

## Splunk Module – 4 & 5

[Creating Lookups](#)

[Creating Field Aliases and Calculated Fields](#)

[Creating Field Extractions](#)

[Creating Tags and Event Types](#)

[Creating Workflow Actions](#)

[Creating Alerts and Scheduled Reports](#)

[Creating and Using Macros](#)

[: Creating Data Models](#)

# Module Objectives

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

# 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

# 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 <b>Lookup table files</b>	Add new
2 <b>Lookup definitions</b>	Add new
3 <b>Automatic lookups</b>	Add new

List existing lookup tables or upload a new file.

Edit existing lookup definitions or define a new file-based or external lookup.

Edit existing automatic lookups or configure a new lookup to run automatically.

# 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.

4 Destination filename \*

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

# 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 windows from the Splunk UI. The left window is titled 'Lookup table files' under 'Lookups > Lookup table files'. It displays a single item with the path '/opt/splunk/etc/users/student10/search/lookups/products.csv'. The 'Sharing' dropdown is set to 'Private' and the 'Permissions' button is highlighted with a green box and an arrow pointing to the right window. The right window is titled 'Permissions' under 'Lookups > Lookup table files > products.csv > Permissions'. It shows the 'Object should appear in' section with 'This app only (search)' selected. 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.

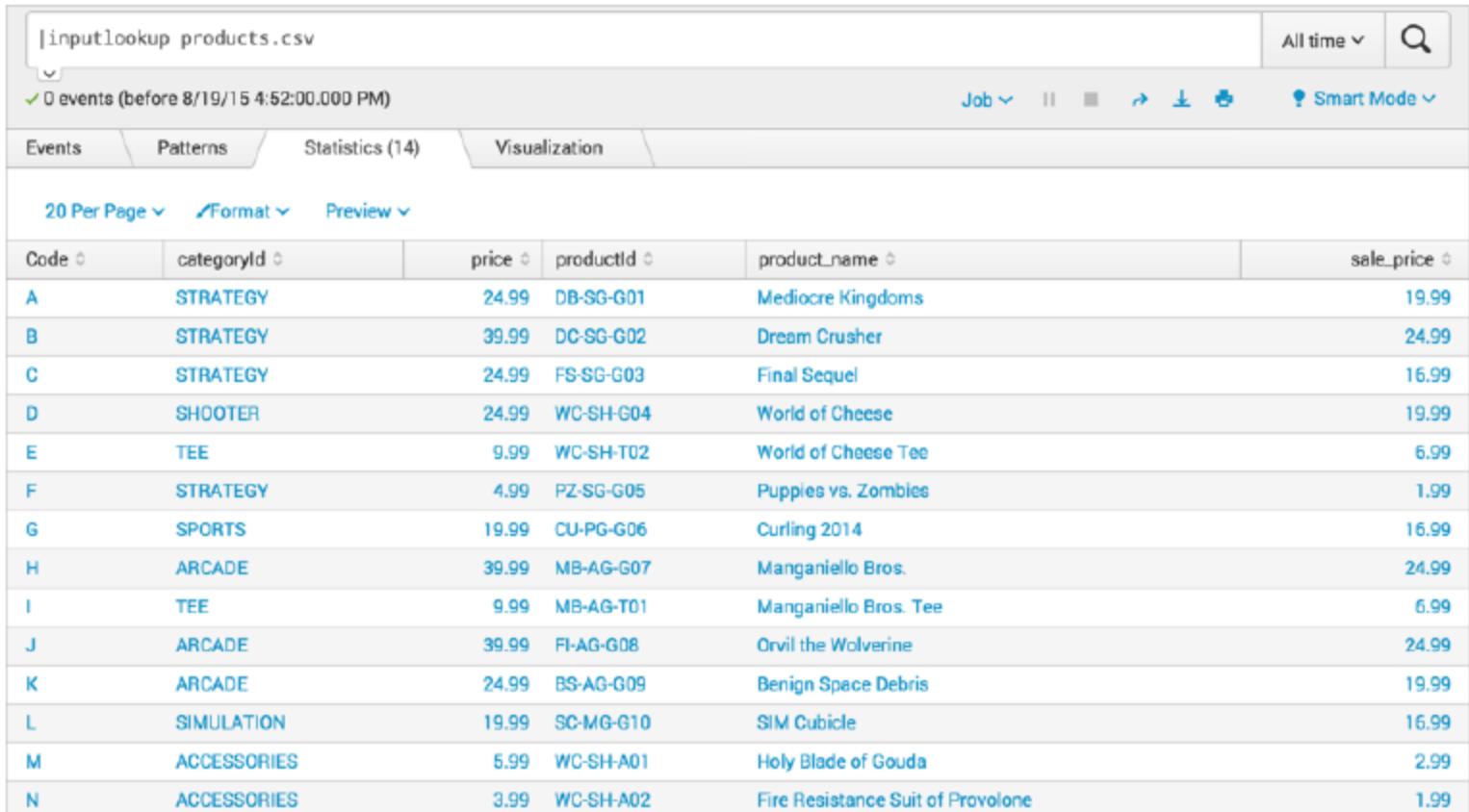
Roles	Read	Write
Everyone	<input checked="" type="checkbox"/>	<input type="checkbox"/>
power	<input type="checkbox"/>	<input type="checkbox"/>
user	<input type="checkbox"/>	<input type="checkbox"/>

# 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 the Splunk interface with the search bar containing `|inputlookup products.csv`. The results pane displays 14 events from a static lookup file. The table has columns: Code, categoryId, price, productId, product\_name, and sale\_price. The data is as follows:

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

# 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

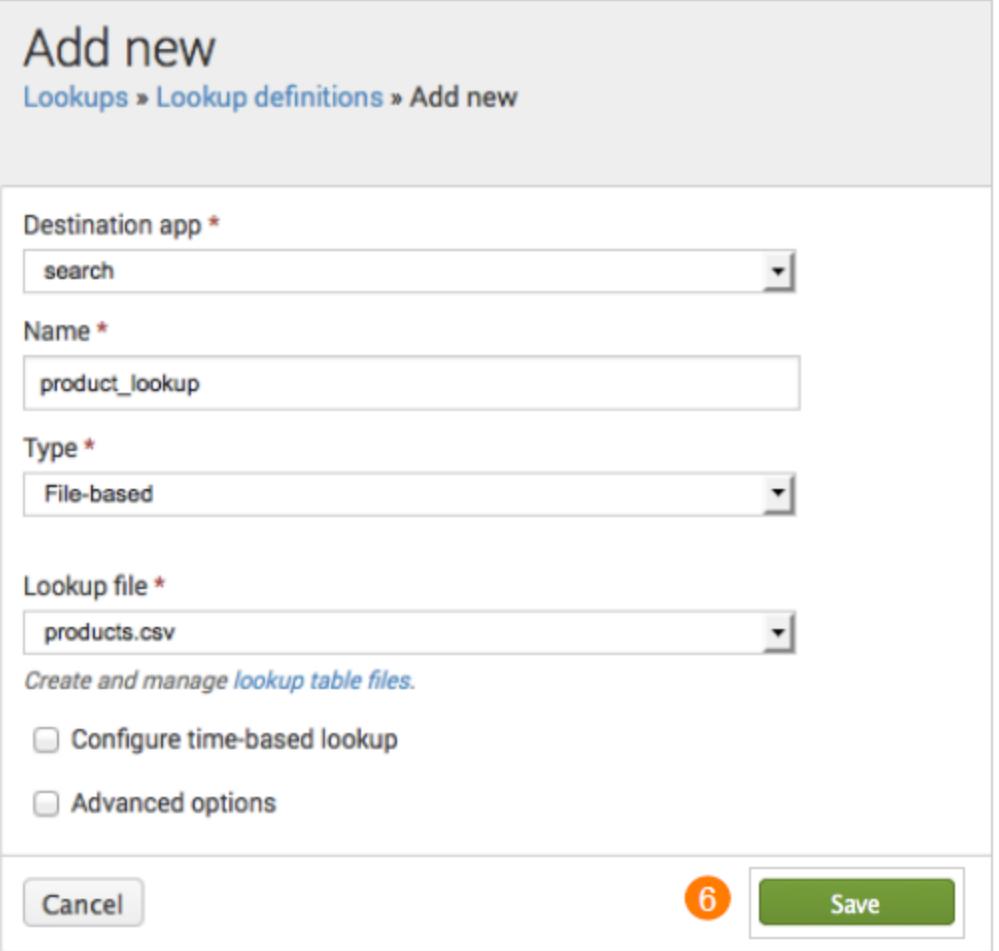
Create and manage [lookup table files](#).

Configure time-based lookup

Advanced options

Cancel

⑥ Save



# 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

The screenshot shows a configuration dialog for a 'Lookup file'. The 'Lookup file' dropdown is set to 'products.csv'. The 'Configure time-based lookup' checkbox is unchecked, while the 'Advanced options' checkbox is checked. Three numbered callouts point to specific fields:

- ① 'Minimum matches': A text input field containing '1'. Below it is a note: 'The minimum number of matches for each input lookup value. Default is 0.'
- ② 'Maximum matches': A text input field containing '1'. Below it is a note: '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.'
- ③ 'Default matches': A text input field containing 'NoInputMatch'. Below it is a note: '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.'

