password for invalid user administrator from 192.162.19.179 port 4784 ssh2 user = administrator
9/15/13 4:35:54.000 PM	Sun Sep 15 2013 16:35:54 www2 sshd[1542]: Failed password for games from 192.162.19.179 port 4180 ssh2 user = games

So Much More Than a “Search Engine”

- Splunk allows you to “store” knowledge along with your IT data
- Institutional knowledge
 - For example: server function or device location
- Learned knowledge
 - For example: identify crash precursors or suspicious activity patterns
- You store these in Splunk using Knowledge Objects

Scenario – Confusing Server Names

- Server names aren't always meaningful to you!

```
host="lnx1721_64_us_west_apache"
```

- Sometimes they reflect a theme or hobby

```
host="giants" OR host="reds" AND NOT host="dodgers"
```

Knowledge Objects – Tags to the Rescue

Tags are metadata you can add to specific field / value pairs

Splunk Enterprise 6

9/11/13 8:37:48.000 PM 12.130.60.5 - - [11/Sep/2013:20:37:48] "GET /cart.do?action=view&itemId=EST-18&productId=FI-AG-G08&JSESSIONID=SD0SL5FF10ADFF4964 HTTP 1.1" 200 2222 "http://www.buttercupgames.com/category.screen?categoryId=ARCADE" "Opera/9.01 (Windows NT 5.1; U; en)" 344

Event Actions

Type	Field	Value	Actions
<input checked="" type="checkbox"/>	host	www1	
<input type="checkbox"/>	JSESSIONID	SD0SL5FF10ADFF4964	
<input type="checkbox"/>	action	view	
<input type="checkbox"/>	bytes	2222	

1

2

3

Edit Tags

Create Tags

Field Value: host=www1

Tag(s): webfarm

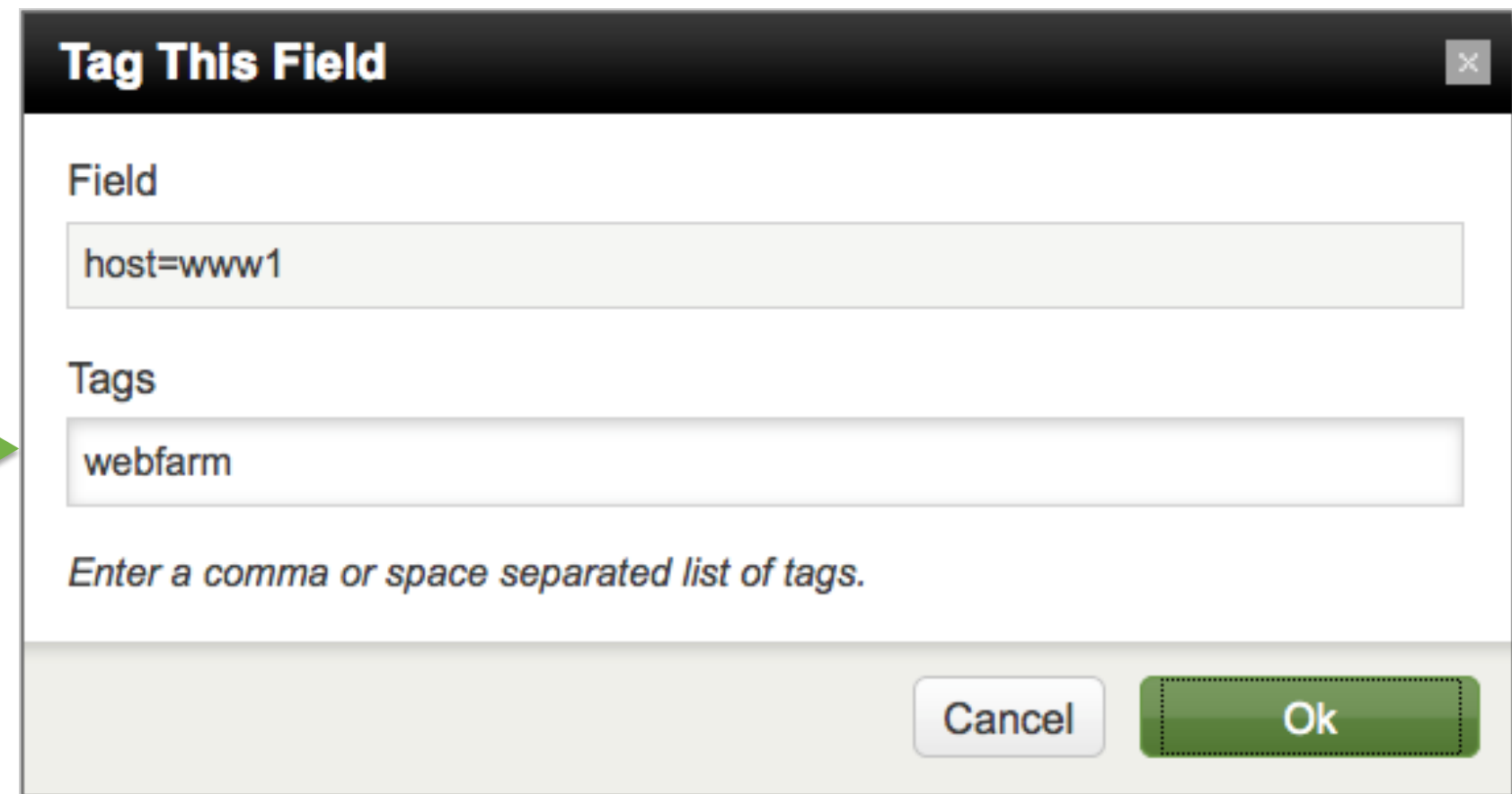
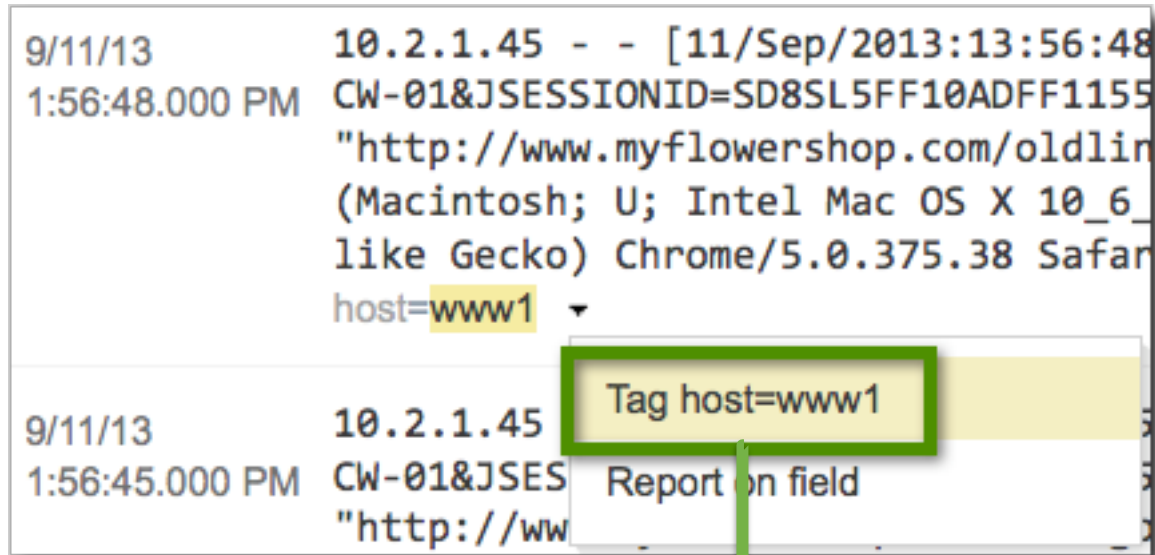
Comma or space separated list of tags.

