.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.

About Me

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

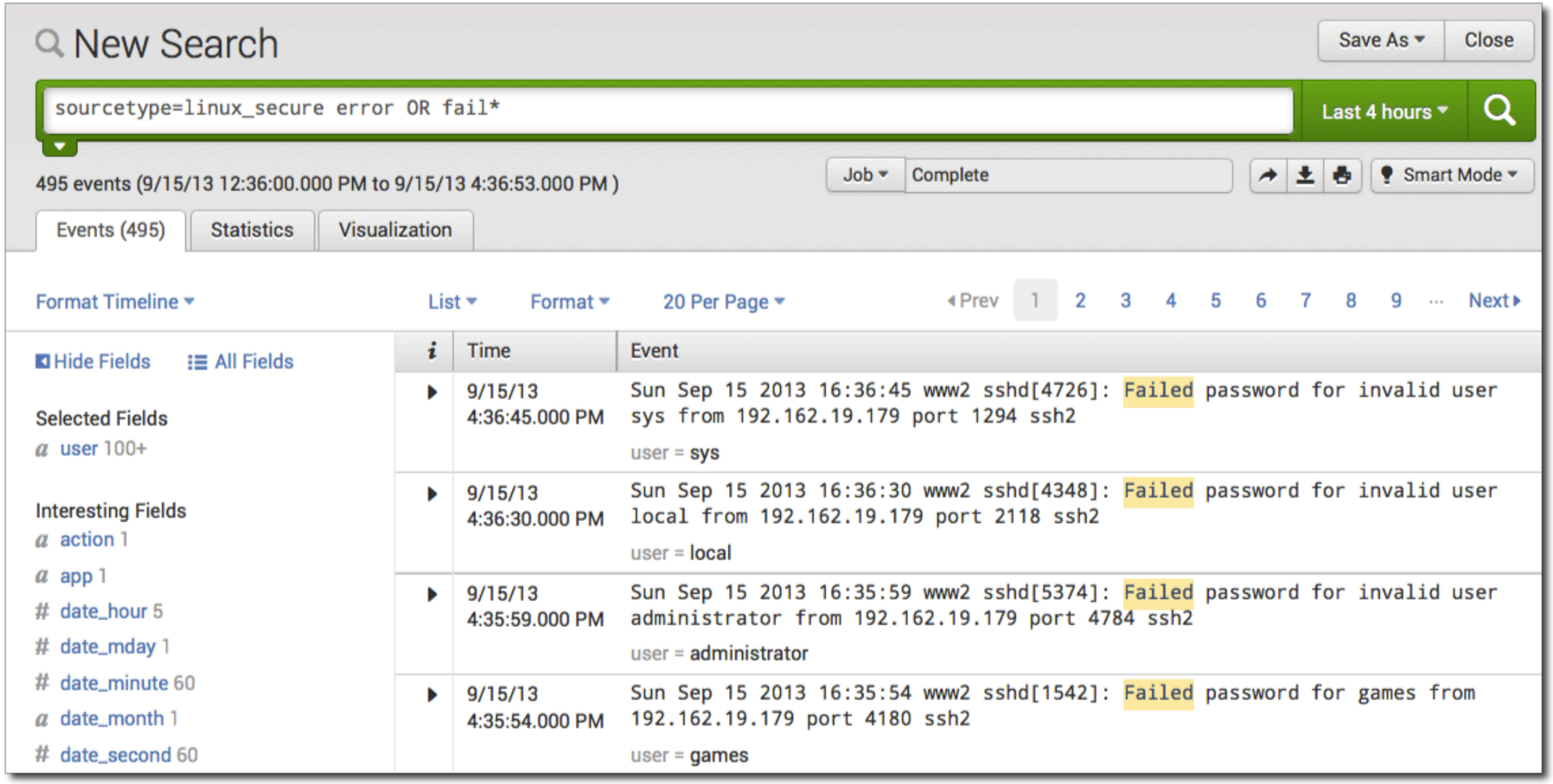
Agenda

- Tags
- Event Types
- Alerts


.conf2013
YOUR DATA
NO LIMITS
Tags
splunk>

Splunk as a “Search Engine”

Type in keywords, hit return, get results …



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"
```

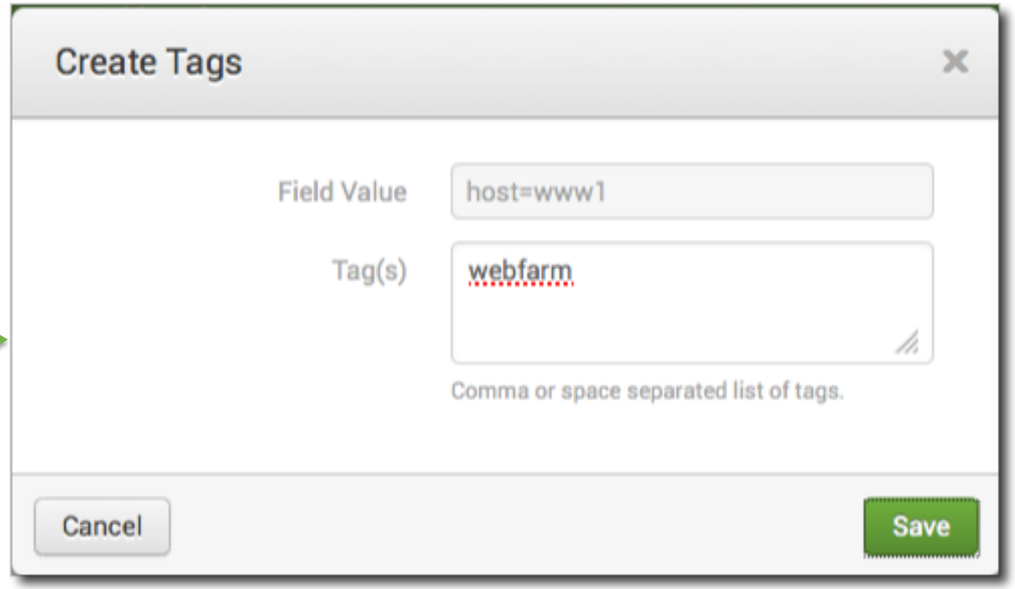
- Sometimes they reflect a theme or hobby

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

Knowledge Objects – Tags to the Rescue

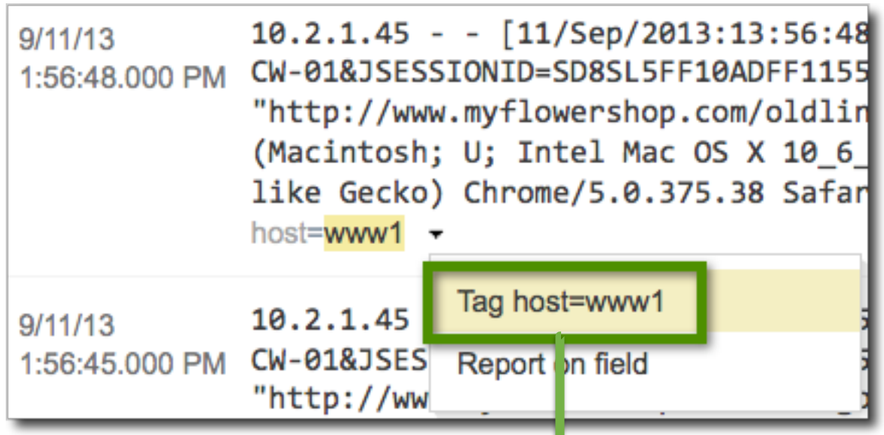
Tags are metadata you can add to specific field / value pairs

Splunk Enterprise 6

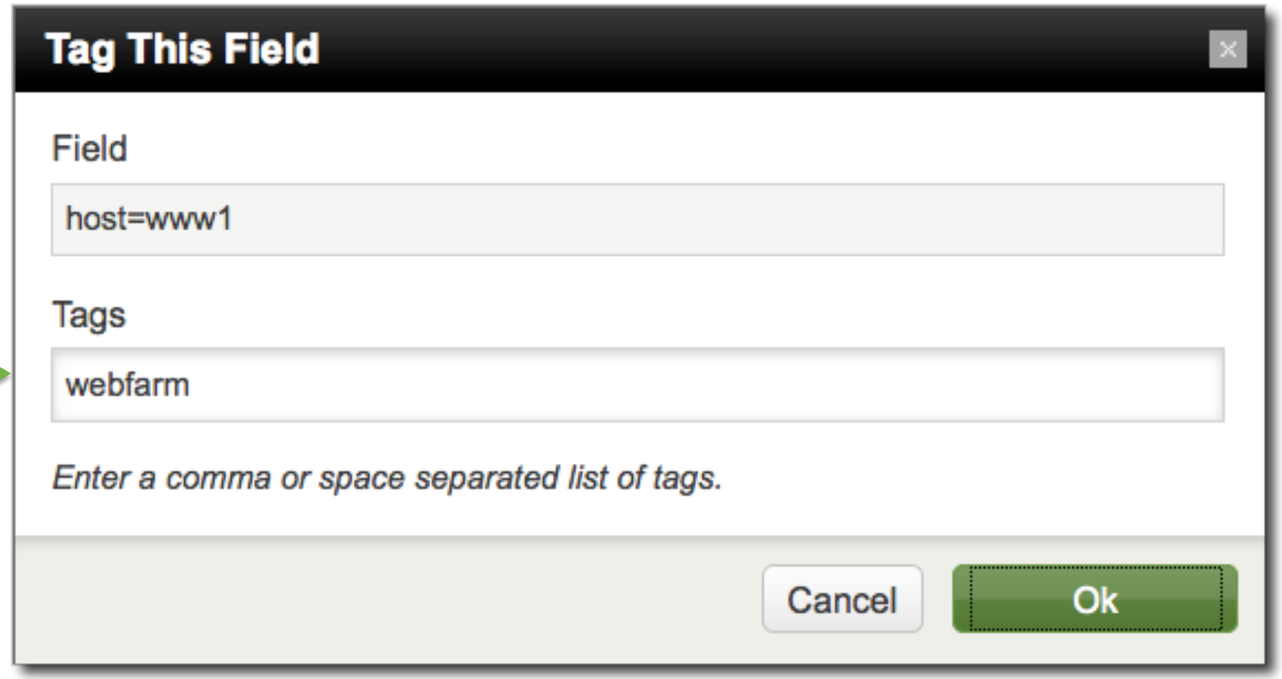


Note: tags are applied to field/value combinations, not fields!