At the bottom left is a 'Cancel' button, and at the bottom right is a green 'Save' button.

# Managing Lookup Definitions

Based on your permissions, you can:

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

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

The screenshot shows a list of five lookup definitions. The last item, 'product\_lookup', is highlighted with a green border, indicating it is selected. The table columns are: Name, Type, Supported fields, Lookup file, Owner, App, Sharing, Status, and Actions. The 'Actions' column for 'product\_lookup' contains links for 'Clone', 'Move', and 'Delete'.

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

# 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

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

- Search Bar:** New Search
- Search String:**

```
sourcetype=access* action=purchase  
| lookup product_lookup productId OUTPUT price product_name  
| stats sum(price) as sales by product_name
```
- Scenario Pop-up:** Calculate the sales for each product in the last 60 minutes.
- Time Range:** Last 60 minutes
- Job Controls:** Job, II, ■, ▶, ▷, Smart Mode
- View Options:** Events, Patterns, Statistics (8), Visualization (selected), 20 Per Page, Format, Preview
- Table Results:** Shows sales data for four products.

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

# 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 *	search
Name *	product_auto_lookup
Lookup table *	product_lookup
Apply to *	sourcetype
named *	access_combine

# 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

The screenshot shows a configuration interface for defining automatic lookup fields. It is divided into two main sections: 'Lookup input fields' and 'Lookup output fields'.  
**Lookup input fields:** This section contains one entry: 'productId' (highlighted with orange circle A). To its right is a 'Delete' button (highlighted with orange circle B). Below this section is a link 'Add another field'.  
**Lookup output fields:** This section contains four entries:

- 'categoryId' (highlighted with orange circle C) followed by a 'Delete' button (highlighted with orange circle D).
- 'price' followed by a 'Delete' button.
- 'product\_name' followed by a 'Delete' button.
- 'sale\_price' followed by a 'Delete' button.

Below these entries is a link 'Add another field'.  
At the bottom of the interface are two buttons: 'Cancel' and 'Save' (highlighted with green box). There is also an unchecked checkbox labeled 'Overwrite field values'.

# 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	<a href="#">Clone</a>   <a href="#">Move</a>   <a href="#">Delete</a>
vendor_sales : LOOKUP-vendor_lookup	dnslookup Vendor OUTPUTNEW VendorId	cfarrell	search	Private   Permissions	Enabled	<a href="#">Clone</a>   <a href="#">Move</a>   <a href="#">Delete</a>

# 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 are divided into two panels:

- Left Panel (Events):** Shows log entries for purchases. One entry for productId `DC-SG-G02` is highlighted with a green arrow pointing to the right panel.
- Right Panel (Statistics):** A table showing the sum of price for each productId and its corresponding product\_name. The row for productId `DC-SG-G02` has a green arrow pointing to the sales value in the Events panel.
- Bottom Panel (Statistics):** A table showing the sales value for each productId. The row for productId `DC-SG-G02` has a green arrow pointing to the sales value in the Events panel.

**Search Results (Top Panel):**

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&SESSIONID=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&JSESSID=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

**Statistics (Right Panel):**

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

**Statistics (Bottom Panel):**

productId	sales
BS-AG-G09	24.99
CU-PG-G06	19.99
DB-SG-G01	24.99
DC-SG-G02	119.97
FS-SG-G03	24.99

# Module Objectives

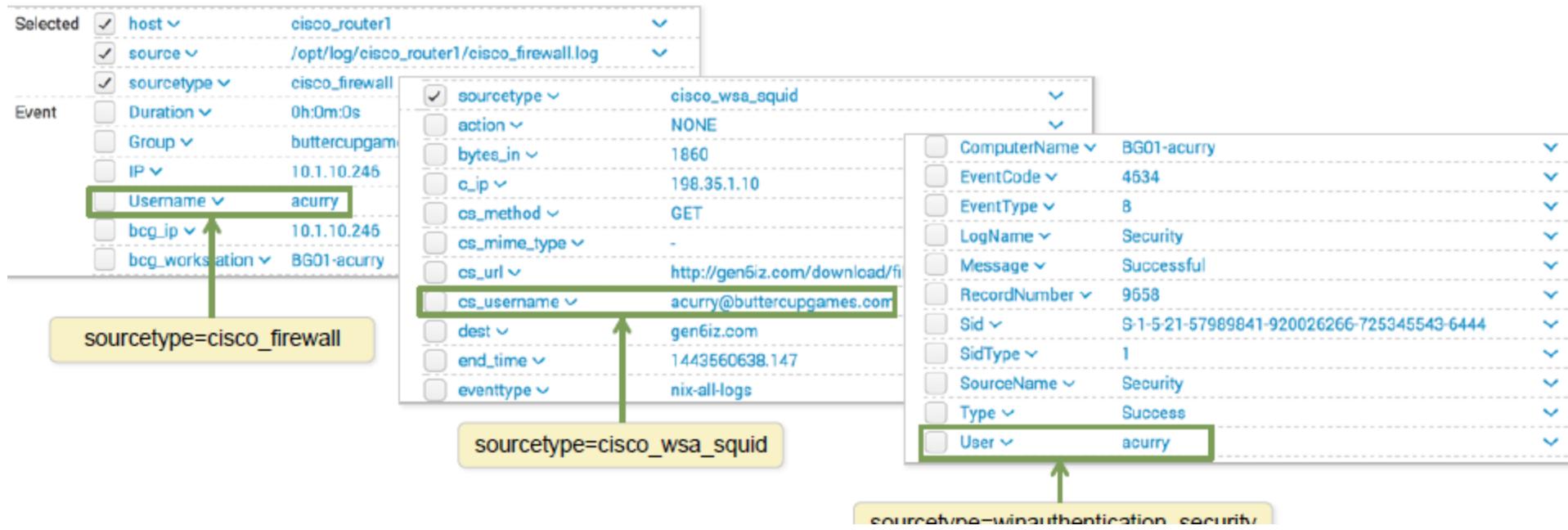
- Create and use field aliases
- Create calculated fields

# 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

# Field Alias Example

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



# 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

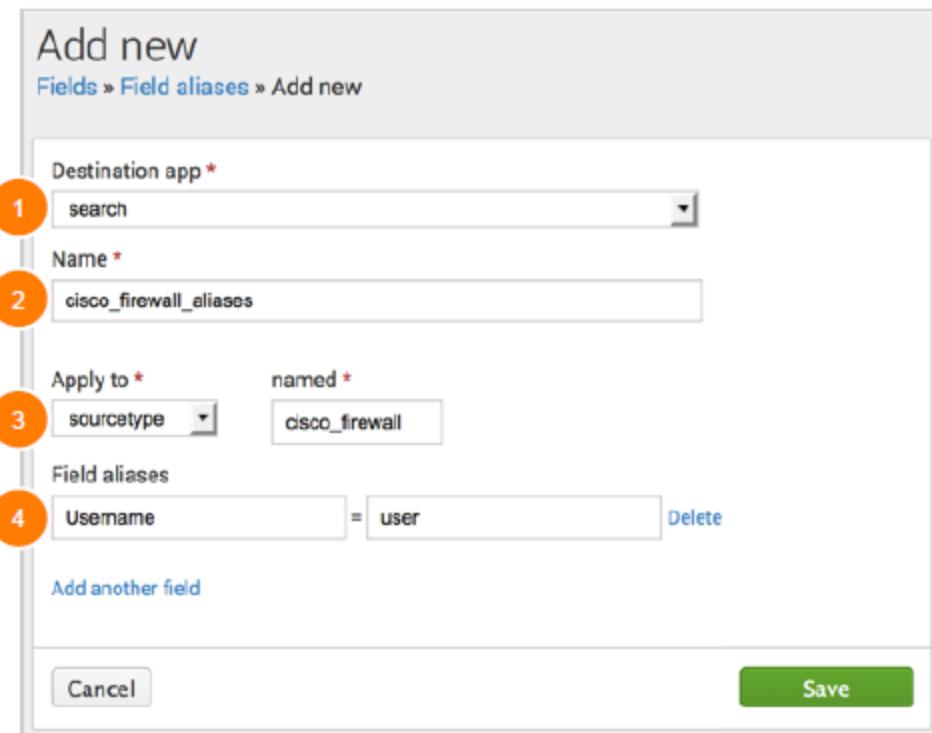
Name \* **2** cisco\_firewall\_aliases

Apply to \* **3** sourcetype named \* cisco\_firewall

Field aliases **4** Username = user Delete

Add another field

Cancel Save



# 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 displays three side-by-side screenshots of a 'Fields > Field aliases > Add new' interface. Each screenshot shows a form for creating a new field alias with the following fields:

- Destination app \***: search
- Name \***: cisco\_firewall\_aliases, cisco\_wsa\_squid\_aliases, or winauthentication\_security\_aliases
- Apply to \***: sourcetype dropdown, named \*: cisco\_firewall, cisco\_wsa\_squid, or winauthentication
- Field aliases**: Username = user, cs\_username = user, or User = user
- Add another field**: link to add more field aliases
- Cancel**: button to cancel the operation
- Save**: button to save the new field alias (only visible in the third screenshot)

The first two screenshots show the configuration for 'cisco\_firewall\_aliases' and 'cisco\_wsa\_squid\_aliases'. The third screenshot shows the configuration for 'winauthentication\_security\_aliases'.