Cancel Save

Note: tags are applied to field/value combinations, not fields!

Knowledge Objects – Tags to the Rescue

Splunk Enterprise 5



Using Tags

Search all hosts tagged as "webfarm"

Full Syntax

Short Form

or

tag::host=webfarm

1,567 events (9/11/13 2:00:00.000 PM to 9/12/13 2:00:19.000 PM)

Events (1,567) Statistics Visualization

Format Timeline ▾ List ▾ Format ▾ 20 Per Page ▾

<input checked="" type="checkbox"/> Hide Fields <input checked="" type="checkbox"/> All Fields	<i>i</i>	Time	Event
Selected Fields @ host 1	▶	9/12/13 1:59:27.000 PM	Thu Sep 12 2013 13: host = www1 webfarm
	▶	9/12/13 1:59:03.000 PM	Thu Sep 12 2013 13: host = www1 webfarm
Interesting Fields			

tag=webfarm

1,573 events (9/11/13 2:00:00.000 PM to 9/12/13 2:02:18.000 PM)

Events (1,573) Statistics Visualization

Format Timeline ▾ List ▾ Format ▾ 20 Per Page ▾

<input checked="" type="checkbox"/> Hide Fields <input checked="" type="checkbox"/> All Fields	<i>i</i>	Time	Event
Selected Fields @ host 1	▶	9/12/13 2:02:09.000 PM	Thu Sep 12 2013 14:0 host = www1 webfarm
	▶	9/12/13 2:01:30.000 PM	Thu Sep 12 2013 14:0 host = www1 webfarm
Interesting Fields			

Note: you can use the short form effectively as long as no other fields have the same tag value

But Who Can See/Use My Tags?

- Initially, tags are created as private knowledge objects
- If you are a power user (or admin) and want other users to see/use your tags, you must share them
 - This is true for all knowledge objects that do not display sharing options upon creation




Sharing Knowledge Objects – 5

1

Administrator | App ▾ | **Manager** | Alerts | Jobs | Logout
? Help | About

2

Knowledge

-  **Searches and reports**
View and edit saved searches and reports. Set permissions.
-  **Event types**
View and edit event types. Set permissions.
-  **Tags**
Create, view and edit tags. Set permissions.

3

Tags

Manage tags on field values.

Tag links

- List by field value pair**
- List by tag name
- All unique tag objects

Sharing Knowledge Objects – 5

4

5

App context Search (search) Owner Any

Show only objects created in this app context [Learn more](#)

List by field value pair

Showing 1-1 of 1 item Results per page

Field value pair ↕	Tag name ↕	App ↕	Sharing ↕	Status ↕	Actions
host=www1	webfarm	search	Private <input type="button" value="Permissions"/>	Enabled Disable all tags for pair	Clone Move Delete

