



Creating Splunk Knowledge Objects

Class Goals

- Provide a deep understanding of what Splunk knowledge objects are and how they are used
- Create and manage the following knowledge objects:
 - Lookups
 - Fields (aliases, calculated, and extractions)
 - Tags and event types
 - Workflow actions
 - Alerts
 - Scheduled reports
 - Macros
 - Data models

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Course Outline

Module 1: Introduction

Module 2: Implementing Knowledge Objects

Module 3: Creating Lookups

Module 4: Creating Field Aliases and Calculated Fields

Module 5: Creating Field Extractions

Module 6: Creating Tags and Event Types

Module 7: Creating Workflow Actions

Module 8: Creating Alerts and Scheduled Reports

Module 9: Creating and Using Macros

Module 10: Creating Data Models

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Module 1: Introduction

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Module Objectives

- Review Buttercup Games
- Become familiar with the source types and event data used during the course
- Identify the categories of knowledge objects
- Define the role of a knowledge manager
- Describe the Common Information Model
- Understand the relationship between the CIM and knowledge objects
- Identify naming conventions
- Review permissions

Buttercup Games, Inc.

- Buttercup Games, Inc.
 - Is a multinational company with its HQ in San Francisco and offices in Boston and London
 - Sells product mainly through its worldwide chain of third party stores, but also sells through its online store
- For more information about Buttercup Games, please see Appendix B



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Buttercup Games Environment

Data	host	sourcetype
AD/DNS data (non-Engineering)	adldapsv1	winauthentication_security
Badge reader data	badgesv1	history_access
Email data	cisco_router1	cisco_esa
Online transactions & Web server	www1	access_combined
	www2	linux_secure
	www3	
Retail sales data	vendorUS1	vendor_sales
Splunk indexer data	splunk1	ps
Web appliance data	cisco_router1	cisco_wsa_squid
Windows system logs	adldapsv1	win_audit

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Your Role at Buttercup Games

- You are a Splunk user assigned to the power role
- You have a great understanding of all your company's data
- Your responsibilities are to create and manage Splunk knowledge objects for your stakeholders
- You implement best practices for naming conventions of all knowledge objects

What are Knowledge Objects?

- Knowledge objects are tools you use to discover and analyze various aspects of your data
 - **Fields and field extractions** - Data interpretation
 - **Event types** - Data classification
 - **Lookups and workflow actions** - Data enrichment
 - **Tags and aliases** – Normalization
 - **Data Models** – Representation of datasets which drives the pivot tool



Note



For more information go to:

<http://docs.splunk.com/Documentation/Splunk/latest/Knowledge/WhatisSplunkknowledge>

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

What is a Knowledge Manager?

A knowledge manager:

- Oversees knowledge object creation and usage for a group or deployment
- Normalizes event data
- Creates data models for Pivot users

Note



For more information go to:

[http://docs.splunk.com/Documentation/Splunk/6.3.0/
Knowledge/Monitorandorganizeknowledgeobjects](http://docs.splunk.com/Documentation/Splunk/6.3.0/Knowledge/Monitorandorganizeknowledgeobjects)

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

What is the Common Information Model (CIM)?

- The Splunk Common Information Model provides a methodology to normalize data
- Leverage the CIM when creating field extractions, event types, and tags to ensure:
 - Multiple apps can co-exist on a single Splunk deployment
 - Object permissions can be set to global for the use of multiple apps
 - Easier and more efficient correlation of data from different sources and source types

CIM Add-On

- Splunk CIM is an add-on available on splunkbase:

- <https://splunkbase.splunk.com/app/1621/>
- Includes pre-configured data models
- Data models consist of a set of standard fields and event category tags relevant to most IT data

- Examples of data models for IT specific domains:

- Email
- Malware
- Network Traffic
- Performance
- Ticket Management
- Web

Note



The installation of the CIM add-on is discussed in the Building Apps class.

Note



Data used by apps like Enterprise Security must adhere to the CIM. If the CIM is not followed, objects such as dashboards, reports, and alerts might not function properly.

Normalized Field Names - Email Data

Field name	Data type	Description	Possible values
action	string	Action taken by the reporting device.	delivered, blocked, quarantined, deleted, unknown
duration	number	The amount of time for the completion of the messaging event, in seconds.	Email
src	string	The system that sent the message. May be <u>aliased</u> from more specific fields, such as src_host, src_ip, or src_name.	

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Normalized Field Names - Network Traffic

Field name	Data type	Description	Possible values
action	string	The action taken by the network device.	allowed, blocked, dropped, unknown
bytes	number	Total count of bytes handled by this device/interface (bytes_in + bytes_out).	
bytes_in	number	How many bytes this device/interface received.	
bytes_out	number	How many bytes this device/interface transmitted.	
src	string	The source of the network traffic (the client requesting the connection). May be aliased from more specific fields, such as src_host, src_ip, or src_name.	

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Normalized Field Names – Web Data

Field name	Data type	Description	Possible values
action	string	The action taken by the server or proxy.	
duration	number	The time taken by the proxy event, in milliseconds.	
http_method	string	The HTTP method used in the request.	GET, PUT, POST, DELETE, etc.
src	string	The source of the network traffic (the client requesting the connection).	
status	string	The HTTP response code indicating the status of the proxy request.	404, 302, 500, and so on.

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Additional CIM Resources

Documentation:

[http://docs.splunk.com/Documentation/Splunk/latest/Knowledge/
UnderstandandusetheCommonInformationModel](http://docs.splunk.com/Documentation/Splunk/latest/Knowledge/UnderstandandusetheCommonInformationModel)

<http://docs.splunk.com/Documentation/CIM/latest/User/Overview>

[http://docs.splunk.com/Documentation/CIM/latest/User/
UsetheCIMtonormalizedataatsearchtime](http://docs.splunk.com/Documentation/CIM/latest/User/
UsetheCIMtonormalizedataatsearchtime)

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Defining Naming Conventions

- To avoid confusion later, develop naming conventions for your Splunk implementation early for knowledge objects like reports, alerts, and dashboards
- This course uses simple names, but using a naming convention is more efficient
 - For example:
 - **Group:** Corresponds to the working group(s) of the user saving the search (examples: SEG. NEG. OPS. NOC)
 - **Search type:** Indicates the type of search (alert, report, summary-index-populating) (examples: Alert, Report, Summary)
 - **Platform:** Corresponds to the platform subjected to the search (examples: Windows, iSeries, Network)

Defining Naming Conventions (cont.)

- ▶ **Category:** Corresponds to the concern areas for the prevailing platforms (examples: DiskExchange, SQL, Event log, CPU, Jobs, Subsystems, Services, Security)
- ▶ **Time interval:** The time interval used by the search or on which the search runs, if it is a scheduled search (examples: 24h, 7d, 3m, etc.)
- ▶ **Description:** A meaningful description of the context and intent of the search, limited to one or two words if possible. Ensures the search name is unique. (examples: Failed_Passwords, Failed_Batch, Top_src_ip)

Examples:

- SEG_Alert_Windows_Eventlog_15m_Failures
- SEG_Report_iSeries_Jobs_12hr_Failed_Batch
- NOC_Summary_Network_Security_24hr_Top_src_ip

Note



For more information go to: <http://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Developnamingconventionsforknowledgeobjecttitles>

Reviewing Permissions

	Description	Create	Read	Edit (write)
Private	Only the person who created the object can use it and edit it	User Power Admin	Person who created it Admin	Person who created it Admin
Shared in App	Object persists in the context of a specific app	Power Admin	User* Power* Admin	User* Power* Admin
Global	Object persists globally across all apps	Admin	User* Power* Admin	User* Power* Admin

* Permission to read and/or write if creator gives permission to that role

By default, **Shared in App** and **Global** gives everyone read permission – write permission is reserved for admin and object creator unless creator edits permissions

Module 2: Creating Lookups

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Module Objectives

- Describe lookups
- Examine a lookup file example
- Create a lookup file and definition
- Configure an automatic lookup
- Use the lookup in searches

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Describing Lookups

- There are use cases where static or relatively unchanging data is required for searches, but is not available in the index
- For example, from an RFID in a badge reader event, you can look up employee information

Scenario



Display badge-ins during the last 4 hours with user name and department.

```
sourcetype=history_access  
| table Address_Description, rfid,  
Username, Department
```

Address_Description	rfid	Username	Department
London	632071692298	yowen	Sales
London	963871339460	rjayaraman	Engineering
London	145297537706	npearce	SecOps
London	145297537706	npearce	SecOps
London	145297537706	npearce	SecOps
San Francisco	569361105570	kpercy	Compliance Officer
Boston	374765319282	emaxwell	ITOps
Boston	108423575302	apucci	Sales
Boston	108423575302	apucci	Sales

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Describing Lookups (cont.)

- Lookups allow you to add more fields to your events:
 - Provide descriptions for http status codes (“file not found”, “service unavailable”)
 - Define sale prices for products
 - Associate RFIDs with user names, IP addresses, and workstation IDs
- Lookups can be defined in a static .csv file or it can be the output of a Python script
- After a field lookup is configured, you can use the lookup fields in searches
- The lookup fields also appear in the Fields sidebar
- Lookup field values are case-sensitive by default
 - Admins can change the `case_sensitive_match` option to `false` in `transforms.conf`
- Manage lookups from **Settings > Lookups**

Defining a File-based Lookup

1. Upload the file required for the lookup
2. Define the lookup type
3. Optionally, configure the lookup to run automatically

Lookups

Create and configure lookups.

	Actions
1 Lookup table files List existing lookup tables or upload a new file .	Add new
2 Lookup definitions Edit existing lookup definitions or define a new file-based or external lookup.	Add new
3 Automatic lookups Edit existing automatic lookups or configure a new lookup to run automatically.	Add new

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Lookup File – Example

- This example displays a lookup .csv file used to associate product information with productId
- First row represents field names (header)
productId, product_name, categoryId, price, sale_price, Code
- The productId field exists in the access_combined events
 - This is the **input** field
- All of the fields listed above are available to search after the lookup is defined
 - These are the **output** fields

```
GNU nano 2.3.1          File: products.csv

productId,product_name,categoryId,price,sale_price,Code
DB-SG-G01,Mediocre Kingdoms,STRATEGY,24.99,19.99,A
DC-SG-G02,Dream Crusher,STRATEGY,39.99,24.99,B
FS-SG-G03,Final Sequel,STRATEGY,24.99,16.99,C
WC-SH-G04,World of Cheese,SHOOTER,24.99,19.99,D
WC-SH-T02,World of Cheese Tee,TEE,9.99,6.99,E
PZ-SG-G05,Puppies vs. Zombies,STRATEGY,4.99,1.99,F
CU-PG-G06,Curling 2014,SPORTS,19.99,16.99,G
MB-AG-G07,Manganiello Bros.,ARCADE,39.99,24.99,H
MB-AG-T01,Manganiello Bros. Tee,TEE,9.99,6.99,I
FI-AG-G08,Orvil the Wolverine,ARCADE,39.99,24.99,J
BS-AG-G09,Benign Space Debris,ARCADE,24.99,19.99,K
SC-MG-G10,SIM Cubicle,SIMULATION,19.99,16.99,L
WC-SH-A01,Holy Blade of Gouda,ACCESSORIES,5.99,2.99,M
WC-SH-A02,Fire Resistance Suit of Provolone,ACCESSORIES,3.99,1.99,N
```

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Creating a Lookup Table

Settings > Lookups > Lookup table files

1. Click New
2. Select a destination app
3. Browse and select the .csv file to use for the lookup table
4. Enter a name for the lookup file
5. Save

Add new
Lookups > Lookup table files > Add new

Destination app *

2 search

Upload a lookup file

3 Browse... products.csv

Select either a plaintext CSV file, a gzipped CSV file, or a KMZ file.
The maximum file size that can be uploaded through the browser is 500MB.

Destination filename *

4 products.csv

Enter the name this lookup table file will have on the Splunk server. If you are uploading a gzipped CSV file, enter a filename ending in ".gz". If you are uploading a plaintext CSV file, we recommend a filename ending in ".csv". For a KMZ file, we recommend a filename ending in ".kmz".

Cancel

5 Save

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Changing Permissions – Lookup File

- By default, lookup tables are created as Private
- To allow others to use the lookup table, the permissions must be changed

The screenshot shows two Splunk interface windows. The left window is titled 'Lookup table files' under 'Lookups > Lookup table files'. It displays a single item: 'products.csv' located at '/opt/splunk/etc/users/student10/search/lookups/products.csv'. The item is owned by 'student10' and is part of the 'search' app. The sharing status is 'Private', and there is a green box around the 'Permissions' link. A large green arrow points from this 'Permissions' link to the right window. The right window is titled 'Permissions' under 'Lookups > Lookup table files > products.csv > Permissions'. It shows the sharing settings: 'Object should appear in' is set to 'This app only (search)' (selected radio button). The 'Permissions' table lists three roles: 'Everyone' (Read checked, Write unchecked), 'power' (Read unchecked, Write unchecked), and 'user' (Read unchecked, Write unchecked). There are 'Cancel' and 'Save' buttons at the bottom.

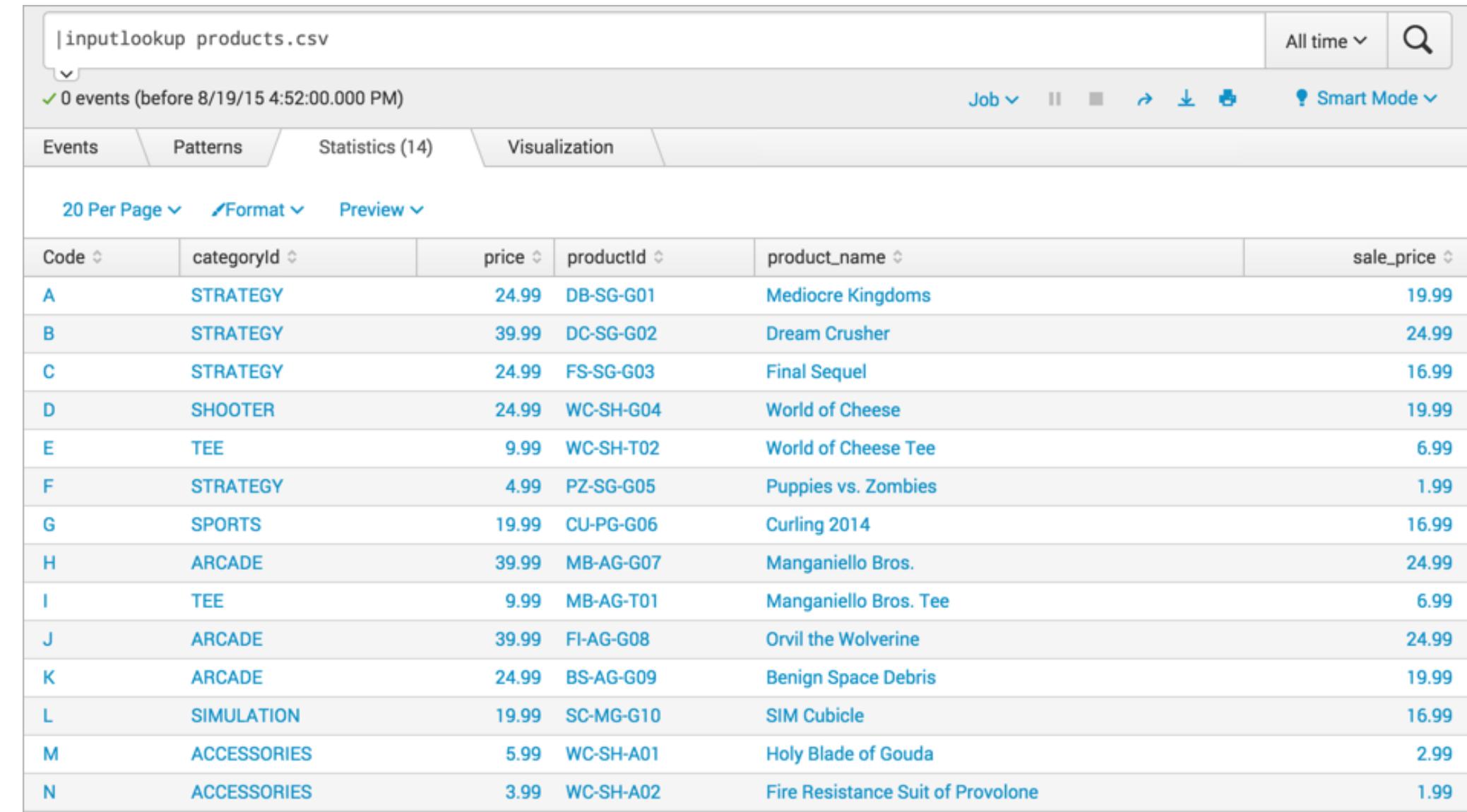
Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

inputlookup Command

- Use the `inputlookup` command to load the results from a specified static lookup
- Useful to:
 - Review the data in the `.csv` file
 - Validate the lookup

Note 

When using the `inputlookup` command, you can specify the filename ending with `.csv` or the lookup definition name



The screenshot shows a Splunk search interface with the search bar containing `|inputlookup products.csv`. The results pane displays 0 events (before 8/19/15 4:52:00.000 PM). The visualization tab is selected, showing a table with the following data:

Code	categoryId	price	productId	product_name	sale_price
A	STRATEGY	24.99	DB-SG-G01	Mediocre Kingdoms	19.99
B	STRATEGY	39.99	DC-SG-G02	Dream Crusher	24.99
C	STRATEGY	24.99	FS-SG-G03	Final Sequel	16.99
D	SHOOTER	24.99	WC-SH-G04	World of Cheese	19.99
E	TEE	9.99	WC-SH-T02	World of Cheese Tee	6.99
F	STRATEGY	4.99	PZ-SG-G05	Puppies vs. Zombies	1.99
G	SPORTS	19.99	CU-PG-G06	Curling 2014	16.99
H	ARCADE	39.99	MB-AG-G07	Manganiello Bros.	24.99
I	TEE	9.99	MB-AG-T01	Manganiello Bros. Tee	6.99
J	ARCADE	39.99	FI-AG-G08	Orvil the Wolverine	24.99
K	ARCADE	24.99	BS-AG-G09	Benign Space Debris	19.99
L	SIMULATION	19.99	SC-MG-G10	SIM Cubicle	16.99
M	ACCESSORIES	5.99	WC-SH-A01	Holy Blade of Gouda	2.99
N	ACCESSORIES	3.99	WC-SH-A02	Fire Resistance Suit of Provolone	1.99

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Creating a Lookup Definition

Settings > Lookups > Lookup definitions

1. Click **New**
2. Select a destination app
3. Name the lookup definition
4. Select the lookup type, either File-based or External
5. From the drop-down, select a lookup file
6. Save

Add new
Lookups » Lookup definitions » Add new

Destination app *

2 search

Name *

3 product_lookup

Type *

4 File-based

Lookup file *

5 products.csv

Create and manage [lookup table files](#).

Configure time-based lookup

Advanced options

Cancel

6 Save

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Advanced Options

Under Advanced options, you can specify:

1. Minimum number of matches for each input lookup value
2. Maximum number of matches for each input lookup value
3. Default value to output, if fewer than the minimum number of matches are present for a given input

Lookup file *

products.csv

Create and manage [lookup table files](#).

Configure time-based lookup

Advanced options

Minimum matches

1

The minimum number of matches for each input lookup value. Default is 0.

Maximum matches

1

Enter a number from 1-1000 to specify the maximum number of matches for each input lookup value. If time-based, default is 1; otherwise, default is 1000.

Default matches

NoInputMatch

If fewer than the minimum number of matches are present for any given input, write out this value one or more times such that the minimum is reached

Cancel

Save

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Managing Lookup Definitions

Based on your permissions, you can:

- Edit permissions
- Delete
- Enable/disable
- Move
- Clone

Note 
Remember to set the permissions for the lookup definition appropriately.

Lookup definitions
[Lookups](#) » [Lookup definitions](#)

Successfully saved "product_lookup" in search.

App context [Search & Reporting \(search\)](#) Owner Any

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

New

Showing 1-5 of 5 items Results per page 50

Name	Type	Supported fields	Lookup file	Owner	App	Sharing	Status	Actions
geo_attr_countries	file	country,region_wb,region_un,subregion,continent,iso2,iso3	geo_attr_countries.csv	No owner	search	Global Permissions	Enabled Disable	Clone
geo_attr_us_states	file	state_name,state_fips,state_code	geo_attr_us_states.csv	No owner	search	Global Permissions	Enabled Disable	Clone
geo_countries	geo	None	geo_countries.kmz	No owner	search	Global Permissions	Enabled Disable	Clone
geo_us_states	geo	None	geo_us_states.kmz	No owner	search	Global Permissions	Enabled Disable	Clone
product_lookup	file	productId,product_name,categoryId,price,sale_price,Code	products.csv	cfarrell	search	Private Permissions	Enabled Disable	Clone Move Delete

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

lookup Command

- If a lookup is not configured to run automatically, use the `lookup` command in your search to use the lookup fields
- **OUTPUT** - If an `OUTPUT` clause is not specified, all fields in the lookup table that are not the match field are used as output fields
- If `OUTPUT` is specified, the output lookup fields overwrite existing fields
- The output lookup fields exist only for the current search
- Use `OUTPUTNEW` when you do not want to overwrite existing fields

[lookup](#) [Help](#) [More »](#)
Explicitly invokes field value lookups.

Examples

There is a lookup table specified in a stanza name 'usertogroup' in `transform.conf`. This lookup table contains (at least) two fields, 'user' and 'group'. For each event, we look up the value of the field 'local_user' in the table and for any entries that matches, the value of the 'group' field in the lookup table will be written to the field 'user_group' in the event.

```
... | lookup usertogroup user as local_user OUTPUT group as user_group
```

Using the lookup Command

New Search

```
sourcetype=access* action=purchase  
| lookup product_lookup productId OUTPUT price product_name  
| stats sum(price) as sales by product_name
```

27 events (7/23/15 3:21:00.000 PM to 7/23/15 4:21:13.000 PM)

Events Patterns Statistics (8) Visualization

20 Per Page ▾ Format ▾ Preview ▾

product_name	sales
Final Sequel	24.99
Holy Blade of Gouda	5.99
Manganiello Bros. Tee	9.99
Orvil the Wolverine	119.97
Puppies vs. Zombies	9.98

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Creating an Automatic Lookup

Settings > Lookups > Automatic lookups

1. Click **New**
2. Select the Destination app
3. Enter a Name for the lookup
4. Select the Lookup table definition
5. Select host, source, or sourcetype to apply the lookup and specify the name.

Add new

Lookups » Automatic lookups » Add new

Destination app *

2 search

Name *

3 product_auto_lookup

Lookup table *

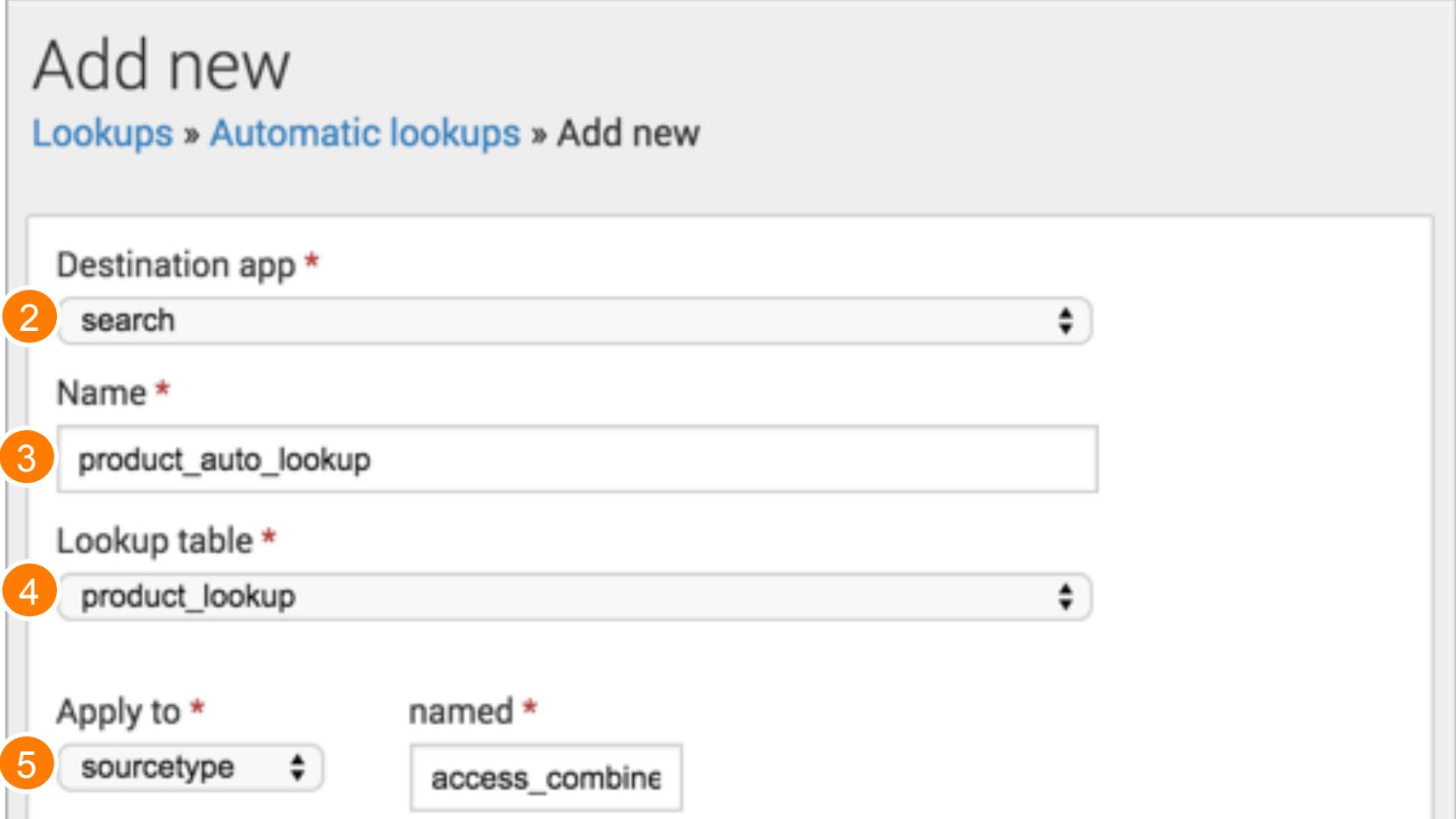
4 product_lookup

Apply to *

5 sourcetype

named *

access_combine



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Creating an Automatic Lookup (cont.)

6. Define the Lookup input fields

- Field(s) that exist in your events that you are relating to the lookup table

A. Column name in CSV

B. Field name in Splunk, if different from column name

7. Define the Lookup output fields

- Field(s) from your lookup table that are added to the events

C. Field name in lookup table

D. Name you want displayed in Splunk, otherwise it inherits the column name

8. Save

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

The screenshot shows the 'Lookup input fields' and 'Lookup output fields' sections of the Splunk Knowledge Objects interface. The 'Lookup input fields' section contains one field, 'productId'. The 'Lookup output fields' section contains four fields: 'categoryId', 'price', 'product_name', and 'sale_price'. Each output field has a corresponding 'Delete' link next to it. Orange circles labeled A, B, C, and D point to the 'productId' field, the 'Delete' link for 'categoryId', the 'categoryId' field, and the 'Delete' link for 'sale_price' respectively. A green box highlights the entire configuration area. At the bottom are 'Overwrite field values' checkbox, 'Cancel' button, and a large green 'Save' button.

Managing Automatic Lookups

Based on your permissions, you can:

- Edit permissions
- Clone
- Delete
- Move

Note 
Remember to set the permissions for the automatic lookup appropriately.

Automatic lookups
[Lookups](#) » Automatic lookups

Successfully saved "vendor_lookup" in search.

App context [Search & Reporting \(search\)](#) Owner Any

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

[New](#)

Showing 1-2 of 2 items Results per page 50

Name	Lookup	Owner	App	Sharing	Status	Actions
access_combined : LOOKUP-product_auto_lookup	product_lookup productId OUTPUTNEW categoryId price product_name sale_price	cfarrell	search	Private Permissions	Enabled	Clone Move Delete
vendor_sales : LOOKUP-vendor_lookup	dnslookup Vendor OUTPUTNEW VendorId	cfarrell	search	Private Permissions	Enabled	Clone Move Delete

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Using the Automatic Lookup

To use an automatic lookup, specify the output fields in your search

The screenshot illustrates the use of automatic lookup in Splunk. The search bar contains the command: `sourcetype=access* action=purchase productId=* | stats sum(price) as sales by productId product_name`. The results table shows two events from July 23, 2015:

Time	Event
7/23/15 5:21:02.000 PM	195.2.240.99 - [23/Jul/2015:17:21:02] "POST /cart.do?action=purchase&itemId=EST-17&JSSESSIONID=SD2SL10FF5ADFF4954 HTTP 1.1" 200 3603 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-17&categoryId=STRATEGY&productId=DC-SG-G02" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 244 host = www2 productId = DC-SG-G02 source = /opt/log/www2/access.log sourcetype = access_combined
7/23/15 5:20:48.000 PM	195.2.240.99 - [23/Jul/2015:17:20:48] "GET /product.screen?productId=SF-BVS-01&JSESSIONID=SD2SL10FF5ADFF4954 HTTP 1.1" 400 3700 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-19" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 646 host = www2 productId = SF-BVS-01 source = /opt/log/www2/access.log sourcetype = access_combined

An arrow points from the(productId) field in the first event to the productId column in the lookup table. Another arrow points from the(productId) field in the second event to the sales column in the lookup table.

The lookup table displays the following data:

productId	product_name	sales
BS-AG-G09	Benign Space Debris	24.99
CU-PG-G06	Curling 2014	19.99
DB-SG-G01	Mediocre Kingdoms	24.99
DC-SG-G02	Dream Crusher	39.99
FI-AG-G08	Orvil the Wolverine	39.99
FS-SG-G03	Final Sequel	24.99

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Describing Time-based Lookups

- If a field in the lookup table represents a timestamp, you can create a time-based lookup
- Example: use DHCP logs to identify users on your network based on their IP address and the timestamp
 - A script might copy DHCP log events to a .csv file when an ACK event occurs

```
ACK: 1 110 08/06/14 11:40:06 171.64.20.120 00:0d:93:b1:9e:d6
```

- .csv file contains the timestamp, IP address, username, and MAC address

```
ackTime,ip,user,macaddress  
06AUG2014 11:40:06,171.64.20.120,bwilson,00:0d:93:b1:9e:d6
```

Configuring Time-based Lookups

1. Specify the name of the time field in the lookup
2. Enter the strftime format of the time field
3. Define the minimum offset in seconds
 - Default is 0
4. Define the maximum offset in seconds
 - There is no maximum offset by default

Configure time-based lookup

Name of time field *

1 ackTime

For time-based lookups, specify the name of the field in the lookup table that represents time.

Time format *

2 %d%m%y %H:%M:%S

Specify the strftime format of the timestamp field. Default format is UTC time.

Minimum offset *

3 0

The minimum time in seconds that the event time may be ahead of lookup entries.

Maximum offset *

4 200000000

The maximum time in seconds that the event time may be ahead of lookup entries.

Note



The offset is the minimum and maximum amounts of time that an event may be later than a lookup entry.

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Additional Lookup Options

In addition to creating and using a file-based lookup, you can also:

- Populate a lookup table with search results
 - `outputlookup` is discussed in the *Advanced Searching & Reporting* class
- Define a field lookup based on an external command; Python- and binary-based scripts
 - For more information, see the *Knowledge Manager Manual*
docs.splunk.com/Documentation/Splunk/latest/Knowledge/Addfieldsfromexternaldatasources
- Use the Splunk DB Connect app to create lookups with data from external SQL databases
- Populate events with fields from an App Key Value Store (KV Store) collection
 - KV Store lookups can only be invoked through REST endpoints or by using search commands such as `lookup`, `inputlookup`, and `outputlookup`, therefore cannot be set up as automatic
 - For more information, see the *Knowledge Manager Manual*
docs.splunk.com/Documentation/Splunk/latest/Knowledge/ConfigureKVstorelookups

Module 3: Creating Field Aliases and Calculated Fields

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Module Objectives

- Create and use field aliases
- Create calculated fields

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

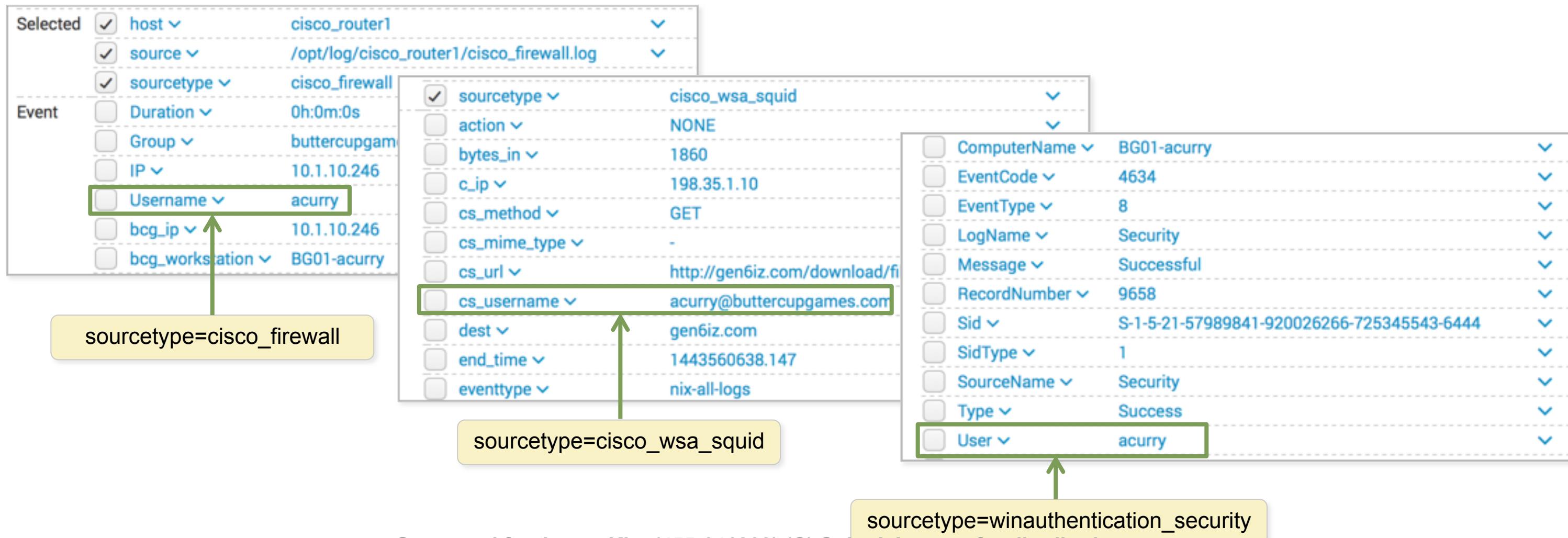
Field Aliases

- A way to normalize data over several sources
- Multiple aliases can be applied to one field
- Applied after field extractions, before lookups
- Can apply field aliases to lookups

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Field Alias Example

- Several source types contain some type of a username field
- To make data correlation and searching easier, normalize the username field



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Creating a Field Alias

Settings > Fields > Field Aliases > New

1. Select the app associated with the field alias
2. Enter a Name for the field alias
3. Apply the field alias to a default field:
 - Host
 - Source
 - Sourcetype
4. Enter the name for the existing field and the new alias

Add new
Fields » Field aliases » Add new

Destination app *

1 search

Name *

2 cisco_firewall_aliases

Apply to *

3 sourcetype cisco_firewall

Field aliases

4 Username = user Delete

Add another field

Cancel Save

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Creating a Field Alias (cont.)