Knowledge Objects – Tags to the Rescue



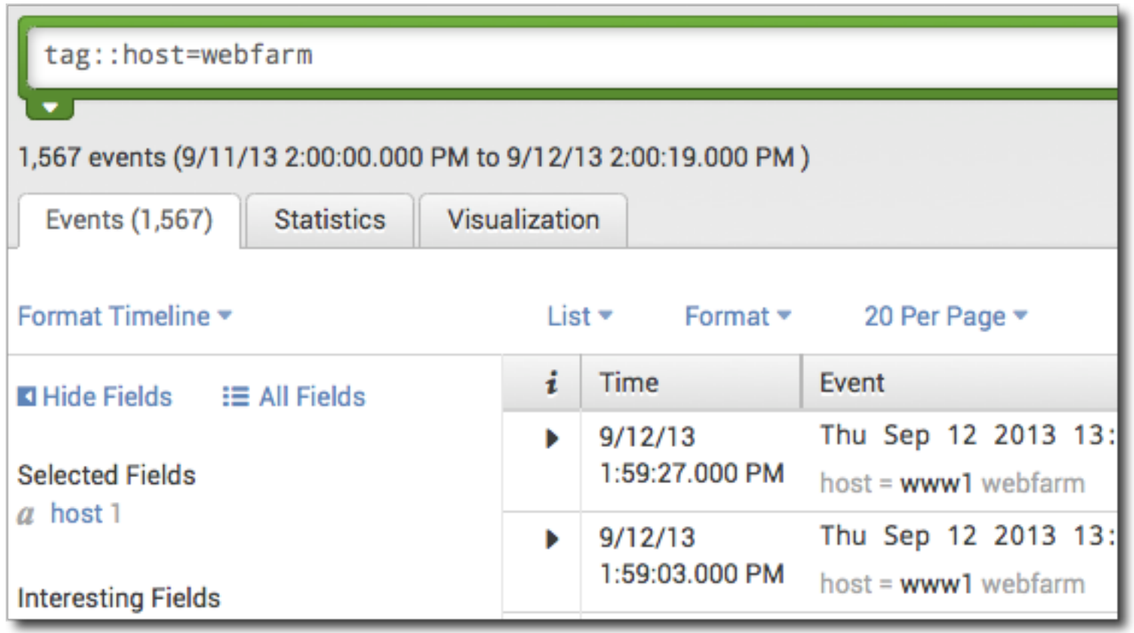
Splunk Enterprise 5



Using Tags

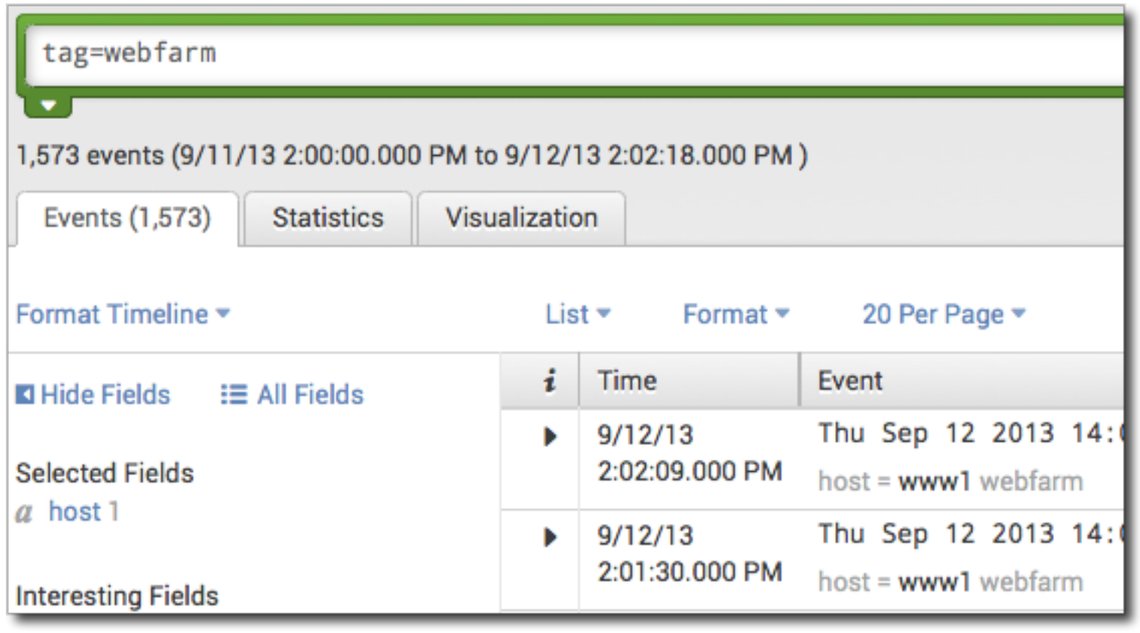
Search all hosts tagged as "webfarm"

Full Syntax



or

Short Form



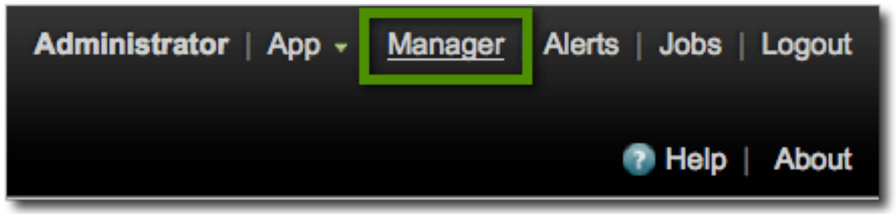
Note: you can use the short form effectively as long as no other fields have the same tag value

But Who Can See/Use My Tags?

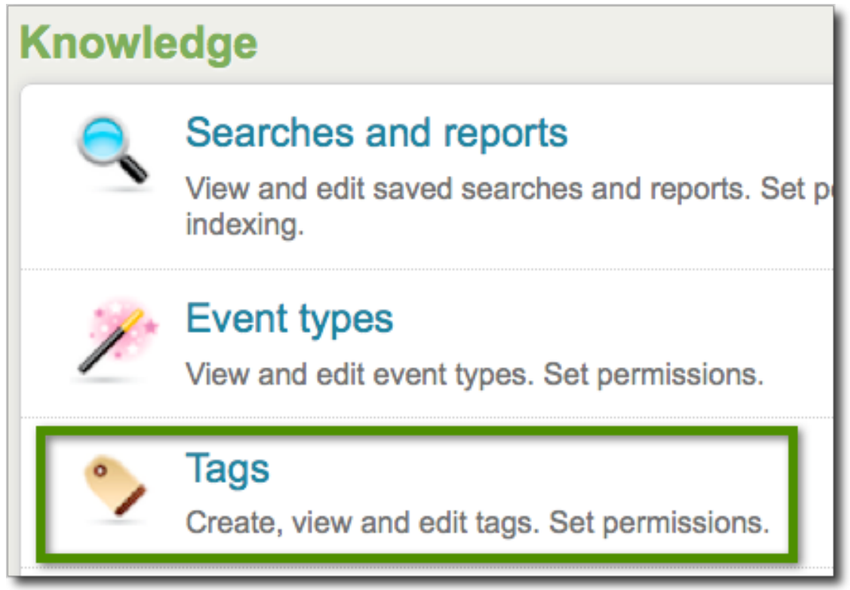
- Initially, tags are created as private knowledge objects
- If you are a power user (or admin) and want other users to see/use your tags, you must share them