Object should appear in

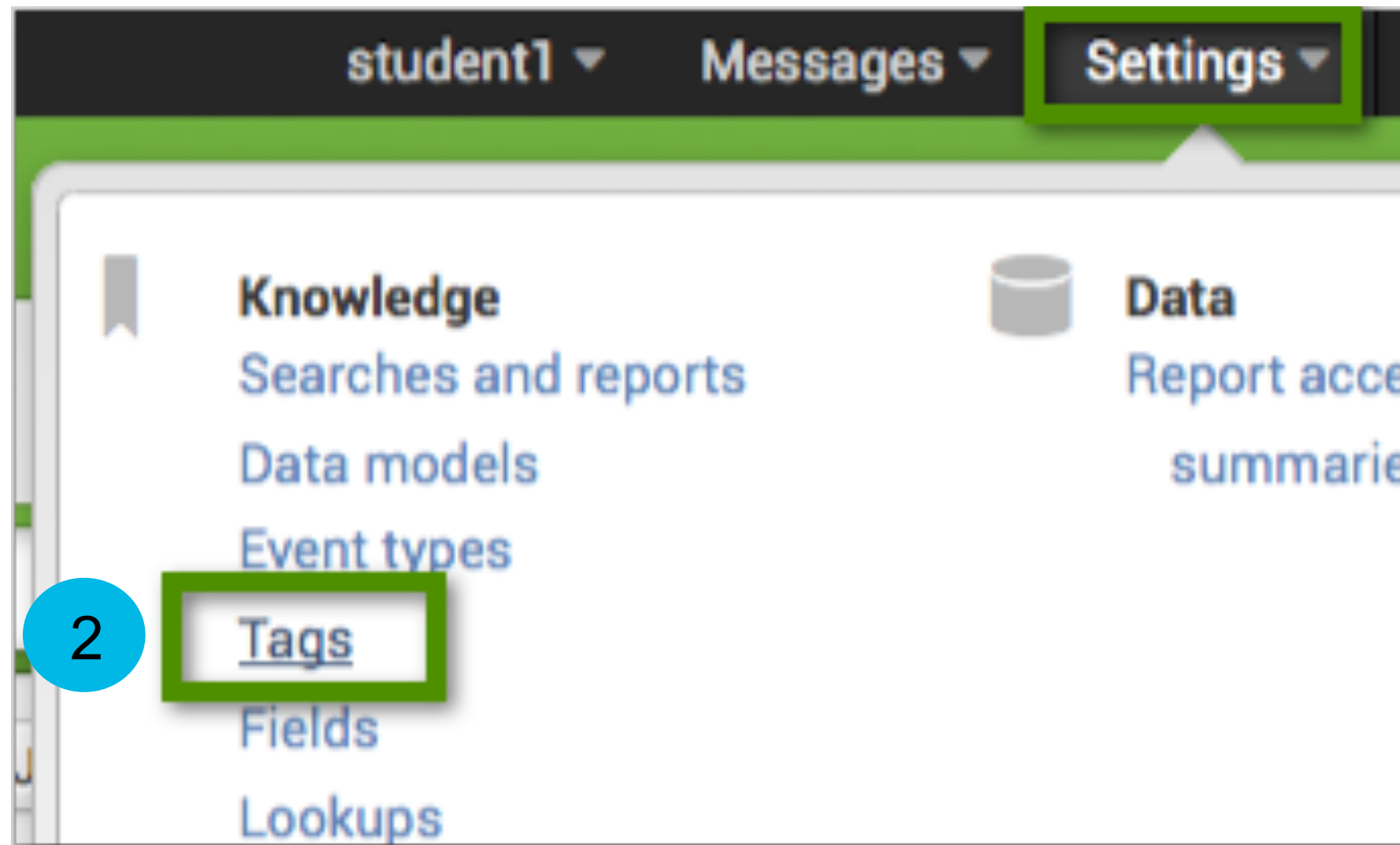
Keep private This app only (search) All apps

Permissions

Roles	Read	Write
Everyone	<input type="checkbox"/>	<input type="checkbox"/>
admin	<input type="checkbox"/>	<input type="checkbox"/>
can_delete	<input type="checkbox"/>	<input type="checkbox"/>
power	<input checked="" type="checkbox"/>	<input type="checkbox"/>
splunk-system-role	<input type="checkbox"/>	<input type="checkbox"/>
user	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Sharing Knowledge Objects – 6

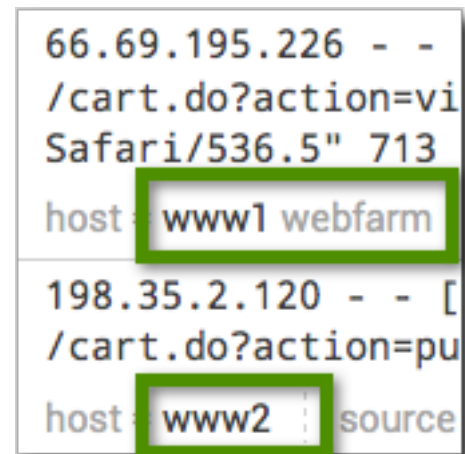
1



Steps 3-5 the same

Things to Remember About Tags

- Tag values are case sensitive
- Permissions of tags always default to Private
- Tags are associated with field/value combinations



The screenshot shows two log entries from Splunk. The first entry has a host value of 'www1 webfarm' and the second entry has a host value of 'www2 source'. Both host values are highlighted with a green box, illustrating that tags are associated with specific field/value combinations.

```
66.69.195.226 - -  
/cart.do?action=vi  
Safari/536.5" 713  
host: www1 webfarm  
198.35.2.120 - - [  
/cart.do?action=pu  
host: www2 source
```

- You cannot use a wildcard to assign a tag across multiple values, but ...