In this example, one field alias will be used for the new ‘user’ field in multiple source types. A new field alias is required for each sourcetype:

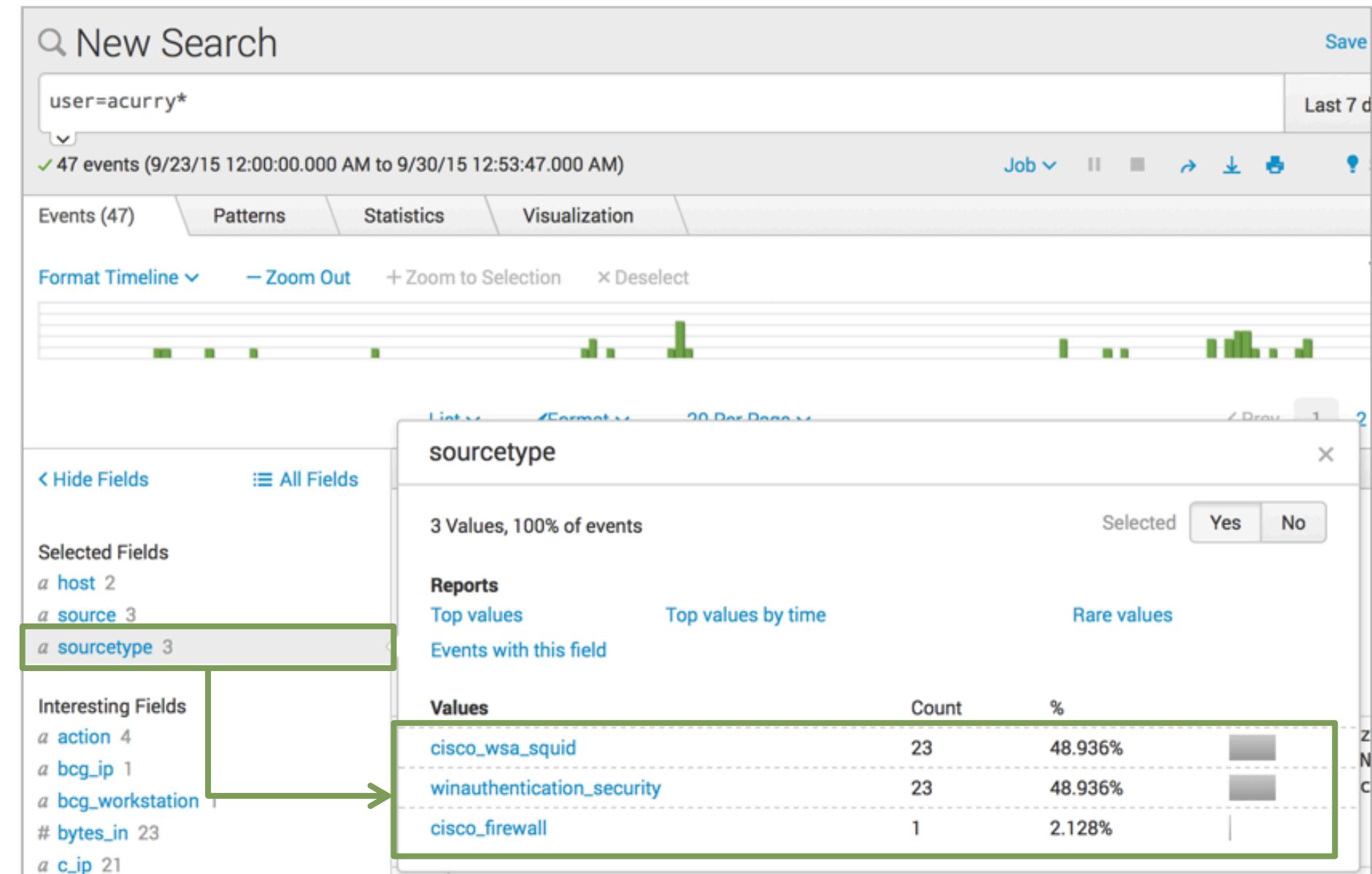
The image consists of three side-by-side screenshots of a Splunk interface for creating field aliases. Each screenshot shows a form with fields for Destination app, Name, Apply to (sourcetype), and Field aliases.

- Screenshot 1 (Left):** Destination app: search. Name: cisco_firewall_aliases. Apply to: sourcetype (selected), named (cisco_firewall). Field aliases: Username = user. Buttons: Cancel.
- Screenshot 2 (Middle):** Destination app: search. Name: cisco_wsa_squid_aliases. Apply to: sourcetype (selected), named (cisco_wsa_squid). Field aliases: cs_username = user. Buttons: Cancel.
- Screenshot 3 (Right):** Destination app: search. Name: winauthentication_security_aliases. Apply to: sourcetype (selected), named (winauthentication). Field aliases: User = user. Buttons: Cancel, Save.

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Testing the Field Alias

After the field alias has been created, perform a new search using the new field alias

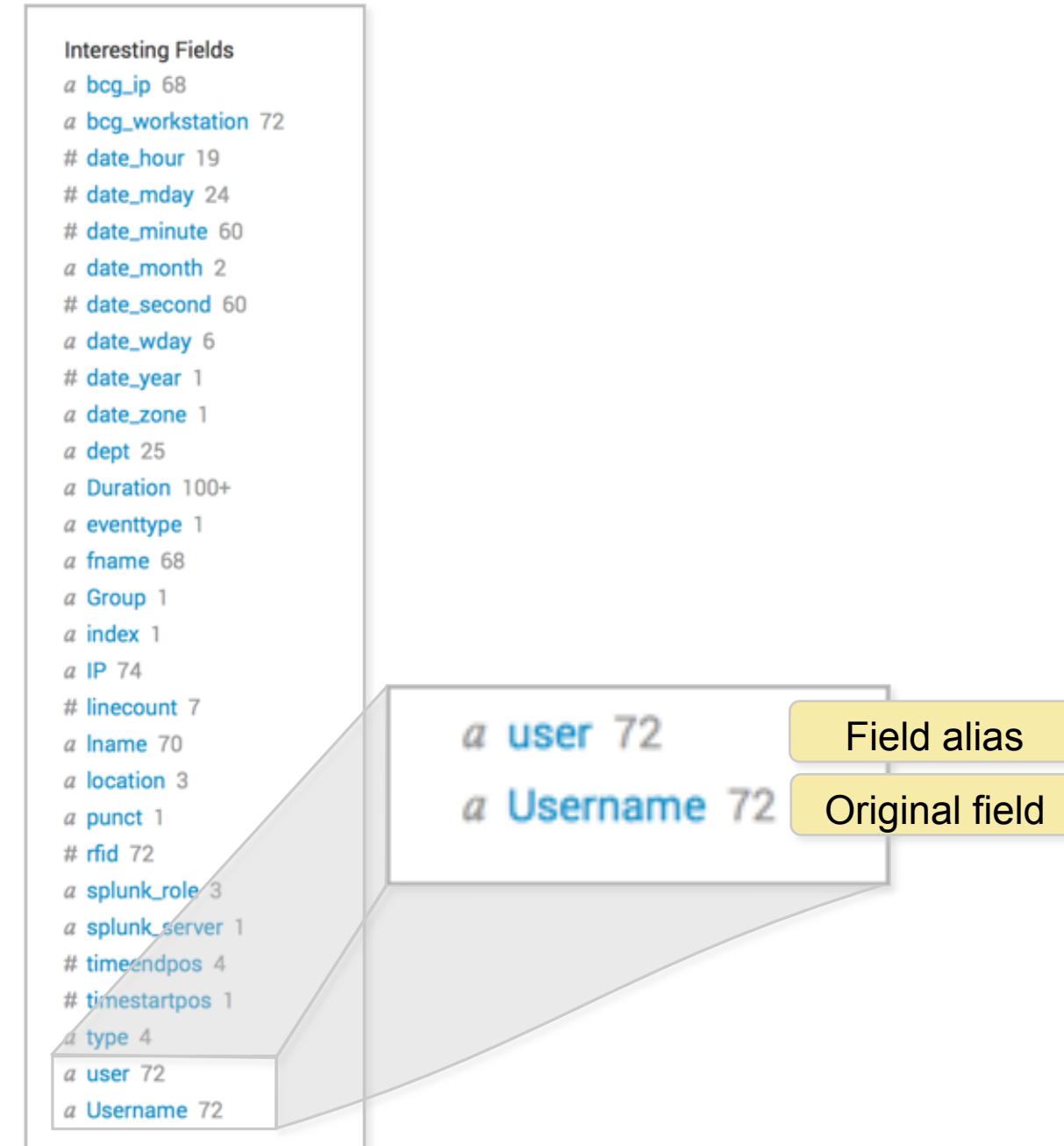


Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Field Alias and Original Fields

When you create a field alias, the original field is not affected.

Both fields will appear in the All Fields list and the Interesting Fields list, if it appears in at least 20% of events.



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Field Aliases and Lookups

After you have defined your field aliases, you can create a lookup table to reference them

The screenshot shows the Splunk interface for defining field aliases. On the left, a sidebar lists 'Fields' and 'Field aliases'. The main area is titled 'cisco_firewall : FIELDALIAS-cisco_firewall'. It shows a 'Field aliases' section where 'Username' is aliased to 'user'. A green box highlights the 'user' alias. An arrow points from this box to a CSV file named 'employees.csv' on the right, which contains a list of employee records with a 'user' field. The 'user' field in the CSV is also highlighted with a green box.

rfid	fname	lname	user	email	dept	location	ip
108423575302	Affen	Pucci	apucci	apucci@buttercupgames.com	Sales	Boston	10.3.10.53
672903009231	Dwight	Hale	dhale	dhale@buttercupgames.com	Sales	Boston	10.3.10.241
398009643042	Phyllis	Bunch	pbunch	pbunch@buttercupgames.com	ITOps	Boston	10.3.10.227
374765319282	Enrique	Maxwell	emaxwell	emaxwell@buttercupgames.com	ITOps	Boston	10.3.10.46
227128834140	David	Johnson	djohnson	djohnson@buttercupgames.com	Engineering	Boston	10.3.10.180
371211812887	Galina	Zuyeva	gzuyeva	gzuyeva@buttercupgames.com	Engineering	Boston	10.3.10.67
249772079712	Louis	Sagers	lsagers	lsagers@buttercupgames.com	SecOps	Boston	10.3.10.21
.....							
417852300683	Amanda	Curry	acurry	acurry@buttercupgames.com	SecOps	San Francisco	10.1.10.252
542830538161	Alan	Dombrowski	adombrowski	adombrowski@buttercupgames.com	SecOps	San Francisco	10.1.10.129
768166372290	Cerys	Farrell	cfarrell	cfarrell@buttercupgames.com	Sales	San Francisco	10.1.10.107
153218951159	Placido	Toscani	ptoscani	ptoscani@buttercupgames.com	Sales	San Francisco	10.1.10.38
994499284304	Ian	King	iking	iking@buttercupgames.com	Sales	San Francisco	10.1.10.201
531253083348	Gabriel	Voronoff	gvoronoff	gvoronoff@buttercupgames.com	Marketing	San Francisco	10.1.10.163
520156890727	Bao	Lu	blu	blu@buttercupgames.com	Marketing	San Francisco	10.1.10.100
727896988001	Lien	Teng	lteng	lteng@buttercupgames.com	ITOps	San Francisco	10.1.10.15
936901629743	Gabriel	Voronoff	gvoronoff	gvoronoff@buttercupgames.com	ITOps	San Francisco	10.1.10.163
230876363319	Meng	Yuan	myuan	myuan@buttercupgames.com	Engineering	San Francisco	10.1.10.172
271108583080	Patrick	Callahan	pcallahan	pcallahan@buttercupgames.com	Engineering	San Francisco	10.1.10.98
569361105570	Kathleen	Percy	kpercy	kpercy@buttercupgames.com	Compliance Officer	San Francisco	10.1.10.216
.....							
145297537706	Nigella	Pearce	npearce	npearce@buttercupgames.com	SecOps	London	10.2.10.70
632071692298	Yanto	Owen	yowen	yowen@buttercupgames.com	Sales	London	10.2.10.170
862417886973	Finlay	Bryan	fbryan	fbryan@buttercupgames.com	Sales	London	10.2.10.166
890313901800	Bradley	Hussain	bhussain	bhussain@buttercupgames.com	ITOps	London	10.2.10.22
425932411002	Naomi	Sharpe	nsharpe	nsharpe@buttercupgames.com	ITOps	London	10.2.10.163
.....							

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Managing Field Aliases

Settings > Fields > Field Aliases

- Edit permissions
- Clone
- Move
- Delete

The screenshot shows the 'Field aliases' page in Splunk. The page title is 'Field aliases' under 'Fields > Field aliases'. There are filters for 'App context' (Search & Reporting (search)) and 'Owner' (Any). A checkbox 'Show only objects created in this app context' is checked. A search bar and a green search icon are at the top right. Below the filters, there is a 'New' button. The table displays three items:

Name	Field aliases	Owner	App	Sharing	Status	Actions
cisco_firewall : FIELDALIAS-cisco_firewall_aliases	Username AS user	cfarrell	search	Private Permissions	Enabled	Clone Move Delete
cisco_wsa_squid : FIELDALIAS-cisco_wsa_squid_aliases	cs_username AS user	cfarrell	search	Private Permissions	Enabled	Clone Move Delete
winauthentication_security : FIELDALIAS-winauthentication_security_aliases	User AS user	cfarrell	search	Private Permissions	Enabled	Clone Move Delete

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

What is a Calculated Field?

- Shortcut for performing repetitive, long, or complex transformations using the eval command
- Must be based on an extracted field
 - Output fields from a lookup table or fields/columns generated from within a search string are not supported

New Search

```
sourcetype="cisco_wsa_squid" | eval bandwidth = sc_bytes/(1024*1024) | stats sum(bandwidth) as "Bandwidth (MB)" by usage | sort -"Bandwidth (MB)"
```

Last 30 days

✓ 3,756 events (11/5/14 12:00:00.000 AM to 12/5/14 11:27:54.000 PM)

Events (3,756) Patterns Statistics (5) Visualization

Job Verbose Mode

20 Per Page Format Preview

usage	Bandwidth (MB)
Personal	42.403496
Unknown	7.627116
Business	6.042235
Borderline	5.397223
Violation	0.211651

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Creating a Calculated Field

Settings > Fields > Calculated Fields > New

1. Select the app that will use the calculated field
2. Select host, source, or sourcetype to apply to the calculated field and specify the related name
3. Name the calculated field
4. Define the eval expression

Add new
Fields » Calculated fields » Add new

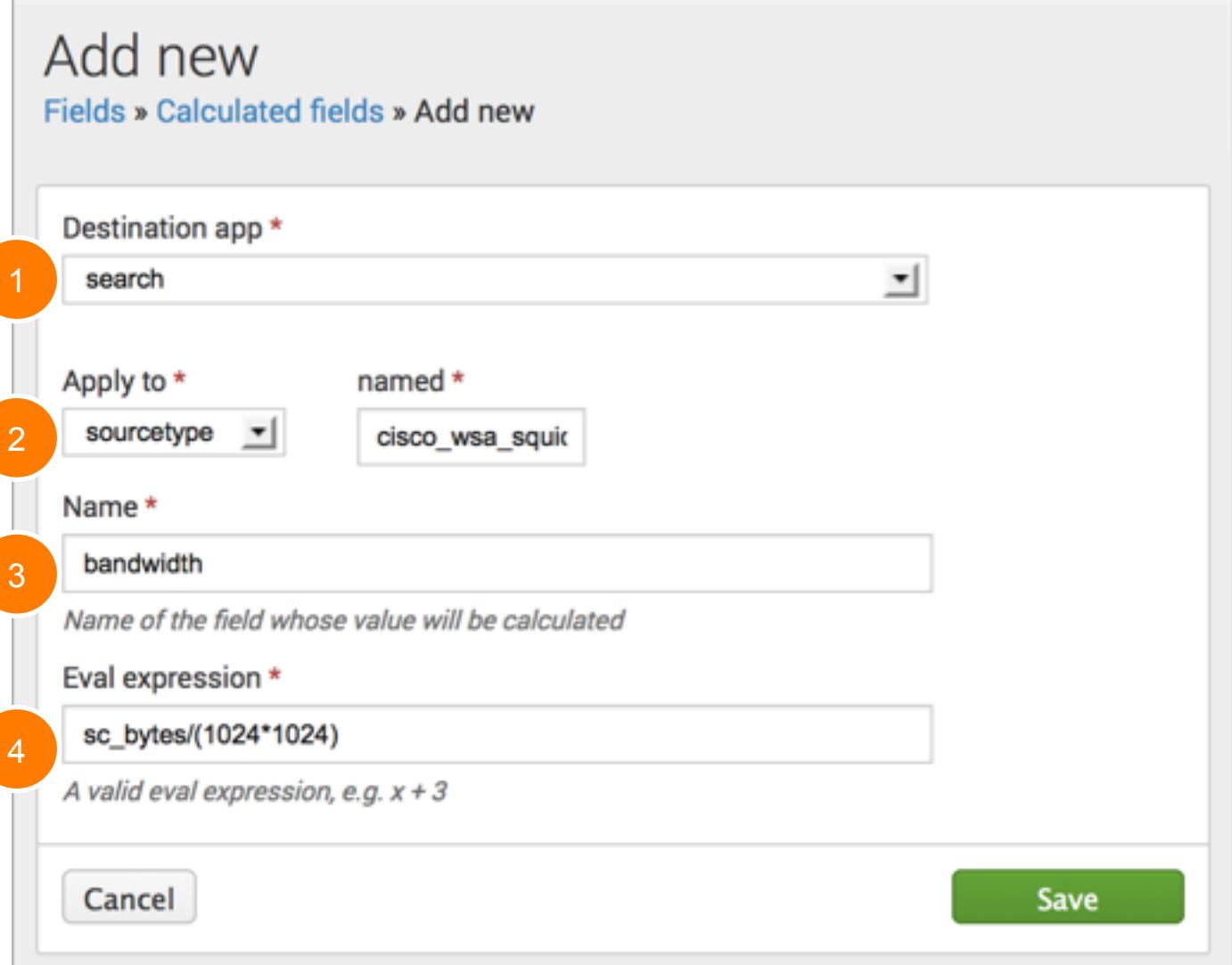
Destination app *
1 search

Apply to *
2 sourcetype named *
cisco_wsa_squic

Name *
3 bandwidth
Name of the field whose value will be calculated

Eval expression *
4 sc_bytes/(1024*1024)
A valid eval expression, e.g. x + 3

Cancel Save



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Using a Calculated Field

After you have created a calculated field, you can use it in a search like any other extracted field:

The screenshot shows the Splunk 'New Search' interface. The search bar contains the command: `sourcetype=cisco_w* | stats sum[bandwidth] as "Bandwidth (MB)" by usage`. The 'usage' field is highlighted with a green box. The search results show 24,614 events from September 15, 2014, to October 15, 2014. The results table has two columns: 'usage' and 'Bandwidth (MB)'. The data is as follows:

usage	Bandwidth (MB)
Borderline	25.102620
Business	43.625436
Personal	193.528267
Unknown	55.086522
Violation	2.034715

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Managing Calculated Fields

Settings > Fields > Calculated Fields

- Edit permissions
- Clone
- Move
- Delete

The screenshot shows the 'Calculated fields' page in the Splunk UI. The title is 'Calculated fields' under 'Fields > Calculated fields'. The search bar includes filters for 'App context: Search & Reporting (search)', 'Owner: Any', and a search input field with a magnifying glass icon. Below the search bar is a checkbox for 'Show only objects created in this app context' with a 'Learn more' link. A green 'New' button is visible. The table below shows one item:

Name	Field name	Eval expression	Owner	App	Sharing	Status	Actions
cisco_wsa_squid : EVAL-bandwidth	bandwidth	sc_bytes/(1024*1024)	cfarrell	search	Private Permissions	Enabled	Clone Move Delete

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Module 4: Creating Field Extractions

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Module Objectives

- Review the Field Extractor (FX) methods
 - Regex
 - Delimiter
- Identify the different options to extract fields using regex or delimiters (FX)
 - Settings
 - Fields sidebar
 - Event actions
- Review the process of extracting fields manually using regular expressions
- Use the Field Extraction Manager to modify extracted fields

Performing Field Extractions

- To extract fields that are static and often needed in searches, use FX
 - Graphical UI
 - Extract fields from events using regex or delimiter
 - Extracted fields persist as a knowledge object
 - Can be shared and re-used in multiple searches
- Access Field Extractor via Settings, Fields Sidebar, or Event Actions menu

Note



For more details, see:
<http://docs.splunk.com/Documentation/Splunk/latest/Knowledge/ExtractfieldsinteractivelywithIFX>

Field Extraction Methods

You can use FX to perform the following field extractions:

- **RegEx**
 - Use this option when your event contains unstructured data like a system log file. FX will attempt to extract the fields using a regular expression that matches similar events.
- **Delimiter**
 - Use this option when your event contains structured data like a .csv file. The data does not have headers and the fields may be separated by:
 - Space
 - Comma
 - Pipe
 - Tabs
 - Other characters

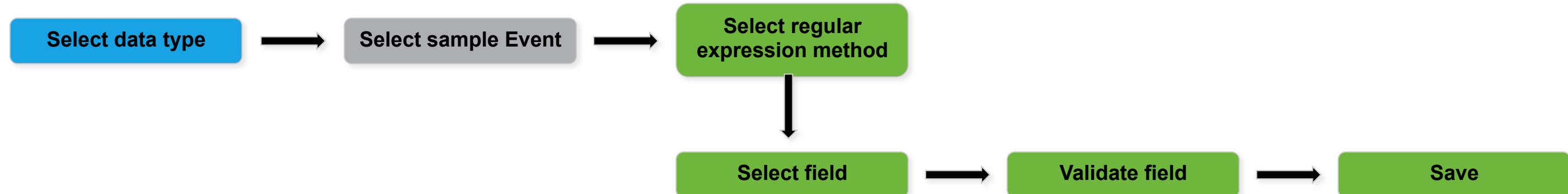
Note



For more details, see:
<http://docs.splunk.com/Documentation/Splunk/latest/Knowledge/ExtractfieldsinteractivelywithIFX>

Field Extraction Workflow – Regular Expression

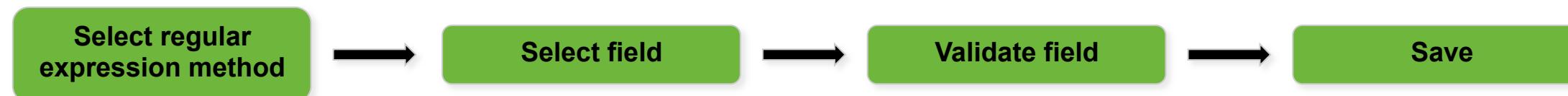
Settings



Fields Sidebar



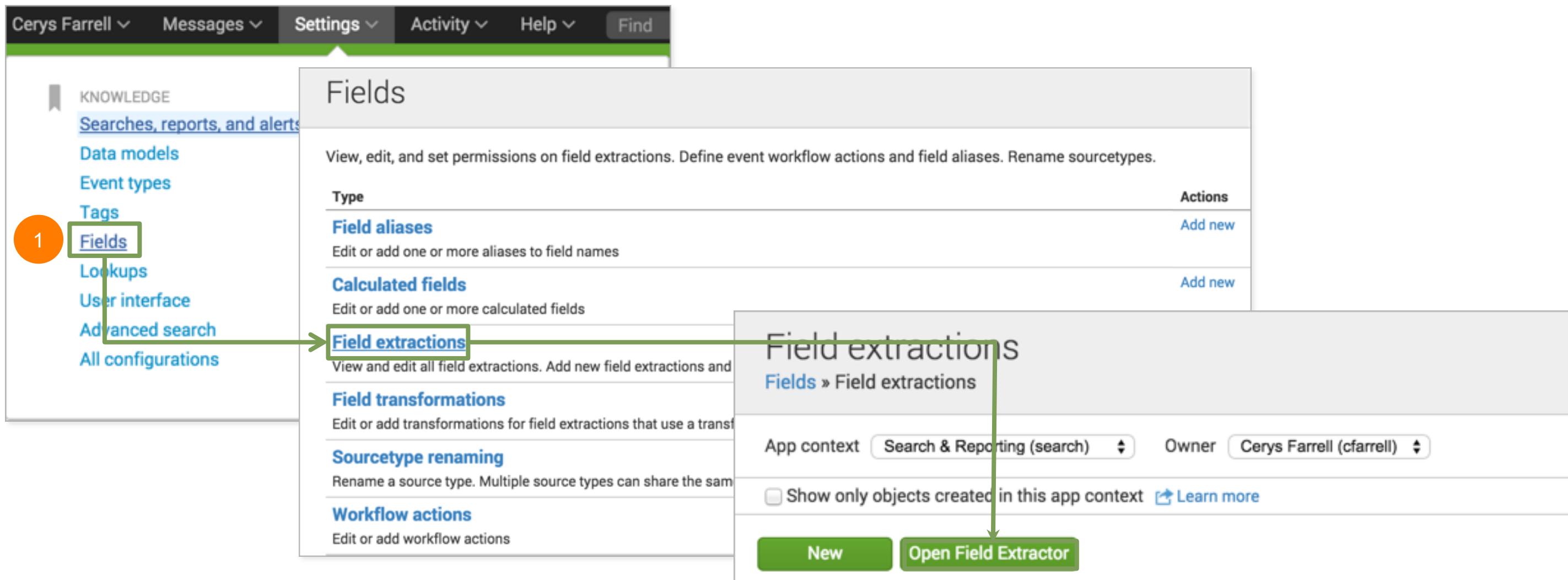
Event Actions



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Regex Field Extractions from Settings

1. Settings > Fields > Field extractions > Open Field Extractor



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Regex Field Extractions from Settings (cont.)

2. Select the Data Type

- sourcetype
- source

3. Select the Source Type

Extract Fields [Existing fields >](#)

Next > Save

Select sample Select method Select fields

Select Sample Event

Choose a source or source type, select a sample event, and click Next to go to the next step. The field extractor will use the event to extract fields. [Learn more](#)

Data Type sourcetype

Source Type – Select Source Type –

linux_secure

linux_secure

About

Format for the /var/log/secure file containing all security related messages on a Linux machine

Privacy Policy

© 2005-2015 Splunk Inc. All rights reserved.

2

3

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Regex Field Extractions from Settings –Select Sample

4. Select a sample event

5. Click Next >

The screenshot shows the 'Extract Fields' wizard with the following steps:

- Step 1: Select sample (highlighted with a red circle)
- Step 2: Select method
- Step 3: Select fields
- Step 4: Save
- Step 5: Next > (highlighted with a red circle)

Select Sample Event

Choose a source or source type, select a sample event, and click Next to go to the next step. The field extractor will use the event to extract fields. [Learn more](#)

[I prefer to write the regular expression myself >](#)

Data Type: sourcetype

Source Type: linux_secure

Events

Tue Jun 30 2015 18:28:56 www2 sshd[5311]: Failed password for invalid user itmadmin from 87.240.128.18 port 1248 ssh2

Events (before 6/30/15 12:29:44.000 PM)

20 per page < Prev 1 2 3 4 5 6 7 8 9 ... Next >

filter Apply Sample: 1,000 events All events

_raw

Tue Jun 30 2015 19:29:29 www3 sshd[3143]: Failed password for invalid user proxy from 67.170.226.218 port 1392 ssh2

Tue Jun 30 2015 19:29:17 www3 sshd[3463]: Failed password for invalid user mysql from 67.170.226.218 port 2790 ssh2

Tue Jun 30 2015 19:29:12 www3 sshd[2879]: Failed password for invalid user irc from 67.170.226.218 port 2033 ssh2

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Regex Field Extractions from Settings –Select Method

6. Select Regular Expression

7. Click Next >

Extract Fields

7

Existing fields >

Select sample Select method Select fields Validate Save

Select Method
Indicate the method you want to use to extract your field(s). [Learn more](#)

Source type `linux_secure`

`Tue Jun 30 2015 18:28:56 www2 sshd[5311]: Failed password for invalid user itmadmin from 87.240.128.18 port 1248 ssh2`

6

Regular Expression

`(.*?)`

Splunk Enterprise will extract fields using a Regular Expression.

Delimiters

`x|y|z`

Splunk Enterprise will extract fields using a delimiter (such as commas, spaces, or characters). Use this method for delimited data like comma separated values (CSV files).

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Regex Field Extractions from Settings –Select Values

8. Select the value(s) you want to extract. In this example, two fields are being extracted.
9. Provide a field name
10. Click **Add Extraction**

Note i
Require option - only the events with that field name will appear in your search results.

Extract Fields

Select sample Select method **Select fields** Validate Save < **Next >** Existing fields >

Select Fields

Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in an event for the regular expression to match. Click on highlighted values in the sample event to modify them. To highlight text that is already part of an existing extraction, first turn off the existing extractions.

[Learn more](#) i

Tue Jun 30 2015 18:28:56 www2 sshd[5311]: Failed password for invalid user itmadmin from 87.240.128.18 8 1248 ssh2

Show Regular Expression >

Preview

If you see incorrect results below, click an additional event to add it to the set of sample events. Highlight its values to include them in the next step.

Events **src_ip**

8 1248 ssh2

9 Field Name: port Sample Value: 1248

10 Add Extraction

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Regex Field Extractions from Settings – Preview

11. Preview the sample events

12. Click Next

The screenshot shows the 'Extract Fields' interface in Splunk. The top navigation bar has tabs: 'Select sample' (disabled), 'Select method' (disabled), 'Select fields' (highlighted with a green dot), 'Validate' (disabled), and 'Save' (disabled). To the right is a progress bar with a green circle at the first step and a grey circle at the second. The number '12' is in an orange circle next to the progress bar. A green 'Next >' button is also in an orange circle. An 'Existing fields >' link is in the top right corner.

Select Fields

Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in an event for the regular expression to match. Click on highlighted values in the sample event to modify them. To highlight text that is already part of an existing extraction, first turn off the existing extractions.

[Learn more ↗](#)

Tue Jun 30 2015 18:28:56 www2 sshd[5311]: Failed password for invalid user itmadmin from 87.240.128.18 port 1248 ssh2

Show Regular Expression > [View in Search ↗](#)

Preview

If you see incorrect results below, click an additional event to add it to the set of sample events. Highlight its values to improve the extraction. You can remove incorrect values in the next step.

Events [src_ip](#) [port](#)

✓ 1,000 events (before 6/30/15 12:50:01.000 PM) [20 per page ↴](#) [< Prev](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) ... [Next >](#)

filter [Apply](#) Sample: 1,000 events [All events ↴](#) All Events [Matches](#) [Non-Matches](#)

	_raw	src_ip	port
✓	Tue Jun 30 2015 19:49:52 www2 sshd[1034]: Failed password for invalid user local from 207.36.232.245 port 1241 ssh2	207.36.232.245	1241
✓	Tue Jun 30 2015 19:49:37 mailsv1 sshd[1580]: Failed password for invalid user dj from 188.143.232.202 port 2660 ssh2	188.143.232.202	2660
✓	Tue Jun 30 2015 19:49:31 mailsv1 sshd[2164]: Failed password for invalid user ubuntu from 188.143.232.202 port 1523 ssh2	188.143.232.202	1523

Generated for James Kim (455 641803) (C) Splunk Inc, not for distribution

Regex Field Extractions from Settings – Validate

13. Validate the proper field values are extracted

14. Click Next

The screenshot shows the 'Extract Fields' interface in Splunk. The 'Validate' step is active, indicated by a green dot on the progress bar. The 'src_ip' field is highlighted in orange, indicating it is the current field being validated. The 'port' field is also present in the raw event data. The validate table displays four events, each with its raw log, extracted fields, and matched values. The first event shows a failed password attempt from IP 207.36.232.245 on port 1241. The second event shows a failed password attempt from IP 188.143.232.202 on port 2660. The third event shows a failed password attempt from IP 188.143.232.202 on port 1523. The fourth event shows an accepted password attempt from IP 10.2.10.163 on port 1097.

_raw	src_ip	port
Tue Jun 30 2015 19:49:52 www2 sshd[1034]: Failed password for invalid user local from 207.36.232.245 port 1241 ssh2	207.36.232.245	1241
Tue Jun 30 2015 19:49:37 mailsv1 sshd[1580]: Failed password for invalid user dj from 188.143.232.202 port 2660 ssh2	188.143.232.202	2660
Tue Jun 30 2015 19:49:31 mailsv1 sshd[2164]: Failed password for invalid user ubuntu from 188.143.232.202 port 1523 ssh2	188.143.232.202	1523
Tue Jun 30 2015 19:49:24 mailsv1 sshd[11061]: Accepted password for nsharpe from 10.2.10.163 port 1097 ssh2	10.2.10.163	1097

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Regex Field Extractions from Settings – Save

15. Review the name for the newly extracted field and set permissions

16. Click Finish

Extract Fields

16

Finish >

Save

Name the extraction and set permissions.

15 Extractions Name EXTRACT- src_ip,port

Owner cfarrell

App search

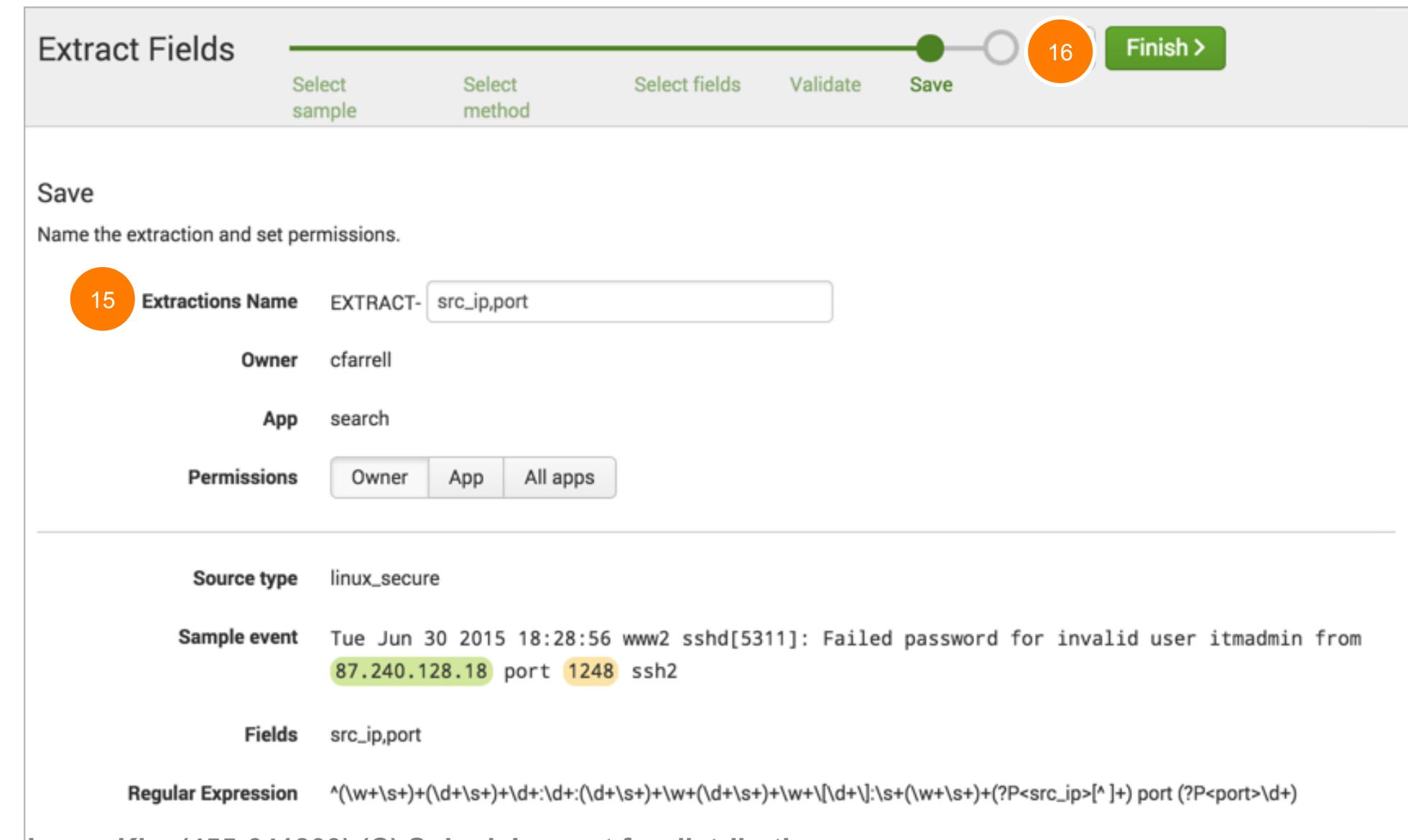
Permissions Owner App All apps

Source type linux_secure

Sample event Tue Jun 30 2015 18:28:56 www2 sshd[5311]: Failed password for invalid user itmadmin from 87.240.128.18 port 1248 ssh2

Fields src_ip,port

Regular Expression ^(\w+\s+)(\d+\s+)+\d+:\d+:(\d+\s+)+\w+(\d+\s+)+\w+\[\d+\]:\s+(\w+\s+)+(?P<src_ip>[^]+) port (?P<port>\d+)



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Using the Extracted Field

New Search Save As ▾ Close

sourcetype=linux_secure| timechart count by src_ip src_ip Last 24 hours 🔍

✓ 7,716 events (6/29/15 4:00:00.000 PM to 6/30/15 4:27:51.000 PM) Job ▾ II ■ ↗ ↓ 🔍 Verbose Mode ▾

Events (7,716) Patterns Statistics (49) Visualization

20 Per Page ▾ Format ▾ Preview ▾ < Prev 1 2 3 Next >

_time	10.1.10.172	10.2.10.163	10.3.10.46	188.138.40.166	194.215.205.19	211.166.11.101	216.221.226.11	27.96.128.0
2015-06-29 16:00:00	11	3	16	0	0	0	3	0
2015-06-29 16:30:00	16	14	36	0	0	0	0	0
2015-06-29 17:00:00	28	8	25	0	0	1	0	0
2015-06-29 17:30:00	25	13	41	0	0	4	0	0
2015-06-29 18:00:00	37	18	17	0	0	0	0	0
2015-06-29 18:30:00	18	8	15	16	0	16	0	0
2015-06-29 19:00:00	22	37	31	0	0	0	0	0
2015-06-29 19:30:00	28	22	23	0	0	0	5	0
2015-06-29 20:00:00	20	21	19	0	0	0	0	6
2015-06-29 20:30:00	11	11	43	0	0	0	0	9

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Regex Field Extractions from the Fields Sidebar

Steps to extract fields:

1. Click **Extract New Fields**
2. Select a sample event
3. Select the **Regex** extraction method
4. Select fields you want to extract and validate
5. Save your field extraction

The screenshot shows the Splunk Fields sidebar with the following interface elements:

- Buttons:** < Hide Fields, All Fields
- Selected Fields:** a host 4, a source 4, a sourcetype 1, a tag 7
- Interesting Fields:** # date_hour 24, # date_mday 2, # date_minute 60, a date_month 1, # date_second 60, a date_wday 2, # date_year 1, a date_zone 1, a eventtype 8, a index 1, # linecount 1, # pid 100+, # port 100+, a process 3, a punct 9, a splunk_server 1, a src_ip 100+, a tag:eventtype 7, # timeendpos 1, # timestamppos 1
- Event Log:** A list of log entries starting with "Tue Jun 30 2015 20:08:22 www1 sshd".
- Bottom Buttons:** 5 more fields, Extract New Fields

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Regex Field Extractions from Event Actions

Steps to extract fields:

1. Select **Extract Fields**
2. Select the **Regex** extraction method
3. Select fields you want to extract and validate
4. Save your field extraction

The screenshot shows the Splunk 'Build Event Type' interface. At the top, there is a log entry: 'Tue Jun 30 2015 20:14:27 mailsv1 sshd[5289]: Failed password for invalid user ssh2'. Below this is a dropdown menu labeled 'Event Actions'. A modal window titled 'Build Event Type' is open, specifically the 'Extract Fields' tab. It contains a 'Show Source' button and a 'tag' checkbox. In the main area, under the heading 'Event', there is a dropdown menu labeled 'eventtype'. To the right of the event type dropdown, several fields are listed with their values and actions: 'mailsv1' (Value), '/opt/log/mailsv1/secure.log' (Value), 'linux_secure' (Value), 'authentication' (Value), 'error' (Value), 'remote' (Value), 'failed_login' (Value), 'nix-all-logs' (Value), 'nix_errors (error)' (Value), 'sshd_authentication (authentication remote)' (Value), 'main' (Value), '1' (Value), '5289' (Value), '2453' (Value), 'sshd' (Value), 'ip-10-222-134-157' (Value), and '128.241.220.82' (Value). Each value has a corresponding 'Actions' column with a dropdown arrow.