# Testing the Field Alias

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

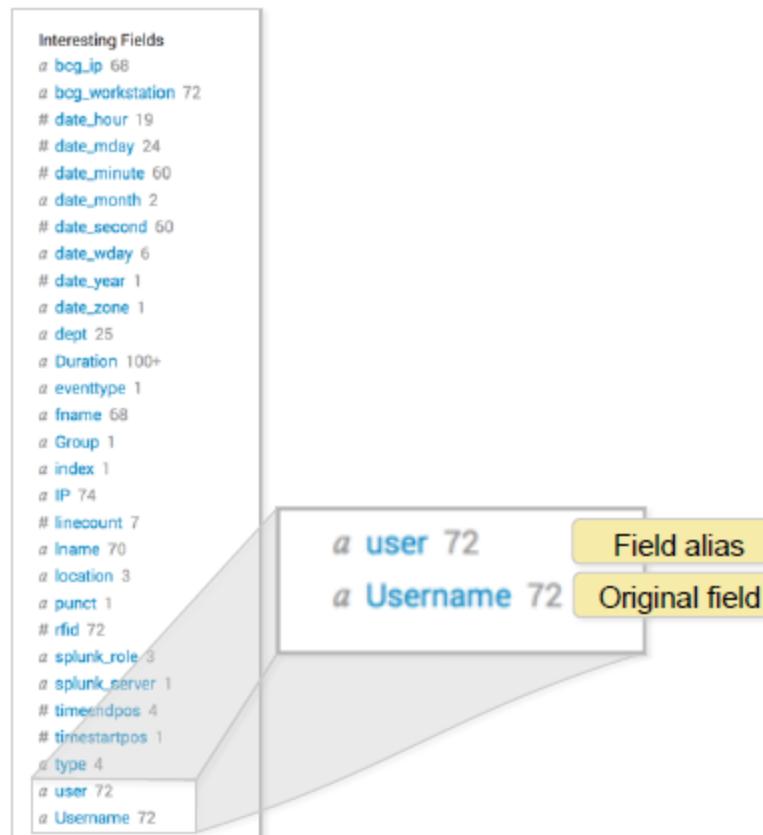
The screenshot shows the Splunk search interface. The search bar contains the query `user=acurry*`. Below the search bar, it says `47 events (9/23/15 12:00:00.000 AM to 9/30/15 12:53:47.000 AM)`. The main pane displays a timeline visualization. On the left, under "Selected Fields", the `a sourcetype` field is highlighted with a green box. A green arrow points from this field to a modal window titled "sourcetype". The modal window shows the following data:

Values	Count	%
cisco_wsa_squid	23	48.936%
winauthentication_security	23	48.936%
cisco_firewall	1	2.128%

# 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.



# Managing Field Aliases

## Settings > Fields > Field Aliases

- Edit permissions
- Clone
- Move
- Delete

The screenshot shows the 'Field aliases' page within a 'Fields' section. The top navigation bar includes 'App context' set to 'Search & Reporting (search)', 'Owner' set to 'Any', and a search bar with a magnifying glass icon. A checkbox for filtering by app context is checked. Below the header is a 'New' button. The main area displays a table of three field aliases, each with a 'Actions' column containing 'Clone | Move | Delete' links.

Name	Field aliases	Owner	App	Sharing	Status	Actions
cisco_firewall : FIELDALIAS:cisco_firewall_aliases	Username AS user	cfarrell	search	Private   Permissions	Enabled	<a href="#">Clone</a>   <a href="#">Move</a>   <a href="#">Delete</a>
cisco_wea_squid : FIELDALIAS:cisco_wea_squid_aliases	ce_username AS user	cfarrell	search	Private   Permissions	Enabled	<a href="#">Clone</a>   <a href="#">Move</a>   <a href="#">Delete</a>
winauthentication_security : FIELDALIAS:winauthentication_security_aliases	User AS user	cfarrell	search	Private   Permissions	Enabled	<a href="#">Clone</a>   <a href="#">Move</a>   <a href="#">Delete</a>

# 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)

Job      Verbose Mode

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

20 Per Page

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

# 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

The screenshot shows a 'Add new' dialog for creating a calculated field. The path 'Fields > Calculated fields > Add new' is visible at the top. The form contains the following fields:

- Destination app \***: search (marked with a red circle labeled 1)
- Apply to \***: sourcetype (marked with a red circle labeled 2)
- named \***: cisco\_wsa\_squic (displayed next to the apply to dropdown)
- Name \***: bandwidth (marked with a red circle labeled 3)
- Eval expression \***: sc\_bytes/(1024\*1024) (marked with a red circle labeled 4)
- Description**: A valid eval expression, e.g.  $x + 3$

At the bottom right are 'Cancel' and 'Save' buttons.

# 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 a Splunk search interface titled "New Search". The search bar contains the command: "sourcetype=cisco\_w\* | stats sum [bandwidth] as "Bandwidth (MB)" by usage". The search results indicate 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

# Managing Calculated Fields

## Settings > Fields > Calculated Fields

- Edit permissions
- Clone
- Move
- Delete

The screenshot shows a list of calculated fields. At the top, there are search and filter options: 'App context' set to 'Search & Reporting (search)', 'Owner' set to 'Any', and a search bar with a magnifying glass icon. Below these are two checkboxes: 'Show only objects created in this app context' and 'Learn more'. A large green 'New' button is centered above the table. The table has columns for Name, Field name, Eval expression, Owner, App, Sharing, Status, and Actions. One row is visible, showing 'cisco\_wsa\_squid : EVAL-bandwidth' in the Name column, 'bandwidth' in the Field name column, 'sc\_bytes/(1024\*1024)' in the Eval expression column, 'cfarrell' in the Owner column, 'search' in the App column, 'Private | Permissions' in the Sharing column, 'Enabled' in the Status column, and 'Clone | Move | Delete' in the Actions column.

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

- 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+

categoryId=strategy

categoryId=sports

- 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 steps to create a tag in Splunk:

- Event Details View:** A log entry is shown with an arrow icon (circled in orange) pointing to the event details. The log details are:  
10/26/15 3:34:00.000 PM 87.194.216.51 - - [26/Oct/2015:22:34:00] "GET /oldlink?itemId=EST-19&JSESSIONID=SD5SLBFF5ADFF4955 HTTP/1.1" 200 3572 "http://www.buttercupgames.com/category.screen?categoryId=STRATEGY" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 654
- Action Panel:** An "Event Actions" dropdown menu is open, showing various fields and their values. A green arrow points from the "Actions" column towards the "Edit Tags" button.
- Edit Tags Dialog:** A modal window titled "Create Tags" is displayed. It contains a "Field Value" input field with the value "categoryId=STRATEGY" and a "Tag(s)" input field with the value "Teen". A green box highlights the "Teen" tag entry.
- Final Step:** A green arrow points from the "Save" button back to the "Edit Tags" button, indicating the flow of the process.

# Viewing Tags

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

#	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 <b>categoryId = STRATEGY</b> Teen host = www2 source = /opt/log/www2/access.log sourcetype = access_combined

cart.do?action=addtocart&itemId=EST-26&prodIP 1.1" 200 3466 "http://www.buttercupgames.com/la/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	SD5SL6FF2ADFF4955	▼
	action	addtocart	▼
	bytes	3466	▼

# Using Tags

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

New Search

Save As ▾ Close

tag=Teen

Last 24 hours ▾

418 events (11/25/14 10:00:00.000 AM to 11/26/14 10:01:40.000 AM)

Job ▾ II ■ ▶ ↓ Smart Mode ▾

Events (418) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection X Deselect 1 hour per column

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

< Hide Fields All Fields i Time Event

Selected Fields

a categoryId 1  
a host 4  
a source 4  
a sourcetype 2

> 11/26/14 9:55:22.000 AM 201.28.109.162 - [26/Nov/2014:17:55:22] "POST /category.screen?categoryId=STRATEGY&JSESSIONID=SD45L6FF10ADFF4956 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

The screenshot shows a Splunk search interface titled 'New Search'. The search bar contains 'tag=Teen'. The results summary indicates 418 events from November 25, 2014, to November 26, 2014. The main view features a 'Timeline' visualization with green bars representing event times. Below the timeline is a table with columns for Time and Event. One event row is expanded, showing details like the IP address (201.28.109.162), timestamp (11/26/14 9:55:22.000 AM), and the raw log entry. The expanded event also highlights specific fields: 'categoryId = STRATEGY Teen', 'host = www2', 'source = /opt/log/www2/access.log', and 'sourcetype = access\_combined'. On the left, a sidebar lists 'Selected Fields' including 'categoryId', 'host', 'source', and 'sourcetype'.