.conf2013

**YOUR DATA
NO LIMITS**

Event Types

splunk>



Knowledge Objects – Event Types

- Event types can help you automatically identify and classify events based on a search string
- An event type is:
 - A meta field based on a search
 - A way of classifying data for searching and reporting
 - Created by users
 - Useful for user knowledge capture and sharing

Classifying Groups of Events

sourcetype="linux_secure" "failed password" Last 4 hours

746 events (9/14/13 5:35:00.000 PM to 9/14/13 9:35:05.000 PM) Job Complete Smart Mode

Events (746) Statistics Visualization

Format Timeline List Format 20 Per Page Prev 1 2 3 4 5 6 7 8 9 Next

<input checked="" type="checkbox"/> Hide Fields <input checked="" type="checkbox"/> All Fields	<i>i</i>	Time	Event
Selected Fields <i>a</i> host 4 <i>a</i> source 4	▶	9/14/13 9:35:03.000 PM	Sat Sep 14 2013 21:35:03 mailsv1 sshd[3046]: Failed password for ncscd from 212.235.92.150 port 4229 ssh2 host = mailsv1 source = /opt/log/mailesv1/secure.log sourcetype = linux_secure
	▶	9/14/13 9:34:30.000 PM	Sat Sep 14 2013 21:34:30 mailsv1 sshd[4639]: Failed password for invalid user local from 212.235.92.150 port 3460 ssh2

Create Event Type for Unknown Login

New Search 1 2 Save As Close

sourcetype="linux_secure" "failed password for invalid user"

291 events (9/15/13 11:39:00.000 AM to 9/15/13 3:39:35.000 PM) Job Complete

Events (291) Statistics Visualization 3 Report Dashboard Panel Alert Event Type

Format Timeline List Format 20 Per Page Prev 1 2 3 4 5 6 7 8 9 ... Next

	i	Time	Event
▶		9/15/13 3:38:43.000 PM	Sun Sep 15 2013 15:38:43 www2 sshd[4506]: Failed password for invalid user uni from 27.96.191.11 port 3132 ssh2 host = www2
▶		9/15/13 3:38:19.000 PM	Sun Sep 15 2013 15:38:19 www2 sshd[2661]: Failed password for invalid user gitolite from 27.96.191.11 port 2987 ssh2

Create Event Type for Unknown Login

Save As Event Type

Name

Search String

Tags

Color

Priority

Determines which style wins, when an event has more than one event type.

Cancel

4

5

Create Event Type for Known Login

Search interface showing a search query and event results. The search query is `sourcetype="linux_secure" "failed password" NOT "for invalid user"`. The results show two events with "Failed password" highlighted in yellow.

Annotations:

- 1: Search bar
- 2: Save As button
- 3: Event Type button in the dropdown menu

Event Type dropdown menu options: Report, Dashboard Panel, Alert, Event Type.

	Time	Event
▶	9/15/13 3:34:33.000 PM	Sun Sep 15 2013 15:34:33 www2 sshd[5022]: Failed password for sync from 27.96.191.11 port 1878 ssh2 host = www2
▶	9/15/13 3:30:24.000 PM	Sun Sep 15 2013 15:30:24 www3 sshd[3662]: Failed password for mail from 76.89.103.115 port 4477 ssh2 host = www3

Create Event Type for Known Login

Save As Event Type

Name

Search String

Tags

Color

Priority

Determines which style wins, when an event has more than one event type.

Cancel

4

5

Color Coding Events in 5

You can color code event types in Splunk Enterprise 5, but not using the **Create > Event type** dialog

1 Build Eventtype

2 Save

3 Name: failure_user_known
Style: red
Priority: Highest

4 Save

OK, So Now What?

Now you can search using the **eventtype** field

```
eventtype="failure_user_known"
```

What's the Big Deal?

Because using a report (saved search) is easier

Reports

Reports are based on single searches and can include vis
Open the report in Pivot or Search to refine the parameter

4 Reports

i	Title ^
▶	Errors in the last 24 hours
▶	Errors in the last hour
▶	License Usage Data Cube
▶	Login failures - known last 4 hours

Searches & Reports ▾

- Errors ▶
- SR Class ▶
- Useful Searches ▶
- Daily License Usage
Timechart - last 4 weeks
- Login failures - known last
24 hours

Here's the Value – Splunk Enterprise 6

i	Time	Event
▶	9/14/13 10:21:05.000 PM	Sat Sep 14 2013 22:21:05 www1 sshd[2906]: Failed password for peevish from 147.213.138.201 port 3262 ssh2 eventtype = failed_login eventtype = failure_user_known eventtype = nix-all-logs eventtype = nix_errors error eventtype = sshd_authentication authentication remote
▶	9/14/13 10:20:31.000 PM	Sat Sep 14 2013 22:20:31 www1 sshd[1769]: Failed password for mail from 147.213.138.201 port 1831 ssh2 eventtype = failed_login eventtype = failure_user_known eventtype = nix-all-logs eventtype = nix_errors error eventtype = sshd_authentication authentication remote
▶	9/14/13 10:20:24.000 PM	Sat Sep 14 2013 22:20:24 www1 sshd[2381]: Failed password for invalid user munin from 147.213.138.201 port 1941 ssh2 eventtype = failed_login eventtype = failure_user_unknown eventtype = nix-all-logs eventtype = nix_errors error eventtype = sshd_authentication authentication remote
▶	9/14/13 10:20:12.000 PM	Sat Sep 14 2013 22:20:12 www1 sshd[4590]: Failed password for invalid user db4 from 147.213.138.201 port 4184 ssh2 eventtype = failed_login eventtype = failure_user_unknown eventtype = nix-all-logs eventtype = nix_errors error eventtype = sshd_authentication authentication remote

Here's the Value – Splunk Enterprise 6

The screenshot shows the Splunk interface with a search query `sourcetype="linux_secure"` and 892 events. A modal window titled 'eventtype' displays the top 10 values for the 'eventtype' field. The 'failure_user_unknown' value is highlighted with a green box.