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Delimiter Field Extractions

Use delimited field extractions when the event log does not have a header and fields are separated by spaces, commas, or characters

In this example, the fields are separated by commas

>	5/11/15 4:00:04.000 AM	"2015-05-13T08:01:30.000-0400",7036,4,Information,HOST0167,System,296651410	host = splunk01 source = /opt/log/adldapsv1/sysmonitor.log sourcetype = sysmon
>	5/11/15 4:00:04.000 AM	"2015-05-13T08:01:16.000-0400",29,1>Error,HOST0167,System,772103058	host = splunk01 source = /opt/log/adldapsv1/sysmonitor.log sourcetype = sysmon
>	5/11/15 4:00:04.000 AM	"2015-05-13T08:01:09.000-0400",35,4,Information,HOST0201,System,507701378	host = splunk01 source = /opt/log/adldapsv1/sysmonitor.log sourcetype = sysmon

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Field Extraction Workflow (Delimiters)

Settings



Fields Sidebar



Event Actions



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Delimiter Field Extractions from Settings

1. Settings > Fields > Field extractions > Open Field Extractor

The screenshot shows the Splunk Settings interface. On the left, there's a sidebar with a 'Fields' link highlighted by a green box and a circled '1'. A green arrow points from this link to the 'Field extractions' link on the main page. The main page has a title 'Fields' and a sub-section 'Field extractions'. At the bottom of this section are two buttons: 'New' and 'Open Field Extractor', with a green arrow pointing to the 'Open Field Extractor' button.

Cerys Farrell ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

KNOWLEDGE

Searches, reports, and alerts

Data models

Event types

Tags

1 Fields

Lookups

User interface

Advanced search

All configurations

Fields

Type

Field aliases

Calculated fields

Field extractions

View and edit all field extractions. Add new field extractions and

Field transformations

Edit or add transformations for field extractions that use a transfor

Sourcetype renaming

Rename a source type. Multiple source types can share the sam

Workflow actions

Edit or add workflow actions

Field extractions

Fields » Field extractions

App context Search & Reporting (search) Owner Cerys Farrell (cfarrell)

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

New Open Field Extractor

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Delimiter Field Extractions from Settings – Select Sample

2. Select the Data Type

- sourcetype
- source

3. Select the Source Type

The screenshot shows the 'Extract Fields' interface in Splunk. The top navigation bar includes 'Existing fields >', a search icon, 'Next >', and 'Save'. The main title is 'Extract Fields' with a progress bar indicating the current step is 'Select sample'. Below the title are buttons for 'Select method', 'Select fields', and 'Save'. The main content area is titled 'Select Sample Event' with a sub-instruction: 'Choose a source or source type, select a sample event, and click Next to go to the next step. The field extractor will use the event to extract fields.' A link 'Learn more' is provided. Two orange circles with numbers are overlaid on the interface: circle 2 is positioned over the 'Data Type' dropdown which contains 'sourcetype', and circle 3 is positioned over the 'Source Type' dropdown which has 'sysmon' selected. A tooltip for 'sysmon' shows its definition: 'sysmon system monitor'. The bottom right corner of the interface includes the copyright notice '© 2005-2015 Splunk Inc. All rights reserved.'

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Delimiter Field Extractions from Settings – Select Event

4. Select a sample event

5. Click **Next >**

Extract Fields

—
Select sample Select method Select fields Save **5** **Next >** Existing fields >

Select Sample Event
Choose a source or source type, select a sample event, and click Next to go to the next step. The field extractor will use the event to extract fields. [Learn more ↗](#)
[I prefer to write the regular expression myself >](#)

Data Type **sourcetype**

Source Type **sysmon**

4 "2015-06-01-13T08:56:45.000-0400",4743,0,Information,"BUSDEV-007",Security,388851661

Events

✓ 5 events (before 6/30/15 3:00:16.000 PM) 20 per page ▾

filter Apply Sample: 1,000 events ▾ All events ▾

_raw ▾

"2015-06-01-13T08:56:45.000-0400",4743,0,Information,"BUSDEV-007",Security,388851661
"2015-06-01-13T08:01:30.000-0400",7036,4,Information,HOST0167,System,296651410
"2015-06-01-13T08:01:16.000-0400",29,1>Error,HOST0167,System,772103058

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Delimiter Field Extractions from Settings – Select Method

6. Select Delimiters
7. Click Next >

Extract Fields

7

Next >

Select sample Select method Rename fields Save

Select Method

Indicate the method you want to use to extract your field(s). [Learn more](#)

Source type sysmon

"2015-06-01-13T08:56:45.000-0400",4743,0,Information,"BUSDEV-007",Security,388851661

(.*?)

Regular Expression

Splunk Enterprise will extract fields using a Regular Expression.

x|y|z

Delimiters

Splunk Enterprise will extract fields using a delimiter (such as commas, spaces, or characters). Use this method for delimited data like comma separated values (CSV files).

6

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Delimiter Field Extractions from Settings - Select Delimiter

8. Select the Delimiter used in your event

The screenshot shows the 'Extract Fields' interface in Splunk. The current step is 'Rename fields', indicated by a green dot on the progress bar. The 'Select sample' and 'Select method' steps are completed. The 'Save' button is visible at the top right.

Rename Fields

Select a delimiter. In the table that appears, rename fields by clicking on field names or values. [Learn more](#)

Delimiter

Space Comma Tab Pipe Other

Preview

Events field1 field2 field3 field4 field5 field6 field7

✓ 5 events (before 6/30/15 3:16:54.000 PM) 20 per page

filter Apply Sample: 1,000 events All events All Events Matches Non-Matches

	_raw	field1	field2	field3	field4	field5	field6	field7
✓	"2015-06-01-13T08:56:45.000-0400",4743,0,Information,"BUSDEV-007",Security,388851661	"2015-06-01-13T08:56:45.000-0400"	4743	0	Information	"BUSDEV-007"	Security	388851661
✓	"2015-06-01-13T08:01:30.000-0400",7036,4,Information,HOST0167,System,296651410	"2015-06-01-13T08:01:30.000-0400"	7036	4	Information	HOST0167	System	
✓	"2015-06-01-13T08:01:16.000-0400",29,1>Error,HOST0167,System,772103058	"2015-06-01-13T08:01:16.000-0400"	29	1	Error	HOST0167	System	

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

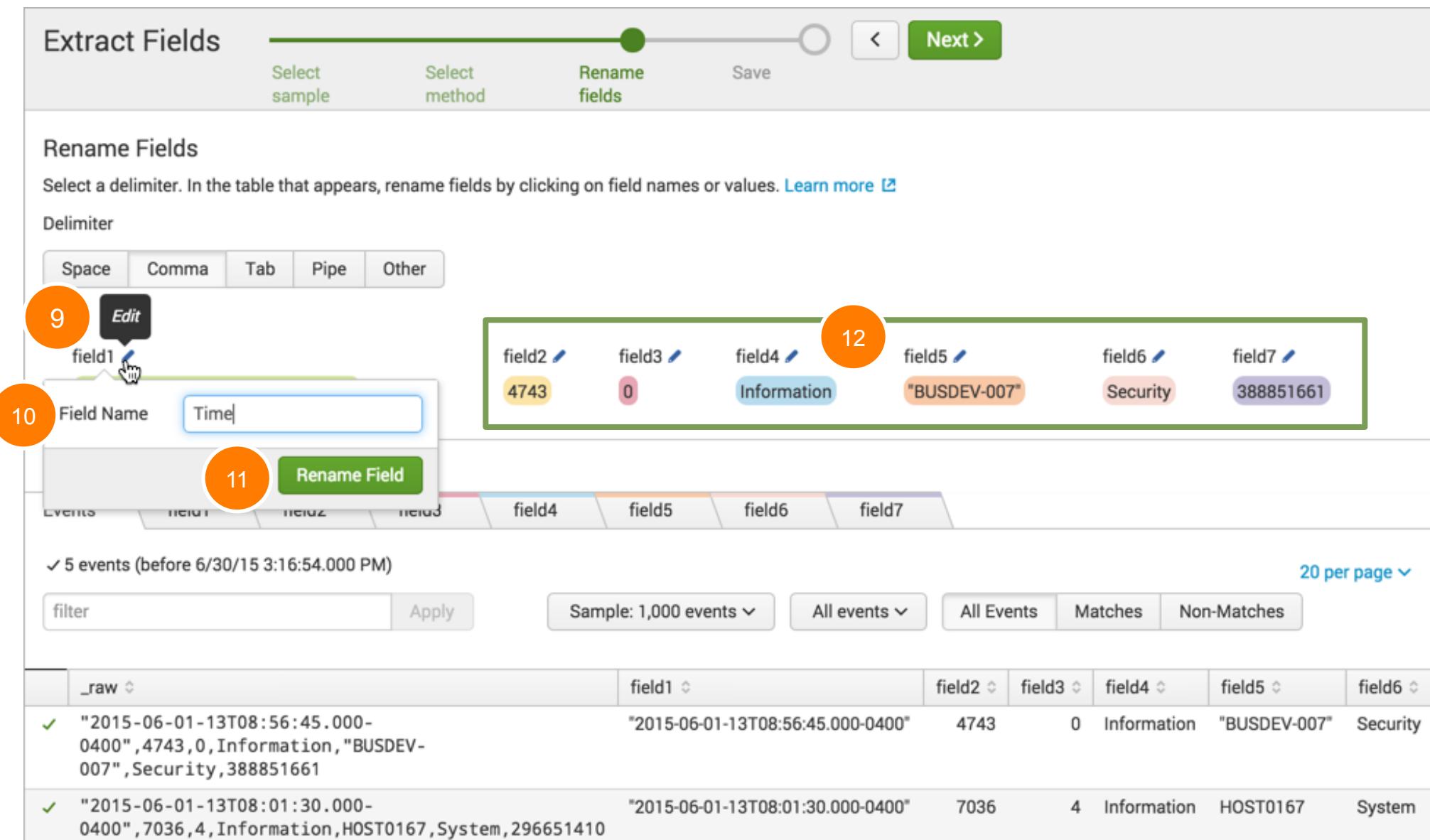
Delimiter Field Extractions from Settings – Rename field

9. Click the  icon next to the default field name

10. Enter a new field name

11. Click **Rename Field**

12. Repeat these steps for all fields



The screenshot shows the 'Extract Fields' interface in Splunk. The top navigation bar has tabs: 'Select sample' (disabled), 'Select method' (disabled), 'Rename fields' (selected), and 'Save'. Below the tabs is a progress bar with a green dot over 'Rename fields'. To the right are 'Next >' and 'Save' buttons.

The main area is titled 'Rename Fields' with the sub-instruction: 'Select a delimiter. In the table that appears, rename fields by clicking on field names or values.' A 'Learn more' link is available.

A 'Delimiter' section includes tabs: Space, Comma, Tab, Pipe, and Other. The 'Space' tab is selected.

The data table lists fields: field1, field2, field3, field4, field5, field6, and field7. Each field has a blue pencil icon for renaming. The first row (field1) is highlighted with a green box. Step 9 points to the pencil icon on 'field1'. Step 10 points to the 'Field Name' input field containing 'Time'. Step 11 points to the 'Rename Field' button. Step 12 points to the 'Information' value in the 'field4' row.

Below the table, it says '✓ 5 events (before 6/30/15 3:16:54.000 PM)' and '20 per page'. There are buttons for 'filter', 'Apply', 'Sample: 1,000 events', 'All events', 'All Events', 'Matches', and 'Non-Matches'.

The bottom part of the interface shows a table of event data:

_raw	field1	field2	field3	field4	field5	field6	field7
"2015-06-01-13T08:56:45.000-0400",4743,0,Information,"BUSDEV-007",Security,388851661	"2015-06-01-13T08:56:45.000-0400"	4743	0	Information	"BUSDEV-007"	Security	
"2015-06-01-13T08:01:30.000-0400",7036,4,Information,HOST0167,System,296651410	"2015-06-01-13T08:01:30.000-0400"	7036	4	Information	HOST0167	System	

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Delimiter Field Extractions from Settings – Rename field (cont.)

13. After all the fields are renamed, click **Next >**

The screenshot shows the 'Extract Fields' interface in Splunk. The progress bar indicates step 13 of 13, with the 'Rename fields' step highlighted. The 'Next >' button is circled in red. Below the progress bar, the 'Rename Fields' section displays a table of event fields. The 'Time' field is highlighted in green, showing the value "2015-06-01-13T08:56:45.000-0400". Other fields shown include EventCode (4743), EventType (0), Type (Information), ComputerName ("BUSDEV-007"), LogName (Security), and RecordNumber (388851661). Below the table, a 'Preview' section shows a list of 5 events with columns for Events, Time, EventCode, EventType, Type, ComputerName, LogName, and RecordNumber. The first two events are fully visible, showing raw log data and extracted field values.

_raw	Time	EventCode	EventType	Type	ComputerName	LogName	RecordNumber
✓ "2015-06-01-13T08:56:45.000-0400", 4743, 0, Information, "BUSDEV-007", Security, 388851661	"2015-06-01-13T08:56:45.000-0400"	4743	0	Information	"BUSDEV-007"	Security	388851661
✓ "2015-06-01-13T08:01:30.000-0400", 7036, 4, Information, HOST0167, System, 296651410	"2015-06-01-13T08:01:30.000-0400"	7036	4	Information	HOST0167		

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Delimiter Field Extractions from Settings – Save

14. Review the name for your extraction and click **Finish >**

Extract Fields

14

Save

Select sample Select method Rename fields Save

Save
Name the extraction and set permissions.

Extractions Name REPORT- sysmon

Owner cfarrell

App search

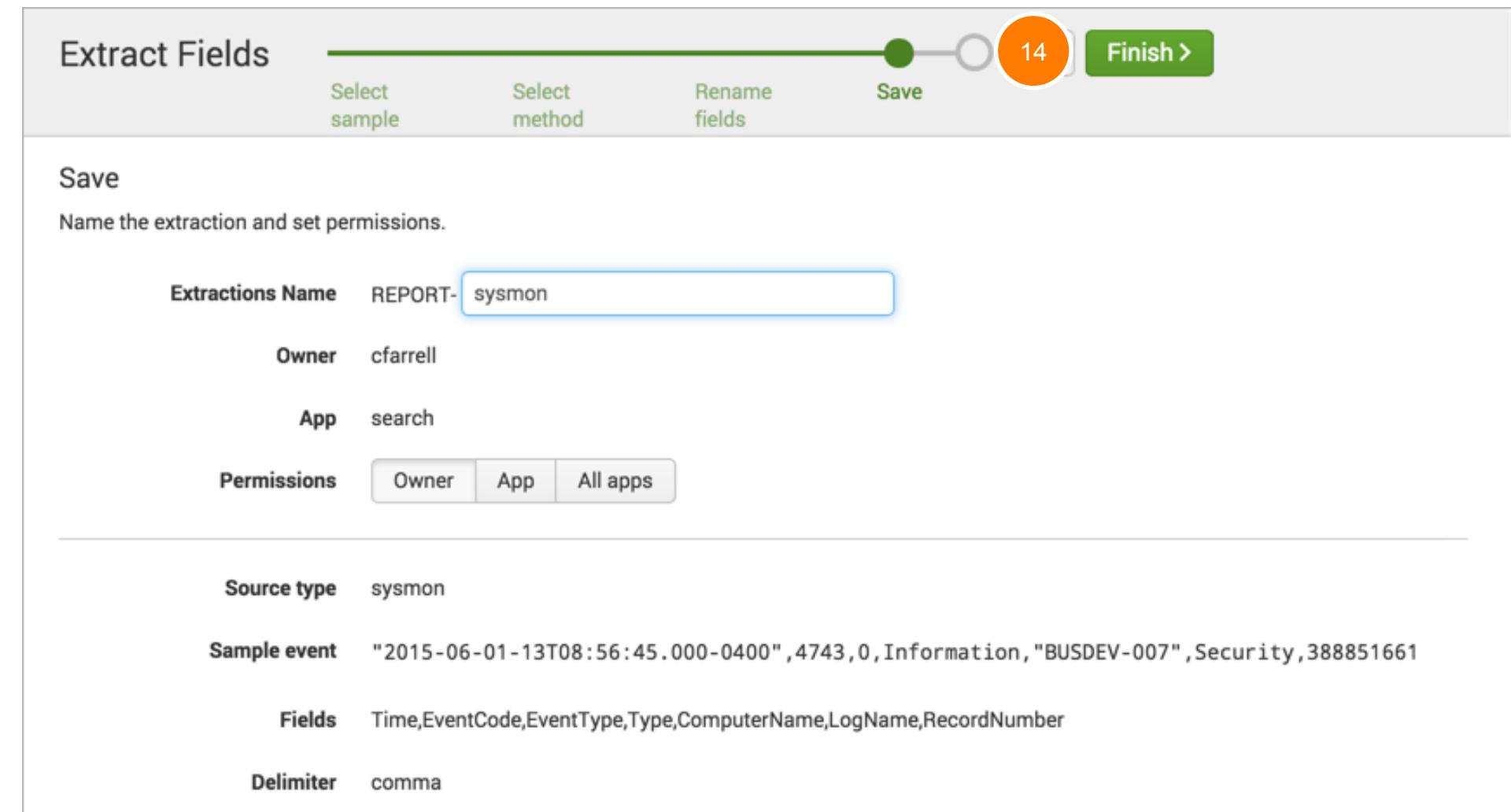
Permissions Owner App All apps

Source type sysmon

Sample event "2015-06-01-13T08:56:45.000-0400",4743,0,Information,"BUSDEV-007",Security,388851661

Fields Time,EventCode,EventType,Type,ComputerName,LogName,RecordNumber

Delimiter comma



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Delimiter Field Extractions from the Fields Sidebar

Steps to extract fields:

1. Click **Extract New Fields**
2. Select a sample event
3. Select the **Delimiters** extraction method
4. Rename fields
5. Save your field extraction

The screenshot shows the Splunk Fields sidebar with the following interface elements:

- Buttons:** < Hide Fields, All Fields
- Section Headers:** Selected Fields, Interesting Fields
- Selected Fields:** a host 4, a source 4, a sourcetype 1, a tag 7
- Interesting Fields:** # date_hour 24, # date_mday 2, # date_minute 60, a date_month 1, # date_second 60, a date_wday 2, # date_year 1, a date_zone 1, a eventtype 8, a index 1, # linecount 1, # pid 100+, # port 100+, a process 3, a punct 9, a splunk_server 1, a src_ip 100+, a tag:eventtype 7, # timeendpos 1, # timestamppos 1
- Links:** 5 more fields, Extract New Fields

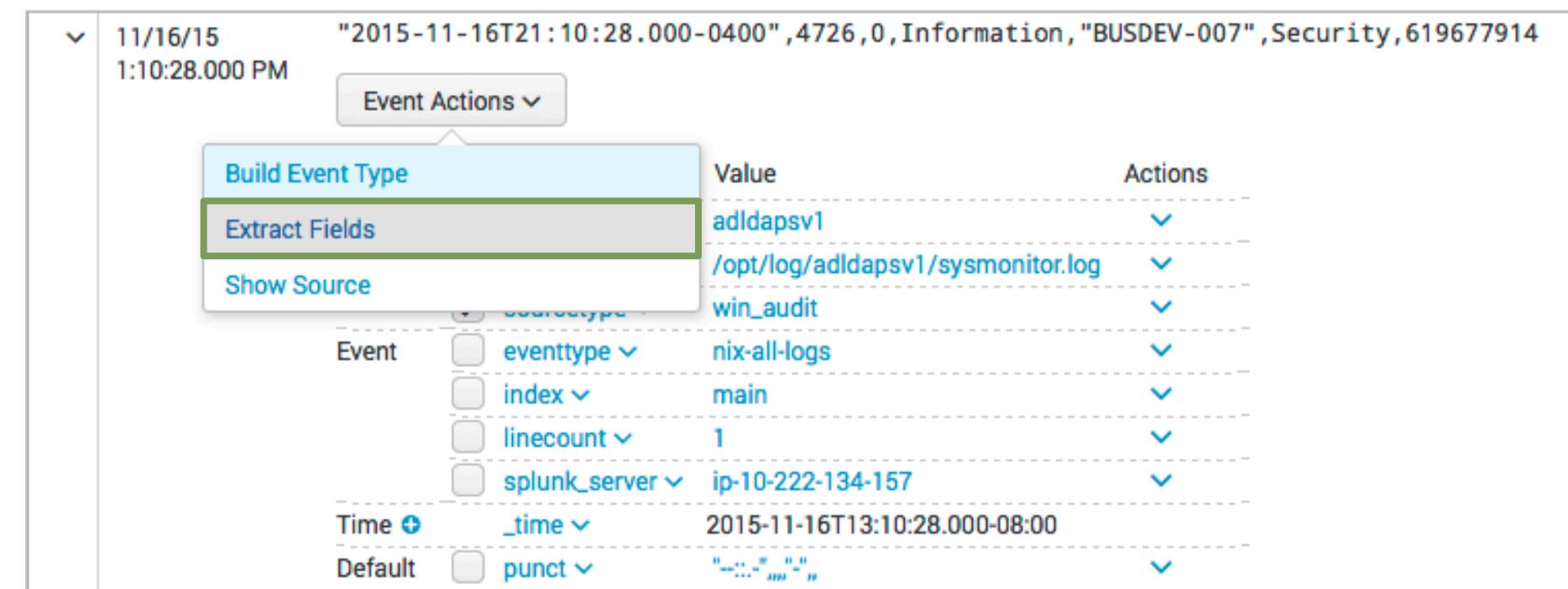
A large diagonal shadow effect is cast over the sidebar area.

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Delimiter Field Extractions from Event Actions

Steps to extract fields:

1. Click **Extract Fields**
 2. Select the **Delimiters** extraction method
 3. Select fields you want to extract and validate
 4. Save your field extraction



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Editing Regex for Field Extractions

1. From **Select Method**, click **Regular Expression**
2. Click **Next >**

The screenshot shows the 'Extract Fields' interface in Splunk. The top navigation bar has tabs: 'Select method' (highlighted in green), 'Select fields', 'Validate', and 'Save'. A progress bar indicates the current step is 'Select method'. Below the tabs, the title 'Select Method' is displayed with the sub-instruction 'Indicate the method you want to use to extract your field(s). [Learn more](#)'. The source type is set to 'linux_secure'. A sample log entry is shown: 'Wed Jul 01 2015 02:36:03 www1 sshd[56828]: Accepted password for nsharpe from 10.2.10.163 port 3327 ssh2'. Two extraction methods are presented: 'Regular Expression' (selected) and 'Delimiters'. The 'Regular Expression' section contains the pattern '(.*?)' and a note: 'Splunk Enterprise will extract fields using a Regular Expression.' The 'Delimiters' section contains the pattern 'x|y|z' and a note: 'Splunk Enterprise will extract fields using a delimiter (such as commas, spaces, or characters). Use this method for delimited data like comma separated values (CSV files.)'.

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Editing Regex for Field Extractions – Select Field

3. Select the field to extract.
4. Provide a **Field Name**
5. Click **Add Extraction**

Note i

For more information about Splunk Regular Expressions, see <http://docs.splunk.com/Documentation/Splunk/6.2/Knowledge/AboutSplunkregularexpressions>

Extract Fields Existing fields >

Select method Select fields Validate Save

Next < >

Select Fields

Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in an event for the regular expression to match. Click on highlighted values in the sample event to modify them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. [Learn more](#)

Wed Jul 01 2015 02:36:03 www1 sshd[56828]: Accepted password [REDACTED] 3 nsharpe from 10.2.10.163 port 3327 ssh2

3

Extract Require

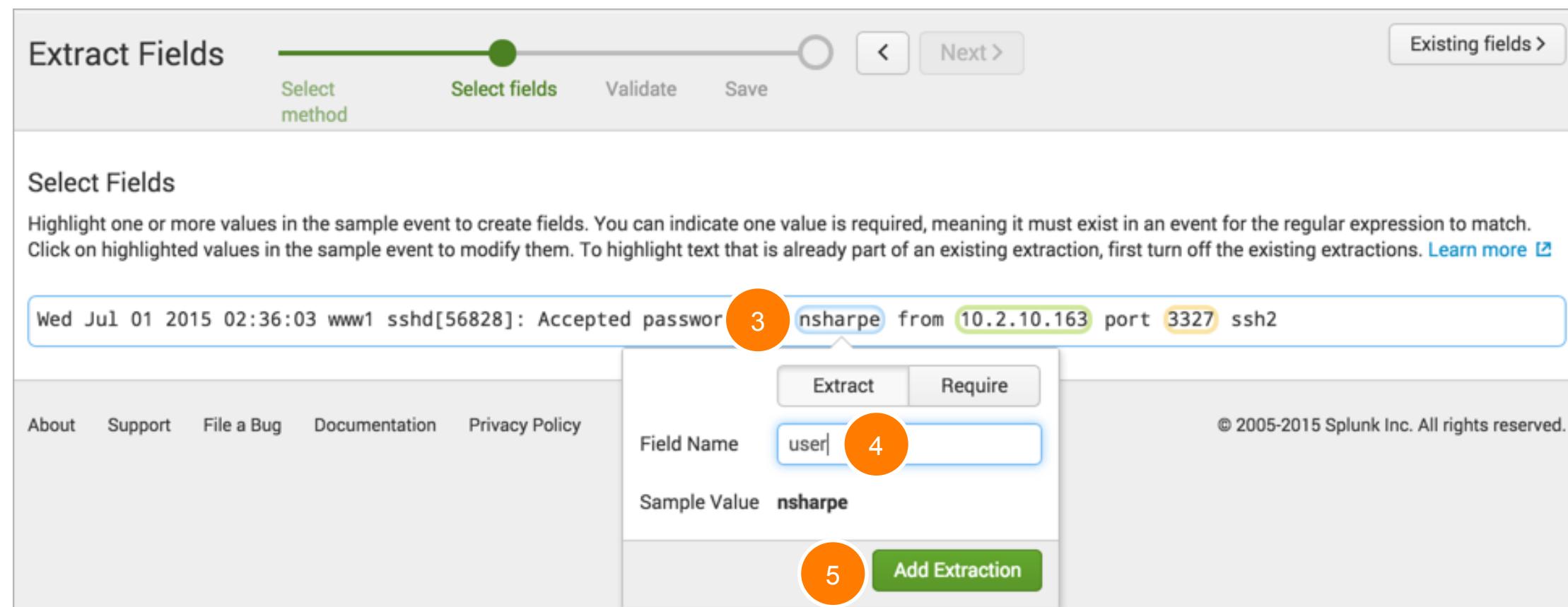
About Support File a Bug Documentation Privacy Policy

Field Name user 4

Sample Value nsharpe

5 Add Extraction

© 2005-2015 Splunk Inc. All rights reserved.



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Editing Regex for Field Extractions – Show Regex

6. Click **Show Regular Expression >**
7. Click **Edit the Regular Expression**

The screenshot shows two instances of the Splunk Extract Fields interface side-by-side. Both instances have a similar layout with tabs for 'Select method', 'Select fields', 'Validate', and 'Save'. A green arrow points from the 'Show Regular Expression' button in the left instance to the 'Edit the Regular Expression' button in the right instance.

Left Instance (Step 6):

- Select Fields**:
Highlight one or more values in the sample event to create fields. Click on highlighted values in the sample event to modify them.
[Link]
- Sample Event:
Wed Jul 01 2015 02:36:03 www1 sshd[56828]: Accepted password for nsharpe from 10.2.10.163 port 3327 ssh2
- Show Regular Expression >** (highlighted with a green box)

Right Instance (Step 7):

- Select Fields**:
Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in an event for the regular expression to match. Click on highlighted values in the sample event to modify them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. [Learn more](#)
[Link]
- Sample Event:
Wed Jul 01 2015 02:36:03 www1 sshd[56828]: Accepted password for nsharpe from 10.2.10.163 port 3327 ssh2
- Hide Regular Expression ▾**
- View in Search ↗**
- Edit the Regular Expression** (highlighted with a green box)

RegEx Display:
^(?:[^ \n]*){10}(?P<user>\w+)

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Editing Regex for Field Extractions – Modify RegEx

8. Update the regular expression
9. Click **Save**

***Once you edit the regular expression, you cannot go back to the Field Extractor UI**

The screenshot shows the 'Extract Fields' page in Splunk. At the top, there are buttons for 'Extract Fields' (highlighted with orange circle 8), '< Back', and 'Existing fields >'. Below this is a warning message: 'If you manually edit and then preview the regular expression below, you cannot return to the automatic field extraction workflow.' A note says to 'Use the event listing below to validate the field extractions produced by your regular expression.' The 'Regular Expression' field contains the value '^(:[^ \n]*){10}(?P<user>\w+)'. To the right of this field are links to 'Regular Expression Reference' and 'View in Search'. At the bottom, there are tabs for 'Events' and 'user' (highlighted with orange circle 9), and buttons for 'Preview' (disabled) and 'Save'.

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Editing Regex for Field Extractions - Save

10. Review the **Extractions Name** and set permissions

11. Click **Finish**

Extract Fields < Back > Finish 11

Save
Name the extraction and set permissions.

10 **Extractions Name** EXTRACT- user

Owner cfarrell

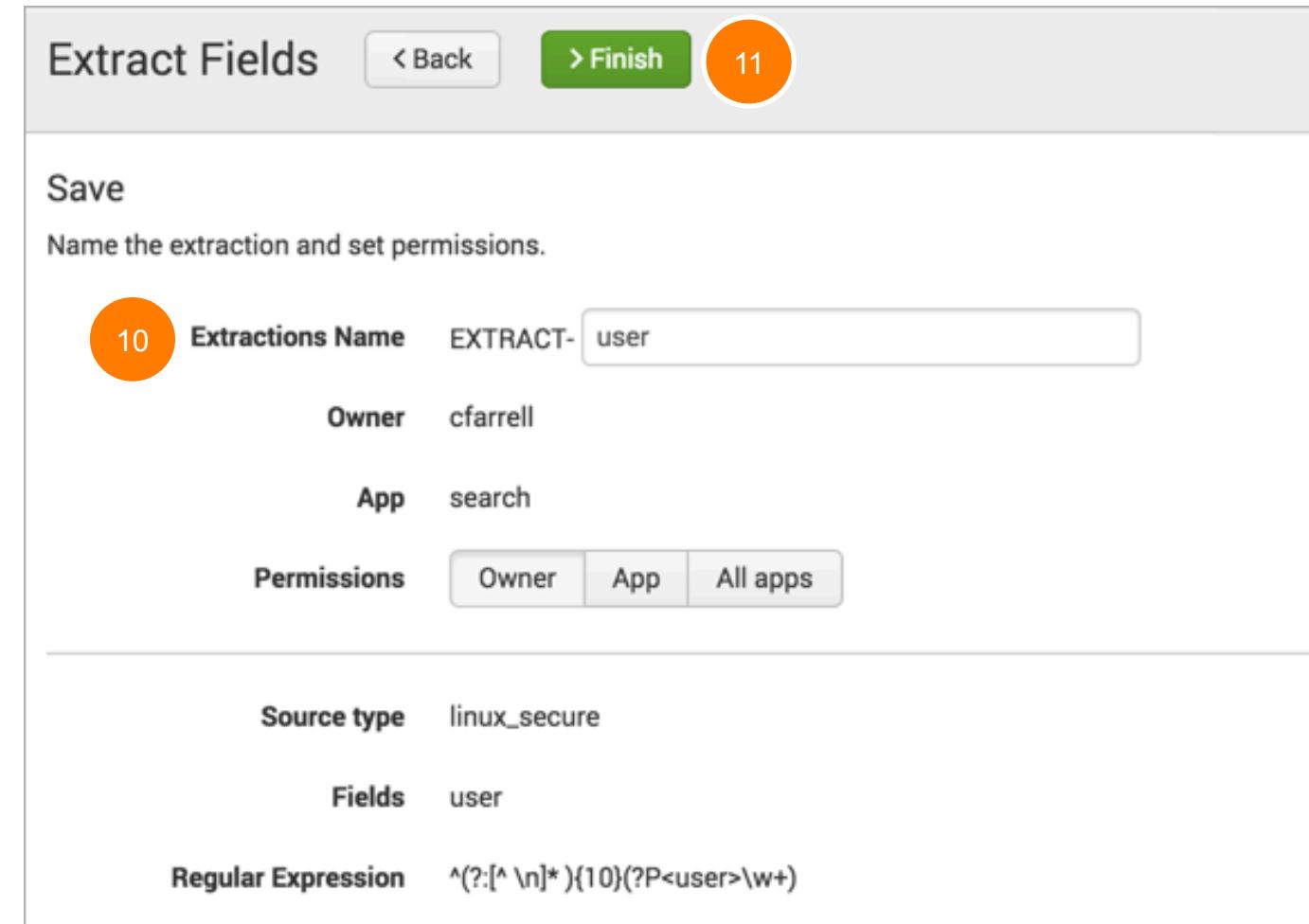
App search

Permissions Owner App All apps

Source type linux_secure

Fields user

Regular Expression `^(?:[^ \n]*)(10)(?P<user>\w+)`



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Managing Field Extractions

Settings > Fields > Field Extractions

- Edit permissions
- Move
- Delete

Note



For more information about directly editing these objects go to:
<http://docs.splunk.com/Documentation/Splunk/latest/Admin/Propsconf>
<http://docs.splunk.com/Documentation/Splunk/latest/Admin/Transformsconf>

Field extractions

Fields » Field extractions

App context Search & Reporting (search) Owner Cerys Farrell (cfarrell)

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

New Open Field Extractor

Showing 1-3 of 3 items Results per page 25

Name	Type	Extraction/Transform	Owner	App	Sharing	Status	Actions
linux_secure : EXTRACT-ip_port	Inline	<code>^(\\w+\\s+)+(\\d+\\s+)+\\d+:\\d:(\\d+\\s+)+\\w+(\\d+\\s+)+\\w+\\n\\d+:\\s+(\\w+\\s+)+(?P<src_ip>[^]+) port (?P<port>\\d+)</code>	cfarrell	search	Private Permissions	Enabled	Move Delete
linux_secure : EXTRACT-user	Inline	<code>^(?:[^ \\n]*){10}(?P<user>\\w+)</code>	cfarrell	search	Private Permissions	Enabled	Move Delete
sysmon : REPORT-sysmon	Uses transform	REPORT-sysmon	cfarrell	search	Private Permissions	Enabled	Move Delete

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Module 5: Creating Tags and Event Types

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Module Objectives

- Create and use tags
- Describe event types and their uses
- Create an event type

Describing Tags

- Tags are like nicknames that you create for related field/value pairs
- Tags make your data more understandable and less ambiguous
 - Example: The following rating system needs to be applied to product categories
 - General – content is approved for all audiences
 - Teen – content is approved for audiences 13+
 - Mature – content is approved for audiences 18+



- You can create one or more tags for any field/value combination
- Tags are case sensitive

Creating Tags

To create a tag:

1. Click on the arrow for event details
2. Under **Actions**, click the down arrow
3. Select **Edit Tags**
4. Name the tag(s) (comma-separated if using multiple tags)

The screenshot illustrates the process of creating a tag in Splunk. It consists of three main panels:

- Event Details Panel (Left):** Shows an event from 10/26/15 at 3:34:00.000 PM. The event details are:
host = www1 | source = /opt/log/www1/access.log | sourcetype = access_combined
The first three fields are highlighted with a green box and labeled with orange circles containing numbers 1, 2, and 3.
- Action Panel (Top Right):** An "Event Actions" dropdown menu is open. It lists various event fields with their current values. A green arrow points from the "Edit Tags" button in the event details panel to the "Edit Tags" button in this panel. The "Edit Tags" button is highlighted with a green box and labeled with orange circle 3. Another green arrow points from the "Edit Tags" button here to the "Edit Tags" button in the modal window.
- Create Tags Modal (Bottom Right):** A modal window titled "Create Tags". It has two input fields: "Field Value" containing "categoryId=STRATEGY" and "Tag(s)" containing "Teen". The "Tag(s)" field is highlighted with a green box and labeled with orange circle 4. A green arrow points from the "Edit Tags" button in the action panel to this field.