  - This is true for all knowledge objects that do not display sharing options upon creation

Sharing Knowledge Objects – 5

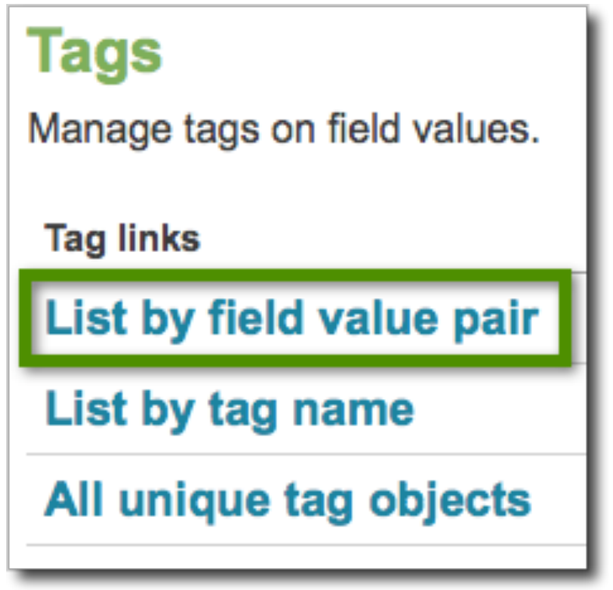
1



2

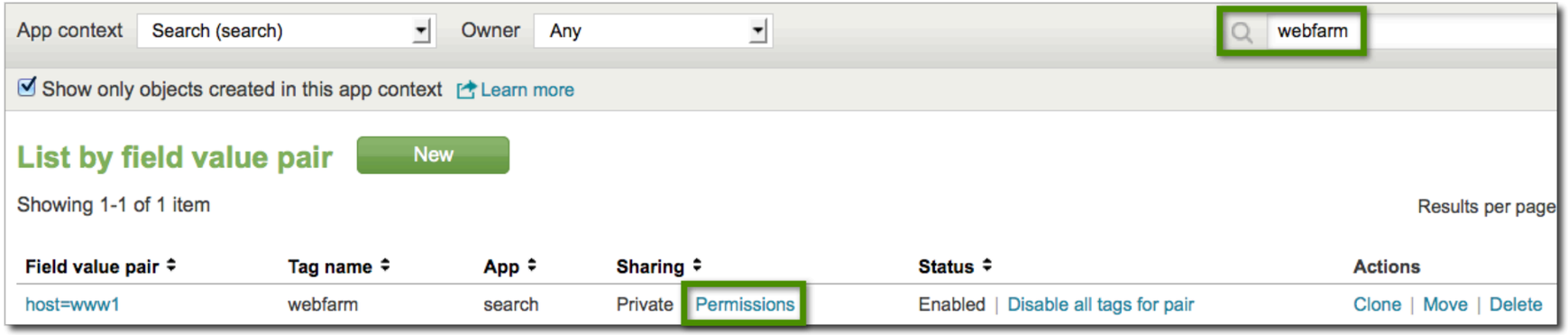


3

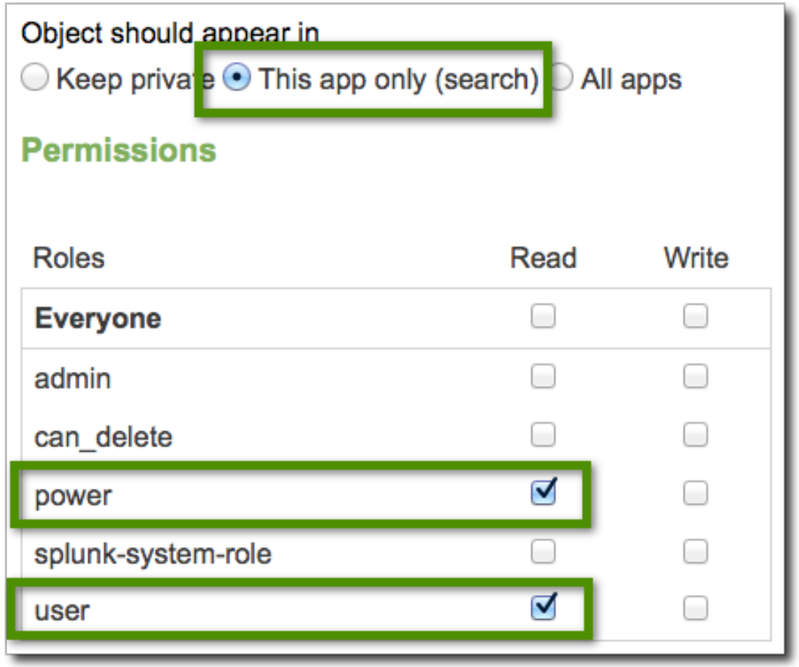


Sharing Knowledge Objects – 5

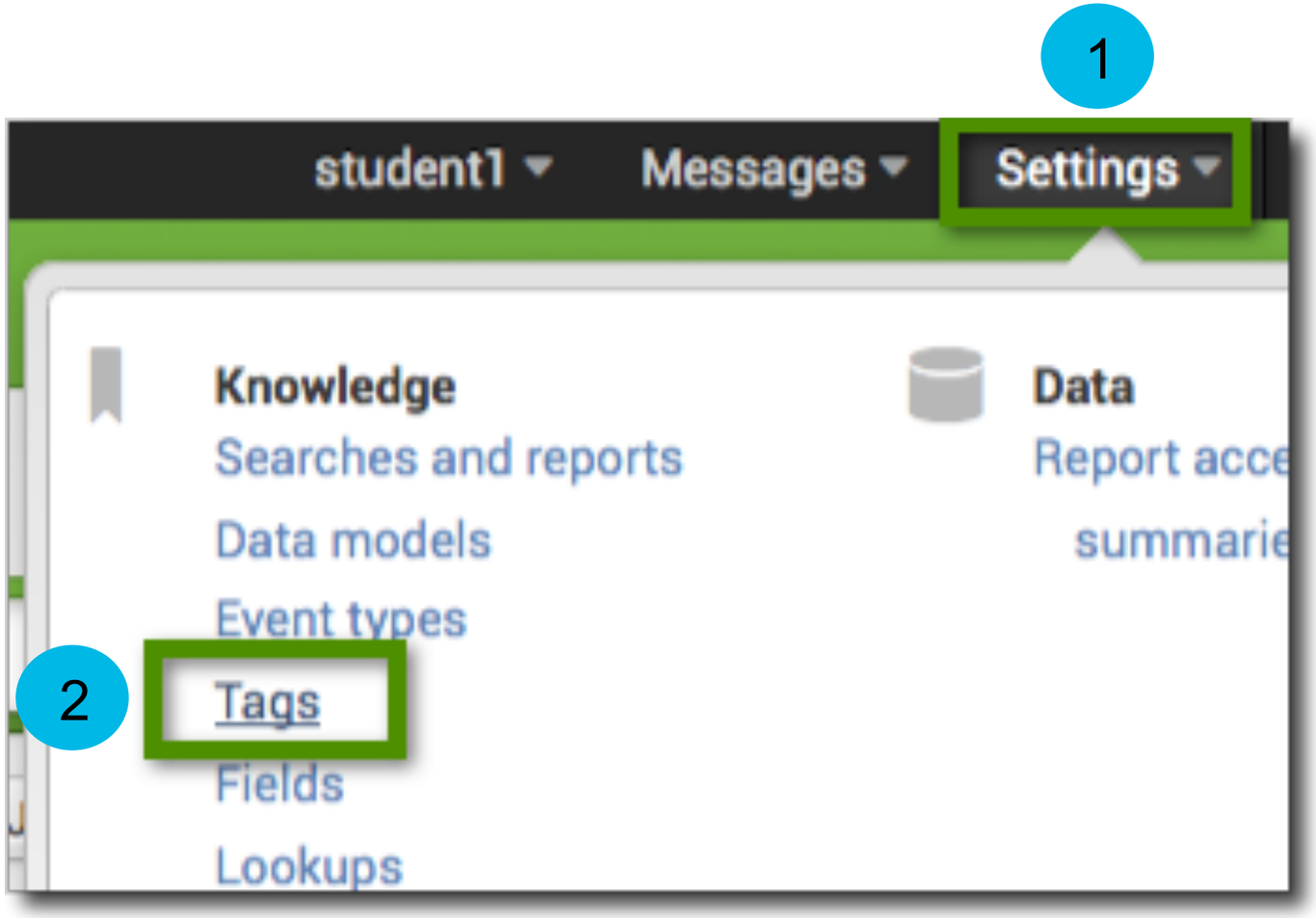
4



5



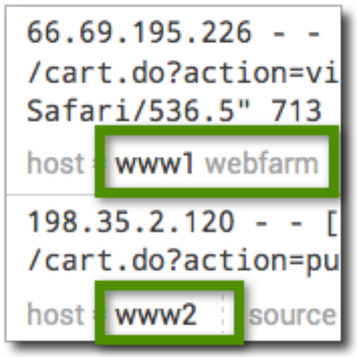
Sharing Knowledge Objects – 6



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



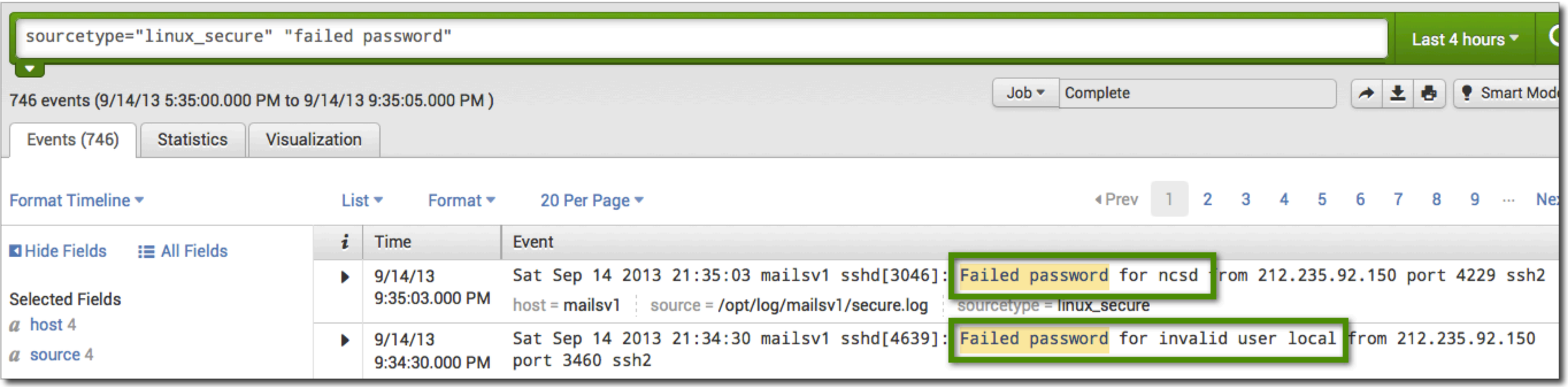
- You cannot use a wildcard to assign a tag across multiple values, but ...


.conf2013
YOUR DATA
NO LIMITS
Event Types
splunk>

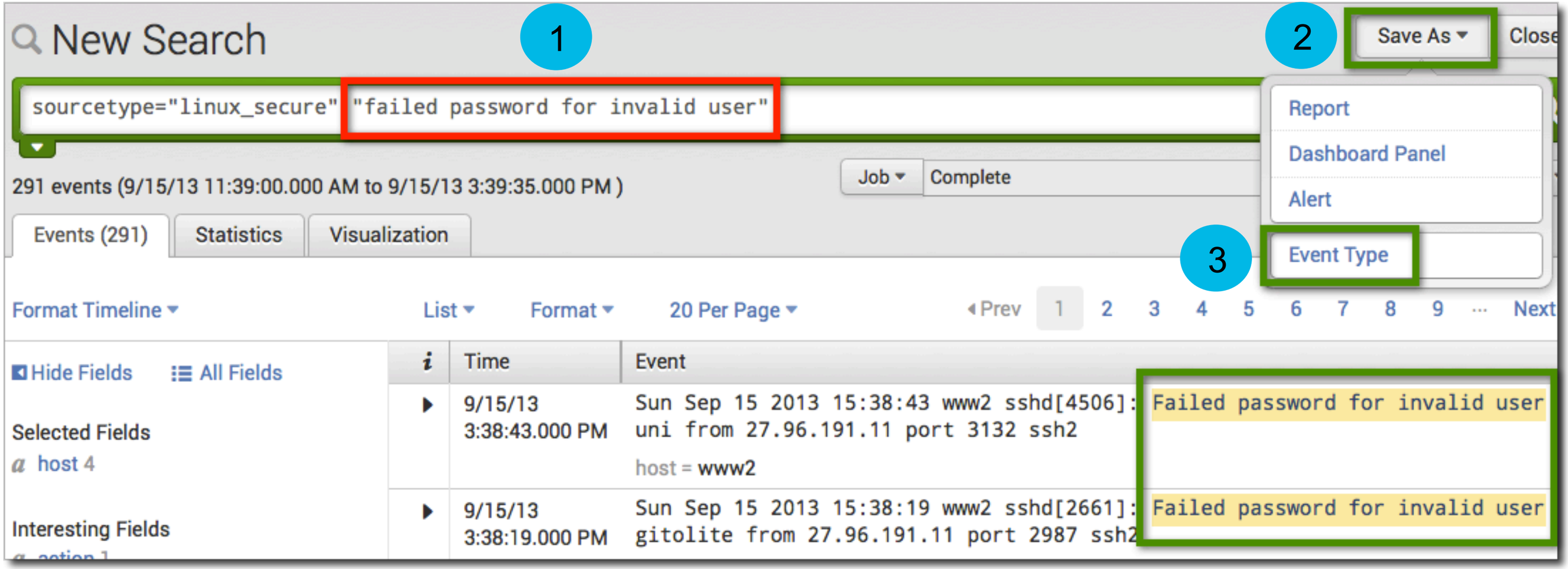