# Searching for Tags

To search for a tag associated with a value:

- tag=<tagname>



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

- tag::<field>=<tagname>



To search for a tag using a partial field value:

- use (\*) wildcard



# Managing Tags

## Settings > Tags

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

The screenshot shows a software interface with a navigation bar at the top. The 'Settings' dropdown is open, revealing several options: KNOWLEDGE (Searches, reports, and alerts; Data models; Event types), DATA (Report acceleration summaries), and Tags. The 'Tags' option is highlighted with a green box and has a green arrow pointing from it to the main content area. The main content area is titled 'Tags' and contains the following text: 'Manage tags on field values.' Below this, there is a table with three rows, each representing a way to list tags:

Tag links	Actions
<a href="#">List by field value pair</a>	<a href="#">Add new</a>
<a href="#">List by tag name</a>	<a href="#">Add new</a>
<a href="#">All unique tag objects</a>	<a href="#">Add new</a>

# 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			
<input type="checkbox"/> Show only objects created in this app context <a href="#">Learn more</a>				<input type="text"/>			
<a href="#">New</a>					Results per page <input type="button" value="25"/>		
Showing 1-3 of 3 items							
Field value pair	Tag name	App	Sharing	Status	Actions		
categoryId=SHOOTER	Mature	search	Private   <a href="#">Permissions</a>	Enabled   <a href="#">Disable all tags for pair</a>	<a href="#">Clone</a>   <a href="#">Move</a>   <a href="#">Delete</a>		
categoryId=SPORTS	General	search	Private   <a href="#">Permissions</a>	Enabled   <a href="#">Disable all tags for pair</a>	<a href="#">Clone</a>   <a href="#">Move</a>   <a href="#">Delete</a>		
categoryId=STRATEGY	Teen	search	Private   <a href="#">Permissions</a>	Enabled   <a href="#">Disable all tags for pair</a>	<a href="#">Clone</a>   <a href="#">Move</a>   <a href="#">Delete</a>		

# Managing Tags (cont.)

## Settings > Tags > List by tag name

- Enable/Disable
- Clone
- Delete

The screenshot shows a list of tags named General, Mature, and Teen. Each tag has a specific field value pair (categoryId=SPORTS, categoryId=SHOOTER, and categoryId=STRATEGY respectively), is owned by cfarrell, and is associated with the search app. The status for all tags is Enabled. The Actions column for each row contains links for Clone and Delete.

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

# 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)				
<input type="checkbox"/> Show only objects created in this app context		<a href="#">Learn more</a>				<input type="button" value=""/>				
New						Results per page				
Showing 1-3 of 3 items						25				
Tag name	Field value pair	Owner	App	Sharing	Status	Actions				
Mature	categoryId=SHOOTER	cfarrell	search	Private   <a href="#">Permissions</a>	Enabled   <a href="#">Disable</a>	<a href="#">Clone</a>   <a href="#">Move</a>   <a href="#">Delete</a>				
General	categoryId=SPORTS	cfarrell	search	Private   <a href="#">Permissions</a>	Enabled   <a href="#">Disable</a>	<a href="#">Clone</a>   <a href="#">Move</a>   <a href="#">Delete</a>				
Teen	categoryId=STRATEGY	cfarrell	search	Private   <a href="#">Permissions</a>	Enabled   <a href="#">Disable</a>	<a href="#">Clone</a>   <a href="#">Move</a>   <a href="#">Delete</a>				

# Adding/Changing the Tag Name

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

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

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

categoryId=SHOOTER

Tags » List by field value pair » categoryId=SHOOTER

Tag name  
Enter one tag per textfield

Mature

# Adding/Changing the Field Value Pair

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

The screenshot illustrates the process of managing field value pairs for a specific tag. On the left, the 'List by tag name' page shows three items: 'General' (categoryId=SPORTS), 'Mature' (categoryId=SHOOTER), and 'Teen' (categoryId=STRATEGY). The 'Teen' row is highlighted with a green border. An arrow points from the 'Teen' row to the right-hand modal window. The modal window is titled 'Teen' and displays the current field value pair: 'categoryId=STRATEGY'. It also includes a placeholder 'example: host=splunk.com', two 'Delete' buttons, an 'Add another field' link, a 'Cancel' button, and a prominent green 'Save' button.