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Viewing Tags

If a selected field value is tagged, the value of the tag appears in the results

i	Time	Event
>	11/26/14 9:55:22.000 AM	201.28.109.162 - - [26/Nov/2014:17:55:22] "POST /category.screen?categoryId=STRATEGY&JSESSIONID=SD4SL6FF10ADFF4956 HTTP 1.1" 200 1109 "http://www.buttercupgames.com/category.screen?categoryId=STRATEGY" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729;.NET4.0C)" 975 categoryId = STRATEGY Teen host = www2 source = /opt/log/www2/access.log sourcetype = access_combined

cart.do?action=addtocart&itemId=EST-26&prod

TP 1.1" 200 3466 "http://www.buttercupgames

lla/5.0 (Macintosh; Intel Mac OS X 10_7_4)

AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 907

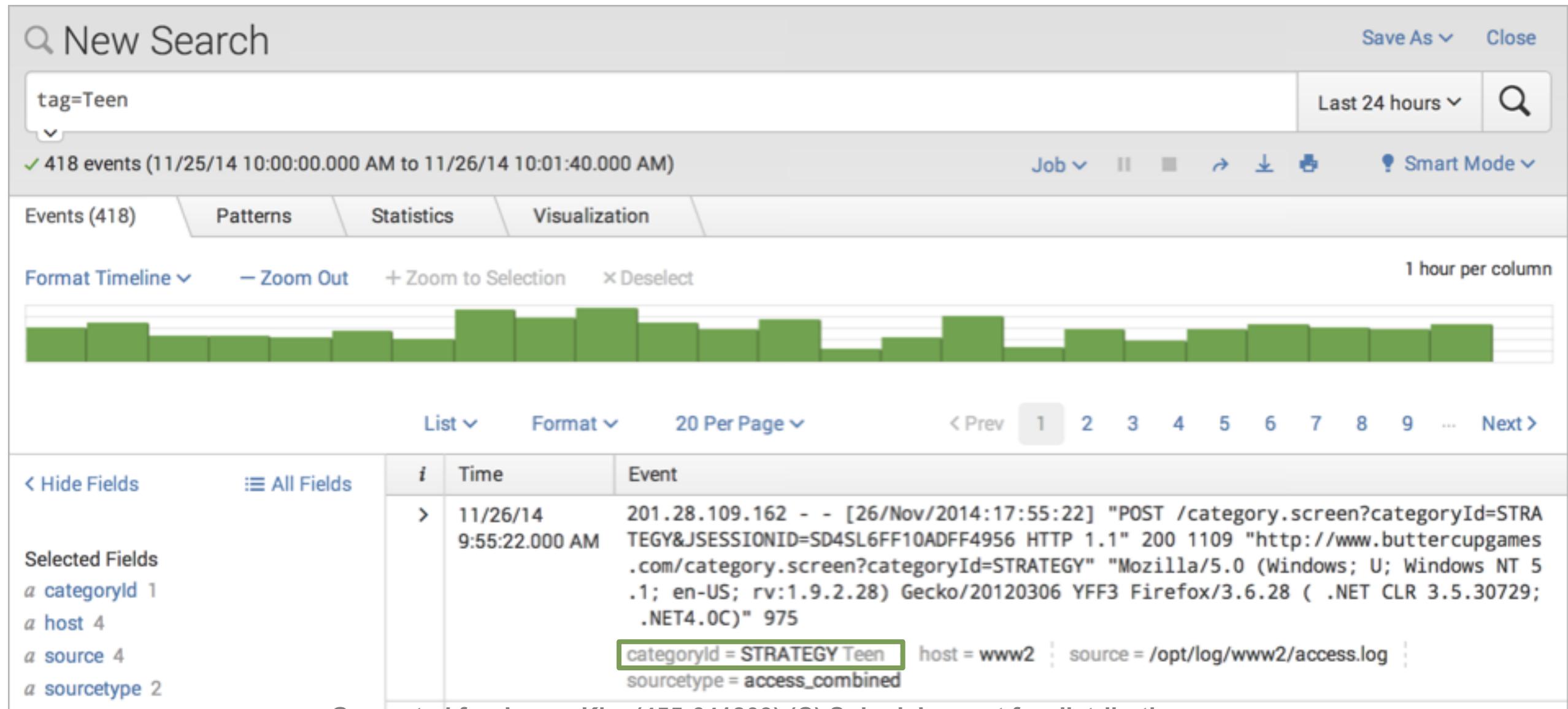
Event Actions ▾

Type	Field	Value	Actions
Selected	host	www3	▼
	source	/opt/log/www3/access.log	▼
	sourcetype	access_combined	▼
Event	JSESSIONID	SD5SL8FF2ADFF4955	▼
	action	addtocart	▼
	bytes	3466	▼
	categoryId	STRATEGY (Teen)	▼

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Using Tags

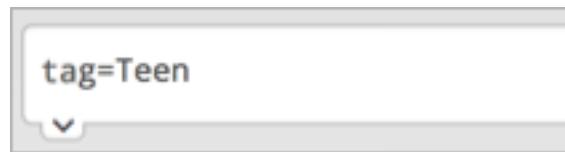
To use tags in a search, use the syntax: **tag=<tag name>**



Searching for Tags

To search for a tag associated with a value:

- tag=<tagnname>



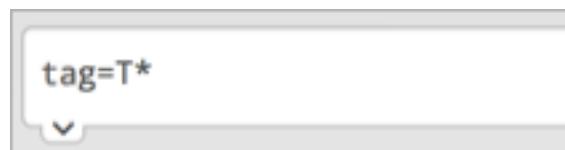
To search for a tag associated with a value on a specific field:

- tag::<field>=<tagnname>



To search for a tag using a partial field value:

- use (*) wildcard



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Managing Tags

Settings > Tags

You can display tags by field value pair, tag name, or all unique tag objects

The screenshot shows the Splunk web interface. At the top is a navigation bar with links for 'Cerys Farrell', 'Messages', 'Settings' (which is currently selected), 'Activity', 'Help', and 'Find'. Below the navigation bar are two main categories: 'KNOWLEDGE' (Searches, reports, and alerts; Data models; Event types) and 'DATA' (Report acceleration summaries). On the left, a sidebar lists several configuration options: Tags (selected and highlighted with a green box), Fields, Lookups, User interface, Advanced search, and All configurations. A green arrow points from the 'Tags' link in the sidebar to the 'Tags' page content area. The 'Tags' page itself has a title 'Tags' and a subtitle 'Manage tags on field values.' It contains three 'Tag links' with 'Actions' columns: 'List by field value pair' (Add new), 'List by tag name' (Add new), and 'All unique tag objects' (Add new).

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Managing Tags (cont.)

Settings > Tags > List by field value pair

- Edit permissions
- Disable all tags for pair – disables the tag in searches and prevents it from being listed under **List by Tag Name** and **All unique tag objects**
- Clone
- Move
- Delete

List by field value pair
Tags » List by field value pair

App context: Search & Reporting (search) Owner: Cerys Farrell (cfarrell)

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

New

Showing 1-3 of 3 items Results per page: 25

Field value pair	Tag name	App	Sharing	Status	Actions
categoryId=SHOOTER	Mature	search	Private Permissions	Enabled Disable all tags for pair	Clone Move Delete
categoryId=SPORTS	General	search	Private Permissions	Enabled Disable all tags for pair	Clone Move Delete
categoryId=STRATEGY	Teen	search	Private Permissions	Enabled Disable all tags for pair	Clone Move Delete

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Managing Tags (cont.)

Settings > Tags > List by tag name

- Enable/Disable
- Clone
- Delete

List by tag name
Tags » List by tag name

App context: Search & Reporting (search) Owner: Cerys Farrell (cfarrell)

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

New

Showing 1-3 of 3 items Results per page: 25

Tag name	Field value pair	Owner	App	Status	Actions
General	categoryId=SPORTS	cfarrell	search	Enabled Disable	Clone Delete
Mature	categoryId=SHOOTER	cfarrell	search	Enabled Disable	Clone Delete
Teen	categoryId=STRATEGY	cfarrell	search	Enabled Disable	Clone Delete

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Managing Tags (cont.)

Settings > Tags > All unique tag objects

- Edit Permissions
- Enable/Disable
- Clone
- Move
- Delete

All unique tag objects
Tags » All unique tag objects

App context: Search & Reporting (search) Owner: Cerys Farrell (cfarrell)

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

New

Showing 1-3 of 3 items Results per page: 25

Tag name	Field value pair	Owner	App	Sharing	Status	Actions
Mature	categoryId=SHOOTER	cfarrell	search	Private Permissions	Enabled Disable	Clone Move Delete
General	categoryId=SPORTS	cfarrell	search	Private Permissions	Enabled Disable	Clone Move Delete
Teen	categoryId=STRATEGY	cfarrell	search	Private Permissions	Enabled Disable	Clone Move Delete

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Adding/Changing the Tag Name

Click **List by field value pair** to add another tag or change the name of the tag

The screenshot shows the Splunk interface for managing tags. On the left, a table lists three items under 'Field value pair'. The first item, 'categoryId=SHOOTER', has its 'Tag name' field ('Mature') highlighted with a green border. A modal window titled 'categoryId=SHOOTER' is open over the table, containing a text input field labeled 'Tag name' with the placeholder 'Enter one tag per textfield'. The input field contains the value 'Mature'. The modal also includes a 'Delete' button next to the input field and a 'Save' button at the bottom right. A large green arrow points from the 'Mature' tag in the table to the 'Tag name' input field in the modal.

Field value pair	Tag name	App	Sharing	Status
categoryId=SHOOTER	Mature	search	Private Permissions	Enabled Dis
categoryId=SPORTS	General	search	Private Permissions	Enabled Dis
categoryId=STRATEGY	Teen	search	Private Permissions	Enabled Dis

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Adding/Changing the Field Value Pair

Click **List by tag name** to add or edit the field value pair for the tag

The screenshot shows two windows from a Splunk interface. The left window is titled 'List by tag name' and shows a table of three items: 'General' (categoryId=SPORTS), 'Mature' (categoryId=SHOOTER), and 'Teen' (categoryId=STRATEGY). The 'Teen' row is highlighted with a green box. A green arrow points from the 'Teen' row to the right window. The right window is titled 'Teen' and shows a 'Field value pair' dialog. It contains a text input field with 'categoryId=STRATEGY' and a 'Delete' link. Below it is an 'Add another field' link. At the bottom are 'Cancel' and 'Save' buttons.

Tag name	Field value pair	Owner	App
General	categoryId=SPORTS	cfarrell	search
Mature	categoryId=SHOOTER	cfarrell	search
Teen	categoryId=STRATEGY	cfarrell	search

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

What is an Event Type?

- A method of categorizing events based on a search
- A useful method for institutional knowledge capturing and sharing
- Can be tagged to group similar types of events

Event Type Scenario

The sales team would like to track all online purchases by product type. An event type for each product category needs to be created:

- Accessories
- Tees
- Arcade games
- Sports games
- Strategy games
- Shooter games

Event Type Example

To differentiate these events, create individual event types

- purchase_accessories

```
4/29/14      221.204.246.72 - - [29/Apr/2014:17:30:58] "POST /cart.do?action=purchase&itemId=EST-19&JSESSIONID=SD9SL5FF9ADFF496  
5:30:58.000 PM 2 HTTP 1.1" 200 2804 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-19&categoryId=ACCESSORIES&  
productId=WC-SH-A02" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 202  
host = www1 | source = /opt/log/www1/access.log | sourcetype = access_combined
```

- purchase_tee

```
4/29/14      202.179.8.245 - - [29/Apr/2014:17:06:33] "POST /cart.do?action=purchase&itemId=EST-6&JSESSIONID=SD10SL2FF4ADFF4964  
5:06:33.000 PM  HTTP 1.1" 200 1260 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-6&categoryId=TEE&productId=  
MB-AG-T01" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CL  
R 3.5.30729; .NET4.0C; .NET4.0E; MS-RTC LM 8; InfoPath.1)" 964  
host = www3 | source = /opt/log/www3/access.log | sourcetype = access_combined
```

Creating an Event Type

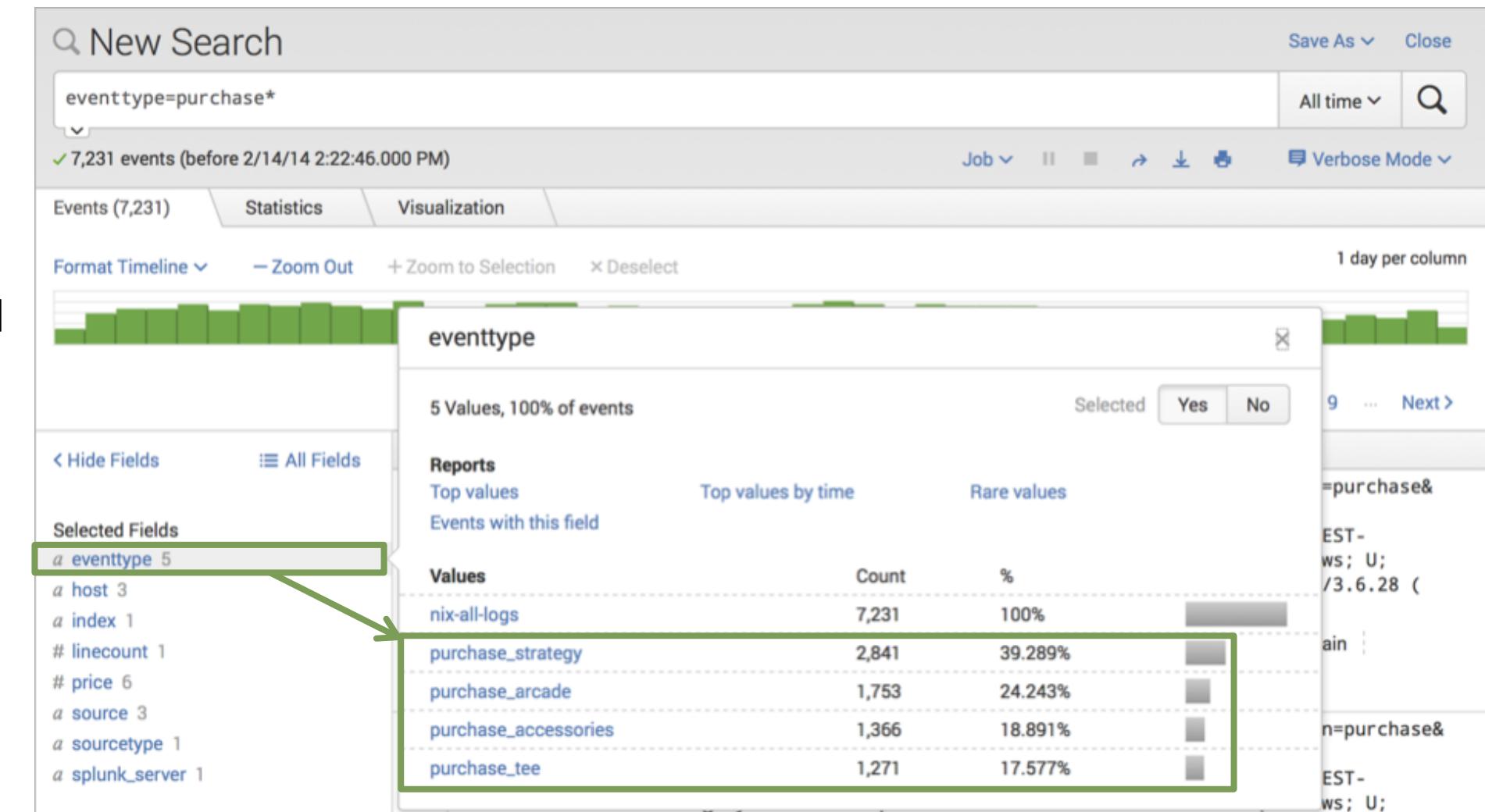
1. Run a search and verify that all results meet your event type criteria
2. From the **Save As** menu, select **Event Type**
3. Provide a name for your event type (name should not contain spaces)

The screenshot illustrates the steps to create an event type in Splunk. On the left, a search results page shows a search for "sourcetype=access_combined action=purchase categoryId=tee". It displays 3,672 events from October 2, 2014, to October 3, 2014. A context menu is open over the search bar, with the "Event Type" option highlighted. An arrow points from this option to the "Save As Event Type" dialog box on the right. The dialog box contains fields for Name ("purchase_tee"), Tags ("purchase, tee"), Color ("none"), and Priority ("5"). A note at the bottom states: "Determines which style wins, when an event has more than one event type." At the bottom right of the dialog is a green "Save" button.

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Using Event Types

- To verify the event type, search for `eventtype=purchase*`
- ‘`eventtype`’ displays in the Fields sidebar and can be added as a selected field
- Splunk evaluates the events and applies the appropriate event types at search time
- Using the Fields sidebar, you can easily view the individual event types, the number of events, and percentage



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Tagging Event Types

You can tag event types two ways:

1. **Settings > Event Types**
2. **Event details > Actions**

The screenshot shows the 'Event Actions' interface. In the 'Type' dropdown, 'Selected' is checked and 'eventtype' is selected. The 'Value' column lists 'nix-all-logs', 'purchase_strategy', 'www3', and 'main'. A green box highlights the 'Edit Tags' button in the 'Actions' column for the 'purchase_strategy' row. A green arrow points from this row down to a 'Create Tags' modal window. The 'Create Tags' window has a 'Field Value' input field containing 'eventtype=purchase_strategy' and a 'Tag(s)' input field containing 'purchase strategy'. A note at the bottom says 'Comma or space separated list of tags.' At the bottom of the window are 'Cancel' and 'Save' buttons.

purchase_strategy
Event types » purchase_strategy

Search string *

sourcetype=access_combined action=purchase categoryId=strategy

Tag(s)
purchase, strategy

Enter a comma-separated list of tags.

Priority
5

Highest priority shows up first in a result.

Cancel Save

- The range for the priority is 1 (highest) to 10 (lowest)

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Managing Event Types

Settings > Event Types

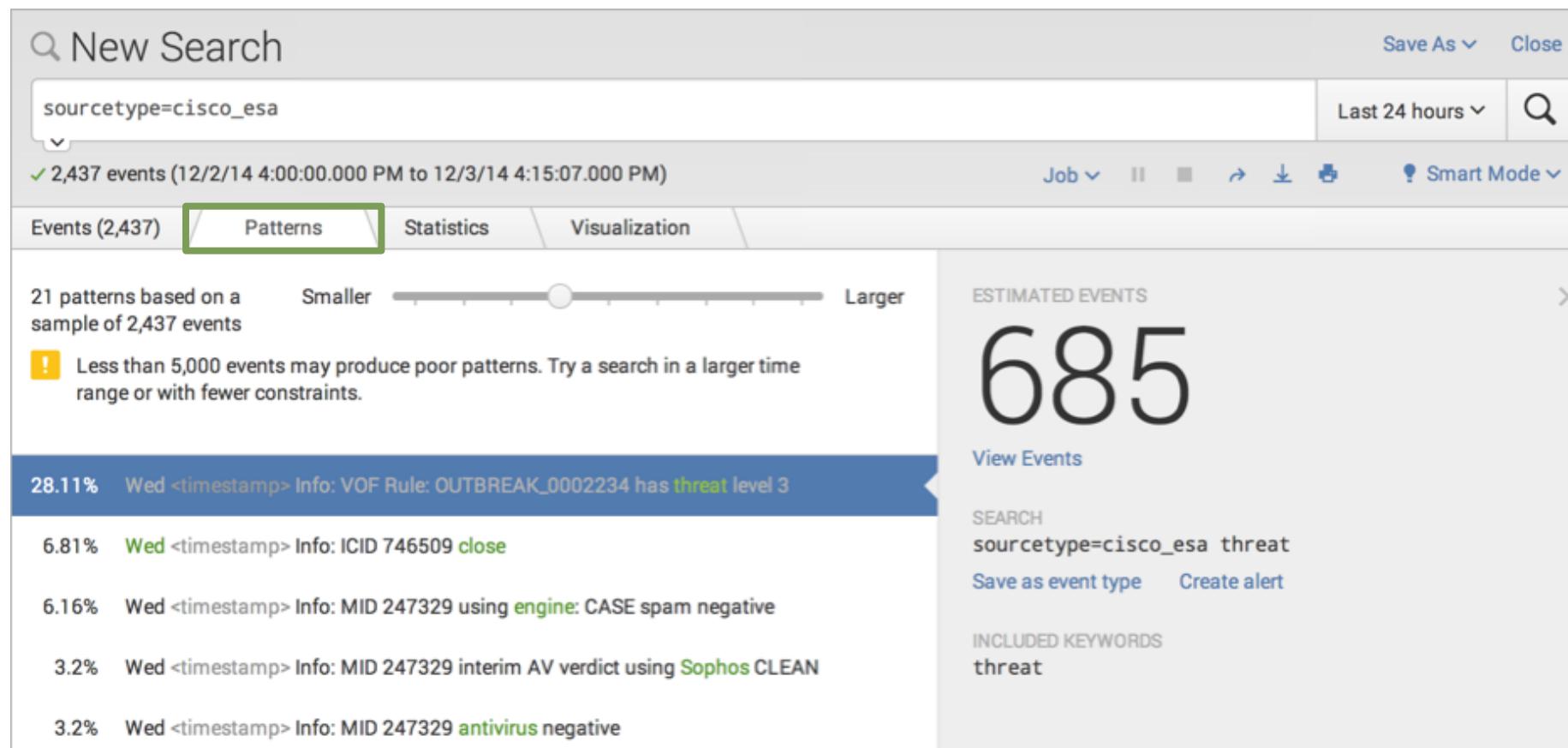
- Edit permissions
- Enable/disable
- Clone
- Move
- Delete

Event types									
App context		Search & Reporting (search)	Owner	Any					
<input checked="" type="checkbox"/> Show only objects created in this app context Learn more									
New									
Showing 1-4 of 4 items							Results per page <input type="button" value="50"/>		
Name	Search string	Tag(s)	Owner	App	Sharing	Status	Actions		
purchase_accessories	sourcetype=access_combined action=purchase categoryId=accessories		admin	search	Private Permissions	Enabled Disable	Clone Move Delete		
purchase_arcade	sourcetype=access_combined action=purchase categoryId=arcade		admin	search	Private Permissions	Enabled Disable	Clone Move Delete		
purchase_strategy	sourcetype=access_combined action=purchase categoryId=strategy	purchase strategy	admin	search	Private Permissions	Enabled Disable	Clone Move Delete		
purchase_tee	sourcetype=access_combined action=purchase categoryId=tee		admin	search	Private Permissions	Enabled Disable	Clone Move Delete		

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Creating an Event Type via Patterns

1. Run a search
2. Select the **Patterns** tab



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Creating an Event Type via Patterns (cont.)

3. Select a pattern where the results meet your event type criteria
4. Click **Save as event type**

The screenshot shows the Splunk interface for creating an event type. On the left, a search results page displays a search for "sourcetype=cisco_esa". It shows 2,437 events over the last 24 hours. A modal window titled "Save As Event Type" is open on the right, containing fields for Name, Tags, Color, and Priority. The "Name" field is highlighted with a green border and contains the value "Potential email threats". The "Search" field in the modal also contains the same search query. The "Save" button at the bottom right of the modal is visible.

New Search

sourcetype=cisco_esa

2,437 events (12/2/14 4:00:00.000 PM to 12/3/14 4:15:07.000 PM)

Events (2,437) Patterns Statistics Visualization

21 patterns based on a sample of 2,437 events

Smaller Larger

Less than 5,000 events may produce poor patterns. Try a search in a larger time range or with fewer constraints.

28.11% Wed <timestamp> Info: VOF Rule: OUTBREAK_0002234 has threat level 3

6.81% Wed <timestamp> Info: ICID 746509 close

6.16% Wed <timestamp> Info: MID 247329 using engine: CASE spam negative

3.2% Wed <timestamp> Info: MID 247329 interim AV verdict using Sophos CLEAN

3.2% Wed <timestamp> Info: MID 247329 antivirus negative

ESTIMATED EVENTS
685

View Events

SEARCH sourcetype=cisco_esa threat

Save as event type Create alert

INCLUDED KEYWORDS threat

Save As Event Type

Search sourcetype=cisco_esa threat

Name Potential email threats

Tags Optional

Color red

Priority 3

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

Cancel Save

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Event Types vs. Saved Reports

- Should I create an event type or a saved report?

- Event Types

- Categorize events based on a search string
 - Tag event types to organize data into categories
 - The eventtype field can be included in a search string
 - Does not include a time range

- Saved Reports

- Search criteria will not change
 - Includes a time range and formatting of the results
 - Share reports with Splunk users and may be added to dashboards

Module 6: Creating Workflow Actions

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Module Objectives

- Create a GET workflow action
- Create a POST workflow action
- Create a Search workflow action

What are Workflow Actions?

- Execute workflow actions from an event in your search results to interact with external resources or run another search
 - **GET** - pass information to an external web resource
 - **POST** - send field values to an external resource
 - **Search** - use field values to perform a secondary search



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Creating a GET Workflow Action

Settings > Fields > Workflow actions > New

1. Select the app
2. Name the workflow action with no spaces or special characters
3. Define the label, which will appear in the Event Action menu
4. Determine if your workflow action applies to a field or event type

Add new

Fields » Workflow actions » Add new

Destination app *

1 search

Name *

2 get_whois_info

Enter a unique name without spaces or special characters. This is used for identifying your workflow action later on within Splunk Settings.

Label *

3 Get info for IPaddress:\$src_ip\$

Enter the label that appears for this action. Optionally, incorporate a field's value by enclosing the field name in dollar signs, e.g. 'Search for ticket number : \$ticketnum\$'.

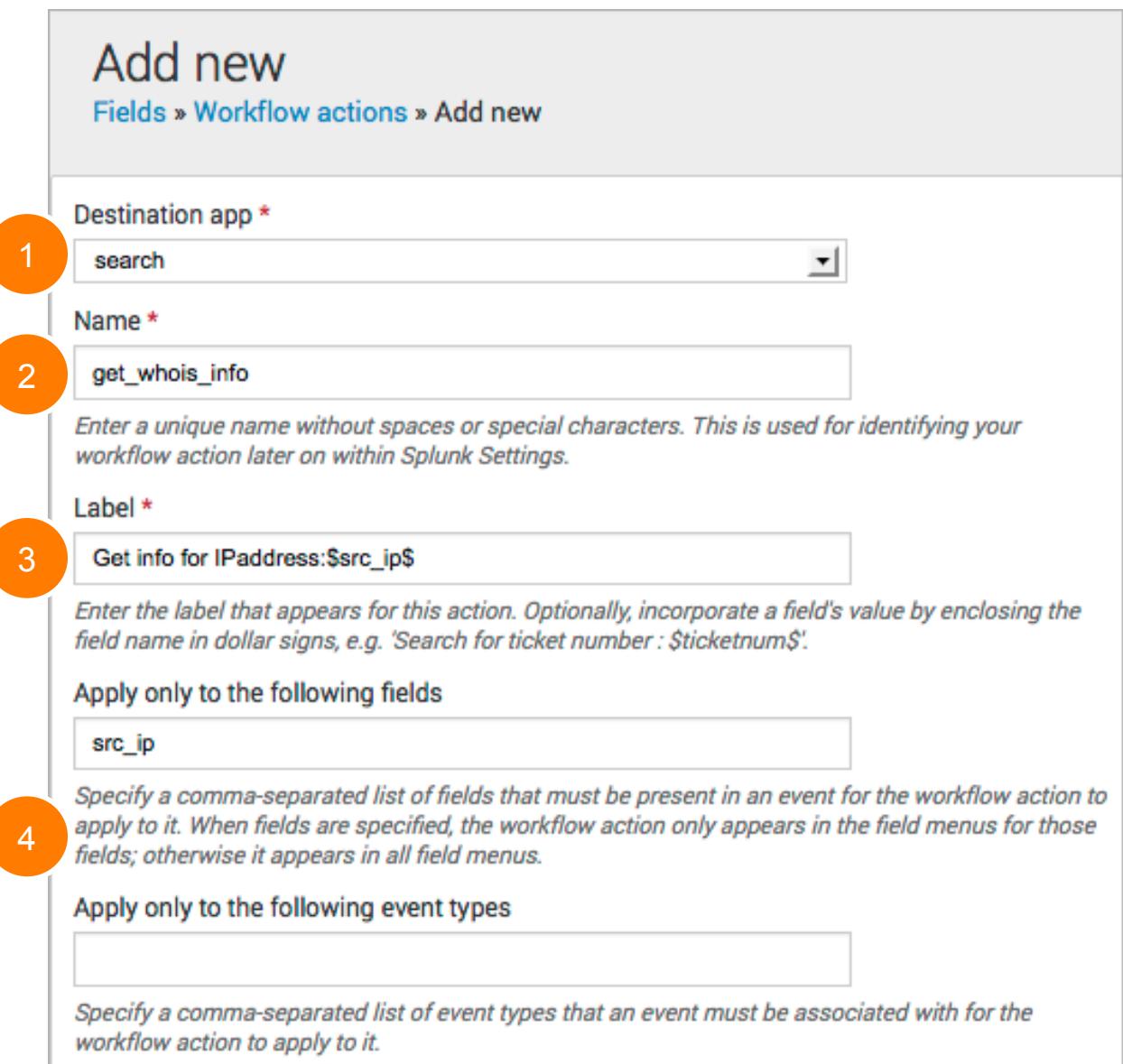
Apply only to the following fields

4 src_ip

Specify a comma-separated list of fields that must be present in an event for the workflow action to apply to it. When fields are specified, the workflow action only appears in the field menus for those fields; otherwise it appears in all field menus.

Apply only to the following event types

Specify a comma-separated list of event types that an event must be associated with for the workflow action to apply to it.



Creating a GET Workflow Action (cont.)

5. From the **Show action in** drop down list, select **Event menu**
6. Select **link** as the **Action type**
7. Enter the URI of where the user will be directed
8. Specify if the link should open in a **New window** or **Current window**
9. Select the Link method of **get**
10. Save

The screenshot shows the 'Link configuration' section of a Splunk Knowledge Object creation form. The fields and their corresponding numbered steps from the list are:

- Step 5: 'Show action in' dropdown set to 'Event menu'.
- Step 6: 'Action type' dropdown set to 'link'.
- Step 7: 'URI' input field containing 'http://who.is/whois-ip/ip-address/\$src_ip\$'. A tooltip below the field says: 'Enter the location to link to. Optionally, specify fields by enclosing the field name in dollar signs, e.g. http://www.google.com/search?q=\$host\$.'
- Step 8: 'Open link in' dropdown set to 'New window'.
- Step 9: 'Link method' dropdown set to 'get'.
- Step 10: 'Save' button at the bottom right.

Testing the GET Workflow Action

The screenshot shows a Splunk search interface on the left and a knowledge object profile on the right.

Splunk Search Results:

2/11/14	Tue Feb 11 2014 23:39:16	www3 sshd[8851]: failed password for nsharpe from 10.2.10.163 port 9767 ssh2
---------	--------------------------	--

Action Menu:

- Event Actions ▾
- Build Event Type
- Get info for IPAddress:10.2.10.163
- Extract Fields
- Show Source

Event Type Selection:

Value

- www3
- /opt/log/www
- linux_secour
- failed_login
- nix-all-logs
- nix_errors (e
- sshd_authent

Knowledge Object Profile:

10.2.10.163 address profile

Overview Diagnostics

Overview for 10.2.10.163

Updated 0 seconds ago

NetRange:	10.0.0.0 - 10.255.255.255
CIDR:	10.0.0.0/8
OriginAS:	
NetName:	PRIVATE-ADDRESS-ABLK-RFC1918-IANA-RESERVED
NetHandle:	NET-10-0-0-0-1
Parent:	
NetType:	IANA Special Use
Comment:	These addresses are in use by many millions of independently operated networks, which might be as small as a single computer connected to a home gateway, and are automatically configured in hundreds of millions of devices. They are only intended for use within a private context and traffic that needs to cross the Internet will need to use a different, unique address.

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Creating a Post Workflow Action

Settings > Fields > Workflow actions > New

Complete steps 1 – 6 as described in the previous example, Creating a GET Workflow Action

Add new
Fields » Workflow actions » Add new

Destination app *

1 search

Name *

2 post_multiple_attempts_to_open_port

Enter a unique name without spaces or special characters. This is used for identifying your workflow action later on within Splunk Settings.

Label *

3 Create ticket - multiple attempts to open port:\$port\$

Enter the label that appears for this action. Optionally, incorporate a field's value by enclosing the field name in dollar signs, e.g. 'Search for ticket number : \$Ticketnum\$'.

Apply only to the following fields

4 port

Specify a comma-separated list of fields that must be present in an event for the workflow action to apply to it. When fields are specified, the workflow action only appears in the field menus for those fields; otherwise it appears in all field menus.

Apply only to the following event types

5 Event menu

Specify a comma-separated list of event types that an event must be associated with for the workflow action to apply to it.

6 link

Show action in

Action type *

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Creating a Post Workflow Action (cont.)

7. Enter the URI of where the user will be directed
8. Open the link in a **New window** or Current window
9. Select the Link method of **post**
10. Provide post argument parameters
11. Save

Link configuration

URI *

7 http://jira.pwnyinc.com/network_issue?new

Enter the location to link to. Optionally, specify fields by enclosing the field name in dollar signs, e.g. http://www.google.com/search?q=\$host\$.