Top 10 Values	Count	%
nix-all-logs	892	100%
sshd_authentication	790	88.565%
failed_login	760	85.202%
nix_errors	760	85.202%
failure_user_unknown	458	51.345%
failure_user_known	302	33.856%
ssh_open	38	4.26%
su_root_session	13	1.457%
su_session	13	1.457%
pam_unix_authentication	8	0.897%

Here's the Value – Splunk Enterprise 5

a eventtype (6)

a index (1)
linecount (1)
pid (81)
a process (1)
a punct (2)
a source (4)
a sourcetype (1)
a splunk_server (1)
a src (5)
a src_in (5)

eventtype (categorical)

Appears in 100% of results
Show only events with this field
Select and show in results

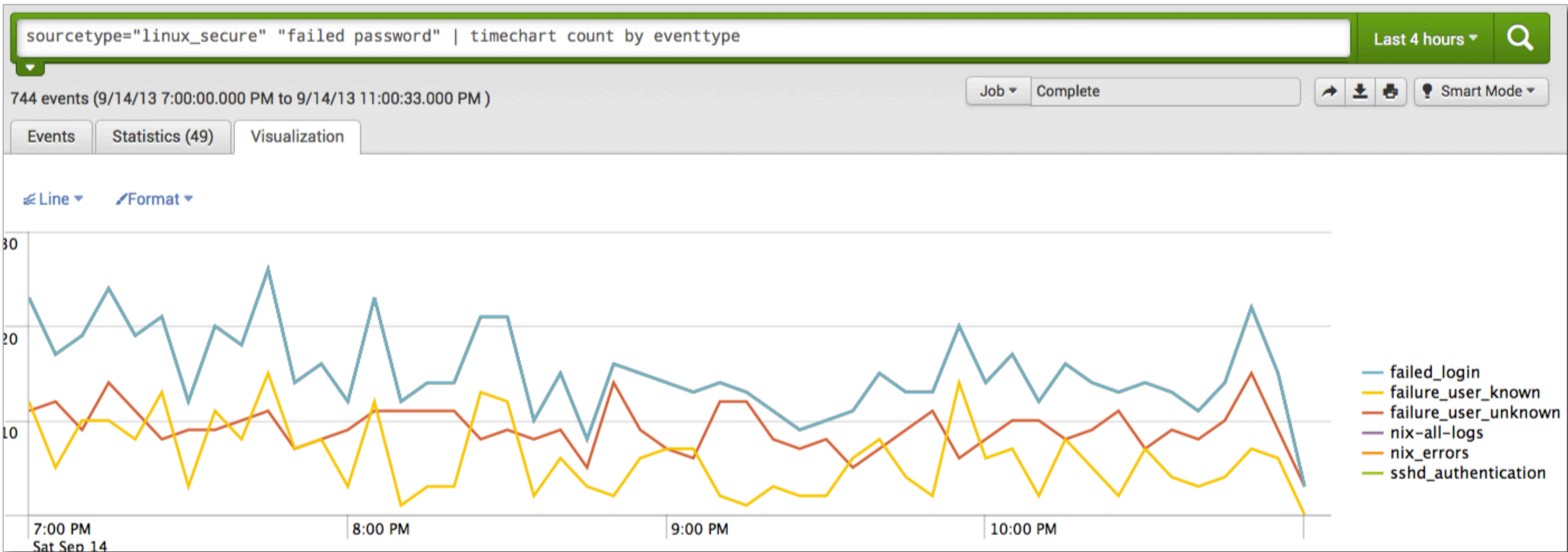
Charts
Top values by time
Top values overall

Values	#	%	
failed_login	82	100%	
nix-all-logs	82	100%	
nix_errors	82	100%	
sshd_authentication	82	100%	
failure_user_unknown	62	75.61%	
failure_user_known	20	24.39%	

9/14/13 2:17:14.000 PM **Sat Sep 14 14:17:14 mailsv1 sshd[3958]: Failed password for invalid user sapadmin from 187.231.45.62 port 2945 ssh2**
host=mailsv1 ▾

9/14/13 2:17:11.000 PM **Sat Sep 14 14:17:11 mailsv1 sshd[2198]: Failed password for apache from 187.231.45.62 port 3629 ssh2**
host=mailsv1 ▾

But Wait, There's More!



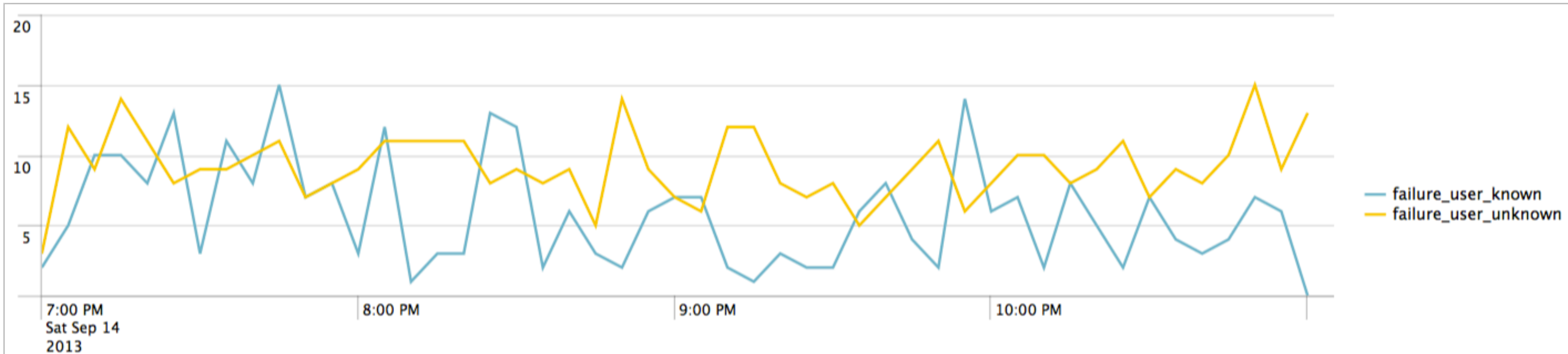
Eliminating the Extraneous Event Types

```
sourcetype="linux_secure" "failed password" | timechart count by eventtype | fields _time, failure_user_unknown, failure_user_known
```