Knowledge Objects – Event Types

- 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

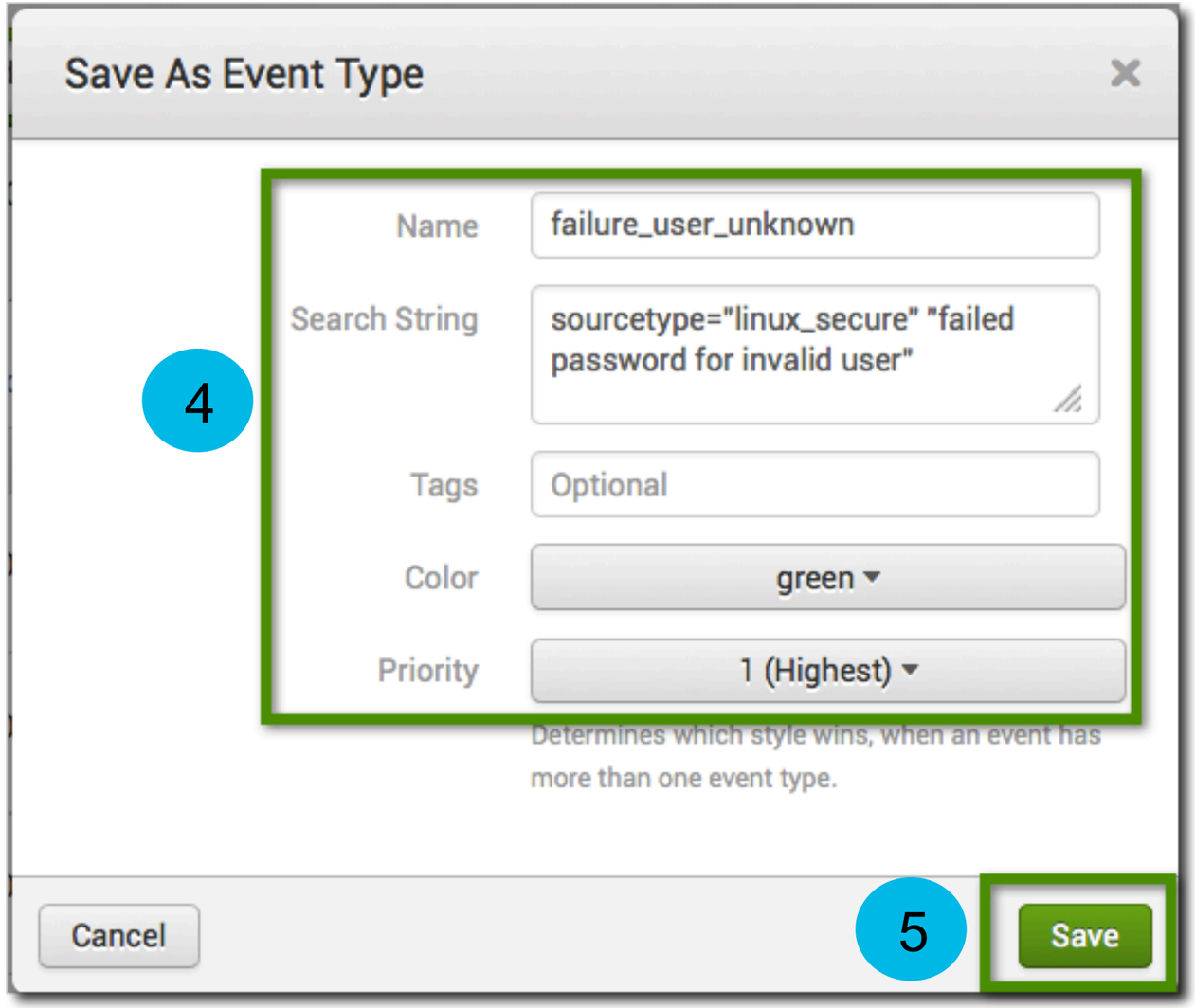
Classifying Groups of Events



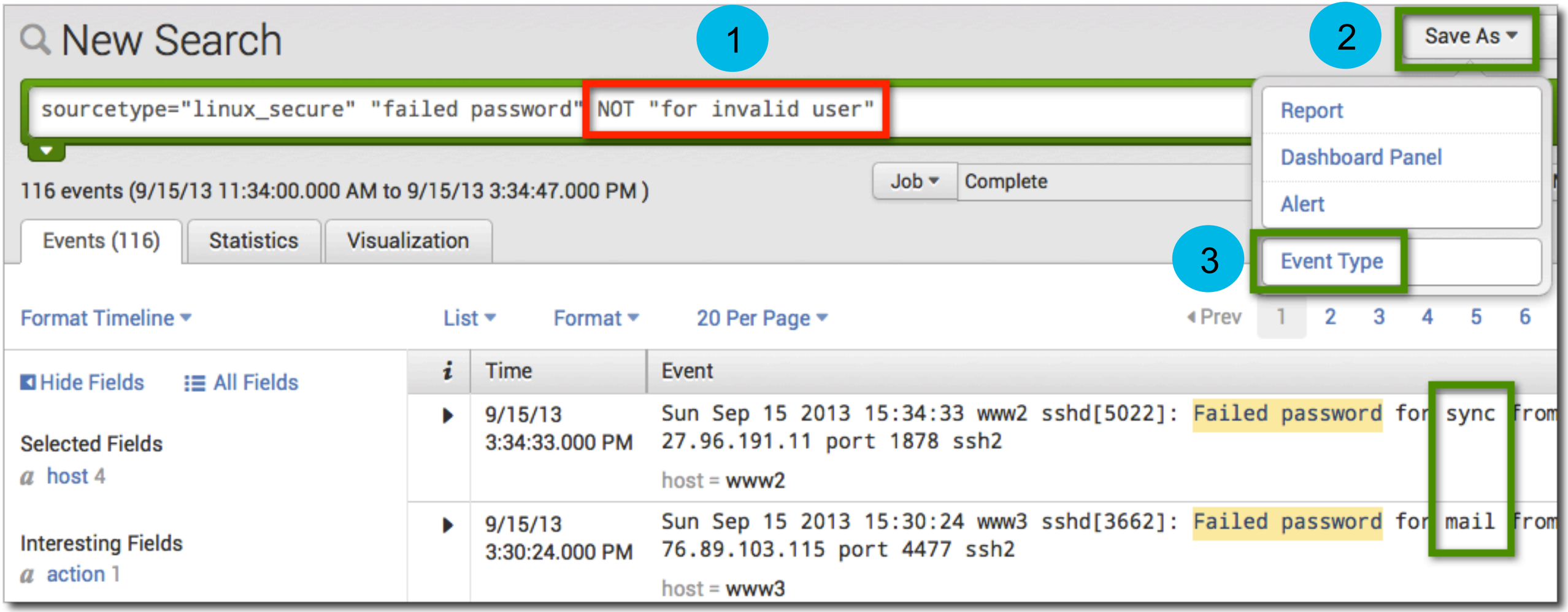
Create Event Type for Unknown Login



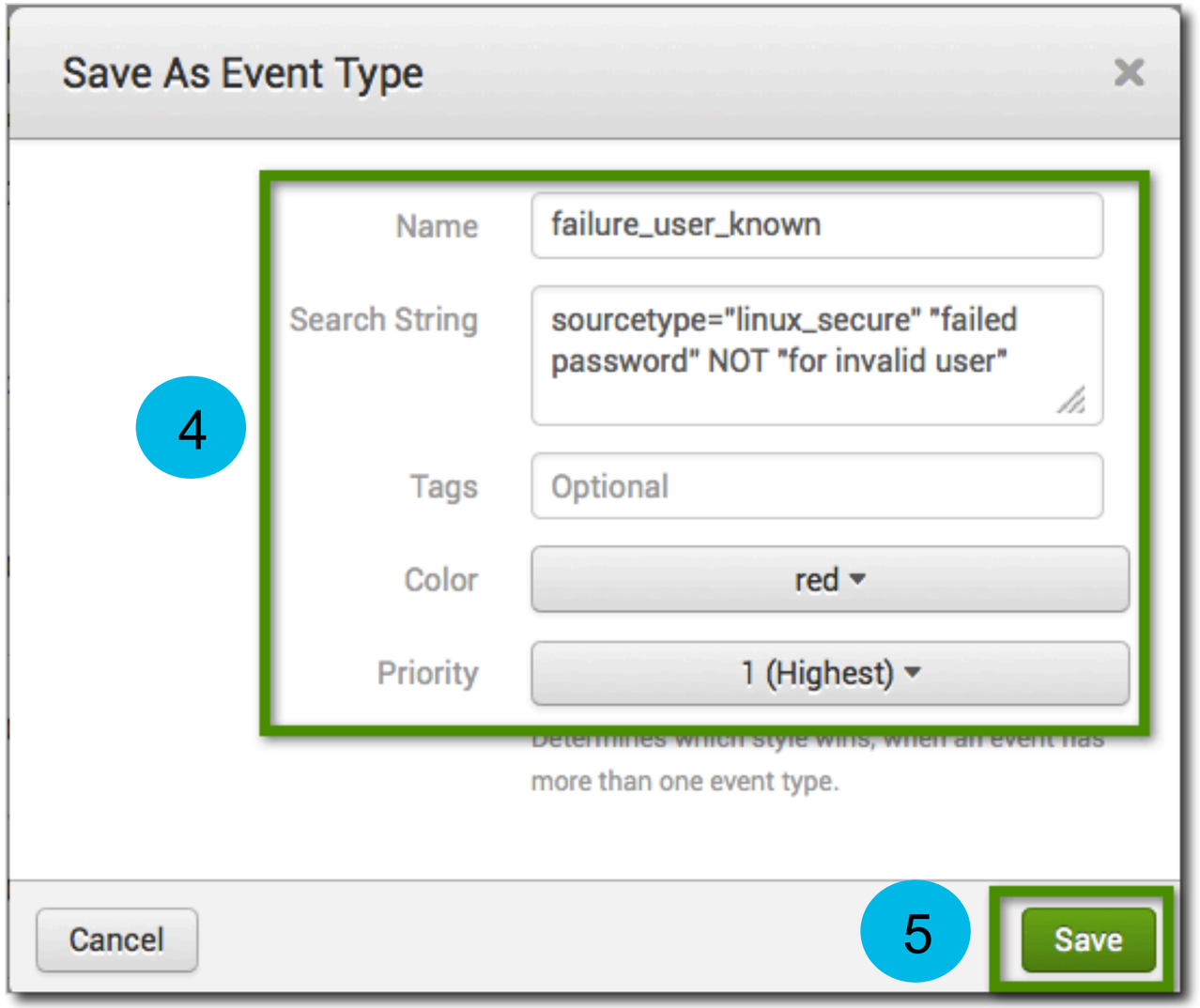
Create Event Type for Unknown Login



Create Event Type for Known Login

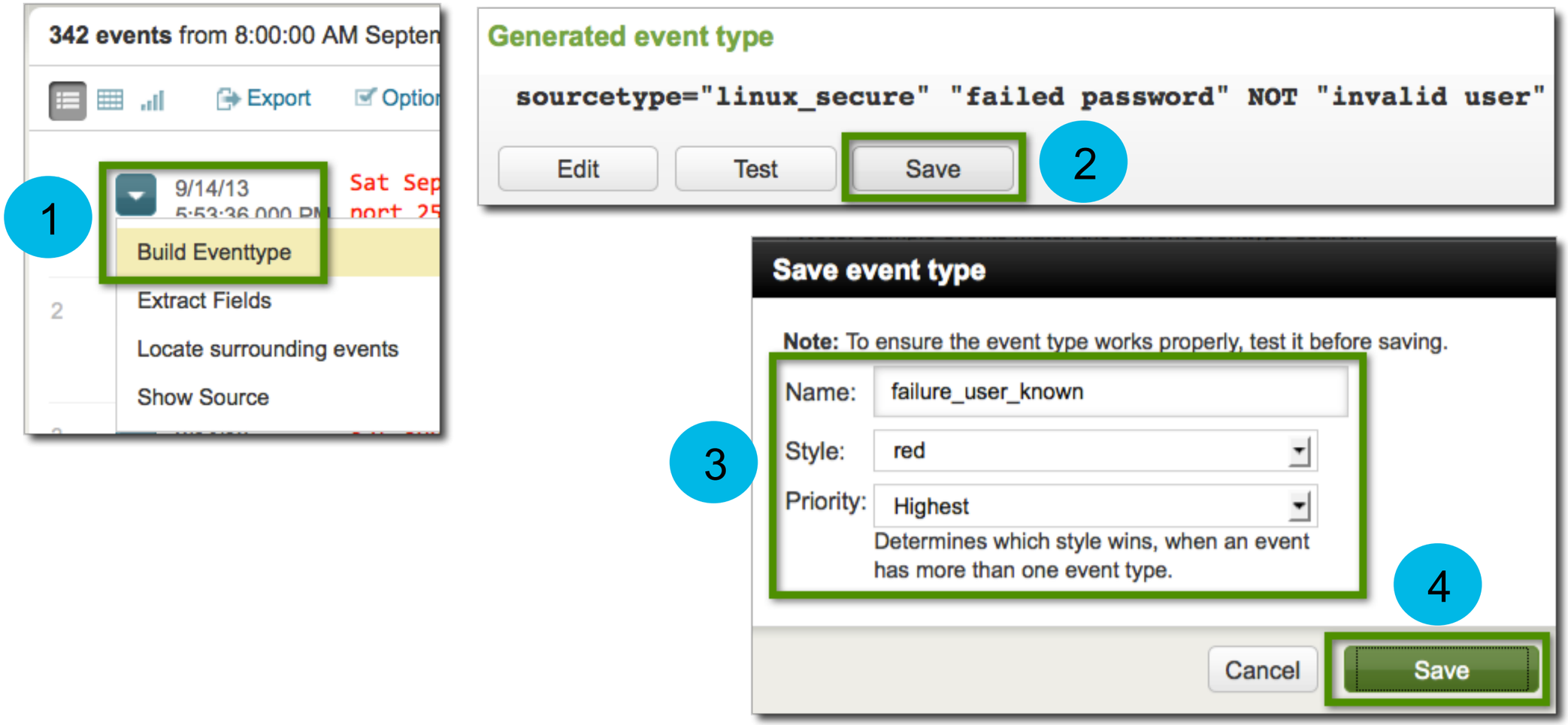


Create Event Type for Known Login



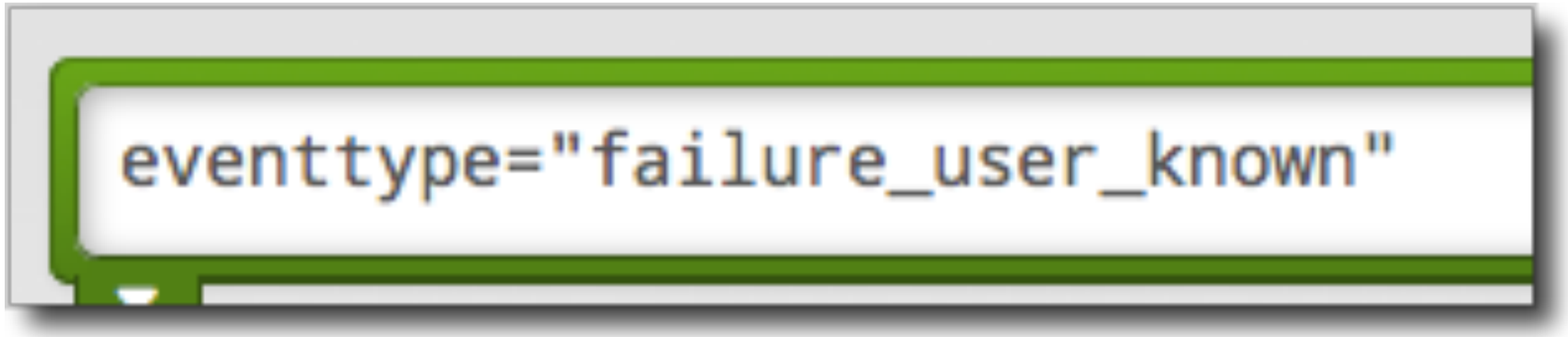
Color Coding Events in 5

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



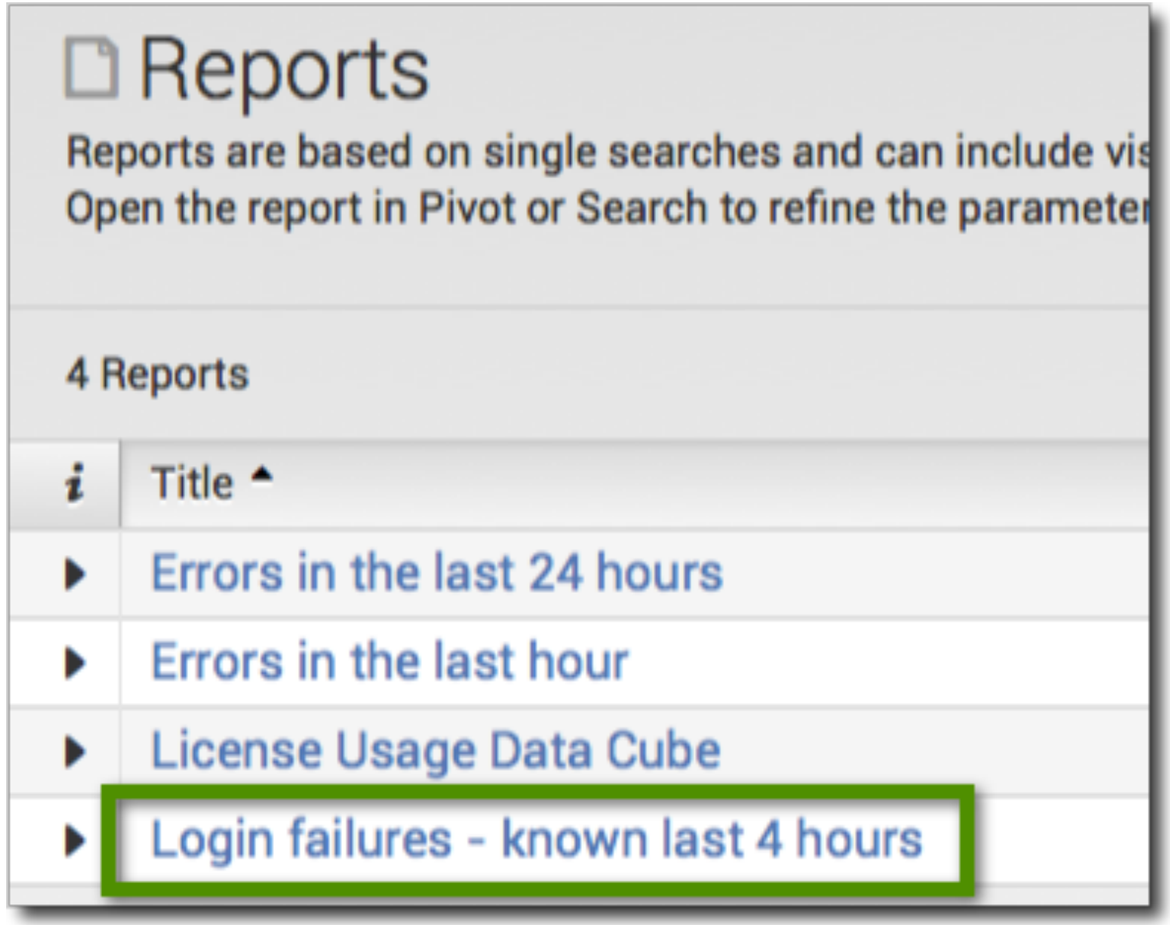
OK, So Now What?