Open link in

8 New window

Link method

9 post

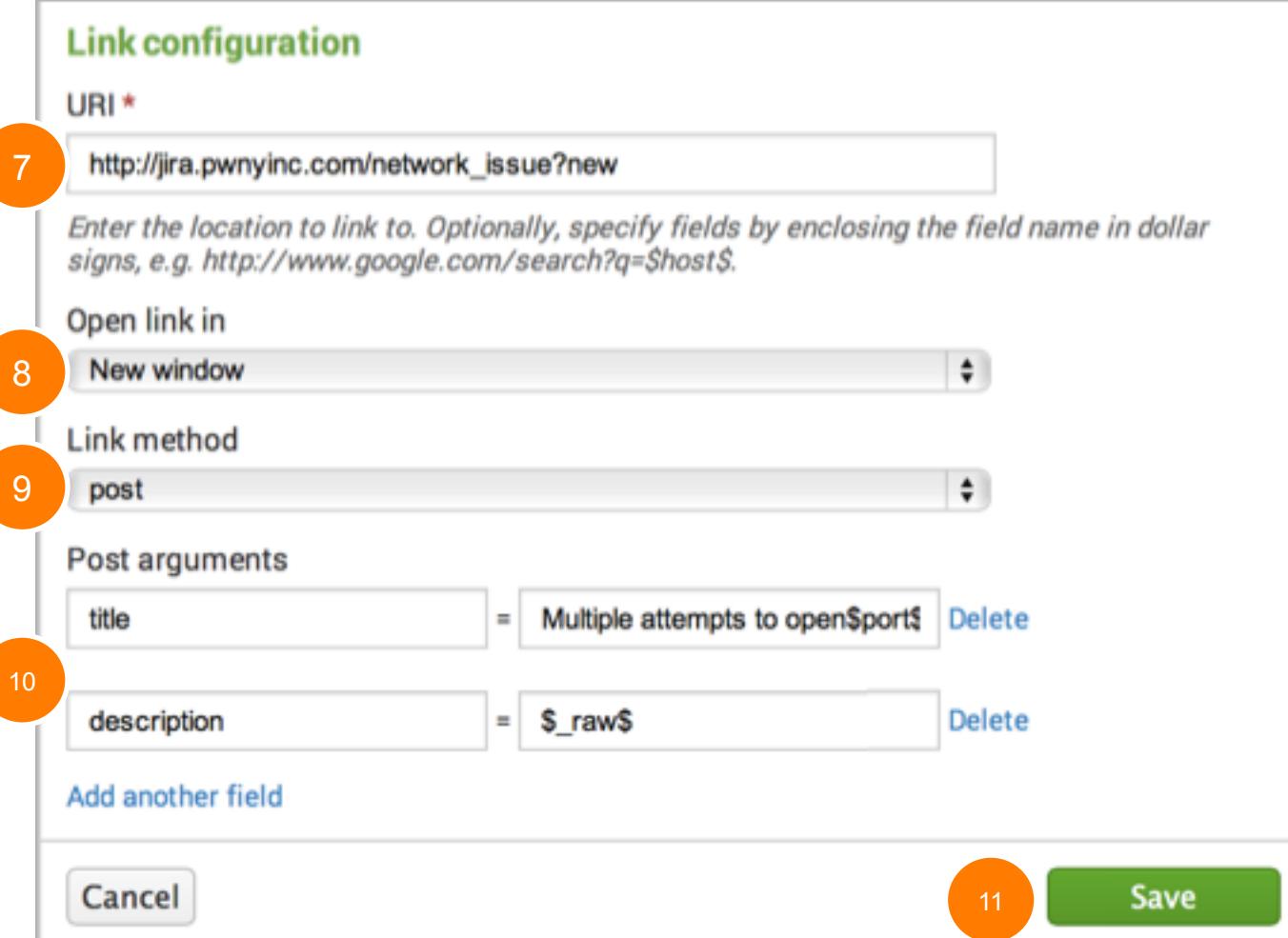
Post arguments

title = Multiple attempts to open\$port\$ Delete

description = \$_raw\$ Delete

Add another field

Cancel 11 Save



Creating a Search Workflow Action

Settings > Fields > Workflow actions > New

Complete steps 1 – 5 as described in the previous example, Creating a GET Workflow Action

6. Select **search** as the Action type

The screenshot shows the 'Add new' screen for creating a workflow action. The path 'Fields > Workflow actions > Add new' is visible at the top. The form fields are numbered 1 through 6:

- Destination app ***: search (Step 1)
- Name ***: search_access_by_ipaddress (Step 2)
- Label ***: Search failed access by IP address: \$src_ip\$ (Step 3)
- Apply only to the following fields**: src_ip (Step 4)
- Show action in**: Event menu (Step 5)
- Action type ***: search (Step 6, highlighted with a green border)

Below the form, a note states: "Enter a unique name without spaces or special characters. This is used for identifying your workflow action later on within Splunk Settings."

For the label field, a note says: "Enter the label that appears for this action. Optionally, incorporate a field's value by enclosing the field name in dollar signs, e.g. 'Search for ticket number: \$Ticketnum\$'."

For the fields section, a note says: "Specify a comma-separated list of fields that must be present in an event for the workflow action to apply to it. When fields are specified, the workflow action only appears in the field menus for those fields; otherwise it appears in all field menus."

For the event types section, a note says: "Specify a comma-separated list of event types that an event must be associated with for the workflow action to apply to it."

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Creating a Search Workflow Action (cont.)

7. Enter the Search string
8. Select the app if it is different from the current app
9. Enter the view name where the search will execute
10. Indicate if the search should run in a New window or the Current window
11. Enter the time range for the search or choose to use the same time range as the search
12. Save

Search configuration

Search string *

7 sourcetype=linux_secure failed src_ip=\$src_ip\$

Enter the search for this action. Optionally, specify fields as \$fieldname\$, e.g. sourcetype=rails controller=\$controller\$ error=*.

Run in app

8 search

Choose an app for the search to run in. Defaults to the current app.

Open in view

9

Enter the name of a view for the search to open in. Defaults to the current view.

Run search in

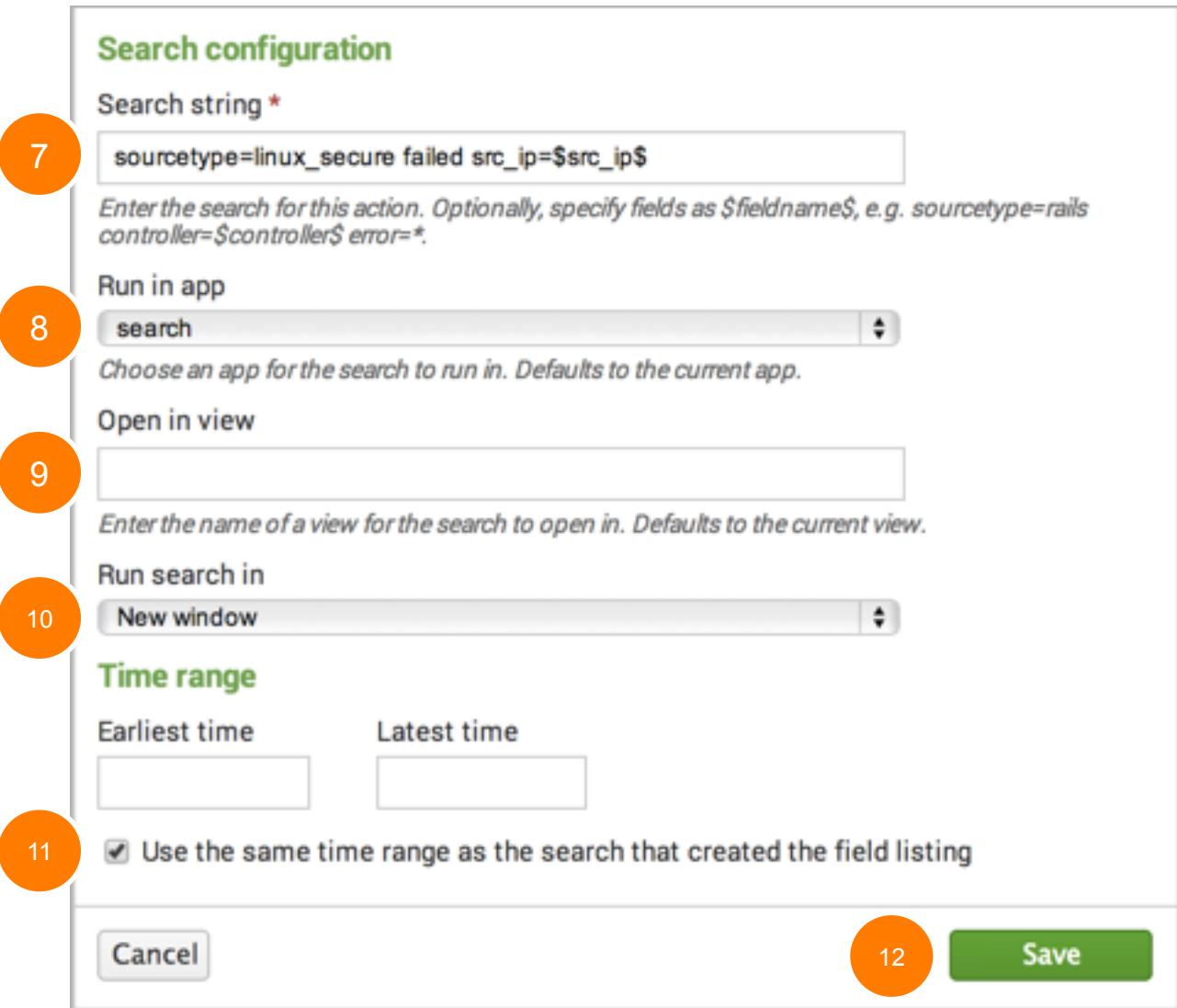
10 New window

Time range

Earliest time Latest time

11 Use the same time range as the search that created the field listing

Cancel 12 Save



Testing the Search Workflow Action

The screenshot shows the Splunk interface with a search results page. On the left, a sidebar displays an event log entry:

10/28/14 Tue Oct 28 2014 21:26:28 www2 sshd[4163]: Failed password for invalid user operator from 10.2.10.163 port 4570 ssh2

Below the event log is a "Event Actions" dropdown menu. One item, "Search failed access by IP address: 10.2.10.163", is highlighted with a green box and has a mouse cursor hovering over it.

The main area is a search interface titled "New Search". The search bar contains the query: "sourcetype=linux_secure failed src_ip=10.2.10.163". Below the search bar, it says "8,048 events (9/28/14 12:00:00.000 AM to 10/28/14 2:26:46.000 PM)".

The search results are displayed in a table with columns: i, Time, and Event. There are two rows of results:

i	Time	Event
>	10/28/14 2:26:40.000 PM	Tue Oct 28 2014 21:26:40 www2 sshd[4317]: Failed password for invalid user itmuser from 10.2.10.163 port 3838 ssh2 host = www2 : source = /opt/log/www2/secure.log : sourcetype = linux_secure : tag = authentication tag = error tag = remote
>	10/28/14 2:26:28.000 PM	Tue Oct 28 2014 21:26:28 www2 sshd[4163]: Failed password for invalid user operator from 10.2.10.163 port 4570 ssh2 host = www2 : source = /opt/log/www2/secure.log : sourcetype = linux_secure : tag = authentication tag = error tag = remote

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Managing Workflow Actions

Settings > Fields > Workflow actions

- Edit permissions
- Enable / disable
- Clone
- Move
- Delete

Workflow actions
Fields » Workflow actions

App context: Search & Reporting (search) Owner: Cerys Farrell (cfarrell)

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

New

Showing 1-2 of 2 items Results per page: 25

Name	Owner	App	Sharing	Status	Actions
get_whois_info	cfarrell	search	Private Permissions	Enabled Disable	Clone Move Delete
search_access_by_ipaddress	cfarrell	search	Private Permissions	Enabled Disable	Clone Move Delete

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Module 7: Creating Alerts and Scheduled Reports

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Module Objectives

- Describe alerts and scheduled reports
- Create alerts and scheduled reports
 - Run the underlying search
 - Set the schedule, conditions, and actions
- View fired alerts and scheduled reports

Alerting Overview

- Splunk alerts are based on searches that can run either:
 - On a regular **scheduled interval**
 - In **real-time**
- Alerts are triggered when the results of the search meet a specific condition that you define
- Based on your needs, alerts can:
 - List in triggered alerts
 - Send emails
 - Trigger scripts
 - Use a webhook
 - Run a custom alert

Creating an Alert

- Run a search
 - In this example, you're searching for server errors: any http request status that begins with 50 over the last 5 minutes
- Select **Save As > Alert**
- Give the alert a Title and Description

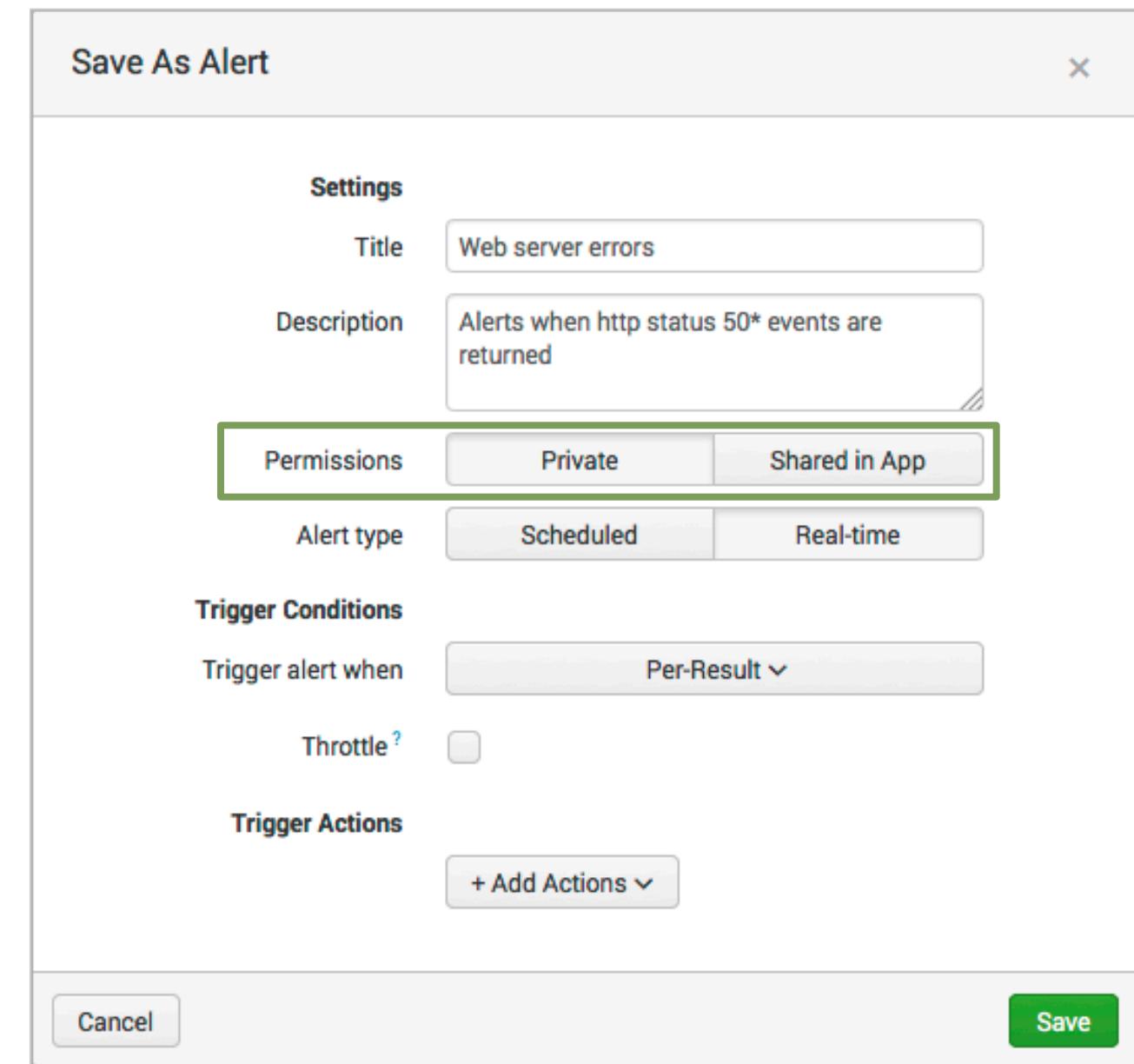
The screenshot shows the Splunk search interface. A search bar at the top contains the query "sourcetype=access_combined status=50*". Below the search bar, it says "193 events (6/28/15 8:00:00.000 AM to 6/29/15 8:49:56.000 AM)". At the bottom, there are tabs for "Events (193)", "Patterns", "Statistics", and "Visualization". A context menu is open from a "Save As" button, listing options: "Report", "Dashboard Panel", "Alert" (which is highlighted with a cursor icon), and "Event Type".

The screenshot shows the "Save As Alert" dialog box. The "Settings" section is highlighted with a green border. It contains fields for "Title" (set to "Web server errors") and "Description" (set to "Alerts when http status 50* events are returned"). Below this are sections for "Permissions" (with "Private" and "Shared in App" options), "Alert type" (with "Scheduled" and "Real-time" options), "Trigger Conditions" (with "Trigger alert when" set to "Per-Result"), "Throttle" (unchecked), and "Trigger Actions" (with a "+ Add Actions" button). At the bottom are "Cancel" and "Save" buttons.

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Setting Alert Permissions

- Set the alert permissions
 - **Private** – only you can access, edit, and view triggered alerts
 - **Shared in app**
 - ▶ All users of the app can view triggered alerts
 - ▶ By default, everyone has read access and power has write access to the alert



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Choosing Real Time or Scheduled Alert Type

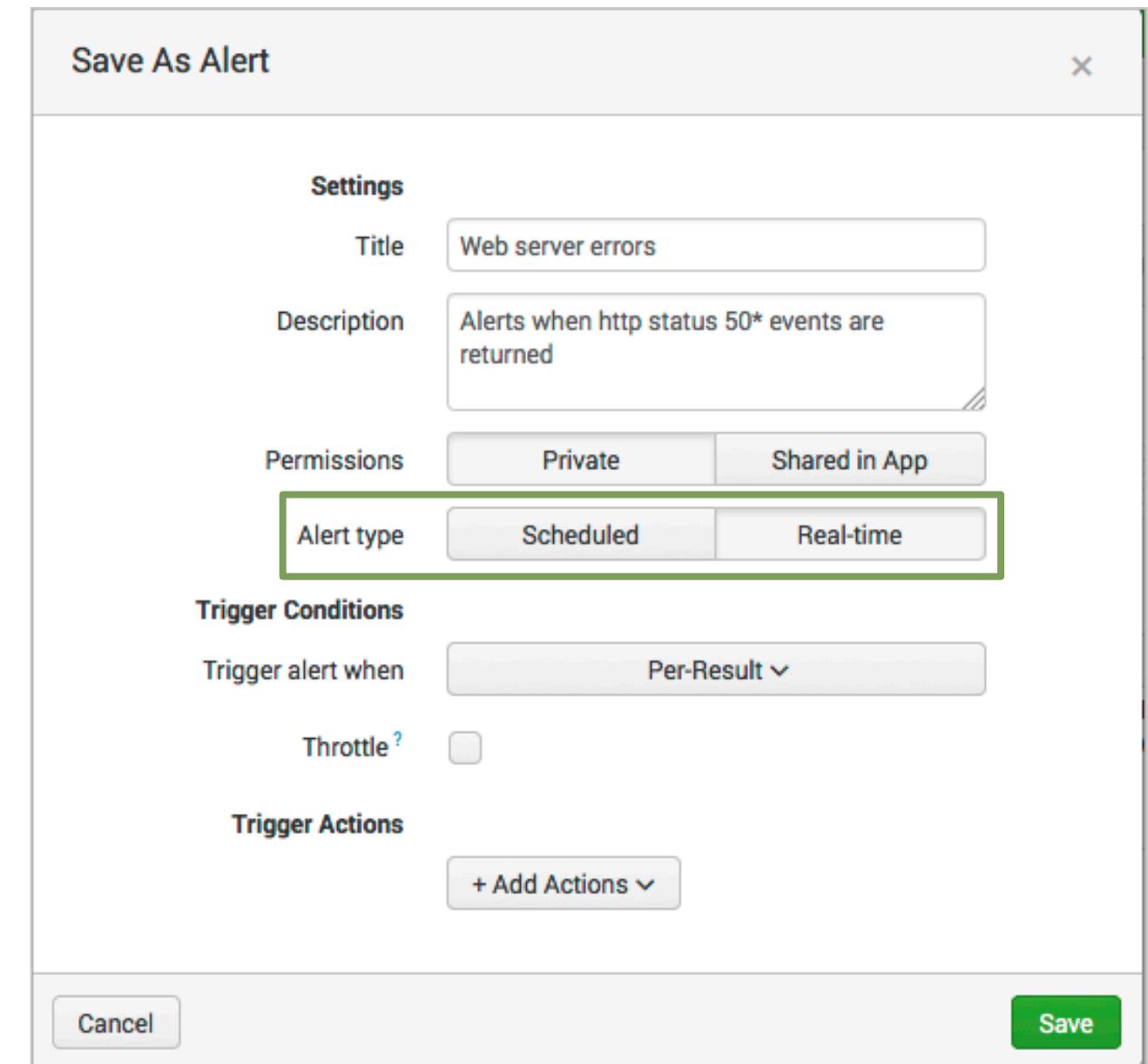
Choose an **Alert type** to determine how Splunk searches for events that may match your alert

- **Real-time alerts**

- Search runs constantly in the background
- Evaluates trigger conditions within a window of time based on the conditions you define

- **Scheduled alerts**

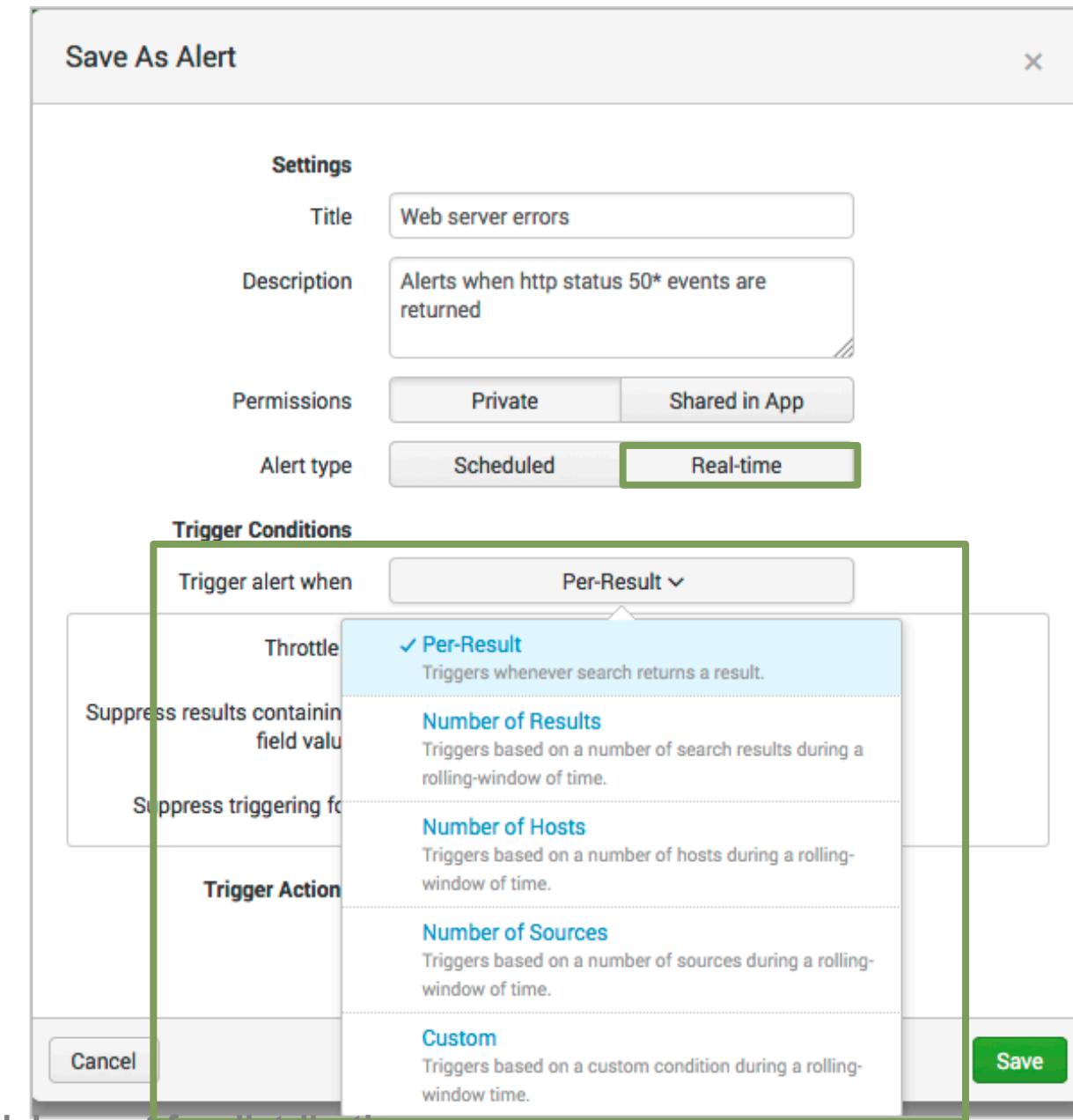
- Search runs at a defined interval
- Evaluates trigger condition when the search completes



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Setting Trigger Conditions – Real-time

- Trigger conditions allow you to capture a larger data set, then apply more stringent criteria to results before executing the alert
- You can set alerts to trigger:
 - **Per Result** – triggers when a result is returned
 - **Number of Results** – define how many results are returned before the alert triggers
 - **Number of Hosts** – define how many unique hosts are returned before the alert triggers
 - **Number of Sources** – define how many unique sources are returned before the alert triggers
 - **Custom** – define custom conditions using the search language



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Setting Trigger Conditions – Real-time (cont.)

- In this example, the trigger condition is set to **Number of Results**
- In this **Real Time** alert example, if the number of results is greater than **2** within **1 minute**, the alert triggers

Save As Alert X

Settings

Title: Web server errors
Description: Alerts when http status 50* events are returned
Permissions: Private | Shared in App
Alert type: Scheduled | **Real-time**

Trigger Conditions

Trigger alert when: Number of Results **is greater than** 2 **in** 1 minute(s) **Trigger**: Once | For each result
Throttle?

Trigger Actions

+ Add Actions Save

Cancel

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Setting the Alert Type – Scheduled

- From the frequency menu, choose to run the search every hour, day, week, month, or on a cron schedule
 - For the scheduled interval options, select the time the search will run
 - For cron schedule, define the cron expression

Save As Alert

Settings
Title: Web server errors
Description: Alerts when http status 50* events are returned
Permissions: Private Shared in App
Alert type: Scheduled Real-time
Earliest: Run on Cron Schedule
Latest: Run on Cron Schedule
Cron Expression: Run on Cron Schedule

The 'Cron Expression' field is highlighted with a green box. Below it are three examples of cron expressions:

- e.g. -1h@h (1 hour ago, to the hour). [Learn More](#)
- e.g. -1h@h (1 hour ago, to the hour). [Learn More](#)
- e.g. 00 18 *** (every day at 6PM). [Learn More](#)

Setting Trigger Conditions – Scheduled

- For the cron schedule, enter the **earliest** and **latest** values to define the time range of the results
- Set trigger conditions for scheduled alerts (same steps outlined for real-time alerts)
 - The alert examines the complete results set after the search is run

Save As Alert

Settings

Title: Web server errors

Description: Alerts when http status 50* events are returned

Permissions: Private Shared in App

Alert type: Scheduled Real-time

Run on Cron Schedule

Earliest: -5m@m e.g. -1h@h (1 hour)
9/30/15 11:05:00.000 PM

Latest: @m e.g. -1h@h (1 hour)
9/30/15 11:10:00.000 PM

Cron Expression: */5 * * * * e.g. 00 18 *** (every 5 minutes)

Trigger Conditions

Trigger alert when: Number of Results
is greater than 2

Trigger: Once For each result

Throttle?:

Trigger Actions

Cancel

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Alert Actions – Trigger Conditions: Once

- **Once** executes actions *one time* for all matching events within the scheduled time and conditions
 - Example: If your alert is scheduled to run every 30 seconds, and 40 results are returned, the alert only triggers and executes actions one time
- Select the **Throttling** option to suppress the actions for results within a specified time range

Save As Alert

Description	Alerts when http status 50* events are returned
Permissions	Private Shared in App
Alert type	Scheduled Real-time
Run on Cron Schedule	
Earliest:	-5m@m 9/30/15 11:05:00.000 PM
Latest:	@m 9/30/15 11:10:00.000 PM
Cron Expression	*/5 * * * * e.g. 00 18 *** (every hour)
Trigger Conditions	
Trigger alert when	Number of Results
is greater than	2
Trigger	Once For each result
Throttle?	<input checked="" type="checkbox"/>
Suppress triggering for	10 minute(s)
Trigger Actions	
+ Add Actions	

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Alert Actions – Trigger Conditions: For Each Result

- **For each result** – executes the alert actions once *for each result* that matches the conditions
- Select the **Throttling** option to suppress the actions for results that have the same field value, within a specified time range
 - Certain situations can cause a flood of alerts, when really you only want one
- Example: In a real time alert, only execute the actions once per status value for the next 30 seconds
 - 70 results are returned in a 1 minute window
 - 50 results include status=500 and 20 include status=503
 - Actions would execute 4 times – once for each of the 2 status values, every 30 seconds

Save As Alert

Description	Alerts when http status 50* events are returned
Permissions	Private Shared in App
Alert type	Scheduled Real-time
Run on Cron Schedule	
Earliest:	-5m@m 9/30/15 11:05:00.000 PM
Latest:	@m 9/30/15 11:10:00.000 PM
Cron Expression	*/5 * * * * e.g. 00 18 *** (eve)
Trigger Conditions	
Trigger alert when	Number of Results
	is greater than 2
Trigger	Once For each result
Throttle?	
Suppress results containing field value	<input checked="" type="checkbox"/> status
Suppress triggering for	10 minute(s)

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Add Trigger Actions

Add Actions

- **Add to Triggered Alerts** – adds the alert to the Activity > Triggered alerts view that shows severity and links to results
 - Choose an appropriate severity for the alert
- **Run a script** – runs a script that can perform some other action
- **Send Email** – sends an email with results to recipients that you define
- **Webhook** – calls a rest endpoint using http post request

Save As Alert

Permissions	Private	Shared in App
Alert type	Scheduled	Real-time
Run on Cron Schedule ▾		
Earliest:	-5m@m 9/30/15 11:05:00.000 PM	
Latest:	@m 9/30/15 11:10:00.000 PM	
Cron Expression	*/5 * * * *	
Trigger Conditions	Trigger alert when	
Number of Results ▾		
is greater than ▾ 2		
Trigger	Once	For each result
Throttle ? <input checked="" type="checkbox"/>		
Suppress results containing field value status		
Suppress triggering for 10		
Trigger Actions		
+ Add Actions ▾		

- 铃铛 [Add to Triggered Alerts](#)
Add this alert to Triggered Alerts list
- 代码 [Run a script](#)
Invoke a custom script
- 信封 [Send email](#)
Send an email notification to specified recipients
- 链接 [Webhook](#)
Generic HTTP POST to a specified URL

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Alert Actions – Send Email

Customize the content of email alerts

- **To** - enter the email address(es) of the alert recipients
- **Priority** – select the priority
- **Subject** – edit the subject of the email (the \$name\$ token is the title of the alert)
- **Message** – provide the message body of the email
- **Include** - select the format of the alert
- **Type** – select the format of the text message

Save As Alert

+ Add Actions ▾

When triggered

Send email

Remove

To:

Priority: Normal ▾

Subject: Splunk Alert: \$name\$

Message: The alert condition for '\$name\$' was triggered.

Comma separated list of email addresses.
Show CC and BCC

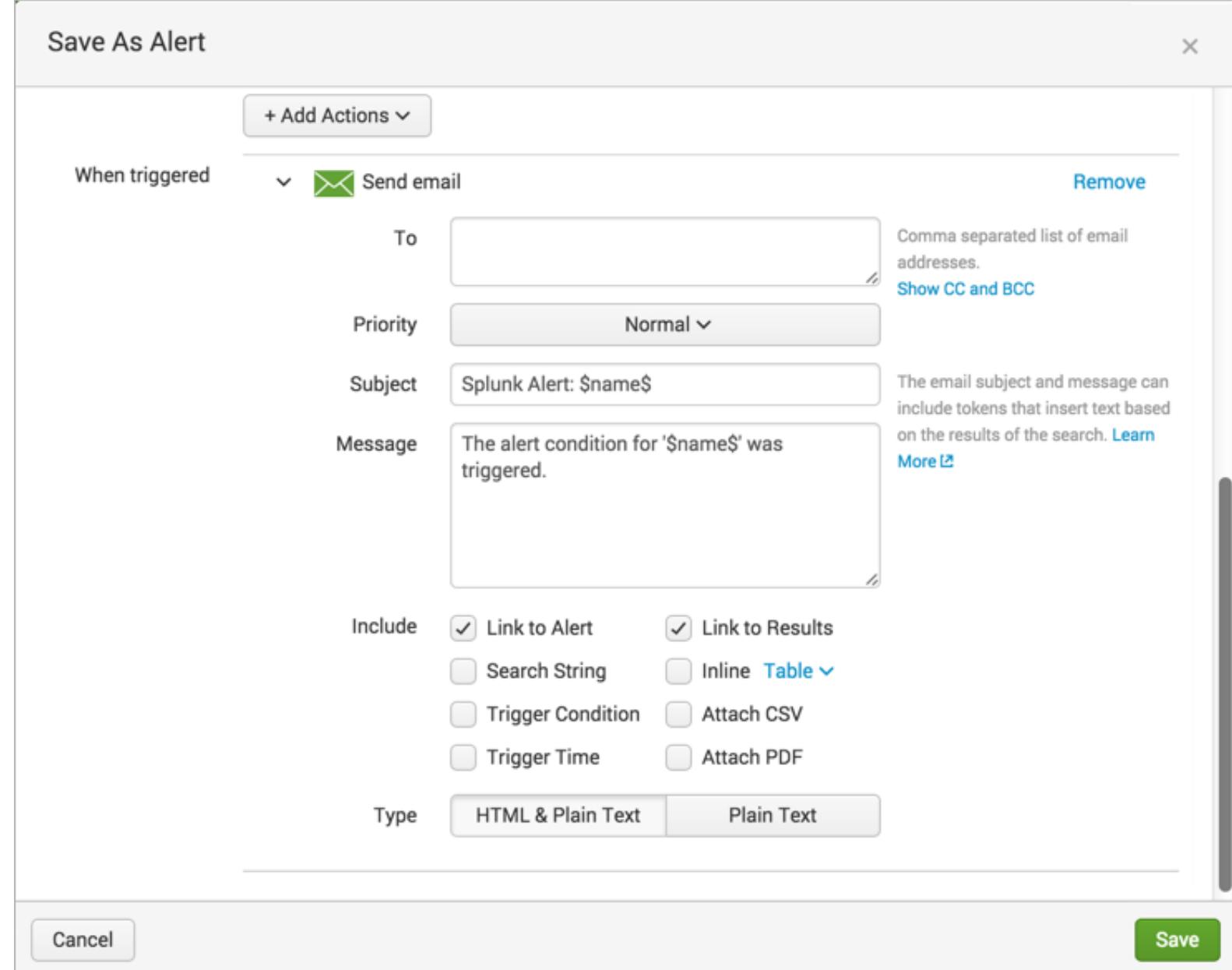
The email subject and message can include tokens that insert text based on the results of the search. [Learn More](#)

Include:

Link to Alert Link to Results
 Search String Inline [Table](#) ▾
 Trigger Condition Attach CSV
 Trigger Time Attach PDF

Type: [HTML & Plain Text](#) [Plain Text](#)

Cancel Save



This screenshot shows the 'Save As Alert' dialog box. At the top, there's a button '+ Add Actions ▾'. Below it, under 'When triggered', there's a 'Send email' action with a 'Remove' link. The main area contains fields for 'To', 'Priority' (set to 'Normal'), 'Subject' ('Splunk Alert: \$name\$'), and 'Message' ('The alert condition for '\$name\$' was triggered'). To the right of these fields, there's explanatory text about tokens and a 'Learn More' link. Below the message field is a section 'Include' with several checkboxes: 'Link to Alert' (checked), 'Link to Results' (checked), 'Search String', 'Inline Table' (with a dropdown arrow), 'Trigger Condition', 'Attach CSV', 'Trigger Time', and 'Attach PDF'. At the bottom, there are 'Type' buttons for 'HTML & Plain Text' (selected) and 'Plain Text'. At the very bottom are 'Cancel' and 'Save' buttons.

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Alert Actions – Run a Script

When an alert is triggered, you can launch a script

- Enter the name of the script
- All alert scripts need to reside in either of the following locations:
 - `$SPLUNK_HOME/bin/scripts`
 - `$SPLUNK_HOME/etc/apps/ <Appname>/bin/scripts`

The screenshot shows the 'Trigger Conditions' and 'Trigger Actions' sections of the Splunk Alert Actions configuration. In the 'Trigger Conditions' section, the 'Trigger alert when' condition is set to 'Number of Results' is greater than 2, with a 'Trigger' option of 'Once'. Below this, there are 'Throttle?' settings and suppression rules for results containing the field value 'status' for 10 minutes. In the 'Trigger Actions' section, a 'Run a script' action is selected under 'When triggered', with the filename 'alertscript.py' specified. A note at the bottom right indicates the script is located in \$SPLUNK_HOME/bin/scripts.

Trigger Conditions

Trigger alert when Number of Results
is greater than 2

Trigger Once For each result

Throttle?