OR

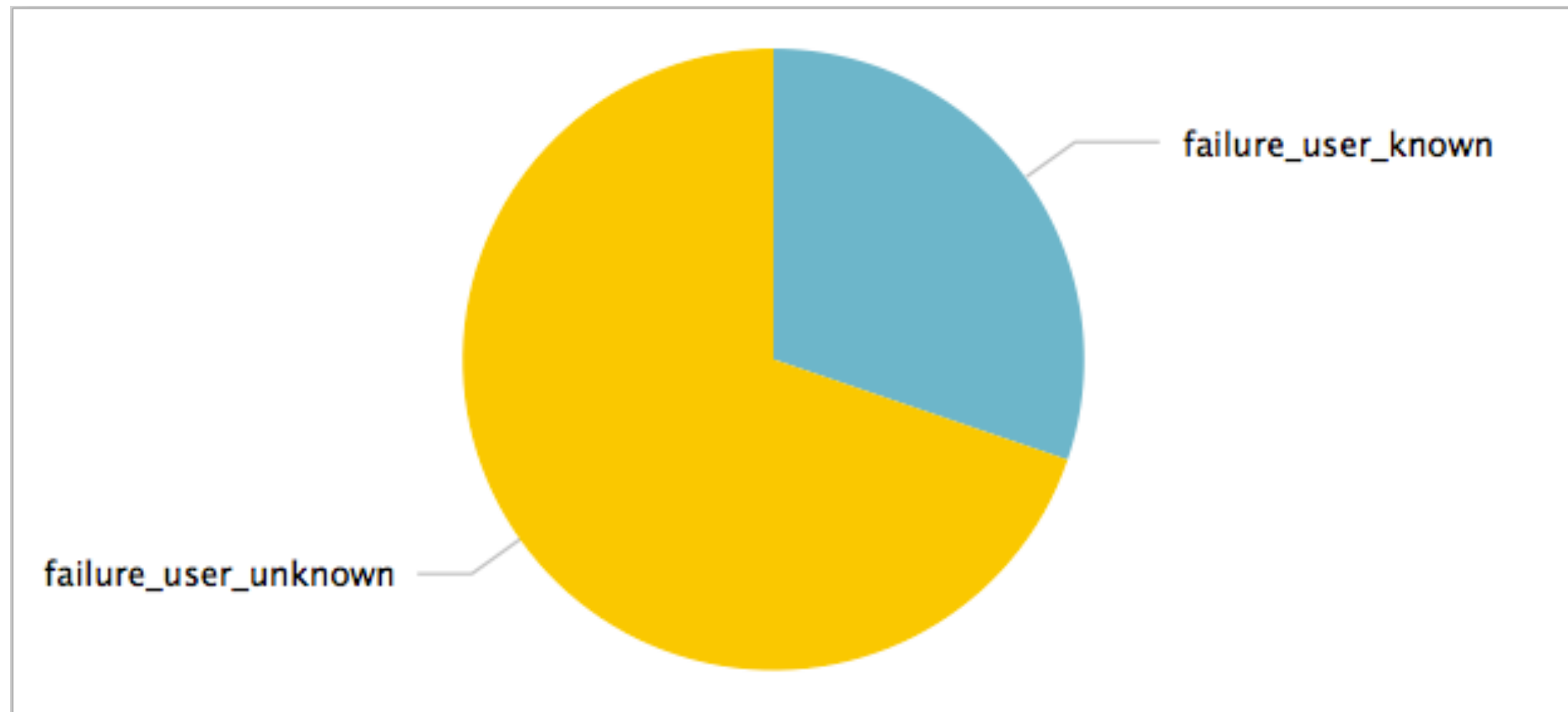
```
sourcetype="linux_secure" "failed password" | timechart count by eventtype | fields - failed*, n*, s*
```

The Finished Product!



Or Perhaps?

```
sourcetype=linux_secure | stats count by eventtype | where eventtype LIKE "failure%"
```





Oh, There's Just One More Thing

If only I could use a wildcard in a tag (and if pigs could fly)...





Oh, There's Just One More Thing

If only I could use a wildcard in a tag (and if pigs could fly)...

The screenshot shows the Splunk search interface. At the top left, there is a search bar with the text "New Search" and a magnifying glass icon. Below the search bar, the search query "host=www*" is entered and highlighted with a red box and a blue circle containing the number "1". To the right of the search bar, there is a "Save As" dropdown menu highlighted with a green box and a blue circle containing the number "2". The dropdown menu is open, showing options: "Report", "Dashboard Panel", "Alert", and "Event Type". The "Event Type" option is highlighted with a red box and a blue circle containing the number "3". Below the search bar, there is a status bar showing "1,041 events (9/14/13 7:26:00.000 PM to 9/14/13 11:26:58.000 PM)" and a "Job" dropdown menu set to "Complete". At the bottom of the search bar, there are three tabs: "Events (1,041)", "Statistics", and "Visualization".

Apply a Tag to the Event Type

Save As Event Type

4 Name web_servers

Search String host=www*

5 Tags web_server

Color none ▼

Priority 5 ▼

Determines which style wins, when an event has more than one event type.