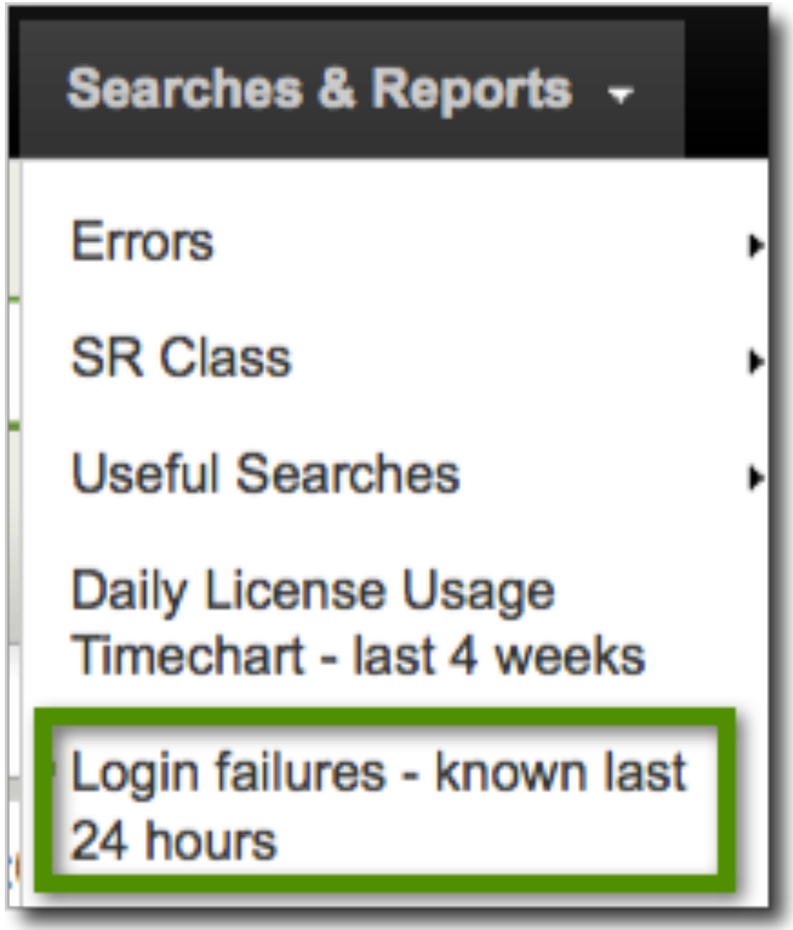
Now you can search using the **eventtype** field



What's the Big Deal?

Because using a report (saved search) is easier

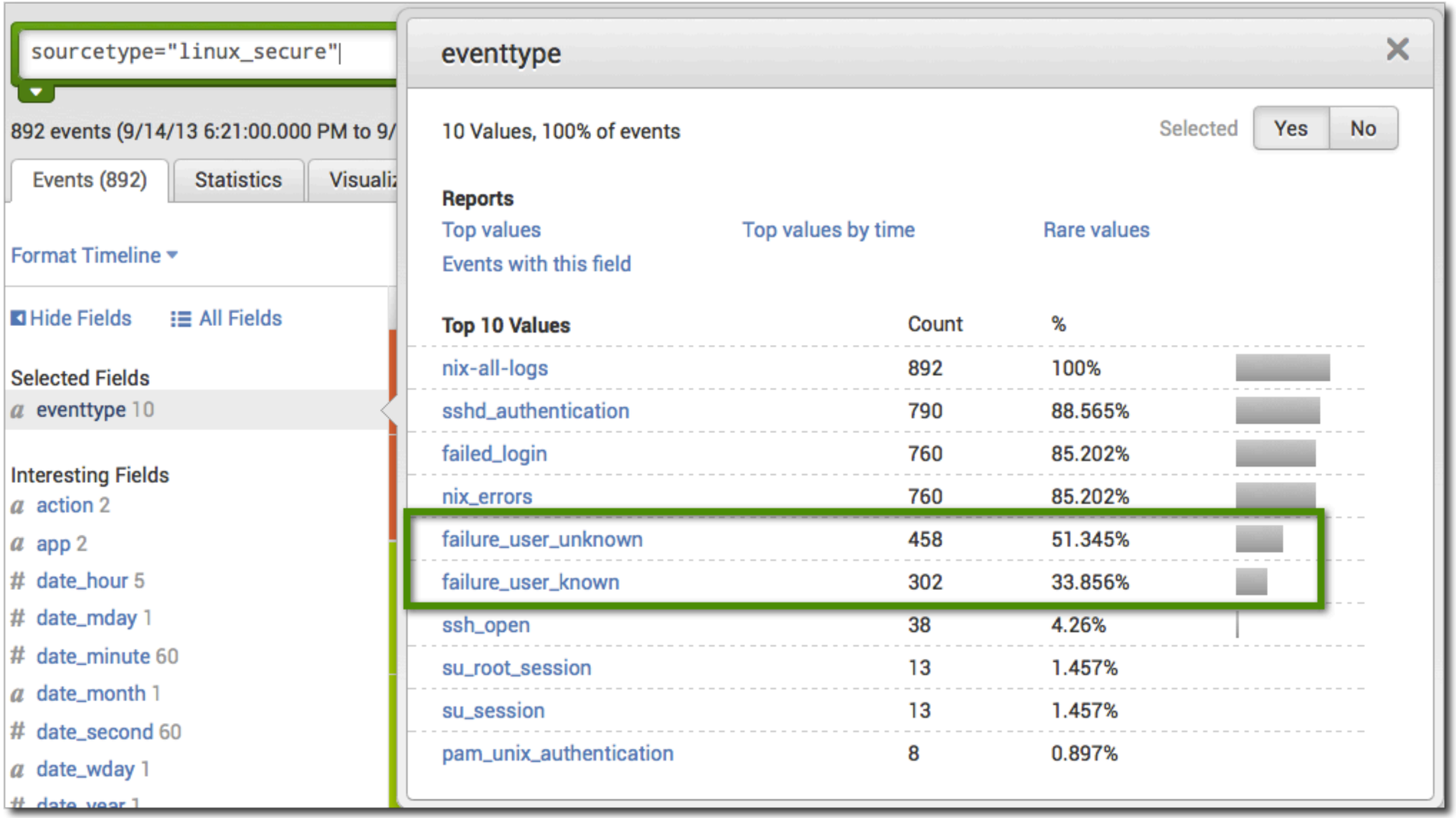




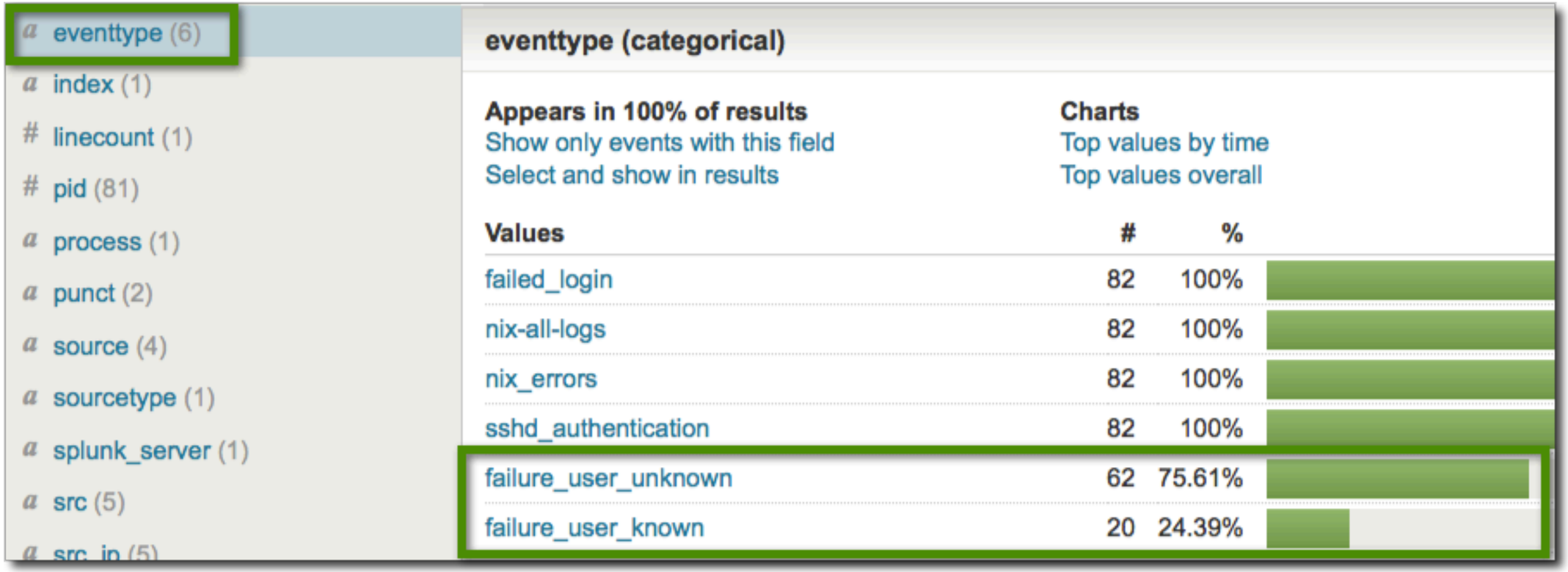
Here's the Value – Splunk Enterprise 6

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

Here's the Value – Splunk Enterprise 6



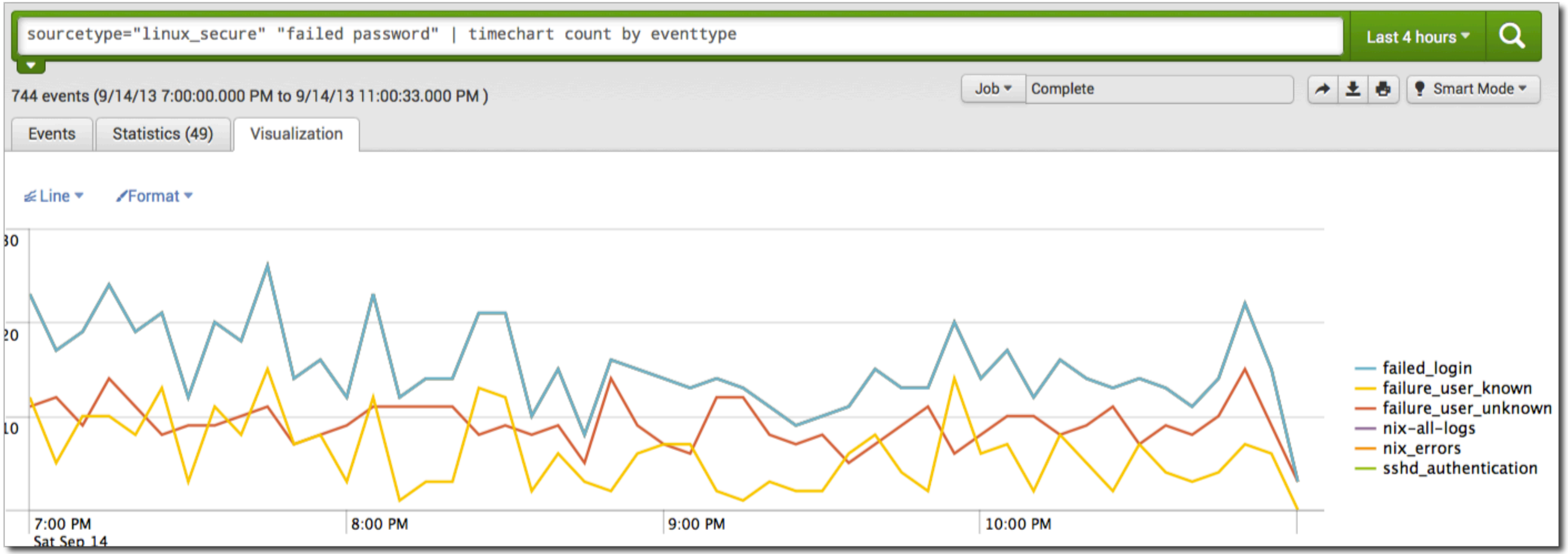
Here's the Value – Splunk Enterprise 5



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!