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

## 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&
productIds=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   2 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
```

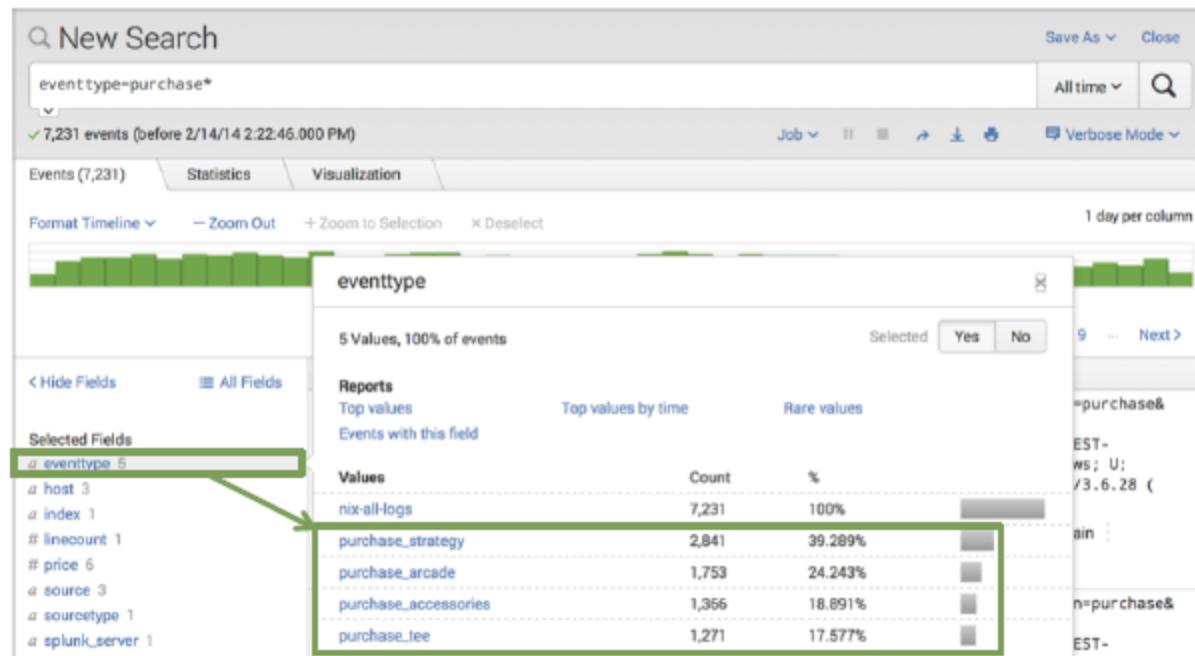
# Creating an Event Type

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 image shows two screenshots illustrating the process of creating an event type. On the left, a search results page displays a query: `sourcetype=access_combined action=purchase categoryId=tee`. The results show 3,672 events from October 2, 2014, to October 3, 2014. A context menu is open at the top right, with the "Event Type" option highlighted. On the right, a "Save As Event Type" dialog box is shown, prompting for a "Name" (set to "purchase\_tee"), "Tags" (set to "purchase, tee"), "Color" (set to "none"), and "Priority" (set to "5"). A note below the priority field states: "Determines which style wins, when an event has more than one event type." At the bottom of the dialog are "Cancel" and "Save" buttons.

# 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



# 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. Under the 'Type' column, 'Selected' is checked for 'eventtype'. The 'Value' column lists 'nix-all-logs' and 'purchase\_strategy'. Below these, under 'Selected', are 'host' and 'index', both checked. An 'Actions' dropdown menu is open, and the 'Edit Tags' option is highlighted with a green box and a downward arrow pointing to the 'Create Tags' modal.

Event Actions

Type	Field	Value	Actions
Selected	eventtype	nix-all-logs purchase_strategy	<input type="button" value="Edit Tags"/>
	host	www3	
	index	main	

Create Tags

Field Value: eventtype=purchase\_strategy

Tag(s): purchase, strategy

The screenshot shows the 'purchase\_strategy' tag creation dialog. It includes fields for 'Search string', 'Tag(s)', 'Priority', and a 'Save' button. The 'Search string' field contains 'sourcetype=access\_combined action=purchase categoryId=strategy'. The 'Tag(s)' field contains 'purchase, strategy'. The 'Priority' field is set to '5'. A note below says 'Highest priority shows up first in a result.'

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)

# Managing Event Types

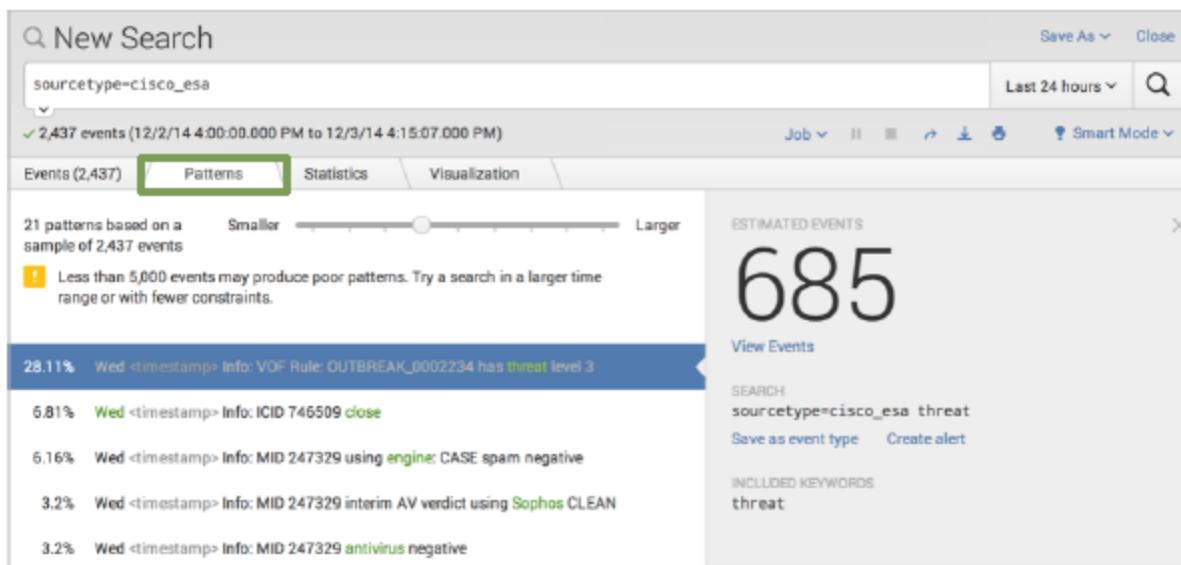
## Settings > Event Types

- 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 <a href="#">Learn more</a>									
New							Results per page		
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		

# Creating an Event Type via Patterns

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



# 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 Search, Name, Tags, Color, and Priority. The "Name" field is highlighted with a green border.

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

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

# 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

- 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

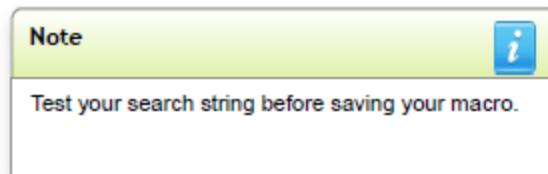
## Macros Overview

- 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

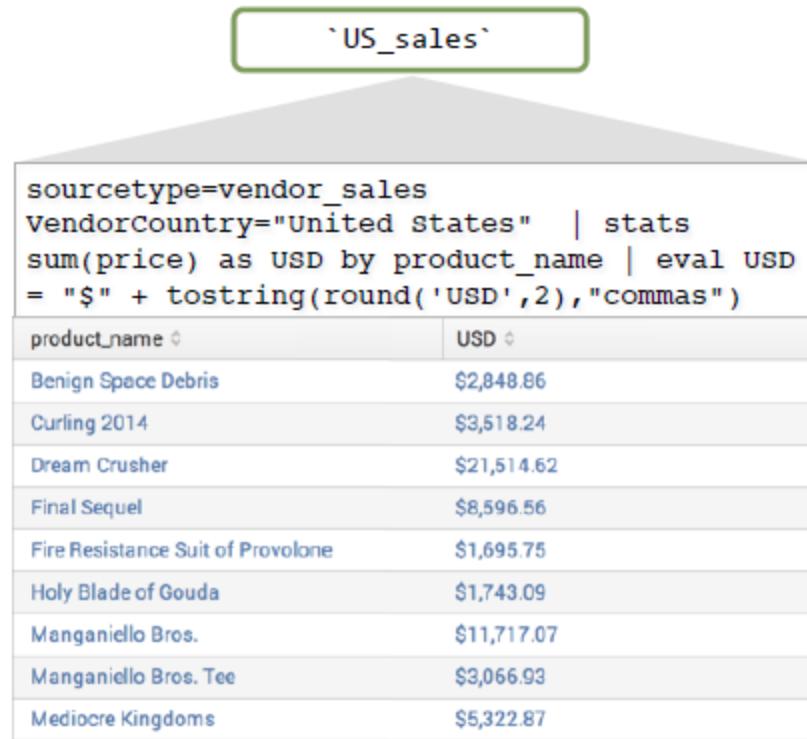
Definition \*

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")
```

# 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 screenshot shows a search interface with a search bar at the top containing the text ``US\_sales``. Below the search bar is a search results table. The table has two columns: `product\_name` and `USD`. The table displays ten rows of data, each consisting of a product name and its corresponding USD value.

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

# 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

# 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

# Validating Macros

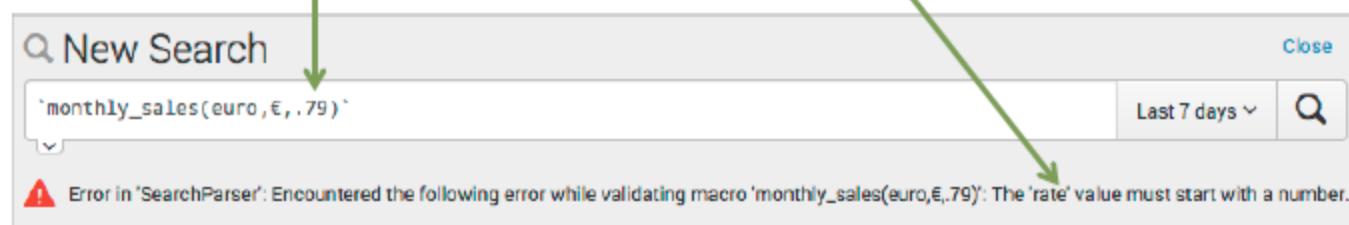
You can validate the argument values in your macro

- 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.



# 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

# 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 Data Model Editor interface. On the left, the 'Buttercup Games Site Activity' object is displayed, listing various event types under 'Web Requests'. A green arrow points from the 'Pivot' tab in the top navigation bar of the Data Model Editor to the 'New Pivot' interface on the right. The 'New Pivot' interface shows a search bar with '99,097 of 99,097 events matched', filters for 'All time', and a pivot table with columns for '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', 'Ovil the Wolverine', and 'Puppies vs. Zombies'. The table contains numerical values for each category.

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	Ovil the Wolverine	Puppies vs. Zombies	
addtocart	12	9	12	14	8	13	15	16	16	12	6	9
changequantity	1	2	0	5	2	2	4	1	4	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	

# 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 indicates the current view is 'Buttercup Games Site Activity' under 'Buttercup\_Games\_Site\_Activity'. The left sidebar lists objects categorized by type: EVENTS, SEARCHES, and TRANSACTIONS. The 'Web Requests' object is selected under EVENTS. The main content area on the right shows the details for the 'Web Requests' object, including its constraints, inherited fields, and extracted fields.