Skip results containing field value status

Skip triggering for 10 minute(s)

Trigger Actions

+ Add Actions

When triggered Run a script

Filename alertscript.py

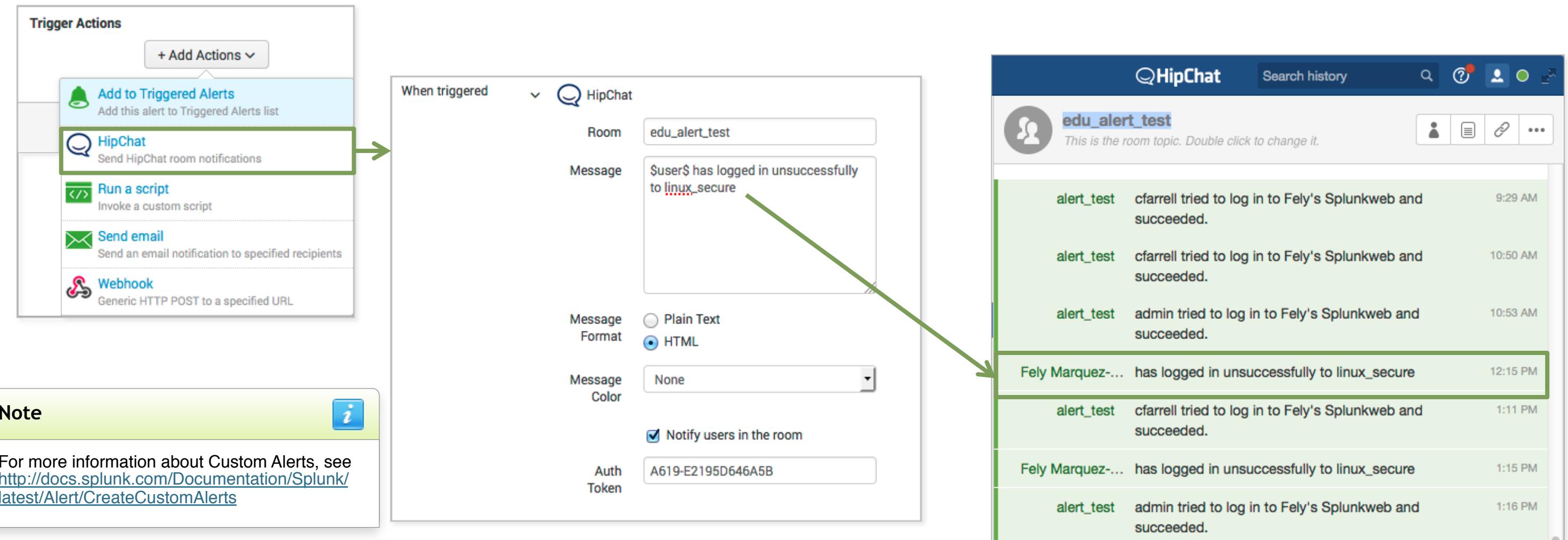
Located in \$SPLUNK_HOME/bin/scripts

Note

The proper permissions to your Splunk server are required to upload your script to these Splunk directories.

Custom Alert Action

- You can create a custom alert actions or download an app from Splunkbase
- In this example, the HipChat Room Notification Alert app is used



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Creating an Alert via Patterns

1. Run a search
 - In this example, you're searching for any patterns on the email server that need to be tracked
2. Select the **Patterns** tab and click **Create alert**
3. Configure your alert settings and **Save**

New Search

sourcetype=cisco_esa

Last 24 hours

2,396 events (6/28/15 11:00:00.000 AM to 6/29/15 11:26:52.000 AM)

Job Verbose Mode

Events (2,396) Patterns Statistics Visualization

13 patterns based on a sample of 2,396 events

Smaller Larger

Less than 5,000 events may produce poor patterns. Try a search in a larger time range or with fewer constraints.

47.08% Mon <timestamp> Info: VOF Rule: OUTBREAK_0002234 has threat level 3

4.3% Mon <timestamp> Info: New SMTP ICID 745700 interface Management (192.168.3.12 0) address 201.19.137.205 reverse dns host 20119137205.user.veloxzone.com.br verified no

4.3% Mon <timestamp> Info: ICID 745700 REJECT SG BLACKLIST match sbrs[10.0: 3.0] SBR 4.0

ESTIMATED EVENTS
1.13K

View Events

SEARCH sourcetype=cisco_esa threat

Save as event type Create alert

INCLUDED KEYWORDS threat

Save As Alert

Settings

Search: sourcetype=cisco_esa threat

Title: Possible email threats

Description: Optional

Permissions: Private Shared in App

Alert type: Scheduled Real-time

Run every day

At: 0:00

Trigger Conditions

Trigger alert when: Number of Results

is greater than: 0

Trigger: Once For each result

Throttle?

Cancel Save

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Viewing Triggered Alerts

- If you elected to list in triggered alerts, you can view the results by accessing **Activity > Triggered Alerts**
- Click **View results** to see the matching events that triggered the alert
- Click **Edit search** to modify the alert definition

The screenshot shows the Splunk web interface with the following details:

- Header:** splunk> Apps ▾ Cerys Farrell ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find
- Search Bar:** App: Search & Reporting (search) Owner: Cerys Farrell (Severity: All Alert: Jobs Triggered Alerts)
- Table:** Shows 15 results from June 29, 2015, detailing fired alerts, app, type, severity, mode, and actions.
- Table Headers:** Time, Fired alerts, App, Type, Severity, Mode, Actions.
- Table Data:**

Time	Fired alerts	App	Type	Severity	Mode	Actions
2015-06-29 18:30:01 PDT	Failed login attempts by user admin	search	Scheduled	High	Digest	View results Edit search Delete
2015-06-29 17:30:01 PDT	Failed login attempts by user admin	search	Scheduled	High	Digest	View results Edit search Delete
2015-06-29 16:30:01 PDT	Failed login attempts by user admin	search	Scheduled	High	Digest	View results Edit search Delete
2015-06-29 16:23:04 PDT	Web server errors	search	Real-time	High	Digest	View results Edit search Delete
2015-06-29 16:22:59 PDT	Web server errors	search	Real-time	High	Digest	View results Edit search Delete
2015-06-29 16:22:54 PDT	Web server errors	search	Real-time	High	Digest	View results Edit search Delete

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Editing Alerts

- From the search bar, click **Alerts**
- Select the alert and click **Edit**

The screenshot shows the Splunk interface with the 'Search & Reporting' tab selected. In the top navigation bar, the 'Alerts' tab is highlighted. On the left, a search bar contains the query `sourcetype=access_combined status=50*`. The main pane displays the 'Alerts' section with the heading 'Alerts'. It describes what alerts are and provides links to view or refine them. Below this, there is a table showing two alerts:

	Title ^	Actions	Owner	App	Sharing
>	Failed login attempts by user admin	Open in Search Edit	cfarrell	search	App
>	Web server errors	Open in Search Edit	cfarrell	search	App

A green arrow points from the 'Edit' link of the second alert row to a context menu that is displayed. This menu includes options such as 'Edit Description', 'Edit Permissions', 'Edit Alert Type and Trigger Condition', 'Edit Actions', 'Disable', 'Clone', and 'Delete'. The 'Edit' option in the menu is also highlighted with a green box.

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Editing Alert Permissions

- Edit alert permissions
 - **Private** – only you can access, edit, and view triggered alerts
 - **Shared in app** – all users of the app can access, edit, and view triggered alerts

The screenshot illustrates the process of editing alert permissions. It consists of two main windows: an 'Alert has been saved' window on the left and an 'Edit Permissions' window on the right.

Alert has been saved (Left Window):

- Header: Alert has been saved
- Message: You can view your alert, change additional settings, or continue editing it.
- Additional Settings:
 - Permissions (highlighted with a green box)
 - Alert Type & Triggers
 - Actions
- Buttons: Continue Editing (disabled), Save

Edit Permissions (Right Window):

- Header: Edit Permissions
- Alert: Web server errors
- Owner: cfarrell
- App: search
- Display For:
 - Owner (selected)
 - App
 - All apps
- Permissions table:

	Read	Write
Everyone	<input type="checkbox"/>	<input type="checkbox"/>
power	<input type="checkbox"/>	<input type="checkbox"/>
user	<input type="checkbox"/>	<input type="checkbox"/>
- Buttons: Cancel, Save

A green arrow points from the 'Permissions' link in the 'Additional Settings' section of the first window to the 'Permissions' section in the second window. Another green arrow points from the 'Edit' link in the 'Permissions' section of the first window to the 'Edit' link in the 'Permissions' section of the second window.

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

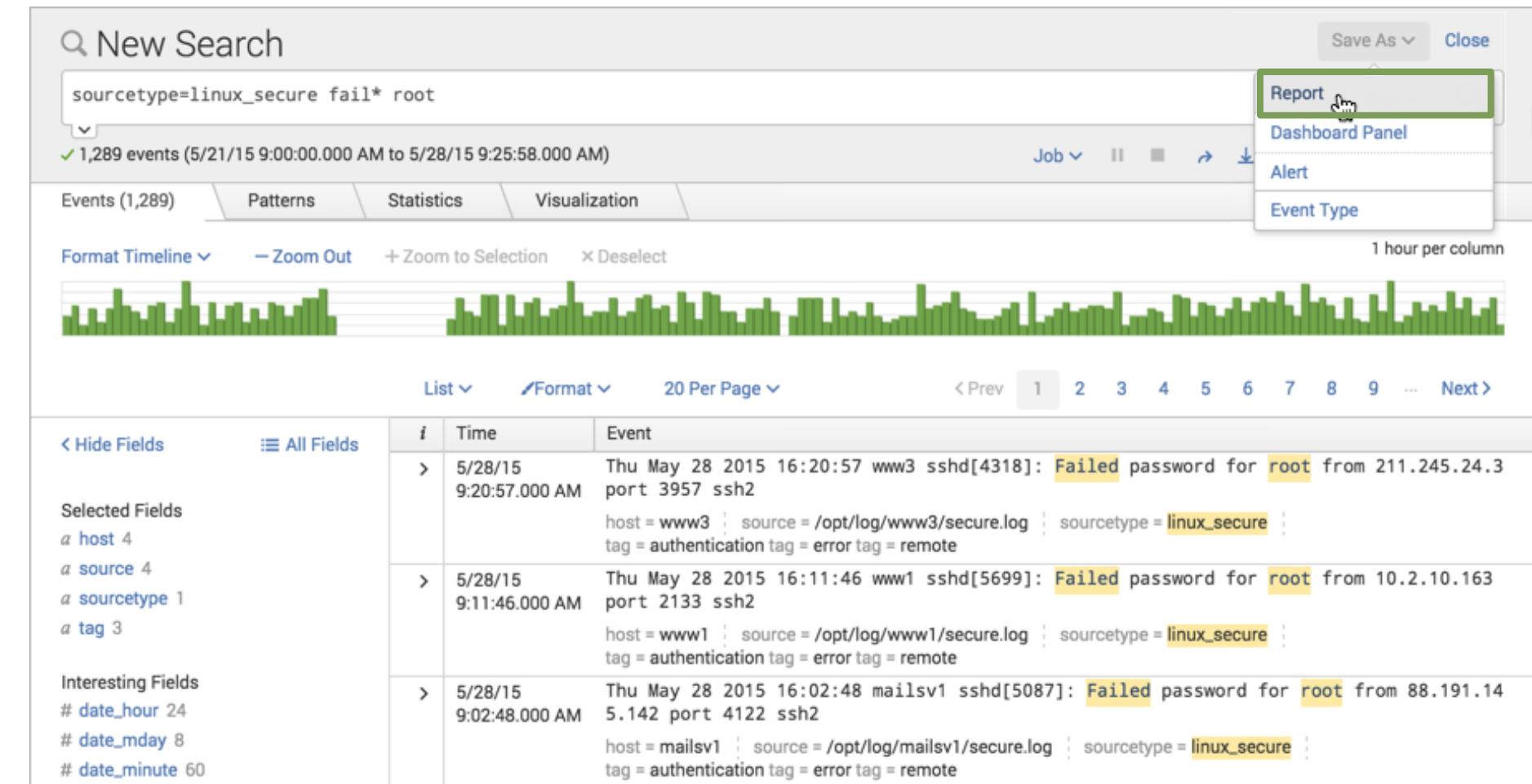
Using Scheduled Reports

- Scheduled Reports are useful for:
 - Monthly, weekly, daily executive/managerial roll up reports
 - Dashboard performance
 - Automatically sending reports via email

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Creating a Scheduled Report

- Create your search
- From the **Save As** menu, select **Report**



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Creating a Scheduled Report (cont.)

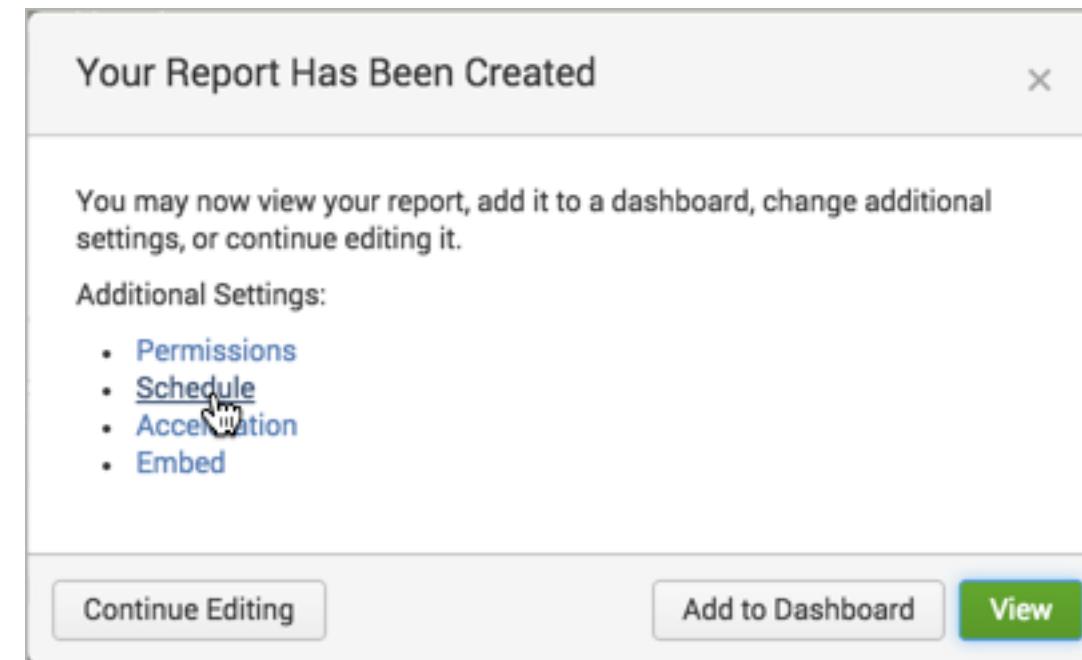
- **Title** – enter a title for your report
- **Description** – provide a description
- **Time Range Picker** – you can add a time range picker to the report
- **Click Save**

Save As Report ×

Title	Failed root logins
Description	linux_secure failed root logins
Time Range Picker	<input type="checkbox"/> Yes <input type="checkbox"/> No
Cancel Save	

Creating a Scheduled Report (cont.)

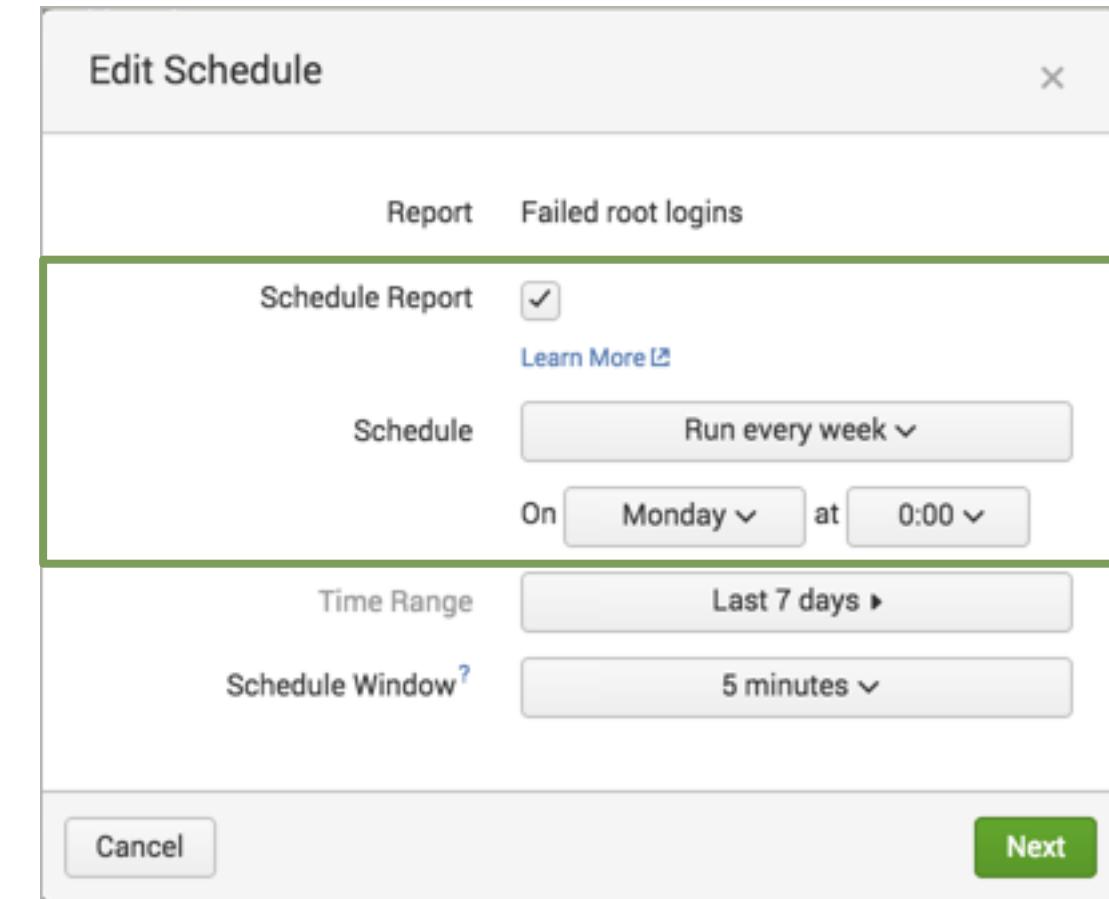
After the report is created, click **Schedule**



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Creating a Scheduled Report – Define Schedule

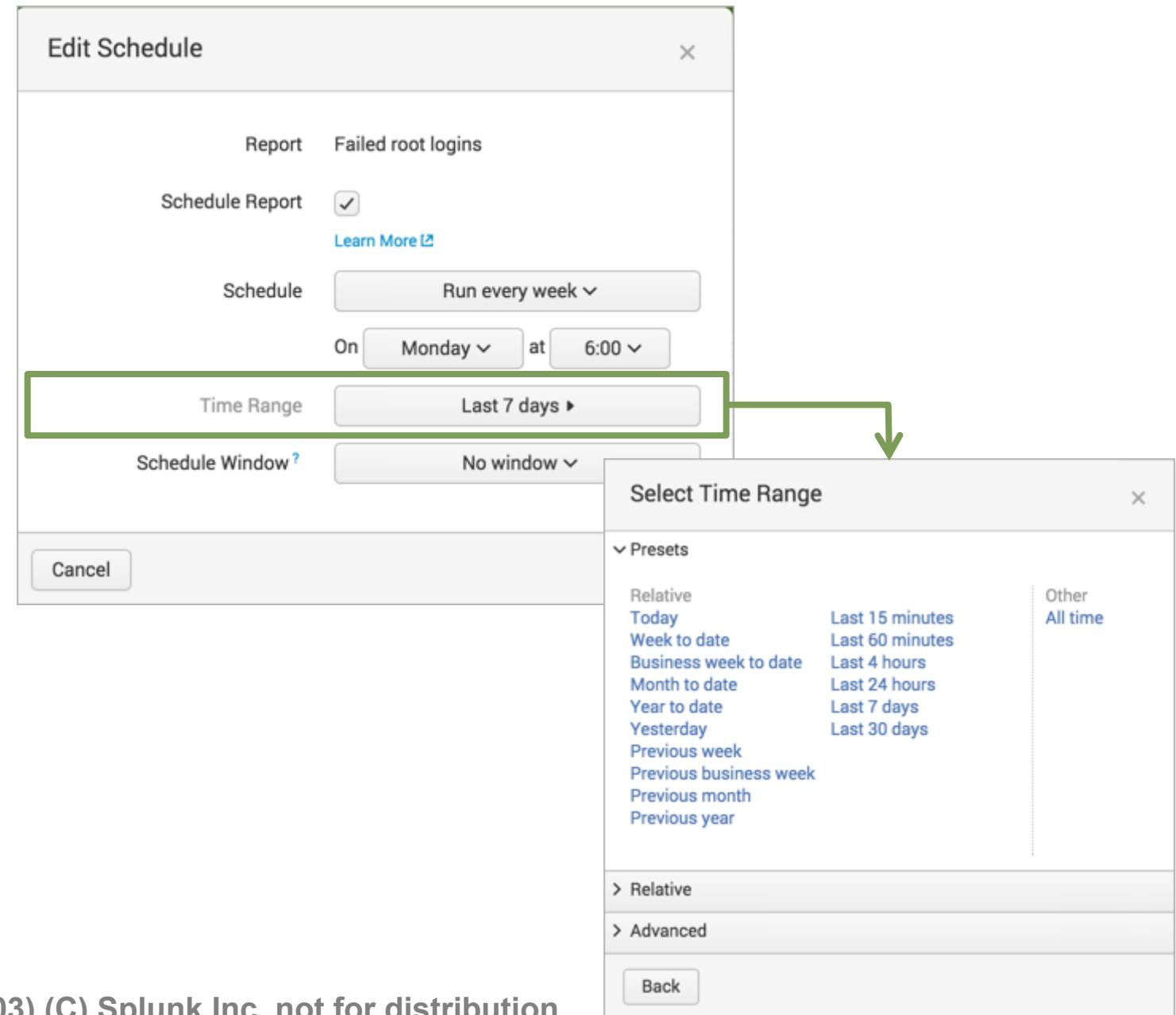
- **Schedule Report** – click this checkbox
- **Schedule** – select the frequency to run the report
 - Run every hour
 - Run every day
 - Run every week
 - Run every month
 - Run on Cron Schedule



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Creating a Scheduled Report – Select Time Range

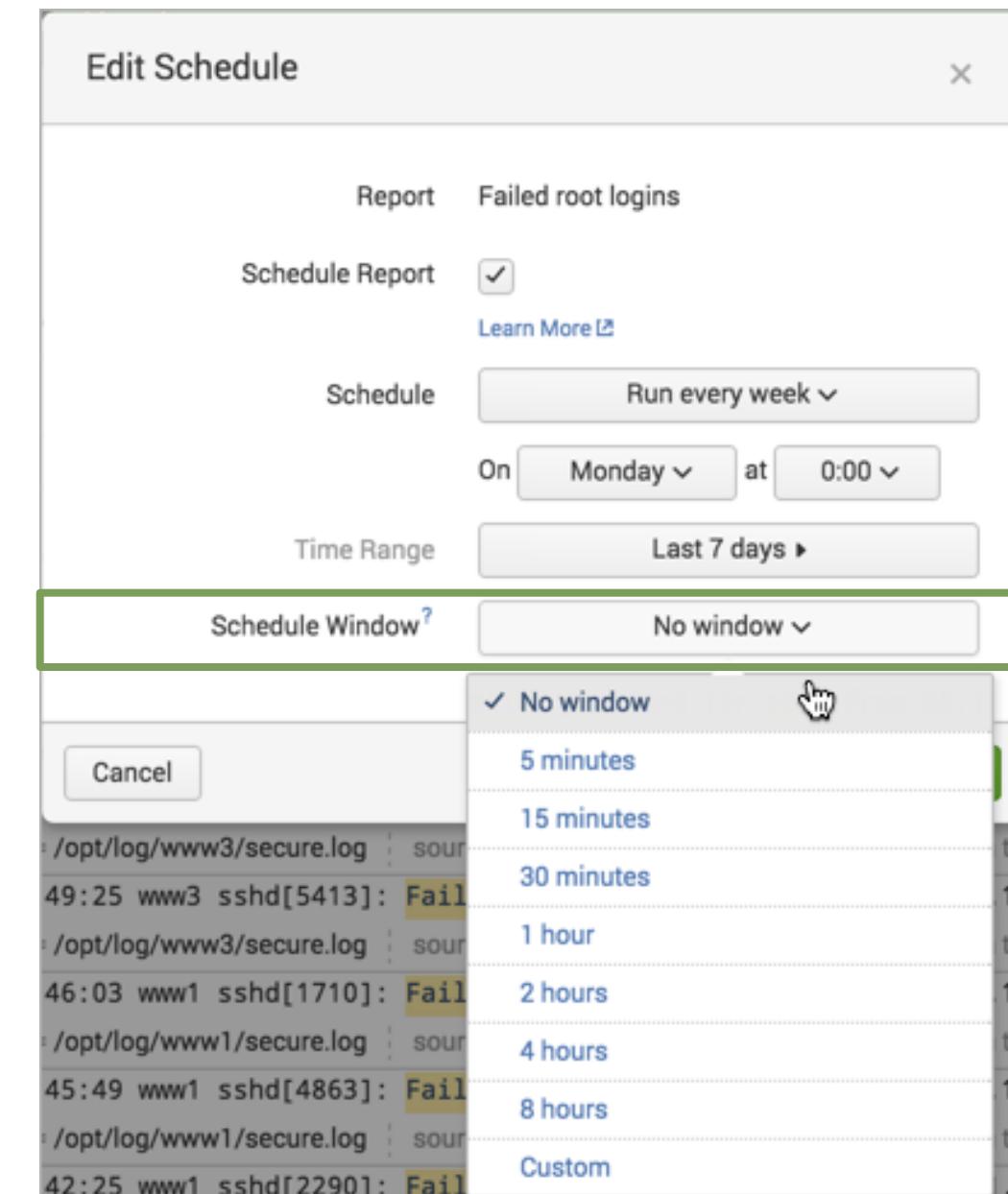
- **Time Range** – By default, the search time range is used
 - Click the time range button to change the time range
 - You can select a time range from Presets, Relative, or Advanced
 - Typically, the time range is relative to the Schedule



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Creating a Scheduled Report – Schedule Window

- **Schedule Window** – This setting determines a time frame to run the report.
 - If there are other reports scheduled to run at the same time, you can provide a window in which to run the report
 - This setting provides efficiency when scheduling several reports to run
- After you configure the schedule report, click **Next**

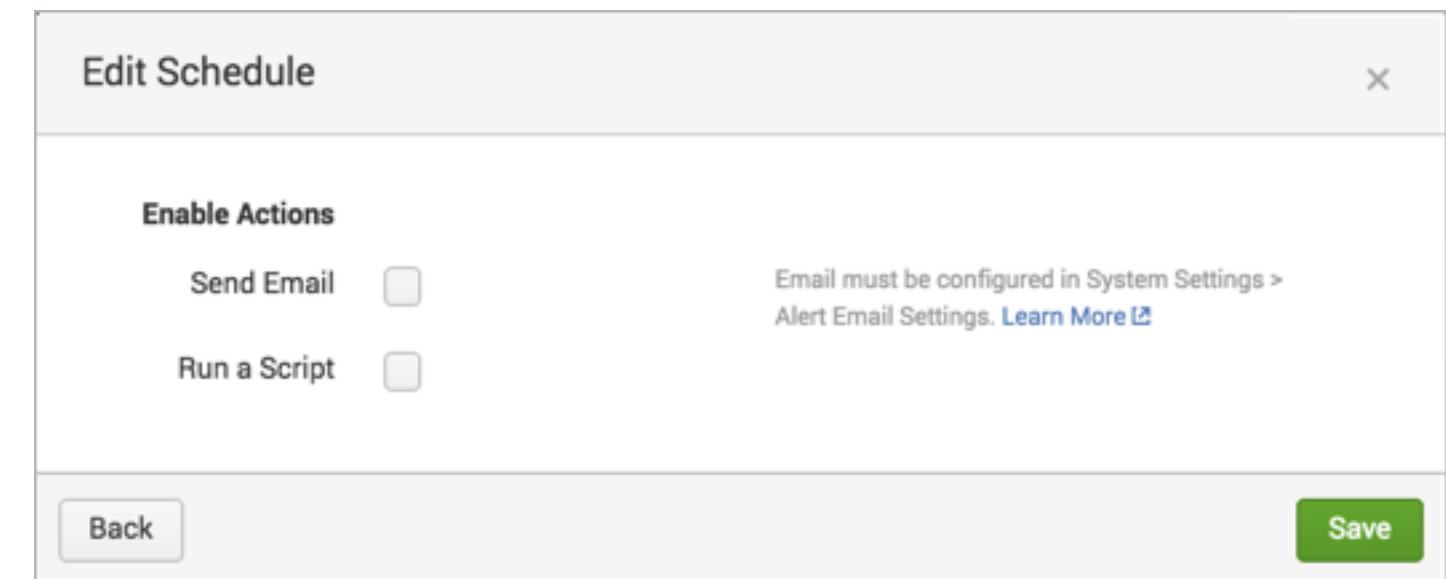


Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Creating a Scheduled Report – Enable Actions

- **Enable Actions**

- **Send Email:** When an alert is triggered, an email is sent to the specified recipient
- **Run a script:** A script is launched when an alert is triggered



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Creating a Scheduled Report – Send Email

1. Enter addresses in the **To** field, separated by a comma
2. Set the priority
3. Edit or keep the default subject
 - the \$name\$ variable includes the name of the report
 - In addition to a message, you can include other options like an inline table of the results, etc.
4. Define the email text type
5. After you have configured the actions, click **Save**

Edit Schedule

Enable Actions

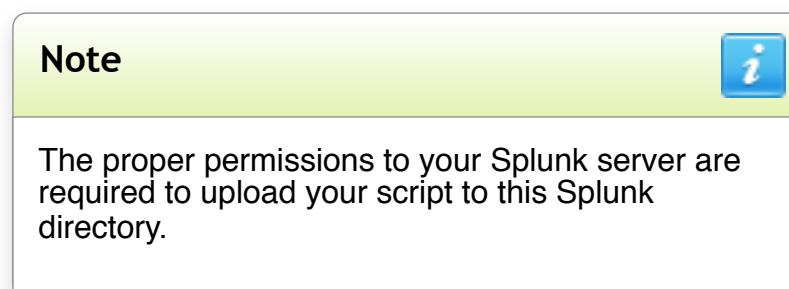
Send Email	<input checked="" type="checkbox"/>	Email must be configured in System Settings > Alert Email Settings. Learn More
To	itops@buttercupgames.com	Comma separated list of email addresses. Show CC and BCC
Priority	High ▾	
Subject	Weekly report: \$name\$	The email subject and message can include tokens that insert text based on the results of the search. Learn More
Message	Weekly report '\$name\$' has run.	
Include	<input checked="" type="checkbox"/> Link to Report <input type="checkbox"/> Search String <input type="checkbox"/> Attach CSV	<input checked="" type="checkbox"/> Link to Results <input type="checkbox"/> Inline Table ▾ <input checked="" type="checkbox"/> Attach PDF
Type	<input type="radio"/> HTML & Plain Text <input checked="" type="radio"/> Plain Text	
Run a Script	<input checked="" type="checkbox"/>	
Filename	loginerrorscript.sh	Located in \$SPLUNK_HOME/bin/scripts

Back Save

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Creating a Scheduled Report – Run a Script

1. Enter the file name of the script
 - The script must reside in the `$SPLUNK_HOME/bin/scripts` directory
2. Click Save



Edit Schedule

Enable Actions

Send Email

To

Priority

Subject

Message

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

Comma separated list of email addresses. [Show CC and BCC](#)

The email subject and message can include tokens that insert text based on the results of the search. [Learn More](#)

Include Link to Report Link to Results
 Search String Inline [Table](#)
 Attach CSV Attach PDF

Type HTML & Plain Text Plain Text

Run a Script

Filename

Located in `$SPLUNK_HOME/bin/scripts`

Back Save

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Managing Scheduled Reports

You can manage reports two ways:

- **Settings > Searches, reports and alerts**

- **Reports Menu**

- Edit description
- Edit permissions
- Edit schedule
- Edit acceleration
- Clone
- Embed
- Delete

The screenshot shows the Splunk Reports interface. At the top, it says "Reports" and provides instructions: "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." Below this, there is a table with three reports: "Failed logins", "Failed root logins", and "Weekly T-shirt Sales". The "Weekly T-shirt Sales" row has a context menu open over it, listing options: "Edit Description" (highlighted), "Edit Permissions" (with a cursor icon pointing to it), "Edit Schedule", "Edit Acceleration", "Clone", "Embed", and "Delete". The table has columns for Title, Actions, Owner, App, Sharing, and Embedding.

i	Title ^	Actions	Owner	App	Sharing	Embedding
>	Failed logins	Open in Search Edit ▾	cfarrell	search	Private	Disabled
>	Failed root logins	Open in Search Edit ▾	cfarrell	search	Private	Disabled
>	Weekly T-shirt Sales	Open in Search Edit Description	cfarrell	search	Private	Disabled

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Managing Reports – Edit Permissions

Display For determines who sees the scheduled report

The image shows two screenshots of the Splunk interface. On the left, the 'Reports' dashboard displays three reports: 'Failed logins', 'Failed root logins', and 'Weekly T-shirt Sales'. The 'Weekly T-shirt Sales' report's 'Actions' menu is open, with 'Edit Permissions' highlighted. A green arrow points from this menu item to the 'Edit Permissions' dialog on the right. The 'Edit Permissions' dialog shows the current settings for the 'Failed root logins' report, which is owned by 'cfarrell' and associated with the 'search' app. The 'Display For' dropdown is set to 'App', with other options 'Owner' and 'All apps' available. The 'Run As' dropdown is set to 'User', with 'Owner' also available. The permissions table lists 'Everyone', 'power', and 'user' with checkboxes for 'Read' and 'Write' access.

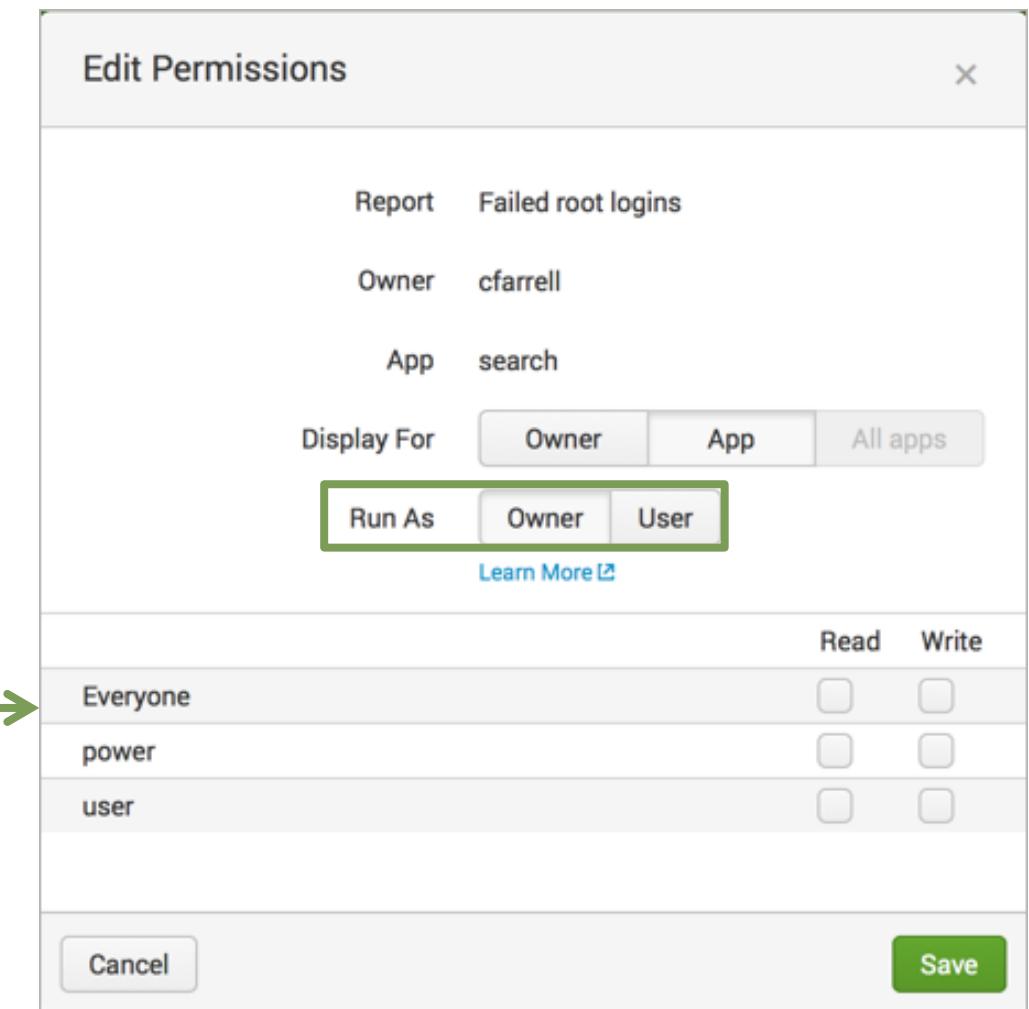
Group	Read	Write
Everyone	<input type="checkbox"/>	<input type="checkbox"/>
power	<input type="checkbox"/>	<input type="checkbox"/>
user	<input type="checkbox"/>	<input type="checkbox"/>

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Managing Reports – Edit Permissions (cont.)