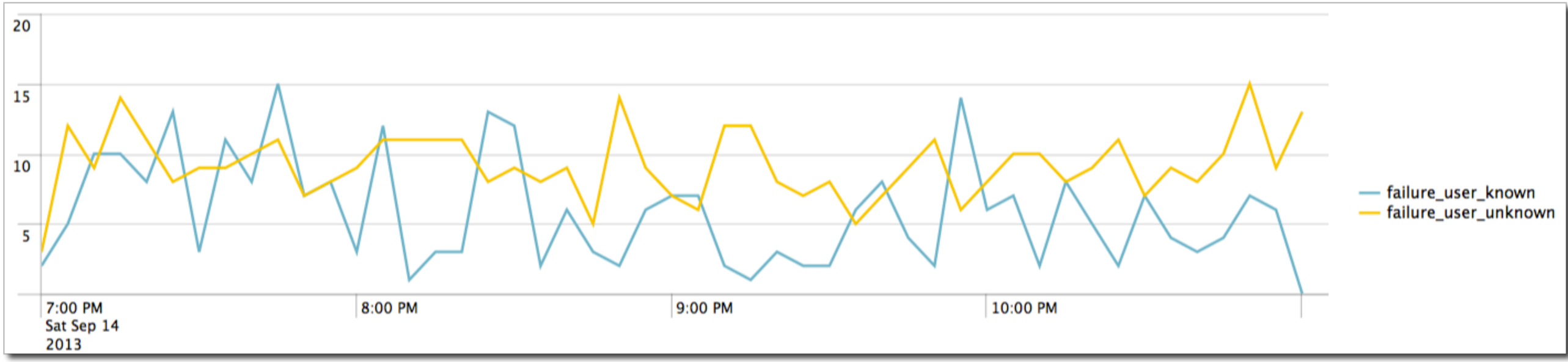
Eliminating the Extraneous Event Types

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

OR

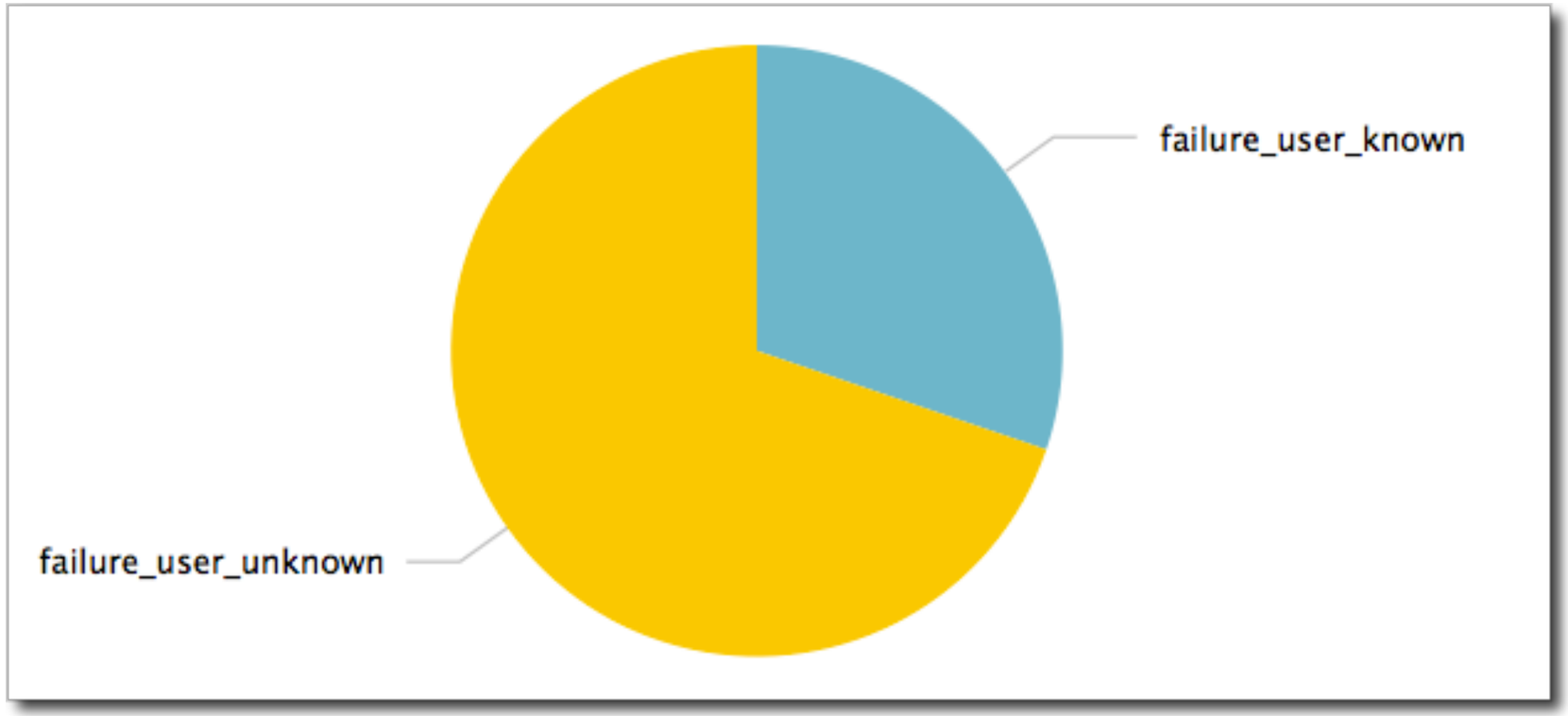
```
sourcetype="linux_secure" "failed password" | timechart count by eventtype | fields - failed*, n*, s*
```

The Finished Product!



Or Perhaps?

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

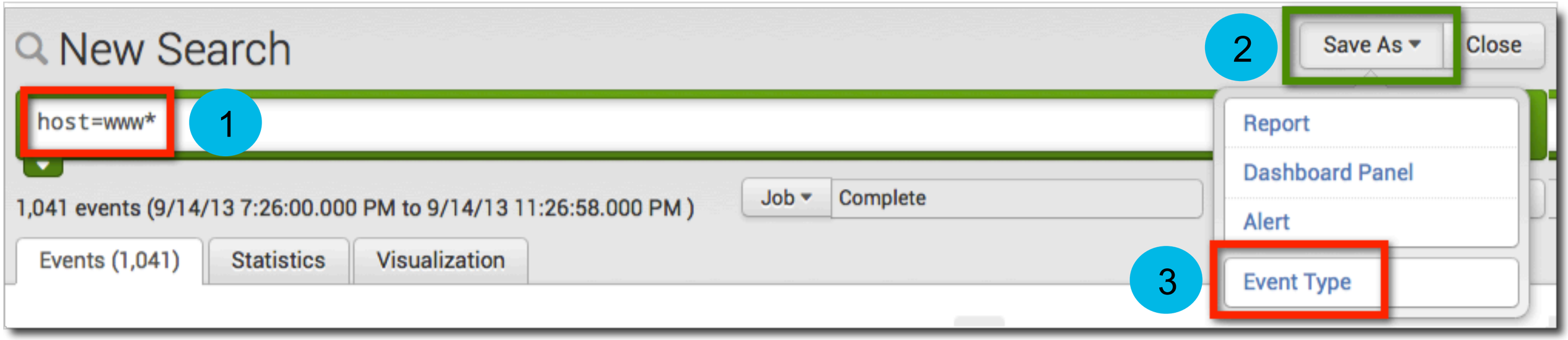


Oh, There's Just One More Thing

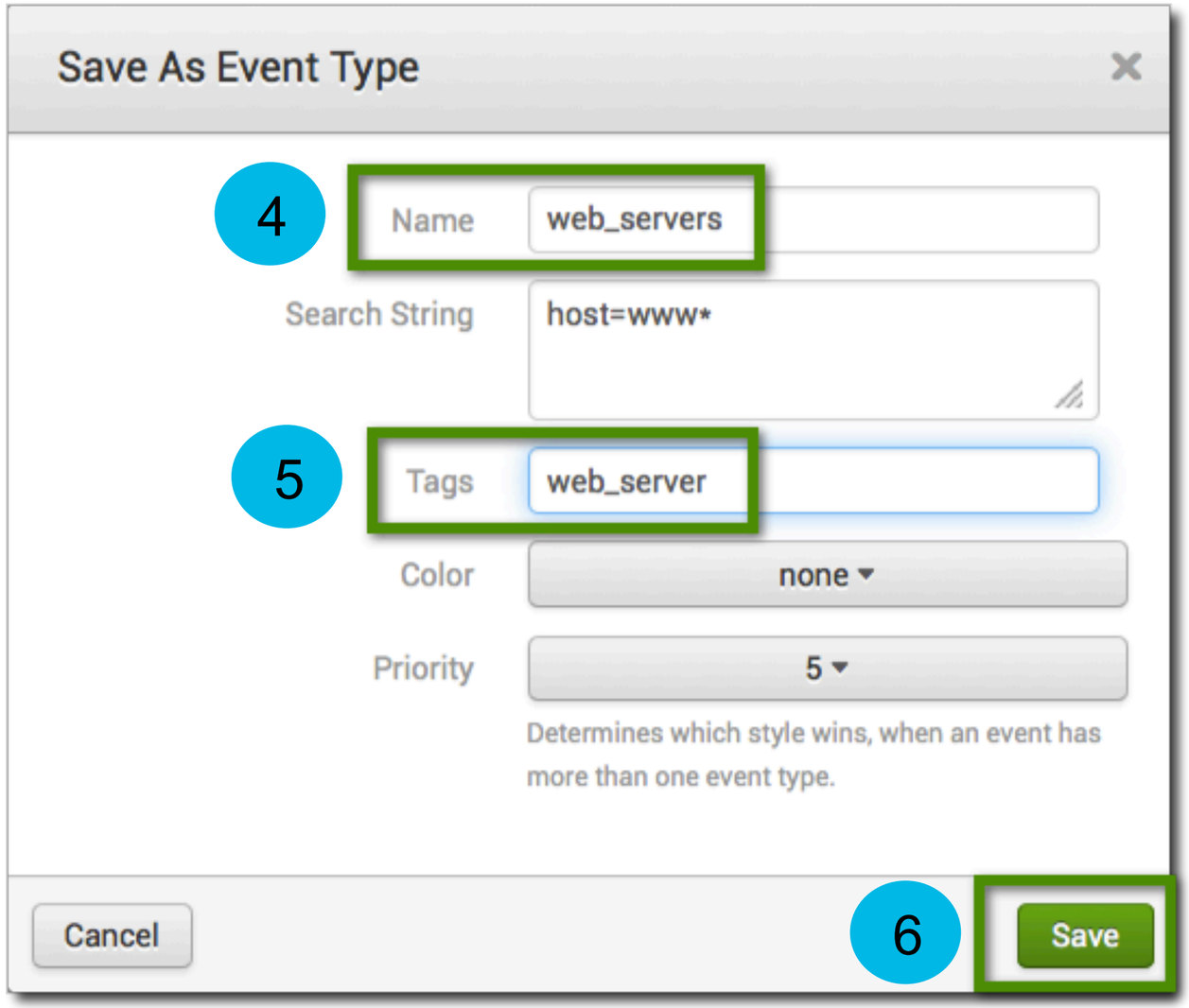
If only I could use a wildcard in a tag (and if pigs could fly)...