CONSTRAINTS		
sourceType=access_combined		
Constraint	Edit	

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

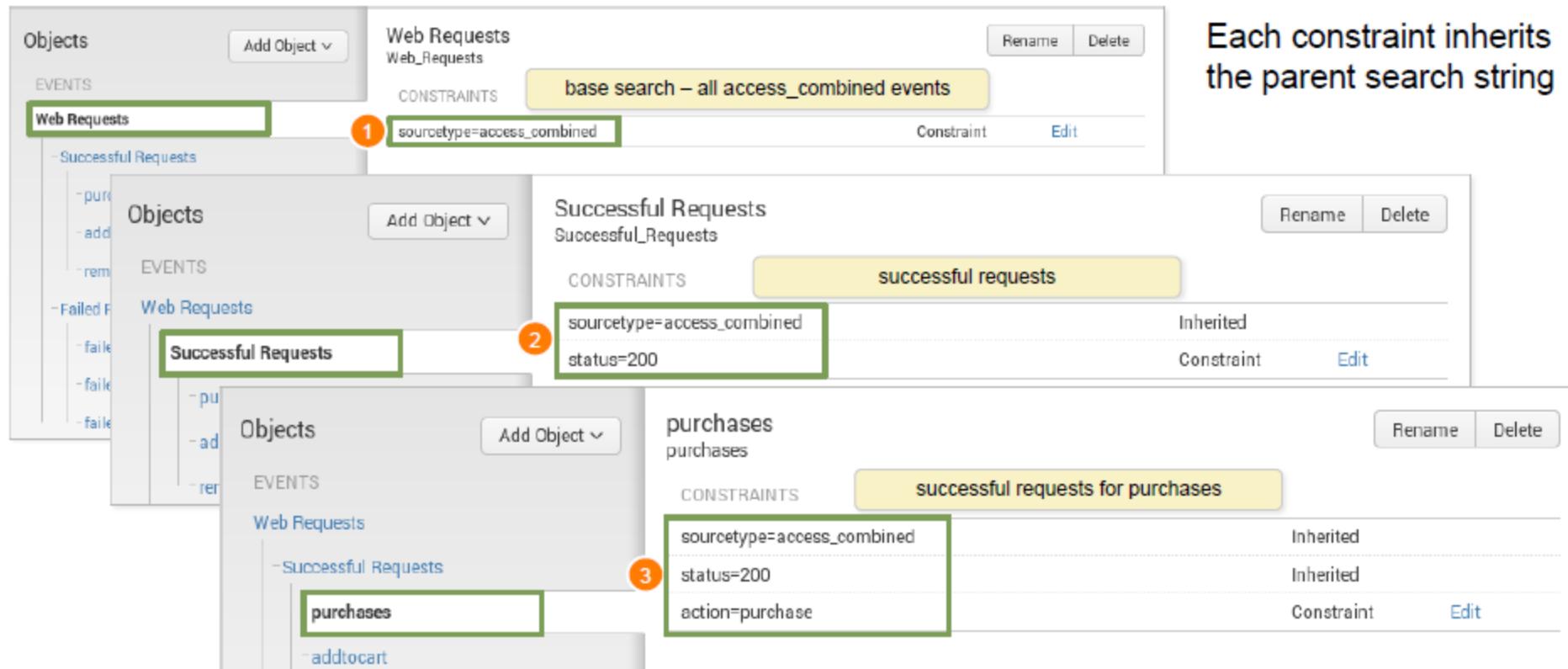
# Data Model Objects

- Data models consist of 3 types of objects
  1. Events
  2. Searches
  3. Transactions

The screenshot shows the Splunk Data Model Objects interface for the 'Buttercup\_Games\_Site\_Activity' data model. The left sidebar lists three categories: EVENTS, SEARCHES, and TRANSACTIONS. The EVENTS category is highlighted with a yellow box and labeled 'events'. The EVENTS section contains a list of actions: 'Successful Requests' (purchases, addtocart, remove) and 'Failed Requests' (failed\_remove, failed\_purchase, failed\_addtocart). The SEARCHES category contains a single entry: 'User'. The TRANSACTIONS category contains a single entry: 'FailedSessionTimes'. The right panel displays the 'Web Requests' object details. It includes a 'CONSTRAINTS' section with the constraint 'sourcetype=access\_combined', an 'INHERITED' section listing '\_time, host, source, and sourcetype with 'Override' status, and an 'EXTRACTED' section listing various attributes like action, bytes, categoryid, clientip, cookie, date\_hour, date\_mday, date\_minute, date\_month, date\_second, and date\_wday, each with an 'Edit' button.

Attribute	Type	Action
_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

# Event Object Hierarchy and Constraints



# Object Attributes

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

Web Requests		
Web_Requests		
CONSTRAINTS		
sourcetype=access_combined	Constraint	Edit
<a href="#">Bulk Edit</a> <a href="#">Add Attribute</a>		
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

## 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.

The screenshot shows the 'Object Attributes' interface for the 'Web Requests' object. At the top, there are 'Rename' and 'Delete' buttons. Below that is a 'CONSTRAINTS' section with the constraint 'sourcetype=access\_combined'. In the 'INHERITED' section, there are four fields: '\_time' (Time), 'host' (String), 'source' (String), and 'sourcetype' (String). In the 'EXTRACTED' section, there are ten fields: 'action' (String), 'bytes' (Number), 'categoryid' (String), 'clientip' (IPv4), 'cookie' (String), 'date\_hour' (Number), 'date\_mday' (Number), 'date\_minute' (Number), 'date\_month' (String), and 'date\_second' (Number). On the right side, there is a dropdown menu under 'Add Attribute' with options: Auto-Extracted (selected), Eval Expression, Lookup, Regular Expression, and Geo IP.

# 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 navigation bar with 'Download', 'Pivot', and 'Documentation' buttons, and a 'Rename' and 'Delete' button on the right. The main area has tabs for 'Objects', 'SEARCHES', and 'User'. Under 'Objects', there's a section for 'EVENTS' with 'Web Requests' expanded, showing sub-categories like 'Successful Requests' (with items: purchases, addtocart, remove) and 'Failed Requests' (with items: failed\_remove, failed\_purchase, failed\_addtocart). Under 'SEARCHES', there's a single entry: 'User'. On the right side, a large text box displays 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's a search bar with 'Search' and 'Edit' buttons, and a 'Bulk Edit' button. A 'Calculated attributes' section lists 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 page, 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.'

# 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

< Back to Data Models

Objects Add Object ▾

EVENTS

Web Requests

- Successful Requests
  - purchases
  - addtocart
  - remove
- Failed Requests
  - failed\_remove
  - failed\_purchase
  - failed\_addtocart

SEARCHES

User

TRANSACTIONS

FailedSessionTimes

FailedSessionTimes

CONSTRAINTS

Group Objects Failed\_Requests

Group By clientip

Max Pause

Max Span

Bulk Edit ▾

Add Attribute ▾

	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

# Creating a Data Model

## Settings > Data Models

The screenshot shows the Splunk web interface. At the top, there is a navigation bar with links for Apps, Messages, Settings, Activity, and Help. The main title is "Data Models". Below the title, a sub-header states: "Data models enable users to easily create reports in the Pivot tool. [Learn More](#)". There are three dropdown filters: "App: Search & Reporting (search)", "Created in the App", and "Owner: Any". A "filter" input field is also present. On the left, a table lists existing data models:

i	Title	Actions	App
>	Splunk's Internal Audit Logs - SAMPLE	Edit ▾ Pivot	search
>	Splunk's Internal Server Logs - SAMPLE	Edit ▾ Pivot	search

A green arrow points from the "New Data Model" button in the top right of the main area down to the "New Data Model" dialog box. The dialog box has the following fields:

- Title:** Buttercup Games Site Activity
- ID:** Buttercup\_Games\_Site\_Activity
- Can only contain letters, numbers and underscores.
- App:** Search & Reporting ▾
- Description:** Web server activity

At the bottom of the dialog box are "Cancel" and "Create" buttons. A yellow callout box points to the "choose app context" button, containing the text: "ID is automatically populated from Title, but can be overridden".

# Adding a Root Event

The screenshot illustrates the process of creating a new event type in the Splunk interface.

**Left Panel:** Shows the navigation menu with "Root Event" selected. A green arrow points from the "Add Object" button to the "Root Event" option in the dropdown.

**Right Panel:** The "Object Name" field contains "Web Request". The "Constraints" field contains "sourcetype=access\_combined". A yellow callout box states: "constraints are essentially search terms – add child events (discussed later in this section) to further "narrow" your search".

**Bottom Panel:** Shows the results of the search. The "Object ID" field shows "Web\_Request". The "Examples" section includes "uri=\"\*.php\*\" OR uri=\"\*.py\*\"", "NOT (referer=null OR referer=\"-\")", and "Examples: uri=\"\*.php\*\" OR uri=\"\*.py\*\" NOT (referer=null OR referer=\"-\")". A yellow callout box says: "click Preview to view the events that the constraint returns".

Event
12.130.60.5 - - [30/Sep/2014:18:19:03] "GET /oldlink?itemId=EST-17&JSESSIONID=SD105L4FF10ADFF4954 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=SD105L4FF10ADFF4954 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=SD105L4FF10ADFF4954 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-606&JSESSIONID=SD105L4FF10ADFF4954 HTTP/1.1" 200 7667 "http://www.buttercupgames.com/cart.do? 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)" 631

## 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

_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.

Auto-Extracted

- Eval Expression
- Lookup
- Regular Expression
- Geo IP

# 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](#)

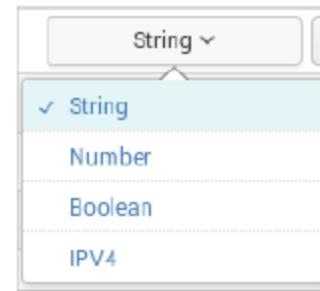
**view a field's example values**

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

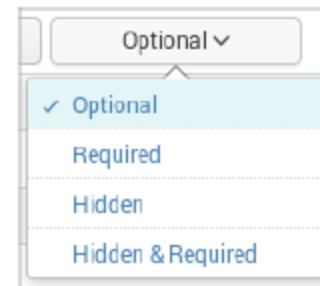
# Attribute Types

- **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 adding a new attribute. On the left, a sidebar lists "Add Attribute", "Auto-Extracted", "Eval Expression" (which is selected and highlighted in green), "Lookup", "Regular Expression", and "Geo IP". A green arrow points from the "Eval Expression" button to the main configuration window. The main window has two tabs: "Eval Expression" and "Attribute".