- **Run As** – determines which user profile is used at run time
 - Owner – all data accessible by the owner appears in the report
 - User – only data allowed to be accessed by the user role appears

The screenshot shows the Splunk Reports interface. On the left, there's a sidebar with a 'Reports' section. Below it, a table lists three reports: 'Failed logins', 'Failed root logins', and 'Weekly T-shirt Sales'. The 'Weekly T-shirt Sales' row has a context menu open, with 'Edit Permissions' highlighted and a green arrow pointing to the 'Edit Permissions' section of the 'Edit Permissions' dialog box on the right.



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Managing Reports – Embed

- To access the report results from a webpage, click **Edit > Embed**
 - Before a report can be embedded, it must be scheduled

The screenshots illustrate the process of enabling report embedding in Splunk:

- The first screenshot shows the Splunk 'Reports' interface with a list of 5 reports. The 'Failed logins' report is selected, and its context menu is open, with the 'Embed' option highlighted.
- The second screenshot shows a modal dialog titled 'Enable Report Embedding'. It contains a message: 'Are you sure you want to enable embedding for this report? An embedded report can be viewed by anyone with access to the web page(s) in which it is inserted.' There are 'Cancel' and 'Enable Embedding' buttons.
- The third screenshot shows the 'Embed' configuration page. The 'Embedding' status is set to 'Enabled'. The generated HTML code is displayed in a text area, starting with '<iframe height="636" width="480" frameborder="0" src="http://54.184.179.177/en-US/embed?s=%2FservicesNS%2Fcfarrell%2Fsearch%2Fsaved%2Fsearches%2FFailed%2520root%2520logins&oid=ysj0DUnWD_ynve3LI9ICrl%5EowLIA%5ERHU4z3xrNeQE74cqmnn3ofHb0Y5izPEtrZBDt%5EMGpq6KXrEZQu%5EqK2Bhx5qsKWJeEsp'.

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Module 8: Creating and Using Macros

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Module Objectives

- Describe macros
- Manage macros
- Create a basic macro
- Use a basic macro
- Define arguments / variables for a macro
- Add and use arguments with a macro

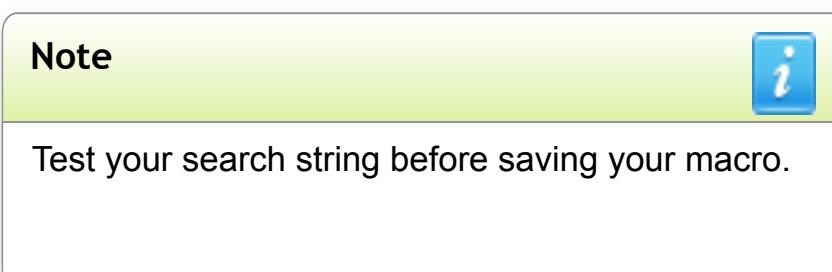
Macros Overview

- Useful when you frequently run searches or reports with similar search syntax
- The time range is selected at search time
- Macros can be a full search string or a portion of a search that can be reused in multiple places
- Allows you to define one or more arguments within the search segment
 - Pass values to the search string when using the macro

Creating a Basic Macro

Settings > Advanced search > Search Macros

1. Click **New**
2. Select the destination app
3. Enter a Name
4. Type the search string
5. Save



Add new

Advanced search » Search macros » Add new

Destination app *

search

Name *

Enter the name of the macro. If the search macro takes an argument, indicate this by appending the number of arguments to the name. For example: mymacro(2)

US_sales

Definition *

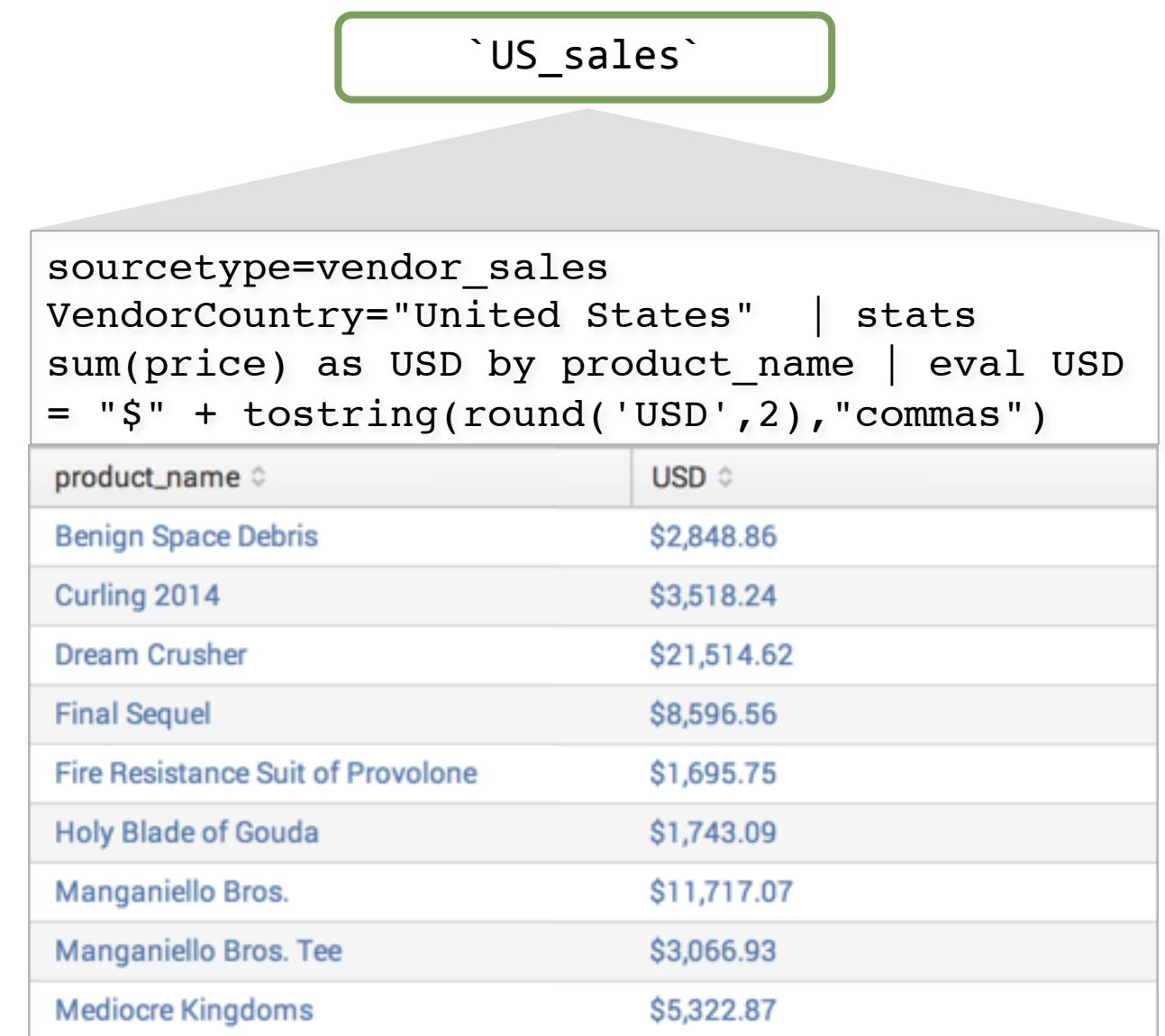
Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in dollar signs. For example: \$arg1\$

```
sourcetype=vendor_sales VendorCountry="United States"
| stats sum(price) as USD by product_name
| eval USD = "$" + tostring(round('USD',2), "commas")
```

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Using a Basic Macro

- Type the macro name into the search bar
- Surround the macro name with the **backtick** (or grave accent) character
 - **`macroname` != 'macroname'**
 - Do not confuse with single-quote character (')
- Pipe to more commands, or precede with search string



The diagram illustrates the use of a macro. A search bar at the top contains the text ``US_sales``, which is highlighted with a green border. An arrow points from this bar down to a search results table. The table has two columns: `product_name` and `USD`. The data is as follows:

product_name	USD
Benign Space Debris	\$2,848.86
Curling 2014	\$3,518.24
Dream Crusher	\$21,514.62
Final Sequel	\$8,596.56
Fire Resistance Suit of Provolone	\$1,695.75
Holy Blade of Gouda	\$1,743.09
Manganiello Bros.	\$11,717.07
Manganiello Bros. Tee	\$3,066.93
Mediocre Kingdoms	\$5,322.87

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Adding Arguments

- Include the number of arguments in parentheses after the macro name
 - monthly_sales(3)
- Within the search definition, use \$arg\$
 - currency=\$currency\$
 - symbol=\$symbol\$
 - rate=\$rate\$
- In the **Arguments** field, enter the name of the argument(s)
- Provide one or more variables of the macro at search time

Add new

Advanced search » Search macros » Add new

Destination app *

search

Name *

Enter the name of the macro. If the search macro takes an argument, indicate this by appending the number of arguments to the name. For example: mymacro(2)

monthly_sales(3)

Definition *

Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in dollar signs. For example: \$arg1\$

```
| stats sum(price) as USD by product_name | eval $currency$ = "$symbol$" + tostring(USD*$rate$, "commas") | eval USD = "$" + tostring(USD, "commas")
```

Use eval-based definition?

Arguments

Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '-' and '_' characters.

currency,symbol,rate

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Using Arguments

When using a macro with arguments,
include the argument(s) in parentheses
following the macro name

```
sourcetype=vendor_sales VendorCountry=Germany  
OR VendorCountry=France OR VendorCountry=Italy  
`monthly_sales(euro,€,.79)`
```

```
sourcetype=vendor_sales VendorCountry=Germany OR  
VendorCountry=France OR VendorCountry=Italy  
| stats sum(price) as USD by product_name |  
eval euro = "€" + tostring(USD*.79, "commas")  
| eval USD = "$" + tostring(USD, "commas")
```

product_name	USD	euro
Benign Space Debris	\$974.61	€770
Curling 2014	\$799.60	€632
Dream Crusher	\$1,479.63	€1,169
Final Sequel	\$324.87	€257
Fire Resistance Suit of Provolone	\$195.51	€154
Holy Blade of Gouda	\$203.66	€161
Manganiello Bros.	\$3,079.23	€2,433
Manganiello Bros. Tee	\$619.38	€489
Mediocre Kingdoms	\$1,274.49	€1,007
Orvil the Wolverine	\$1,719.57	€1,358
Puppies vs. Zombies	\$44.91	€35
SIM Cubicle	\$1,139.43	€900
World of Cheese	\$1,299.48	€1,027
World of Cheese Tee	\$619.38	€489

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Validating Macros

You can validate the argument values in your macro

- Validation Expression

- You can enter an expression for each argument

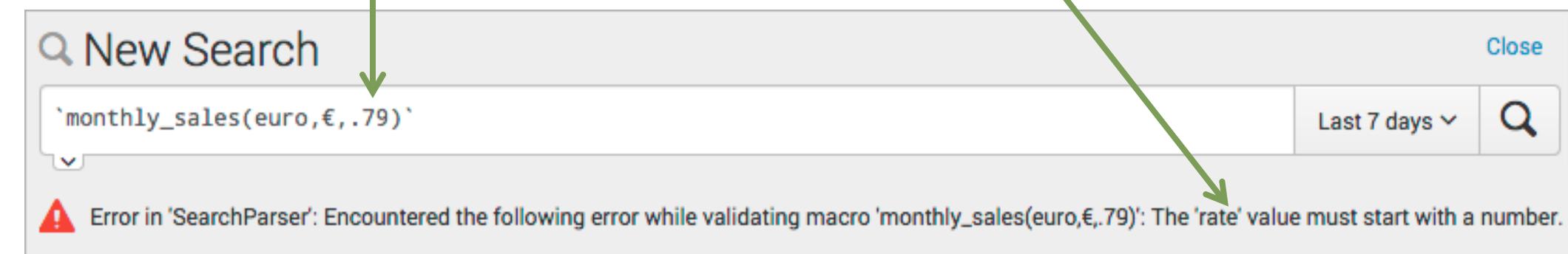
- Validation Error Message

- This is the message that appears when you run the macro

Arguments
Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, currency,symbol,rate

Validation Expression
Enter an eval or boolean expression that runs over macro arguments.
isnum(\$rate\$)

Validation Error Message
Enter a message to display when the validation expression returns 'false'.
The 'rate' value must start with a number.



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Managing Macros

Settings > Advanced search > Search macros

- Edit permissions
- Enable / disable
- Clone
- Move
- Delete

Search macros
Advanced search » Search macros

App context: Search & Reporting (search) Owner: Cerys Farrell (cfarrell)

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

New

Showing 1-4 of 4 items Results per page: 25

Name	Definition	Arguments	Owner	App	Sharing	Status	Actions
US_sales	sourcetype=vendor_sales VendorCountry="United States" stats sum(price) as USD by product_name eval USD = "\$" + tostring(round("USD',2),"commas")		cfarrell	search	Private Permissions	Enabled Disable	Clone Move Delete
currency	sourcetype=access_combined action=purchase productId=* eval price = "\$" + tostring(round('price',2),"commas") table product_name, price		cfarrell	search	Private Permissions	Enabled Disable	Clone Move Delete
currency(2)	sourcetype=access_combined product_name=* eval \$price1\$ = "\$currency1\$" + tostring(round('\$price1\$',2),"commas") table product_name, \$price1\$	price1,currency1	cfarrell	search	Private Permissions	Enabled Disable	Clone Move Delete
monthly_sales(3)	stats sum(price) as USD by product_name eval \$currency\$ = "\$currency_symbol\$" + tostring(USD*\$rate\$, "commas") eval USD = "\$" + tostring(USD, "commas")	currency1,currency_symbol,rate	cfarrell	search	Private Permissions	Enabled Disable	Clone Move Delete

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Module 9: Creating Data Models

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Objectives

- Describe the relationship between data models and Pivot
- Identify data model objects
- Identify object attributes
- Create a data model
- Use a data model in Pivot

Reviewing Pivot

In the Using Splunk course, you learned how to use the Pivot interface to create reports and dashboards. As a knowledge manager, you are responsible for building the data model that provides the objects for Pivot.

The screenshot shows the Splunk interface with two main windows. On the left is the 'Buttercup Games Site Activity' Data Model browser, and on the right is the 'New Pivot' interface.

Data Model Browser (Left):

- Header:** Buttercup Games Site Activity, Buttercup_Games_Site_Activity, < Back to Data Models
- Objects:** Add Object ▾
- EVENTS:** Web Requests (selected), Web_Requests
- Constraints:** sourcetype=access_combined
- Actions:** Bulk Edit ▾
- INHERITED:** _time (Time), host (String), source (String), sourcetype (String)
- EXTRACTED:** 42
- Web Requests:**
 - Successful Requests
 - purchases
 - add
 - remove
 - Failed Requests
 - removed
 - purchases
 - adds

Pivot Interface (Right):

- Header:** New Pivot, 99,097 of 99,097 events matched, Save As... ▾, Clear, Successful Requests ▾, Documentation ▾
- Filters:** All time, action
- Split Columns:** product_name
- Column Values:** Count of Success...
- Table:** A pivot table showing event counts across various categories. The columns are: action, Benign Space Debris, Curling 2014, Dream Crusher, Final Sequel, Fire Resistance Suit of Provolone, Holy Blade of Gouda, Manganiello Bros., Manganiello Bros. Tee, Mediocre Kingdoms, Orvil the Wolverine, Puppies vs. Zombies.

action	Benign Space Debris	Curling 2014	Dream Crusher	Final Sequel	Fire Resistance Suit of Provolone	Holy Blade of Gouda	Manganiello Bros.	Manganiello Bros. Tee	Mediocre Kingdoms	Orvil the Wolverine	Puppies vs. Zombies
addtocart	12	9	12	14	8	13	15	16	12	6	9
changequantity	1	2	0	5	2	2	4	1	4	4	1
purchase	6	4	7	6	4	7	6	8	4	2	5
remove	3	5	2	5	3	2	6	3	3	2	2
view	6	6	12	14	18	11	11	13	16	12	11

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Overview of Data Models

- Hierarchically structured data set that generates searches and drives Pivot
 - Pivot reports are created based on data models

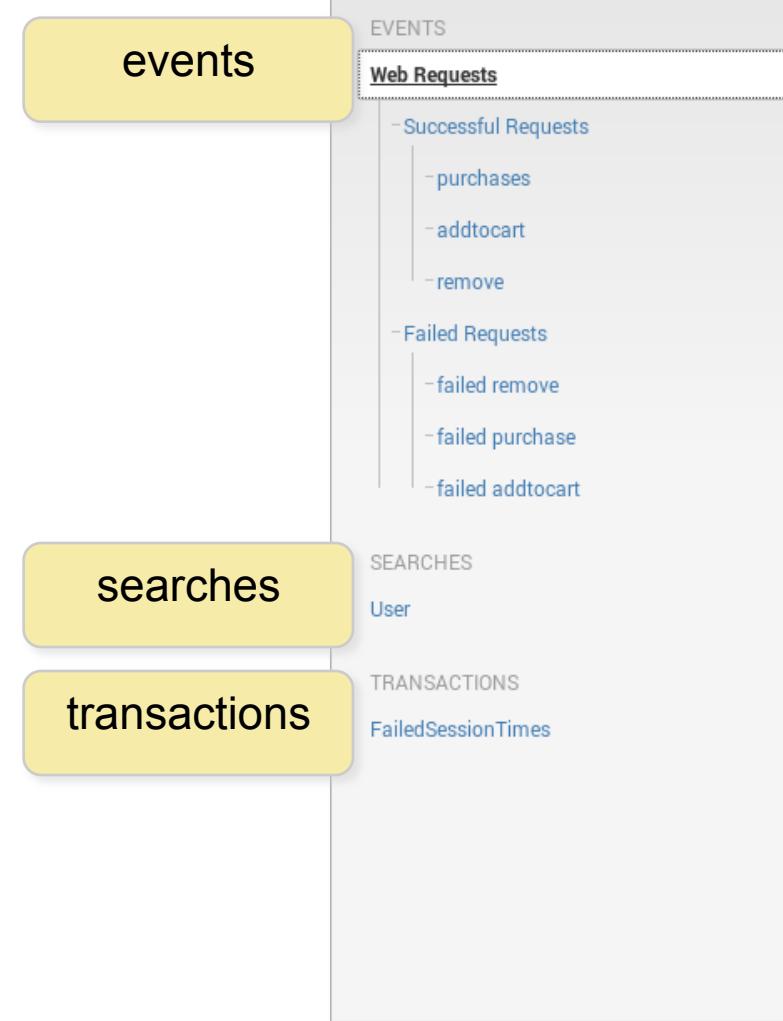
The screenshot shows the Splunk Data Model Editor interface. The title bar reads "splunk> App: Search & Reporting > Buttercup Games Site Activity Buttercup_Games_Site_Activity". The top right includes user information (Cerys Farrell) and navigation links (Messages, Settings, Activity, Help). The main area is titled "Buttercup Games Site Activity" and "Buttercup_Games_Site_Activity". It features a left sidebar with sections for "Objects", "EVENTS" (with "Web Requests" selected), "SEARCHES", and "TRANSACTIONS". The "Web Requests" section shows a hierarchy: "Successful Requests" (purchases, addtocart, remove) and "Failed Requests" (failed remove, failed purchase, failed addtocart). To the right, the "Web Requests" object is defined with a constraint "sourcetype=access_combined". The "INHERITED" section lists attributes: _time (Time, Override), host (String, Override), source (String, Override), and sourcetype (String, Override). The "EXTRACTED" section lists attributes: action (String, Edit), bytes (Number, Edit), categoryId (String, Edit), clientip (IPv4, Edit), cookie (String, Edit), and date_hour (Number, Edit).

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Data Model Objects

- Data models consist of 3 types of objects

1. Events
2. Searches
3. Transactions



Screenshot of the Splunk Data Model Objects interface for the 'Buttercup Games Site Activity' data model. The 'Web Requests' object is selected. The interface shows the following details:

- CONSTRAINTS**: sourcetype=access_combined
- EXTRACTED**: A list of fields with their data types and edit options:
 - _time: Time (Override)
 - host: String (Override)
 - source: String (Override)
 - sourcetype: String (Override)
 - action: String (Edit)
 - bytes: Number (Edit)
 - categoryId: String (Edit)
 - clientip: IPv4 (Edit)
 - cookie: String (Edit)
 - date_hour: Number (Edit)
 - date_mday: Number (Edit)
 - date_minute: Number (Edit)
 - date_month: String (Edit)
 - date_second: Number (Edit)
 - date_wday: String (Edit)

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Data Model Events

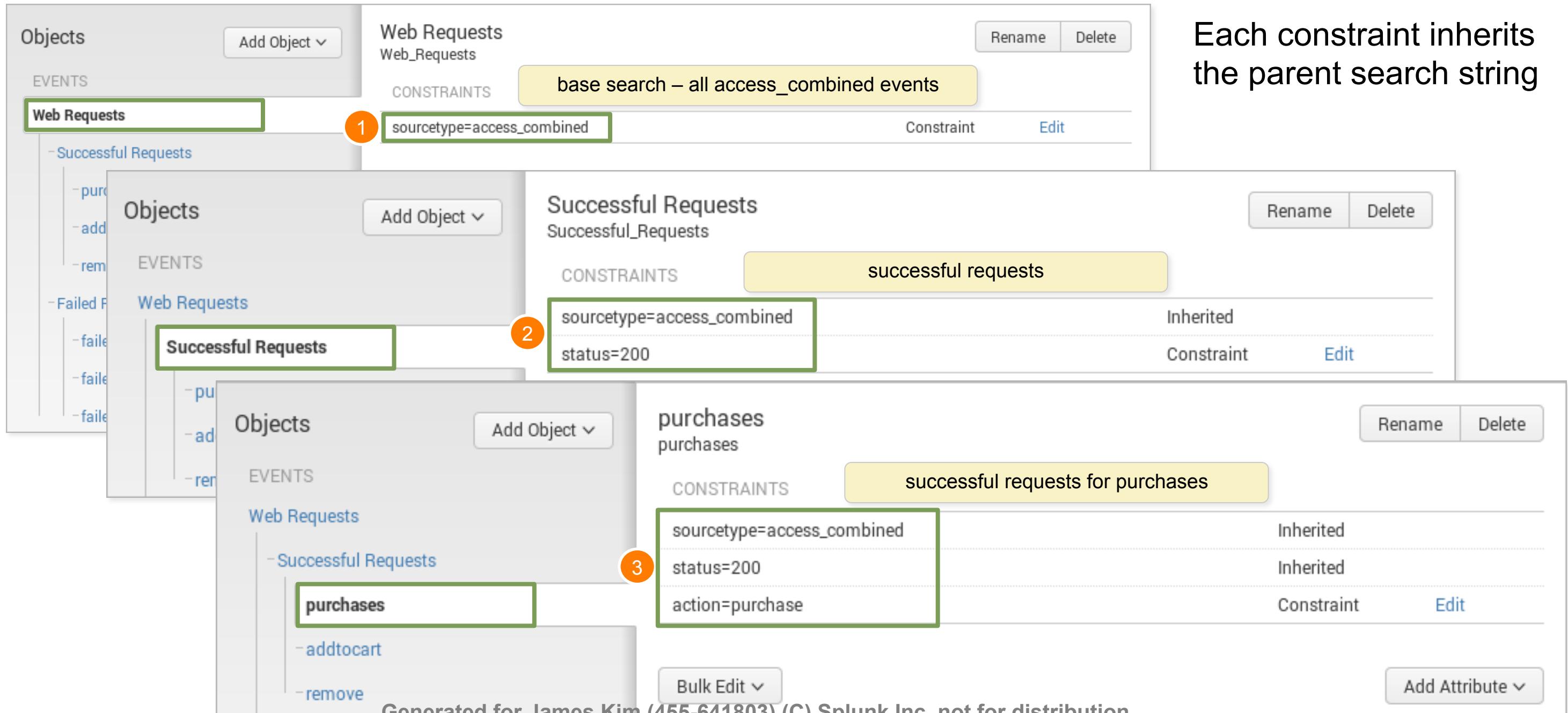
- **Event objects** contain constraints and attributes
- **Constraints** are essentially the search broken down into a hierarchy
- **Attributes** are the fields and properties associated with the events

The screenshot shows the Splunk Data Model Editor interface. On the left, the 'Objects' sidebar lists 'EVENTS' like 'Web Requests', 'SEARCHES' like 'connection_status', and 'TRANSACTIONS' like 'FailedSessionTimes'. The main panel displays the 'Web Requests' object details:

- CONSTRAINTS:** sourcetype=access_combined (highlighted with a yellow box labeled 'base search').
- INHERITED:** Fields: _time, host, source, sourcetype (highlighted with a yellow box labeled 'fields').
- EXTRACTED:** Fields: action, bytes, categoryid, clientip, cookie.

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Event Object Hierarchy and Constraints



Each constraint inherits
the parent search string

Object Attributes

- Attributes are the fields you want to include in the objects
- Like constraints, attributes are inherited from parent objects

INHERITED		
<input type="checkbox"/> _time	Time	Override
<input type="checkbox"/> host	String	Override
<input type="checkbox"/> source	String	Override
<input type="checkbox"/> sourcetype	String	Override
EXTRACTED		
<input type="checkbox"/> action	String	Edit
<input type="checkbox"/> bytes	Number	Edit
<input type="checkbox"/> categoryid	String	Edit
<input type="checkbox"/> clientip	IPv4	Edit
<input type="checkbox"/> cookie	String	Edit
<input type="checkbox"/> date_hour	Number	Edit
<input type="checkbox"/> date_mday	Number	Edit
<input type="checkbox"/> date_minute	Number	Edit
<input type="checkbox"/> date_month	String	Edit
<input type="checkbox"/> date_second	Number	Edit

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Object Attributes (cont.)

- **Auto-Extracted** – can be default fields or manually extracted fields
- **Eval Expression** – a new field based on an expression that you define
- **Lookup** – leverage an existing lookup table
- **Regular Expression** – extract a new field based on regex
- **Geo IP** – add geographical fields such as latitude/longitude, country, etc.

Attribute	Type	Action
_time	Time	Edit
host	String	Edit
source	String	Edit
sourcetype	String	Edit
action	String	Edit
bytes	Number	Edit
categoryid	String	Edit
clientip	IPv4	Edit
cookie	String	Edit
date_hour	Number	Edit
date_mday	Number	Edit
date_minute	Number	Edit
date_month	String	Edit
date_second	Number	Edit

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Data Model Search Objects

- Arbitrary searches that include transforming commands to define the dataset that they represent
- Search objects can also have attributes, which are added via the **Add Attribute** button

The screenshot shows the Splunk Data Model Editor interface. At the top, there's a title bar with the name of the search object: "Buttercup Games Site Activity". Below the title, there are sections for "Objects", "EVENTS", and "SEARCHES". The "EVENTS" section contains a tree view of "Web Requests" with categories like "Successful Requests" and "Failed Requests", each containing sub-items such as "purchases", "addtocart", "remove", "failed remove", "failed purchase", and "failed addtocart". The "SEARCHES" section contains a single entry: "User". To the right of the main interface, there's a large text area displaying a complex search command:

```
_time=* host=* source=* sourcetype=*
uri=* status<600 clientip=* referer=*
useragent=* (sourcetype = access_*
OR source = *.log) | eval
userid=clientip | stats first(_time) as earliest,
last(_time) as latest,
list(uri_path) as uri_list by userid
```

Below this command, there are "Edit" and "Search" buttons. Further down, under the "EXTRACTED" section, there are four attributes with their types and edit buttons:

Attribute	Type	Edit
earliest	Number	Edit
latest	Number	Edit
uri_list	String	Edit
userid	String	Edit

At the bottom of the interface, there are links for "About", "Support", "File a Bug", "Documentation", and "Privacy Policy", along with a copyright notice: "© 2005-2014 Splunk Inc. All rights reserved."

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Data Model Transaction Objects

- Enable the creation of objects that represent transactions
- Use fields that have already been added to the model using event or search objects

Buttercup Games Site Activity
Buttercup_Games_Site_Activity

[Edit](#) [Download](#) [Pivot](#) [Documentation](#)

[Back to Data Models](#)

Objects		FailedSessionTimes		
		FailedSessionTimes		
EVENTS		CONSTRAINTS		
Web Requests		Group Objects	Failed_Requests	Transaction
- Successful Requests		Group By	clientip	Edit
- purchases		Max Pause		
- addtocart		Max Span		
- remove				
- Failed Requests				
- failed remove				
- failed purchase				
- failed addtocart				
SEARCHES				
User				
TRANSACTIONS				
FailedSessionTimes				

[Add Object](#) [Rename](#) [Delete](#)

[Bulk Edit](#) [Add Attribute](#)

INHERITED

	Type	Required	Override
<input type="checkbox"/> _time	Time	Required	Override
<input type="checkbox"/> duration	Number	Required	Override
<input type="checkbox"/> eventcount	Number	Required	Override
<input type="checkbox"/> host	String		Override
<input type="checkbox"/> source	String		Override
<input type="checkbox"/> sourcetype	String		Override

EXTRACTED

	Type	Edit
<input type="checkbox"/> action	String	Edit
<input type="checkbox"/> browser	String	Edit
<input type="checkbox"/> bytes	Number	Edit
<input type="checkbox"/> categoryId	String	Edit
<input type="checkbox"/> clientip	IPv4	Edit
<input type="checkbox"/> cookie	String	Edit

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Search and Transaction Object Considerations

- There must be at least one event or search object before adding a transaction object
- Search and Transaction objects cannot benefit from persistent data model acceleration
 - Acceleration is discussed later in the module
- Think carefully about the reports your users will run
 - Can the same report be achieved with event objects?
- As you learn to create data models, consider the types of reports your users will run
 - Will they need raw events or transactional data?

Creating a Data Model

Settings > Data Models

The screenshot shows the Splunk UI for creating a new data model. At the top, there's a navigation bar with links for Apps, Settings, Activity, and Help. Below that is the 'Data Models' page, which lists existing data models like 'Splunk's Internal Audit Logs - SAMPLE' and 'Splunk's Internal Server Logs - SAMPLE'. On the right, a 'New Data Model' modal is open. It has fields for Title (set to 'Buttercup Games Site Activity'), ID (set to 'Buttercup_Games_Site_Activity'), App (set to 'Search & Reporting'), and Description ('Web server activity'). A note in the modal states: 'ID is automatically populated from Title, but can be overridden'. Another note says: 'choose app context'. At the bottom of the modal are 'Cancel' and 'Create' buttons. A green arrow points from the 'New Data Model' button on the main page to the modal window.

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Adding a Root Event

The screenshot illustrates the process of creating a Root Event in Splunk. On the left, the 'Root Event' option is selected from a dropdown menu. A green arrow points from this selection to a detailed configuration window on the right. This window contains fields for 'Object Name' (set to 'Web Request') and 'Constraints' (set to 'sourcetype=access_combined'). A yellow callout box notes that constraints are search terms used to narrow results. Below the configuration is a preview section showing 1,000 events. A green arrow points from the 'Preview' button to another yellow callout box stating, 'click Preview to view the events that the constraint returns'. The preview table lists several log entries, such as:

Event
12.130.60.5 - - [30/Sep/2014:18:19:03] "GET /oldlink?itemId=EST-17&JSESSIONID=SD10SL4FF10ADFF4954 HTTP 1.1" 200 1704 "http://www.buttercupgames.com/product.screen?productId=WC-SH-G04" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 397
12.130.60.5 - - [30/Sep/2014:18:18:17] "GET /product.screen?productId=WC-SH-T02&JSESSIONID=SD10SL4FF10ADFF4954 HTTP 1.1" 200 2877 "http://www.buttercupgames.com/oldlink?itemId=EST-17" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 520
12.130.60.5 - - [30/Sep/2014:18:17:54] "GET /product.screen?productId=SF-BVS-01&JSESSIONID=SD10SL4FF10ADFF4954 HTTP 1.1" 500 2158 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 631
12.130.60.5 - - [30/Sep/2014:18:17:39] "GET /cart.do?action=remove&itemId=EST-6&productId=CU-PG-G06&JSESSIONID=SD10SL4FF10ADFF4954 HTTP 1.1" 200 2667 "http://www.buttercupgames.com/oldlink?itemId=EST-6" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 100

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Adding a Root Event (cont.)

- In this example, the root event of this data model represents all web requests
- The Inherited attributes are default fields.
- Use **Add Attributes > Auto-Extracted** to add more fields

Buttercup Games Site Activity
Buttercup_Games_Site_Activity

[Edit](#) [Download](#) [Pivot](#) [Documentation](#)

[Back to Data Models](#)

Objects [Add Object](#)

EVENTS

Web Request [Rename](#) [Delete](#)

CONSTRAINTS

sourcetype=access_combined [Constraint](#) [Edit](#)

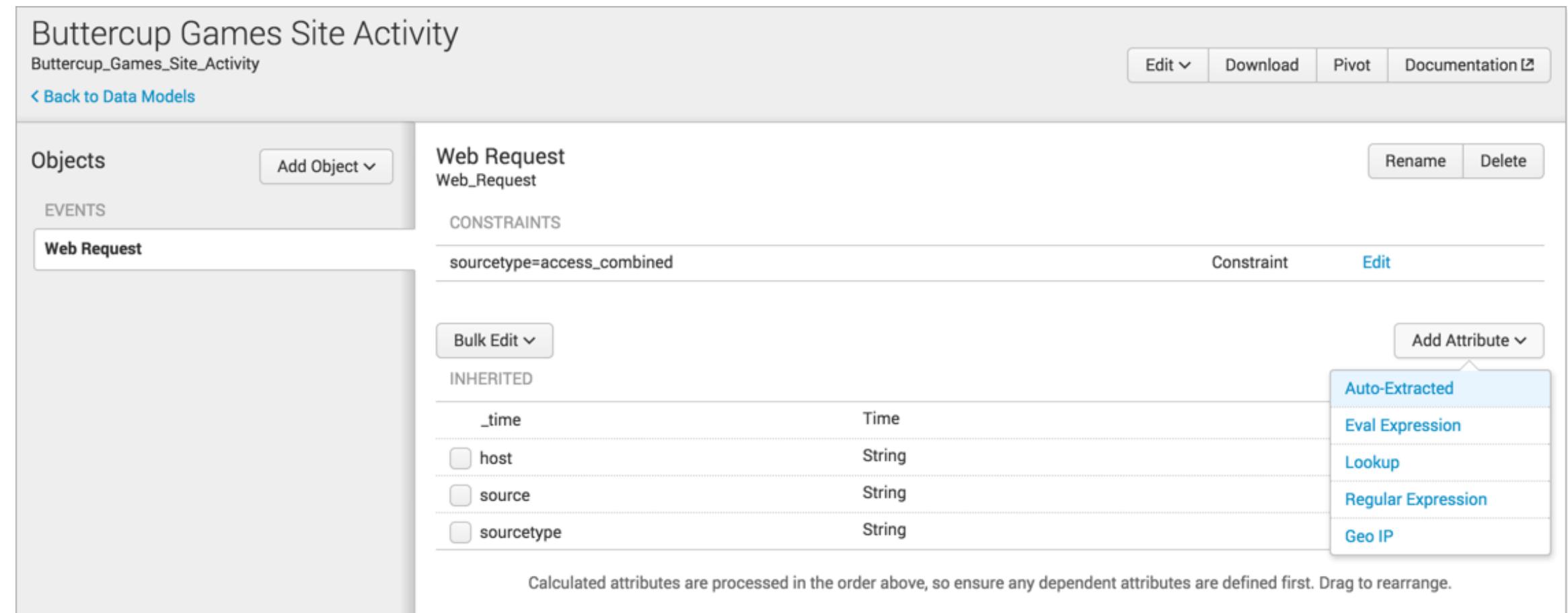
Bulk Edit [Add Attribute](#)

INHERITED

	Type	
_time	Time	
<input type="checkbox"/> host	String	
<input type="checkbox"/> source	String	
<input type="checkbox"/> sourcetype	String	

Calculated attributes are processed in the order above, so ensure any dependent attributes are defined first. Drag to rearrange.