Cancel Save

6

Search for the Event Type

The screenshot shows a Splunk search interface. At the top, a search bar contains the query `tag=web_server`, which is highlighted with a red box. Below the search bar, it indicates that 15,838 events were found for the time range from 9/9/13 1:00:00.000 AM to 9/16/13 1:39:01.000 AM. The interface has tabs for 'Events (15,838)', 'Statistics', and 'Visualizations'. The 'Statistics' tab is active, showing a 'host' field with 3 values representing 100% of the events. A 'Reports' section offers options like 'Top values' and 'Events with this field'. A table titled 'Values' lists the top three host values: 'www2' (5,579), 'www3' (5,283), and 'www1' (4,976). The 'www2' and 'www3' rows in this table are highlighted with a green box. On the left side, there are sections for 'Selected Fields' (showing 'host 3') and 'Interesting Fields' (listing 'action 7', 'app 2', 'bytes 100+', and 'categoryId 8').

tag=web_server

15,838 events (9/9/13 1:00:00.000 AM to 9/16/13 1:39:01.000 AM)

Events (15,838) Statistics Visualizations

Format Timeline ▾

Hide Fields All Fields

Selected Fields

- host 3

Interesting Fields

- action 7
- app 2
- bytes 100+
- categoryId 8

host

3 Values, 100% of events

Reports

- Top values
- Events with this field

Values	Count
www2	5,579
www3	5,283
www1	4,976

Things to Remember About Event Types

- Event type names are case sensitive
- Permissions of event types always default to Private
- Event types consist of simple searches (no search commands)
- Don't go crazy! Excessive event typing can cause degradation of search performance
- You can remove unwanted event types from reports using search commands

.conf2013

**YOUR DATA
NO LIMITS**

Alerts

splunk>

Scenario – 24/7 Monitoring

- Servers and devices run 24/7
- Hackers, bugs, and crashes are lurking 24/7
- Humans aren't 24/7 – they need things like sleep, vacations, lunch, or just a few minutes away from staring at a screen in a freezing cold server room!

Splunk Alerts Never Sleep!

- Searches can be run on a schedule and be setup to “do something” based on the results
- We call these **alerts**

Alerting Scenario – Public User Logins

- Hackers need a user name AND password to access your systems
- Public web pages often contain names of CEOs, sales folks, etc.



Godfrey R. Sullivan
President, Chief Executive Officer and Chairman



Sheren Bouchakian
Vice President Human Resources



David F. Conte
Senior Vice President and Chief Financial Officer



Robin K. Das
Chief Architect and Co-founder



William B. Gaylord
Senior Vice President, Business Development

Create Your Tags

9/15/13 3:45:01.000 PM	Sun Sep 15 2013 15:49 user = gsullivan public
9/15/13 3:42:31.000 PM	Sun Sep 15 2013 15:42 user = sbouchakian public
9/15/13 3:42:07.000 PM	Sun Sep 15 2013 15:42 user = dconte public

Search for the Tag and Create the Alert

The screenshot shows the Splunk 'New Search' interface. At the top left, there is a search bar with the text 'New Search'. To the right of the search bar are two buttons: 'Save As' (highlighted with a green box) and 'Close'. Below the search bar is a search query: 'sourcetype="linux_secure" tag::user="public"'. The entire query is enclosed in a green box, and the tag portion 'tag::user="public"' is specifically highlighted with a red box. Below the search bar, the results are shown as '0 events (9/15/13 11:59:00.000 AM to 9/15/13 3:59:39.000 PM)'. At the bottom of the search bar, there are three tabs: 'Events (0)', 'Statistics', and 'Visualization'. On the right side of the interface, a dropdown menu is open, showing options: 'Report', 'Dashboard Panel', 'Alert' (highlighted with a green box), and 'Event Type'.

Set the Alert Schedule

Save As Alert ✕

Title

Description

Alert type Scheduled

Trigger condition

Number of results is

in

Configure Alert Actions and Permissions

Save As Alert

Enable Actions

List in Triggered Alerts Triggered Alerts is available in the activity menu.

Severity High ▾

Send Email Email must be configured in System Settings > Alert Email Settings. [Learn More](#)

Subject

Email addresses Comma separated list.

Include results None Inline CSV PDF

Run a Script

Action Options

When triggered, execute actions Once For each result

Throttle ?

Cancel Back Save

Alert Created!

Failed Logins for Public Users

Edit ▾

Enabled: Yes. [Disable](#)

Actions: List in Triggered Alerts. [Edit](#)

Alert Type: Real-time. [Edit](#)

App: search

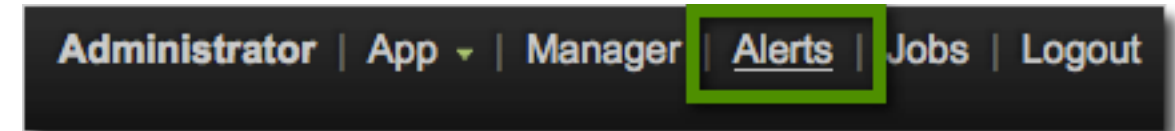
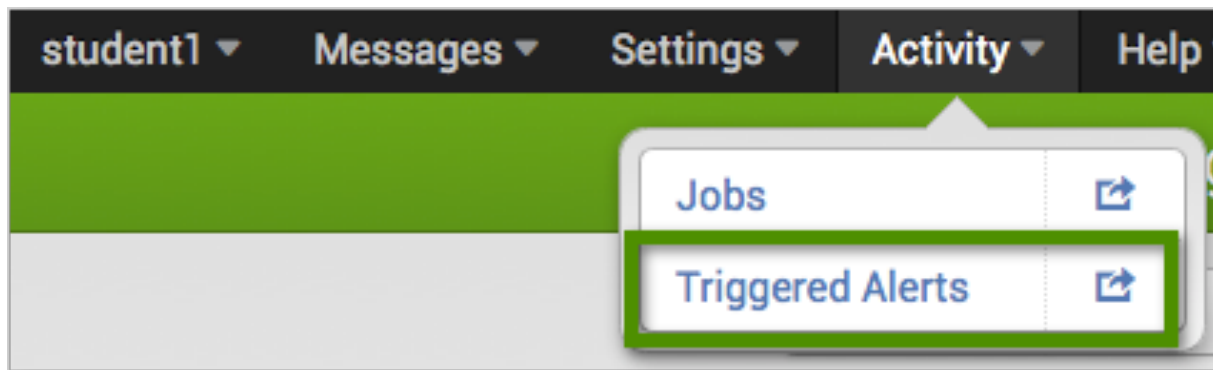
Trigger Condition: Number of Results is > 1 in 30 minutes. [Edit](#)