Oh, There's Just One More Thing

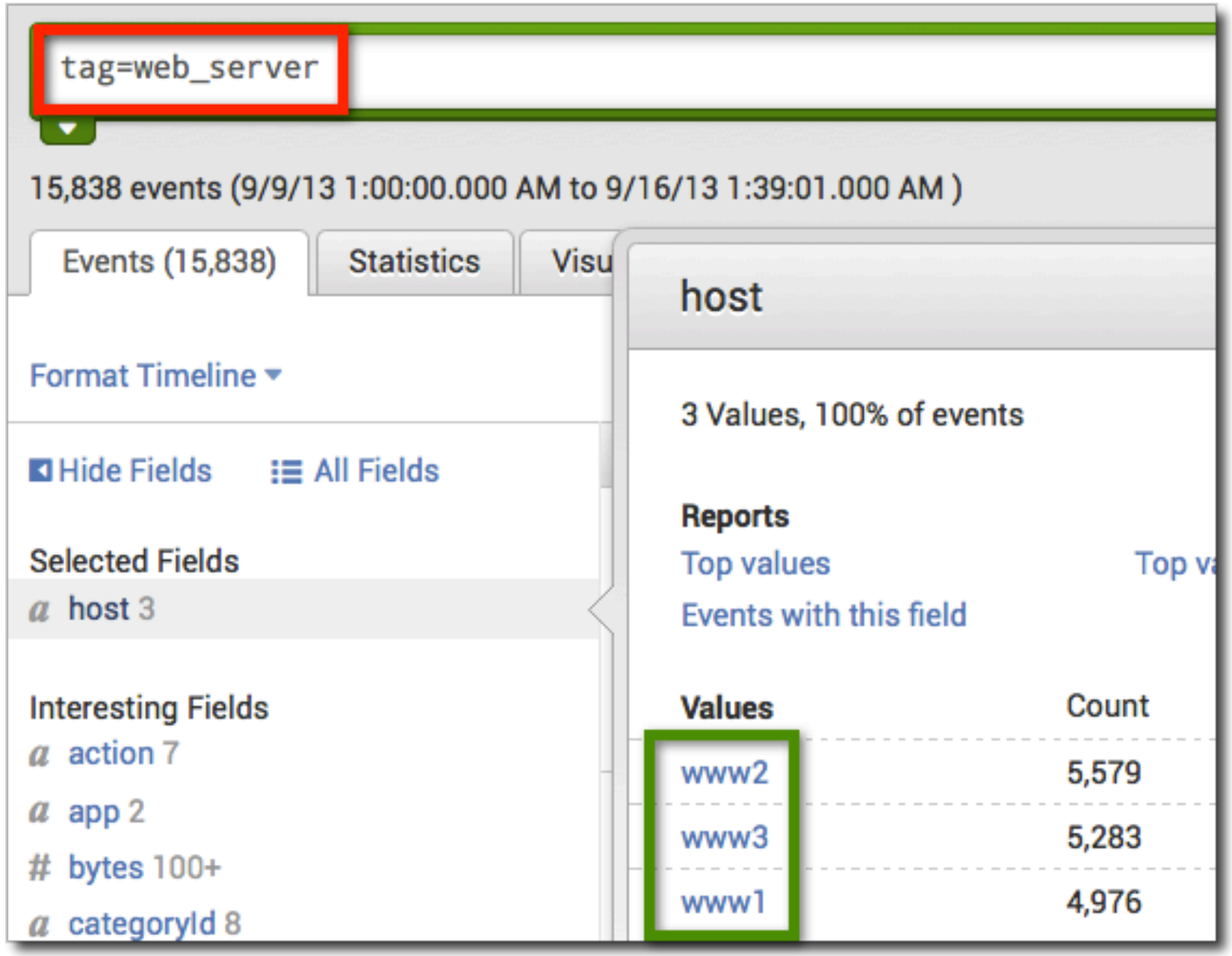
If only I could use a wildcard in a tag (and if pigs could fly)...



Apply a Tag to the Event Type



Search for the Event Type



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

Alerts

Scenario – 24/7 Monitoring

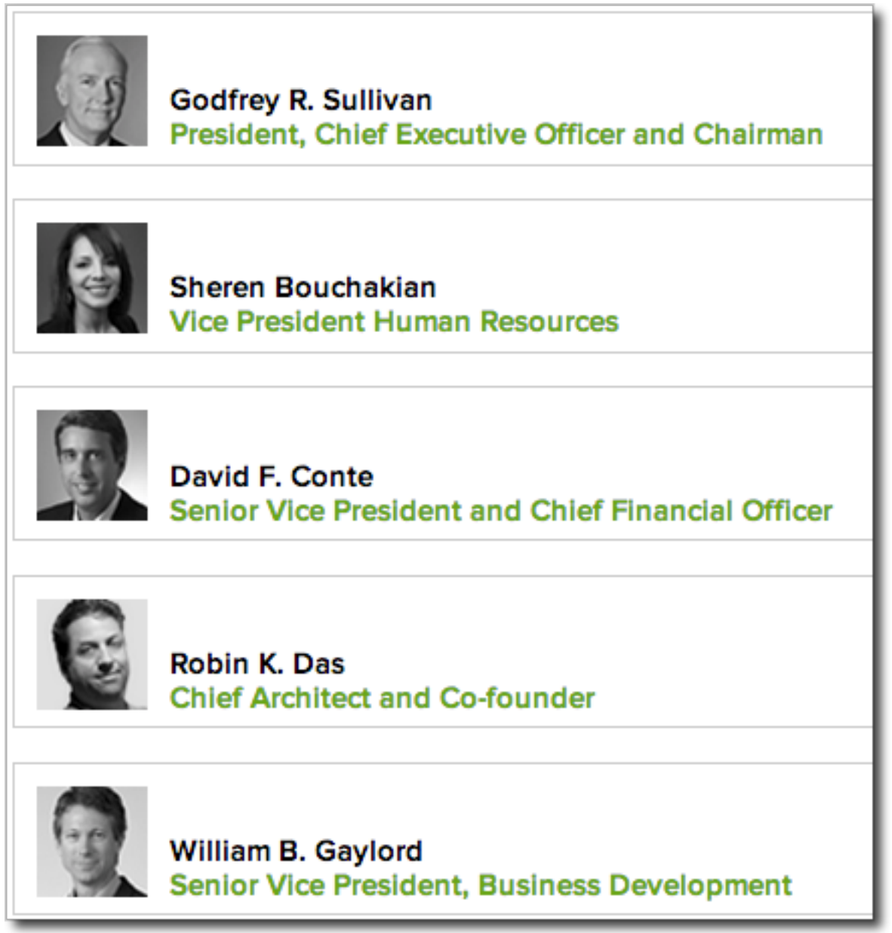
- Servers and devices run 24/7
- Hackers, bugs, and crashes are lurking 24/7
- Humans aren't 24/7 – they need things like sleep, vacations, lunch, or just a few minutes away from staring at a screen in a freezing cold server room!

Splunk Alerts Never Sleep!

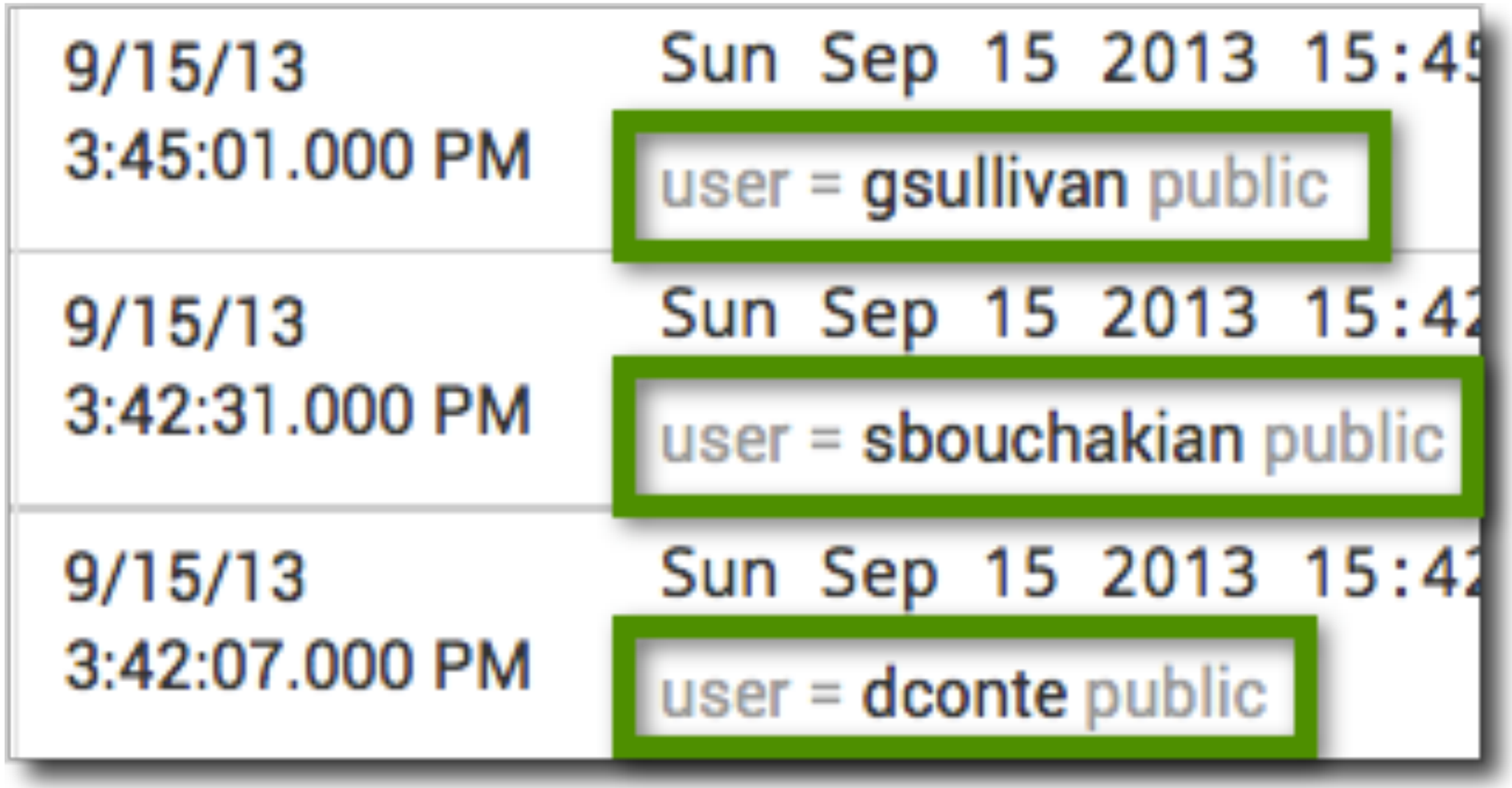
- Searches can be run on a schedule and be setup to “do something” based on the results
- We call these **alerts**

Alerting Scenario – Public User Logins

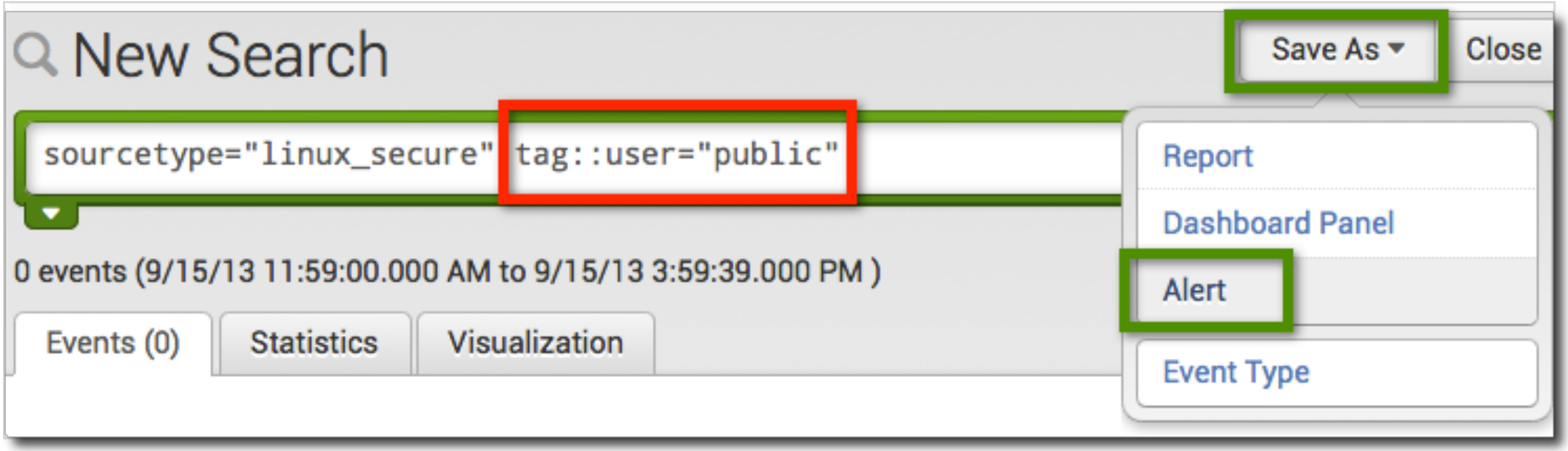
- Hackers need a user name AND password to access your systems
- Public web pages often contain names of CEOs, sales folks, etc.