**Eval Expression Tab:**

- Code input field: `if(status>399, "Web error", "OK")`
- Examples section:
  - `case(error == 404, "Not found", error == 500, "Internal Server Error")`
  - `if(cidrmatch("192.0.0.0/16", clientip), "local", "other")`
- [Learn More](#)

**Attribute Tab:**

- Field Name: `errorReason`
- Display Name: `Error Reason`
- Type: `String`
- Flags: `Optional`

A yellow callout box with the text "click Preview to verify your eval expression returns events" points to the "Preview" button. The "Preview" button is highlighted in green. Below the preview area, there are tabs for "Events" and "Values", with "Events" selected. It shows 0 events (before 10/1/15 10:27:35.000 PM) and a sample of 1,000 events. A green arrow points down from the "Preview" button to the event table.

time	errorReason	host	source	sourcetype	action	category	price	product name	productID	status	Code	J
2015-10-01 22:24:58	OK	www3	/opt/log/www3/access.log	access_combined	view		24.99	FS-SG-G03	200	S		
2015-10-01	Web error	www3	/opt/log/www3/access.log	access_combined	addtocart			SF-BVS-01	406	S		

# 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

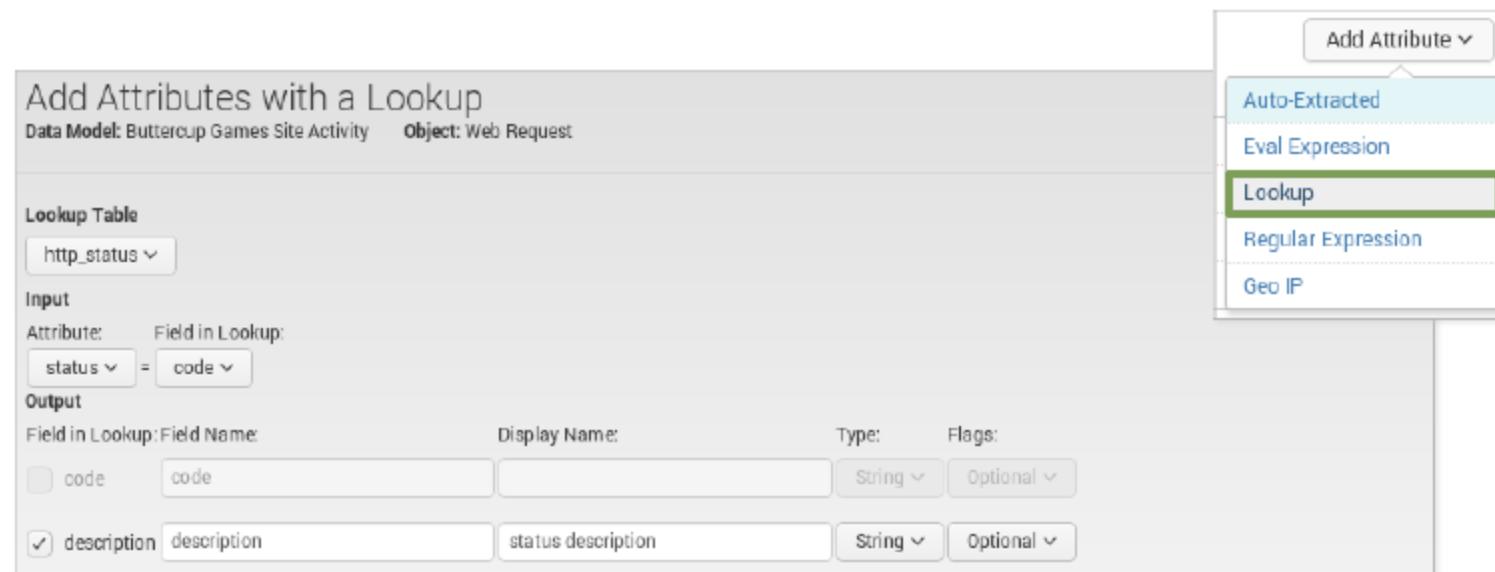
Add Attributes with a Lookup  
Data Model: Buttercup Games Site Activity Object: Web Request

Lookup Table: http\_status

Input:  
Attribute: status = Field in Lookup: code

Output:  
Field in Lookup: Field Name: code Display Name: code Type: String Flags: Optional  
Field in Lookup: Field Name: description Display Name: status description Type: String Flags: Optional

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



# Adding Attributes – Lookups (cont.)

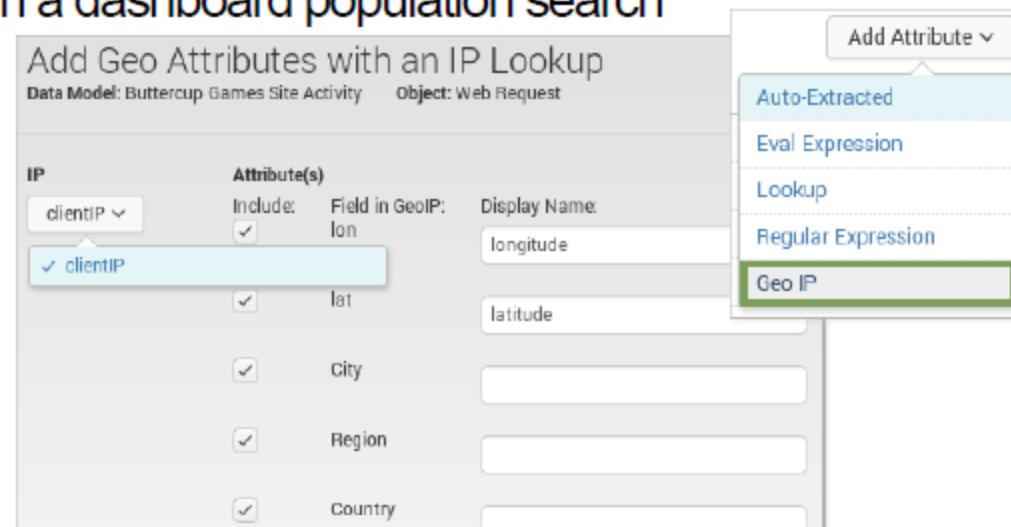
- Use Preview to test your lookup settings
- Use the Events and Values tab to verify your results

Screenshot of the "Edit Attributes with a Lookup" interface in a Data Model. The interface shows a "Lookup Table" set to "Http.status.Lookup". The "Input" section shows "Attribute: Field in Lookup: status" and "Output: Field in Lookup: Field Name: code". The "Events" tab shows "1,000 events (before 3/4/14 2:46:03.000 PM)". The "Values" tab shows a table of HTTP status codes and their counts:

Value	Count	%
OK.	884	88.400
Service Unavailable.	31	3.100
Not Acceptable.	18	1.800
Internal Server Error.	17	1.700
Request Timeout.	13	1.300
Not Found.	11	1.100
Bad Request.	9	0.900
HTTP Version Not Supported.	9	0.900
Forbidden.	8	0.800

# Adding Attributes - GeoIP

- 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



# 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)

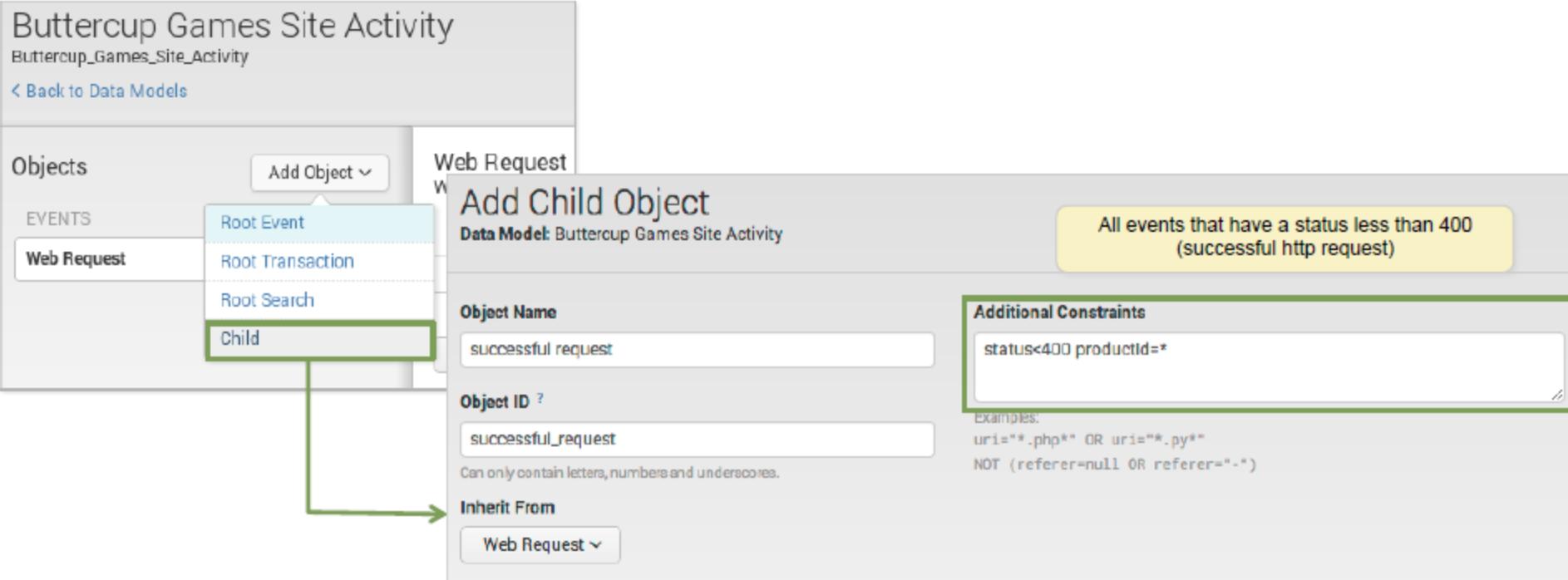
Object Name: successful request

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=".")