Permissions: Private. Owned by student1. [Edit](#)

Alert Manager

Splunk Enterprise 6

Splunk Enterprise 5



App Search & Reporting (search) Owner student1 (stude Severity All Alert All

Showing 1-25 of 58 results

Time	Fired alerts	App	Type	Severity	Mode	Actions
2013-09-15 16:22:58 UTC	Failed Logins for Public Users	search	Real-time	High	Digest	View results Edit search Delete
2013-09-15 16:22:56 UTC	Failed Logins for Public Users	search	Real-time	High	Digest	View results Edit search Delete
2013-09-15 16:22:54 UTC	Failed Logins for Public Users	search	Real-time	High	Digest	View results Edit search Delete
2013-09-15 16:22:51 UTC	Failed Logins for Public Users	search	Real-time	High	Digest	View results Edit search Delete
2013-09-15 16:22:49 UTC	Failed Logins for Public Users	search	Real-time	High	Digest	View results Edit search Delete

Questions

lbowser@splunk.com

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!

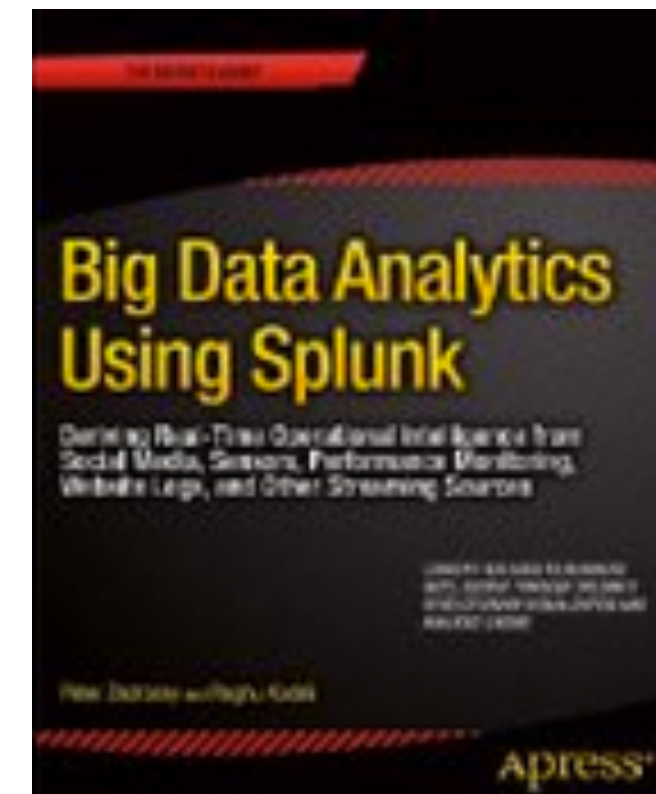
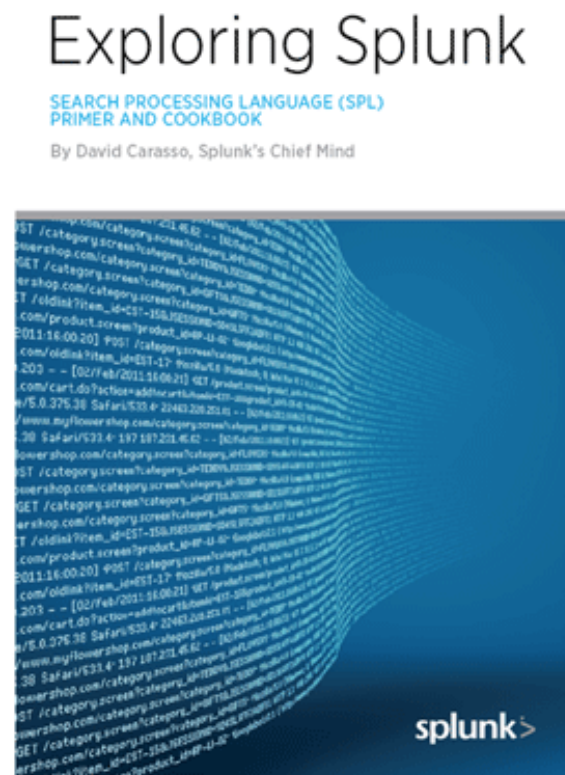
3 Sign up for Splunk Education!



Additional Resources

www.splunk.com/goto/education

- Creating Splunk Enterprise 6 Knowledge Objects (4.5 hour class)
- Searching and Reporting with Splunk (9-hour class)
- Advanced Searching and Reporting with Splunk (9-hour class)



.conf2013

**YOUR DATA
NO LIMITS**

THANK YOU

splunk>