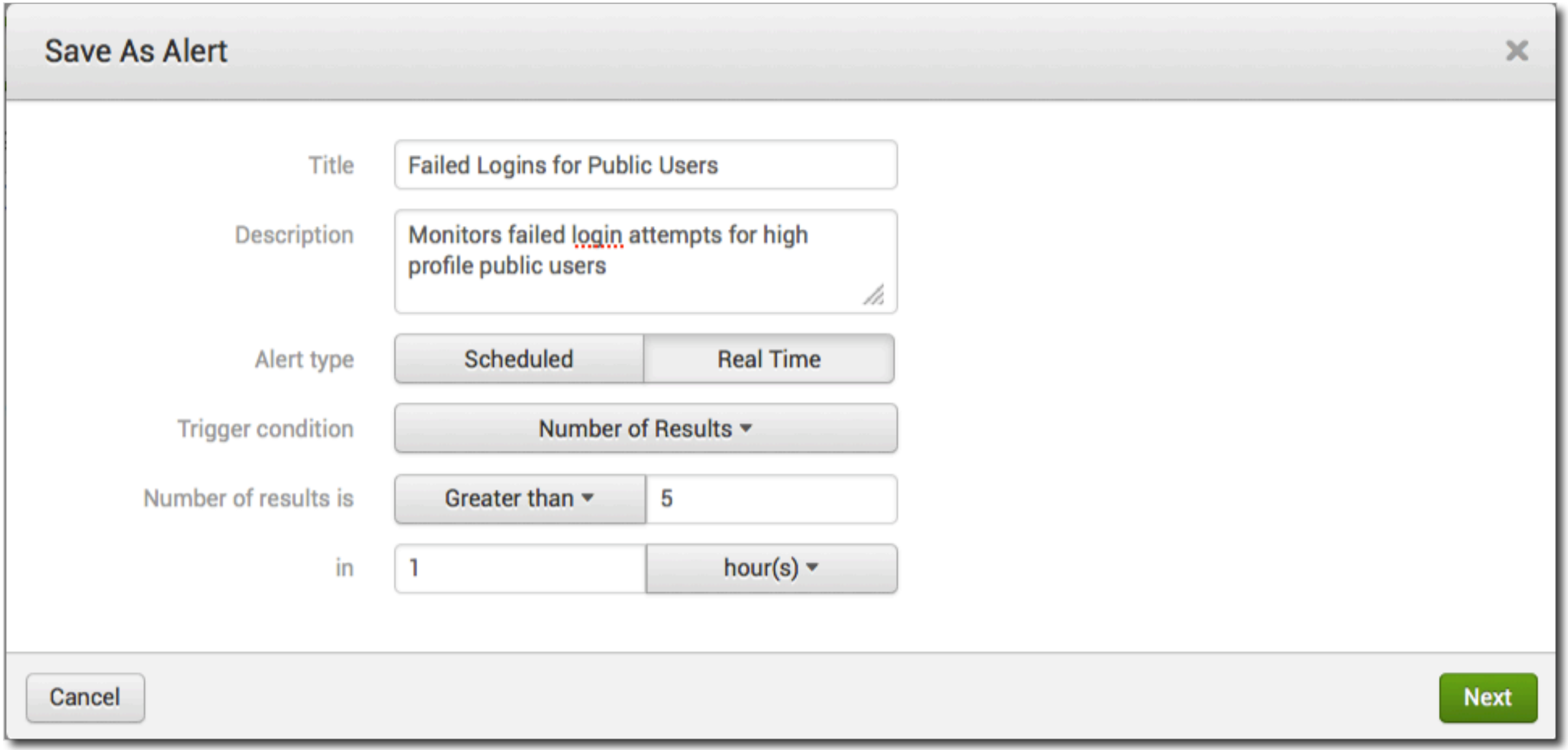
Create Your Tags



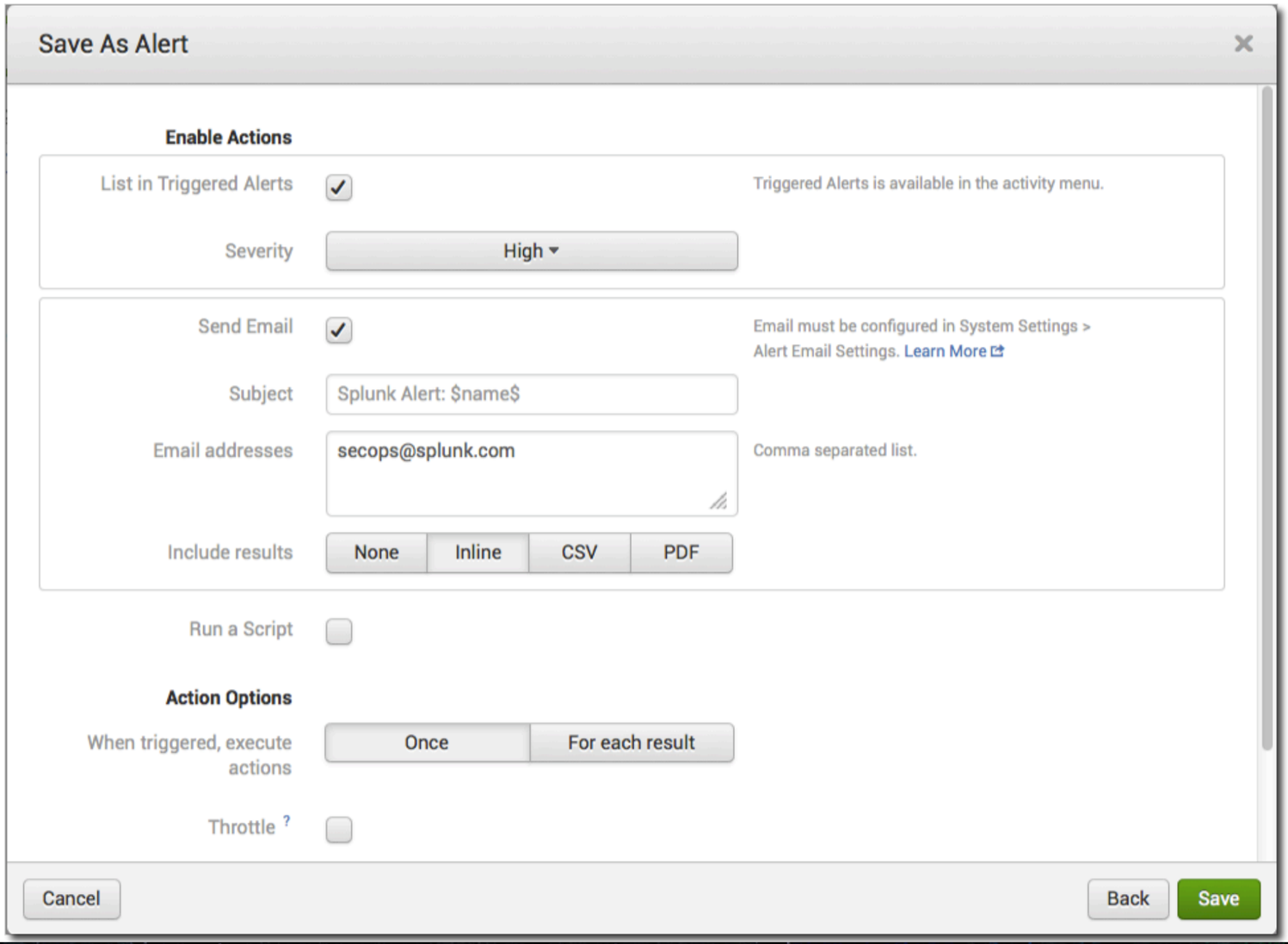
Search for the Tag and Create the Alert



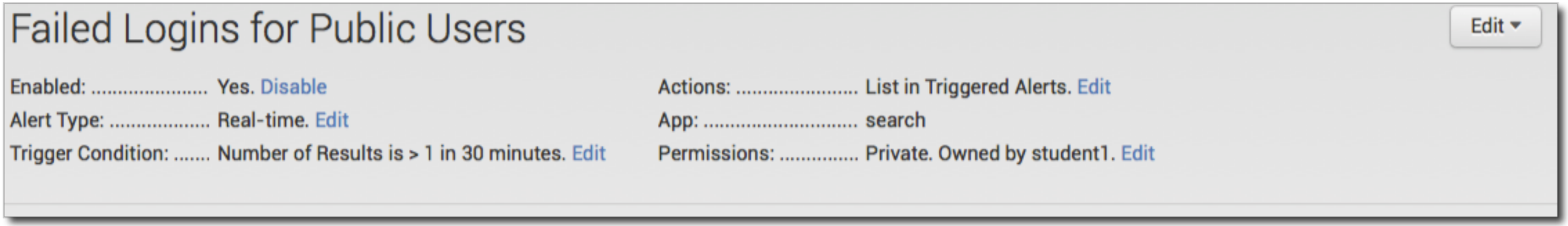
Set the Alert Schedule



Configure Alert Actions and Permissions

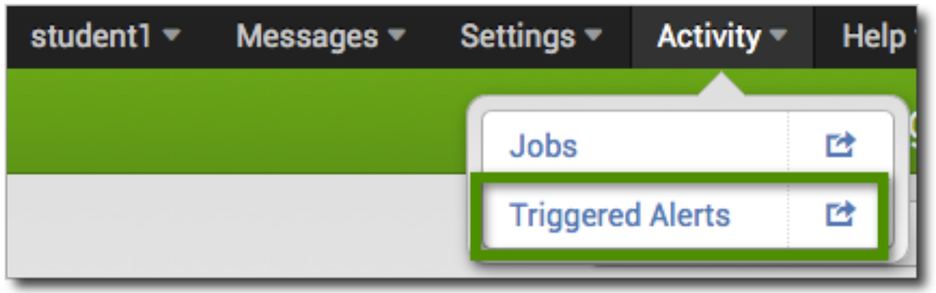


Alert Created!

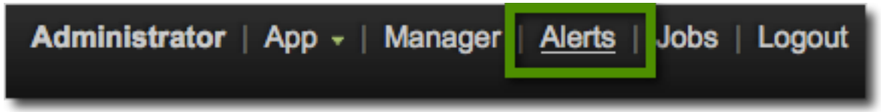


Alert Manager

Splunk Enterprise 6



Splunk Enterprise 5



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

«prev 1 2 3 next» 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

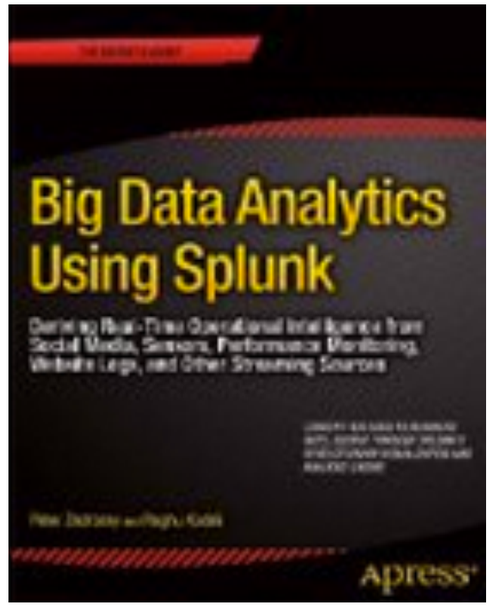
2. Take the survey & **WIN A PASS FOR .CONF2014**… Or one of these bags!

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>