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution



Adding Attributes – Auto-Extracted (Fields)

Fields that already exist for the constraint can be added as attributes to the data model

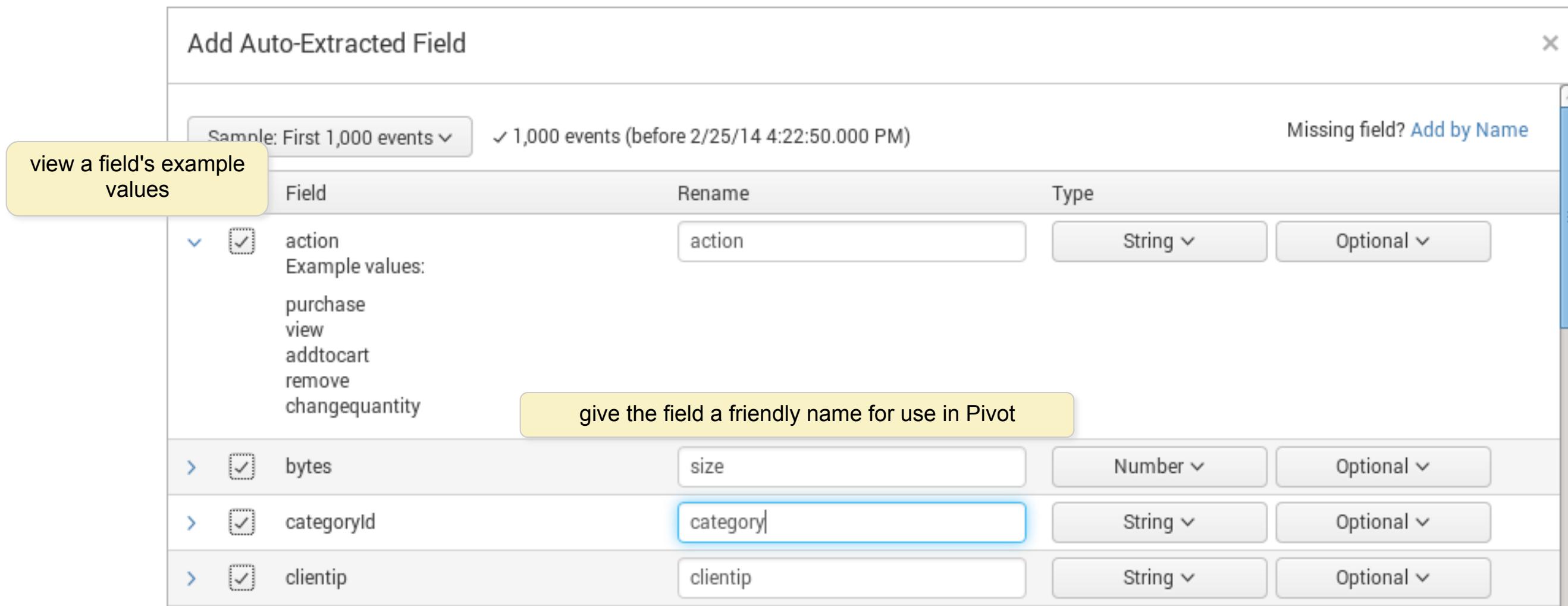
Add Auto-Extracted Field

Sample: First 1,000 events ✓ 1,000 events (before 2/25/14 4:22:50.000 PM) Missing field? Add by Name

view a field's example values

Field	Rename	Type
<input checked="" type="checkbox"/> action Example values: purchase view addtocart remove changequantity	action	String ✓ Optional
> <input checked="" type="checkbox"/> bytes	size	Number ✓ Optional
> <input checked="" type="checkbox"/> categoryId	category	String ✓ Optional
> <input checked="" type="checkbox"/> clientip	clientip	String ✓ Optional

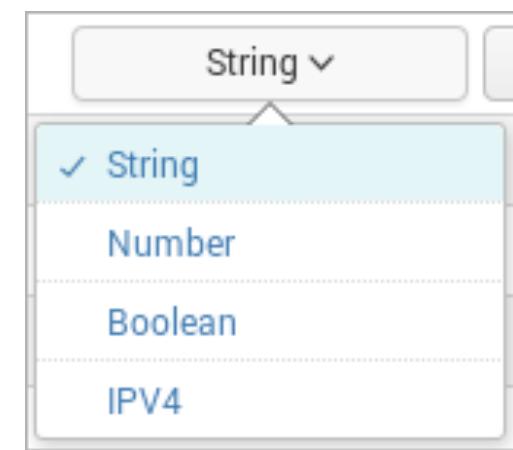
give the field a friendly name for use in Pivot



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

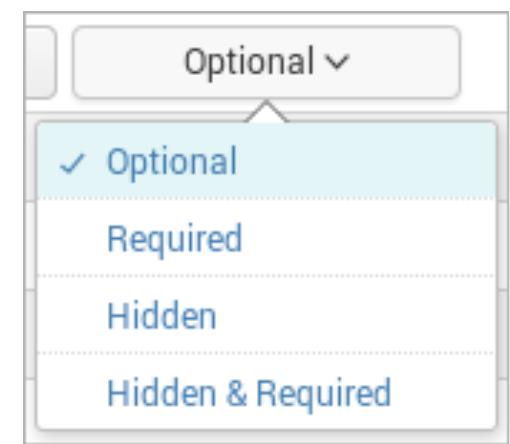
Attribute Types

- **String:** Field values are recognized as alpha-numeric
- **Number:** Field values are recognized as numeric
- **Boolean:** Field values are recognized as true/false or 1/0
- **IPV4:** Field values are recognized as IP addresses
 - This is an important field type, as at least one IPV4 attribute type must be present in the data model in order to add a Geo IP attribute



Attribute Flags

- **Required:** Only events that contain this field are returned in Pivot
- **Optional:** This field doesn't have to appear in every event
- **Hidden:** This field is not displayed to Pivot users when they select the object in Pivot
 - Use for fields that are only being used to define another attribute, such as an eval expression
- **Hidden & Required:** Only events that contain this field are returned, and the fields are hidden from use in Pivot



Adding Attributes – Eval Expressions

You can define a new field using an eval expression

- In this example, we create a field named Error Reason that evaluates the value of the status field

The screenshot shows the Splunk interface for creating a new attribute. On the left, a sidebar menu has 'Eval Expression' selected. A green arrow points from this selection to the main configuration window. The main window is titled 'Eval Expression' and contains the following fields:

- Eval Expression:** `if(status>399, "Web error", "OK")`
- Attribute:**
 - Field Name:** `errorReason`
 - Display Name:** `Error Reason`
 - Type:** `String`
 - Flags:** `Optional`
- A yellow callout box says: `click Preview to verify your eval expression returns events`.
- Events:** Shows 0 events (before 10/1/15 10:27:35.000 PM). A button below says `Sample: 1,000 events`.
- Values:** A table showing event details. The first row is partially visible: `_time 2015-10-01 22:24:58`, `errorReason OK`, `host www3`, `source /opt/log/www3/access.log`, `sourcetype access_combined`, `action view`, `category`, `price 24.99`, `product name FS-SG-G03`, `productid 200`, `status 200`, `Code S`. The second row is: `_time 2015-10-01 22:24:57`, `errorReason Web error`, `host www3`, `source /opt/log/www3/access.log`, `sourcetype access_combined`, `action addtocart`, `category`, `price`, `product name SF-BVS-01`, `productid 406`, `status`, `Code S`.

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Adding Attributes – Lookups

- Leverage an existing lookup definition to add fields to your event object
- Configure the lookup attribute in the same way as an automatic lookup

Add Attributes with a Lookup

Data Model: Buttercup Games Site Activity Object: Web Request

Lookup Table: http_status

Input:

Attribute: status Field in Lookup: code

Output:

Field in Lookup: Field Name:	Display Name:	Type:	Flags:
<input type="checkbox"/> code	code	String	Optional
<input checked="" type="checkbox"/> description	status description	String	Optional

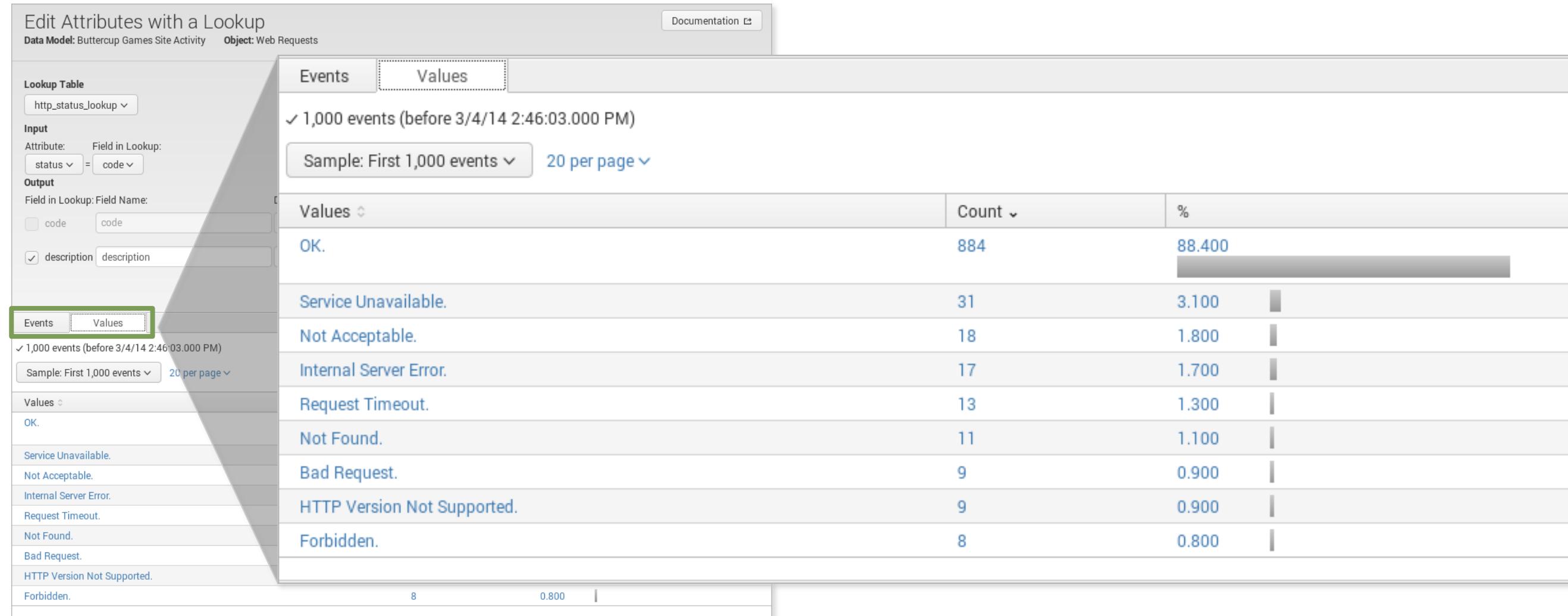
Add Attribute ▾

- Auto-Extracted
- Eval Expression
- Lookup**
- Regular Expression
- Geo IP

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Adding Attributes – Lookups (cont.)

- Use Preview to test your lookup settings
- Use the Events and Values tab to verify your results



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Adding Attributes – Regular Expression

The screenshot shows the 'Add Attributes with a Regular Expression' configuration page. At the top, it displays the 'Data Model: Buttercup Games Online Sales' and 'Object: Web Requests'. On the left, under 'Extract From', there is a dropdown menu set to '_raw'. In the center, the 'Regular Expression' field contains the pattern `userAgent=(?<browser>[*()]+)`. To the right, the 'Attribute(s)' section shows a single attribute named 'browser' with 'Field Name:' and 'Display Name:' both set to 'browser'. The 'Type:' dropdown is set to 'String'. A vertical sidebar on the right lists several extraction methods: 'Auto-Extracted' (selected), 'Eval Expression', 'Lookup', 'Regular Expression' (which is highlighted with a green border), and 'Geo IP'. At the bottom right are three buttons: 'Cancel', 'Preview', and a green 'Save' button.

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Adding Attributes – Regular Expression (cont.)

You can define a new field using a regular expression

Add Attributes with a Regular Expression

Data Model: Buttercup Games Online Sales Object: Web Requests

Extract From: _raw

Regular Expression: userAgent=(?<browser>[*](+))

Attribute(s): Field Name: browser Display Name: browser Type: String Flags: Optional

Click Preview to view the events that Match or Don't Match the regular expression

Events browser

✓ 1,000 events (before 10/1/15 10:54:18.000 PM)

filter Apply Sample: 1,000 events All events All Events Matches Non-Matches

20 per page < Prev 1 2 3 4 5 6 7 8 9 ... Next >

_raw	browser
✗ 71.192.86.205 - - [01/Oct/2015:22:54:01] "GET /cart.do?action=addtocart&itemId=EST-26&productId=WC-SH-G04&JSESSIONID=SD3SL3FF8ADFF4961 HTTP 1.1" 200 1186 "http://www.buttercupgames.com/product.screen?productId=WC-SH-G04" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 889	
✗ 71.192.86.205 - - [01/Oct/2015:22:53:46] "GET /category.screen?categoryId=ARCADE&JSESSIONID=SD3SL3FF8ADFF4961 HTTP 1.1" 200 1102 "http://www.buttercupgames.com/product.screen?productId=FI-AG-G08" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 400	
✗ 71.192.86.205 - - [01/Oct/2015:22:53:37] "GET /cart.do?action=addtocart&itemId=EST-27&productId=FI-AG-G08&JSESSIONID=SD3SL3FF8ADFF4961 HTTP 1.1" 200 2488 "http://www.buttercupgames.com/category.screen?categoryId=ARCADE" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 742	

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Adding Attributes - GeolP

- Map visualizations require latitude/longitude fields
- To use Geo IP Lookup, at least one IP field must be configured as an IPv4 type
- While the map function isn't available in Pivot, the data model can be called using the `| pivot` command and `<map>` element in a dashboard population search

- Select the field that contains the mapping to lat/lon
- Identify the lat/lon and geo fields in the data

Add Geo Attributes with an IP Lookup
Data Model: Buttercup Games Site Activity Object: Web Request

IP	Attribute(s)	Display Name:
clientIP	Include: <input checked="" type="checkbox"/> Field in GeolP: lon	longitude
	<input checked="" type="checkbox"/> lat	latitude
	<input checked="" type="checkbox"/> City	
	<input checked="" type="checkbox"/> Region	
	<input checked="" type="checkbox"/> Country	

Add Attribute ▾
Auto-Extracted
Eval Expression
Lookup
Regular Expression
Geo IP

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Adding Child Events

When you define a new child object, you give it one or more additional constraints

Buttercup Games Site Activity
Buttercup_Games_Site_Activity
< Back to Data Models

Objects

EVENTS

Web Request

Add Object ▾

Root Event

Root Transaction

Root Search

Child

Web Request

Add Child Object

Data Model: Buttercup Games Site Activity

All events that have a status less than 400 (successful http request)

Object Name

successful request

Object ID ?

successful_request

Can only contain letters, numbers and underscores.

Inherit From

Web Request ▾

Additional Constraints

status<400 productId=*

Examples:
uri="*.php*" OR uri="*.py*"
NOT (referer=null OR referer="-")

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Adding Child Events (cont.)

- Child events inherit all attributes from the parent events
 - You can add more attributes to child events

The screenshot shows the 'Add Attribute' interface for a 'successful request' event type. At the top right are 'Rename' and 'Delete' buttons. Below that is a 'CONSTRAINTS' section with two entries: 'sourcetype=access_combined' (Inherited) and 'status<400 productId='*. Underneath is a 'Bulk Edit' dropdown menu. The main area is titled 'INHERITED' and contains a list of attributes with their types and override status:

Attribute	Type	Override
_time	Time	Override
action	String	Override
bytes	Number	Override
categoryId	String	Override
change_type	String	Override
clientip	String	Override
cookie	String	Override
date_hour	Number	Override
date_mday	Number	Override

To the right of the table is a vertical dropdown menu labeled 'Add Attribute' with options: Auto-Extracted, Eval Expression, Lookup, Regular Expression, and Geo IP.

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Adding a Transaction

- You can add a transaction to the data model
- The transaction object below would equate to the search:
`sourcetype=access_* | transaction clientip maxpause=10s`

Add Transaction Object
Data Model: Buttercup Games Site Activity

You must specify at least one of the optional fields.

Object Name: visit duration

Object ID?: visit_duration

Can only contain letters, numbers and underscores.

Select an object from the data model to base the transaction on

Web Requests

+ Group by clientip

Duration

Max Pause: 10 Seconds

Max Span: Seconds

Optional: Optionally select max pause and max span

Root Event
Root Transaction (selected)
Root Search
Child

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Adding a Transaction (cont.)

- You can then add an eval expression or any other attribute to your transaction to further define the results
- This example shows dividing the duration field value by 60 to convert the duration field to minutes

Add Attributes with an Eval Expression
Data Model: Buttercup Games Site Activity Object: visit duration

Eval Expression
duration/60

Attribute
Field Name: visitDuration Display Name: visitDuration Type: String Flags: Optional

visit duration
visit_duration

CONSTRAINTS

Group Objects	Web_Request	Transaction
Group By	clientip	Edit
Max Pause	10m	
Max Span		

Bulk Edit ▾

INHERITED

<input type="checkbox"/> time	Time
<input type="checkbox"/> duration	Number
<input type="checkbox"/> eventcount	Number

EXTRACTED

<input type="checkbox"/> action		Edit
<input type="checkbox"/> bytes		Edit

Add Attribute ▾

Auto-Extracted

- Eval Expression** (highlighted)
- Lookup
- Regular Expression
- Geo IP

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Using the Data Model in Pivot (cont.)

The New Pivot window automatically populates with a count of events for the selected object.

New Pivot

✓ 1,226 events (9/25/15 4:00:00.000 PM to 10/2/15 4:48:09.000 PM)

Filters

Last 7 days

Split Rows

Count of Failed Requests

1226

Save As... ▾

Split Columns

+ Column Values

Count of Failed R...

Select a Data Object

< Back

- i 10 Objects in Buttercup Games Site Activity
- > Web Requests
- > Successful Requests
- > purchase
- > add
- > remove
- > Failed Requests
- > purchase
- > add
- > remove
- > visit duration

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Using the Data Model in Pivot

- Click Pivot to access the Select an Object window
- Choose an object from the selected data model to begin building the report

Buttercup Games Site Activity
Buttercup_Games_Site_Activity

[Edit](#) [Download](#) **Pivot** [Documentation](#)

[← Back to Data Models](#)

Objects [Add Object](#)

EVENTS

Web Requests [Web_Requests](#)

CONSTRAINTS

sourcetype=access_combined [Constraint](#)

[Bulk Edit](#)

INHERITED

_time [Time](#)

Successful Requests

- [purchase](#)
- [add](#)
- [remove](#)

Select a Data Object

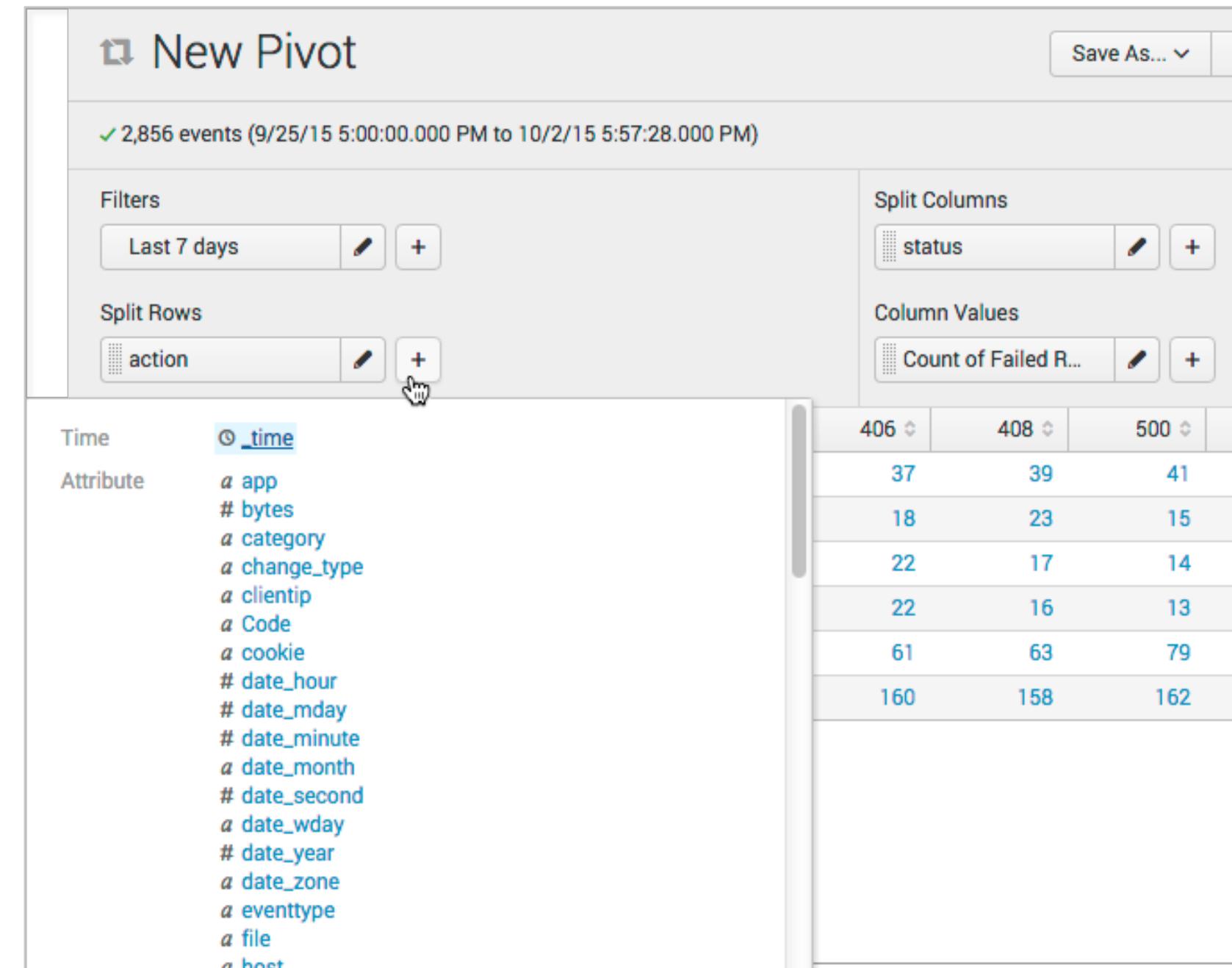
[← Back](#)

- [10 Objects in Buttercup Games Site Activity](#)
- [Web Requests](#)
- [Successful Requests](#)
- [purchase](#)
- [add](#)
- [remove](#)
- Failed Requests**
- [purchase](#)
- [add](#)
- [remove](#)
- [visit duration](#)

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Pivot – Using Attributes

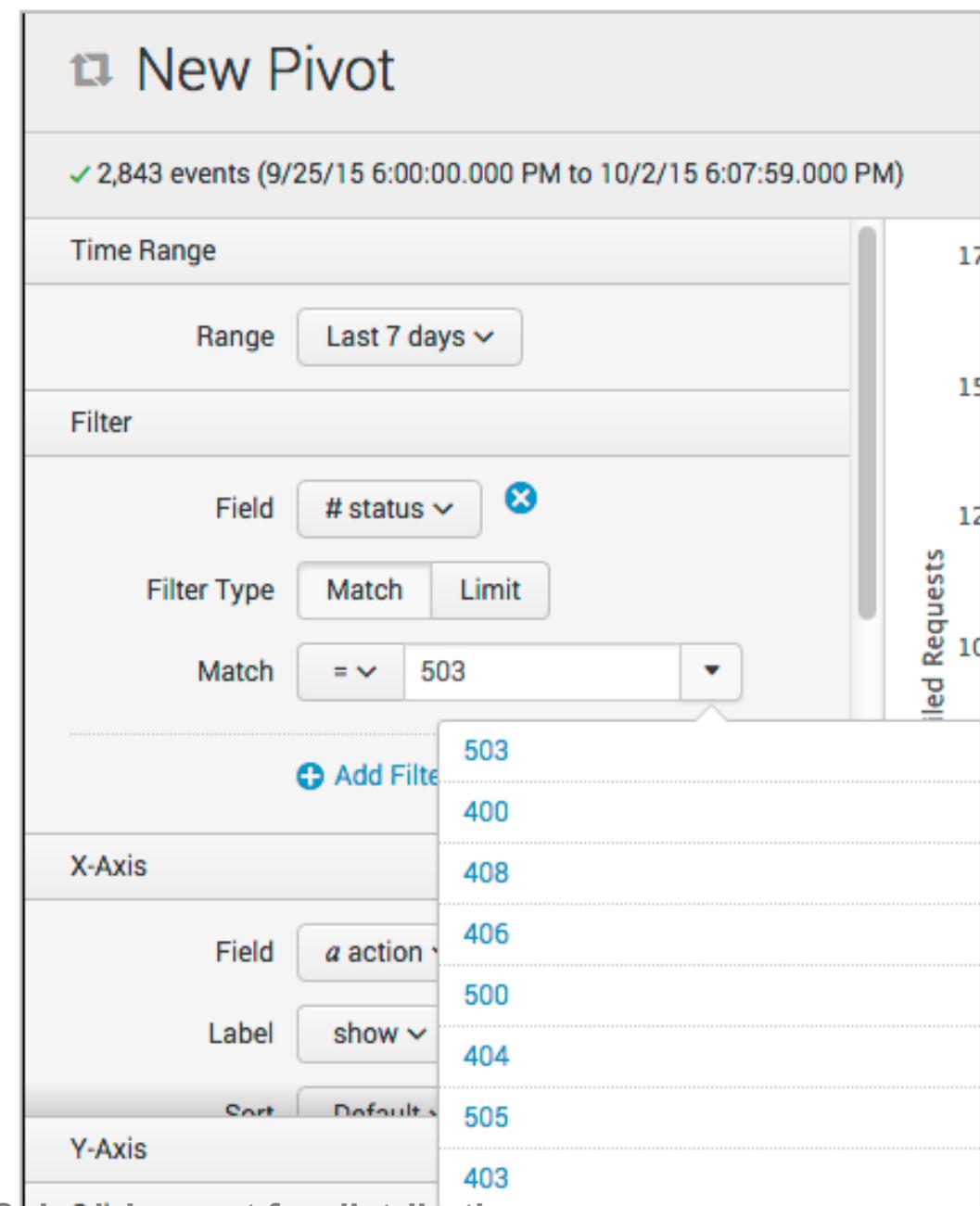
- The attributes associated with each object are available as splits for rows or columns
- In this example, the Pivot report will show a count of failed request actions by status



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Pivot – Using Attributes (cont.)

- Attributes are also available for use as filters
- In this example, the Pivot report is filtered to only return results where status=503



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Underlying Search

New Pivot

523 events (9/25/15 6:00:00.000 PM to 10/2/15 6:16:14.000 PM)

Save As... Clear Failed Requests

New Search

| pivot Buttercup_Games_Site_Activity failed_request count(failed_request) AS "Count of Failed Requests" SPLITROW
action AS action SPLITCOL status FILTER status = 503 SORT 100 action ROWSUMMARY 0 COLSUMMARY 0 NUMCOLUMNS 100 SHOWOTHER 0

Last 7 days

526 events (9/25/15 8:00:00.000 PM to 10/2/15 8:12:06.000 PM)

Save As Close

Events (526) Patterns Statistics (5) Visualization

Job Last 7 days Verbose Mode

Column Format

Count of Failed Requests

Action	Count of Failed Requests
addtocart	35
changequantity	25
purchase	145
remove	30
view	70

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Underlying Search (cont.)

```
| pivot Buttercup_Games_Site_Activity failed_request  
count(failed_request) AS "Count of Failed requests"  
  
SPLITROW action AS action TOP 100  
count(failed_request)  
  
SPLITCOL status  
FILTER status = 503
```

Data model name

Object name

Split row field (or attribute)

Split column field (or attribute) and filter field/value pair

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Set Permissions

- When a data model is created, the owner can determine access based on the following permissions:
 - Who can see the data models
 - Owner, App, or All Apps
 - Which users can perform which actions (Read/Write)
 - Everyone
 - Power
 - User
 - Admin-defined roles, if applicable

Edit Permissions

Data Model: Buttercup Games Site Activity

Owner: cfarrell

App: search

Display For: Owner App All Apps

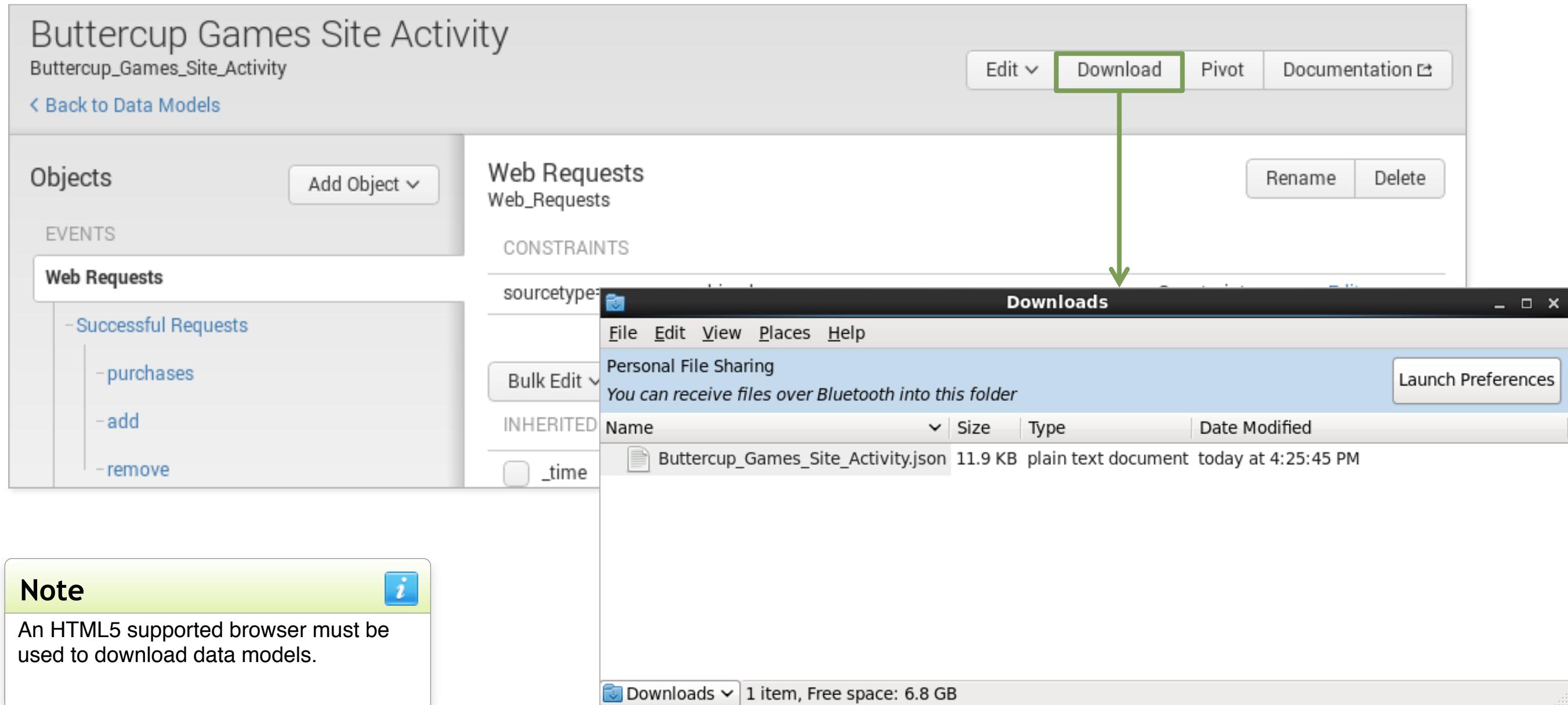
	Read	Write
Everyone	<input checked="" type="checkbox"/>	<input type="checkbox"/>
power	<input checked="" type="checkbox"/>	<input type="checkbox"/>
user	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Cancel Save

Download and Upload Data Models

- Use the Splunk Web interface to download or upload data models:
 - Back up important data models
 - Collaborate with other Splunk users to create/modify/test data models
 - Move data models from a test environment to production instance

Downloading a Data Model



Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Uploading a Data Model

The screenshot illustrates the process of uploading a new data model in Splunk. On the left, the main 'Data Models' page shows a list of existing data models, including 'Splunk's Internal Audit Logs - SAMPLE' and 'Splunk's Internal Server Logs - SAMPLE'. A green arrow points from the 'Upload Data Model' button in the top navigation bar to the 'Upload New Data Model' dialog box on the right. The dialog box contains fields for 'File' (set to 'Buttercup_Games_Site...'), 'ID' (set to 'data_model_from_Cerys'), 'App' (set to 'Search & Reporting'), and 'Dashboard Permissions' (set to 'Private'). A 'Save' button is at the bottom right of the dialog. The central part of the interface shows a specific data model named 'Buttercup Games Site Activity' with its details: 'data_model_from_Cerys', 'Web Requests' object, and constraints like 'sourcetype=access_combined'. A green arrow also points from the 'Save' button back to the main data model page.

splunk> Apps >

Lien Teng > Messages > Settings > Activity > Help >

Data Models

Data models enable users to easily create reports in the Pivot tool. [Learn More](#)

App: Search & Reporting (search) > Created in the App > Owner: Any > filter

i	Title ^	Actions	App	Owner	Share
>	Splunk's Internal Audit Logs - SAMPLE	Edit > Pivot	search	nobody	Ap
>	Splunk's Internal Server Logs - SAMPLE	Edit > Pivot	search	nobody	Ap

splunk> App: Search & Reporting > Lien Teng >

Buttercup Games Site Activity

data_model_from_Cerys

< Back to Data Models

Objects Add Object >

EVENTS

Web Requests

Successful Requests

- purchases
- add
- remove

Web Requests

Web_Requests

CONSTRAINTS

sourcetype=access_combined

Bulk Edit >

INHERITED

time Constraint Edit

Add Attribute >

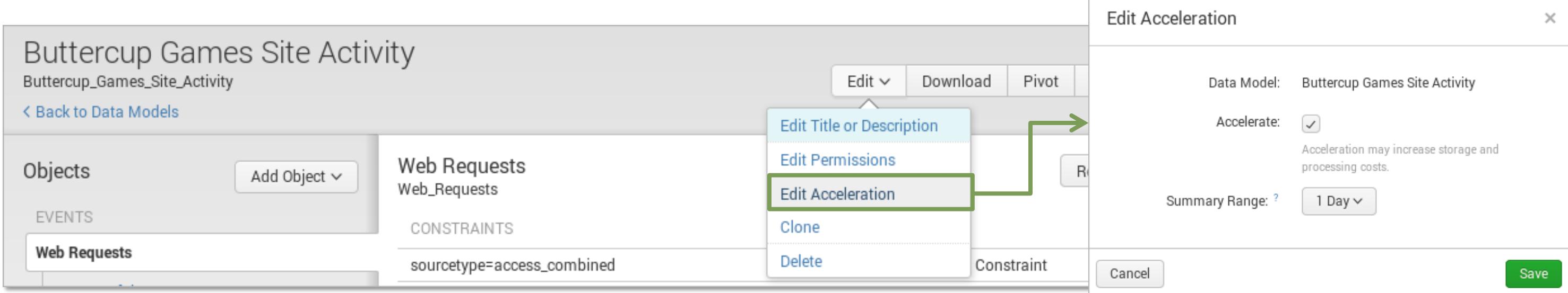
Override

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Accelerating a Data Model

- With persistent data model acceleration, all fields in the model become "indexed" fields in the table
- You must have administrative permissions or the accelerate_datamodel capability to accelerate a data model
- Private data models cannot be accelerated
- Accelerated data models cannot be edited

Note  Only root events can be accelerated. If there are multiple root events, only the first root event is accelerated.



The screenshot shows the Splunk UI for managing data models. On the left, the 'Buttercup Games Site Activity' data model is displayed with sections for Objects, EVENTS, and CONSTRAINTS. A context menu is open over the 'Web Requests' object, with the 'Edit Acceleration' option highlighted. To the right, a modal window titled 'Edit Acceleration' is open, showing the 'Data Model' as 'Buttercup Games Site Activity' and the 'Accelerate' checkbox checked. A note in the modal states: 'Acceleration may increase storage and processing costs.' The 'Save' button is at the bottom right of the modal.

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Support Programs

• Community

- **Splunk Answers:** answers.splunk.com
Post specific questions and get them answered by Splunk community experts.
- **Splunk Docs:** docs.splunk.com
These are constantly updated. Be sure to select the version of Splunk you are using.
- **Wiki:** wiki.splunk.com
A community space where you can share what you know with other Splunk users.
- **IRC Channel:** #splunk on the EFNet IRC server Many well-informed Splunk users “hang out” here.

• Global Support

Support for critical issues, a dedicated resource to manage your account – 24 x 7 x 365.

- **Email:** support@splunk.com
- **Web:** http://www.splunk.com/index.php/submit_issue

• Enterprise Support

Access your customer support team by phone and manage your cases online 24 x 7
(depending on support contract).

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution

Thank You

Generated for James Kim (455-641803) (C) Splunk Inc, not for distribution