The screenshot shows the 'Buttercup Games Site Activity' data model interface. On the left, there's a tree view under 'EVENTS' with 'Web Request' selected. A green box highlights the 'Child' node under 'Web Request'. A green arrow points from this node to the 'Add Child Object' dialog box on the right. The dialog box has 'Data Model: Buttercup Games Site Activity' and 'Object Name: successful request'. It also contains an 'Additional Constraints' section with the query 'status<400 productId=\*'. Below this, examples like 'uri="\*.php\*" OR uri="\*.py\*" NOT (referer=null OR referer=".")' are shown. The 'Inherit From' dropdown is set to 'Web Request'.

## Adding Child Events (cont.)

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

The screenshot shows a software interface for managing event configurations. At the top, it displays the event name "successful request" and two buttons: "Rename" and "Delete". Below the name, there is a section titled "CONSTRAINTS" containing a single constraint: "sourcetype=access\_combined" with the status "Inherited". To the right of this constraint are "Constraint" and "Edit" buttons.

Below the constraints, there is a "Bulk Edit" dropdown and an "Add Attribute" dropdown. The "Add Attribute" dropdown is open, showing a list of options: "Auto-Extracted", "Eval Expression" (which is highlighted in blue), "Lookup", "Regular Expression", and "Geo IP".

The main configuration area is titled "INHERITED" and lists several attributes:

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

## Using the Data Model in Pivot (cont.)

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

The screenshot shows the 'New Pivot' window with the following details:

- Title Bar:** 'New Pivot' with a 'Save As...' dropdown.
- Event Count:** '1,226 events (9/25/15 4:00:00.000 PM to 10/2/15 4:48:09.000 PM)'.
- Filters:** 'Last 7 days' with edit (+) and add (+) buttons.
- Split Rows:** '+'
- Column Values:** 'Count of Failed R...' with edit (+) button.
- Right Panel:** 'Select a Data Object' tree view:
  - < Back
  - i 10 Objects in Buttercup Games Site Activity
  - > Web Requests
    - > Successful Requests
      - > purchase
      - > add
      - > remove
    - > Failed Requests
      - > purchase
      - > add
      - > remove
    - > visit duration

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

# 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

< Back to Data Models

Edit ▾ Download Pivot Documentation ▾

Objects Add Object ▾

EVENTS

Web Requests Web\_Requests

CONSTRAINTS

sourcetype=access\_combined Constraint

Successful Requests

- purchase
- add
- remove

Bulk Edit ▾

INHERITED

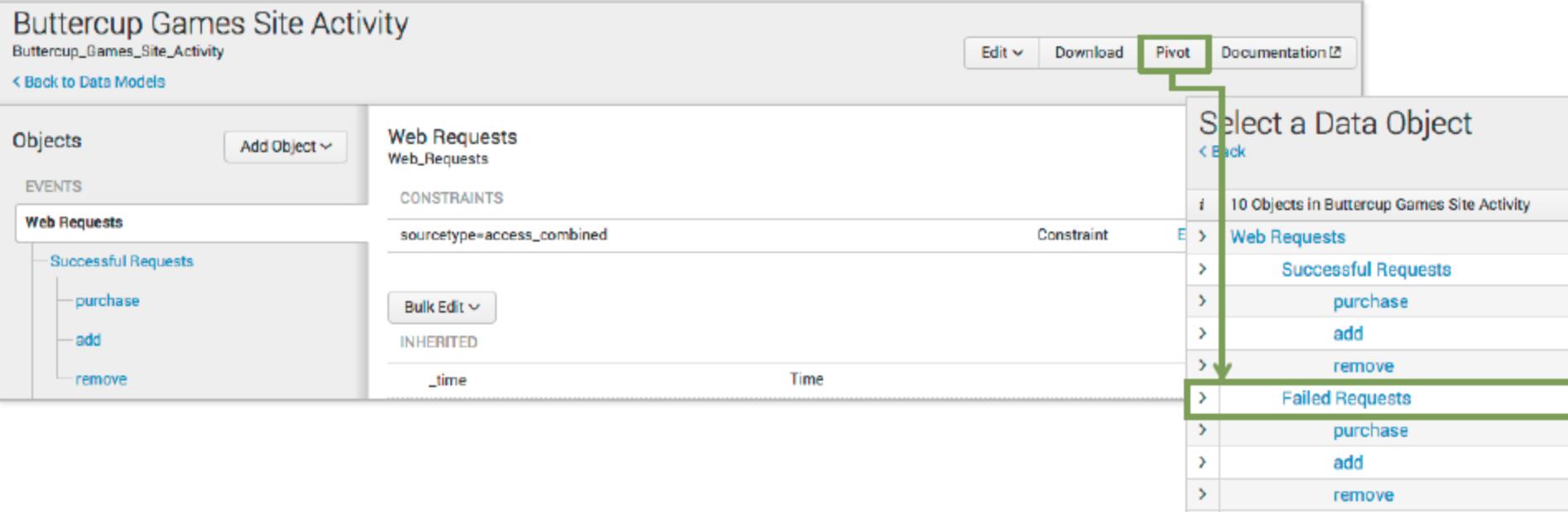
\_time Time

Select a Data Object

< Back

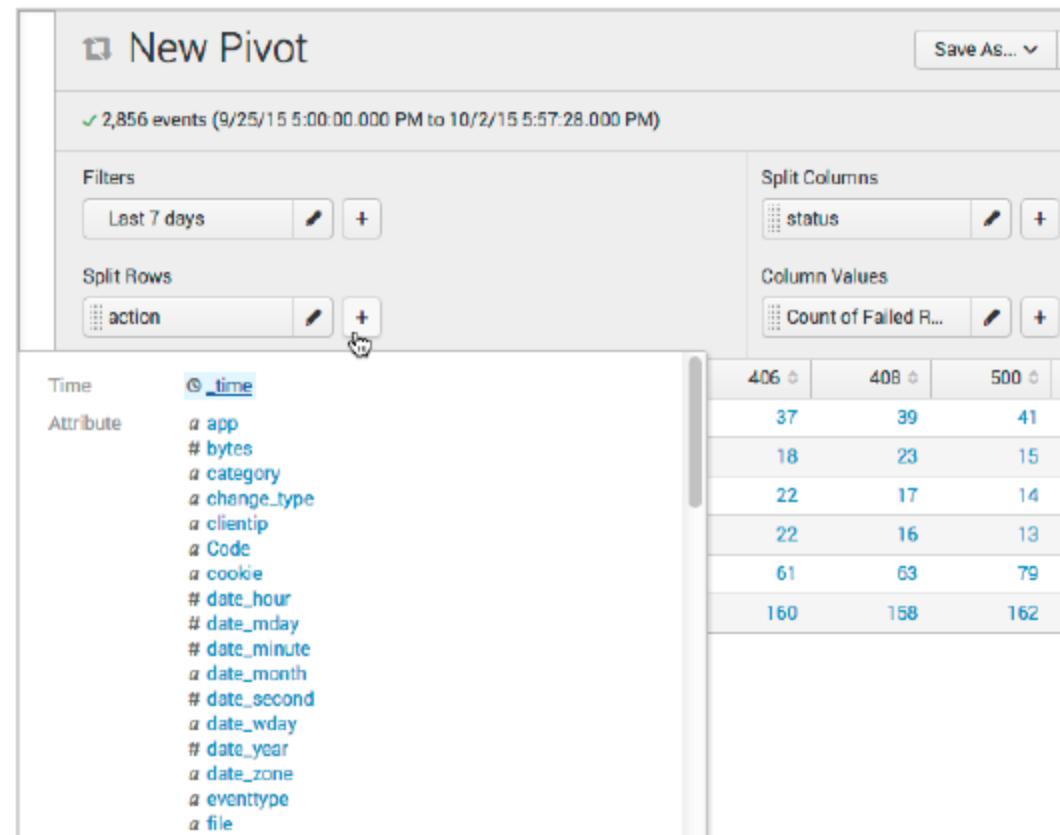
i 10 Objects in Buttercup Games Site Activity

- Web Requests
- Successful Requests
  - purchase
  - add
  - remove
- Failed Requests
  - purchase
  - add
  - remove



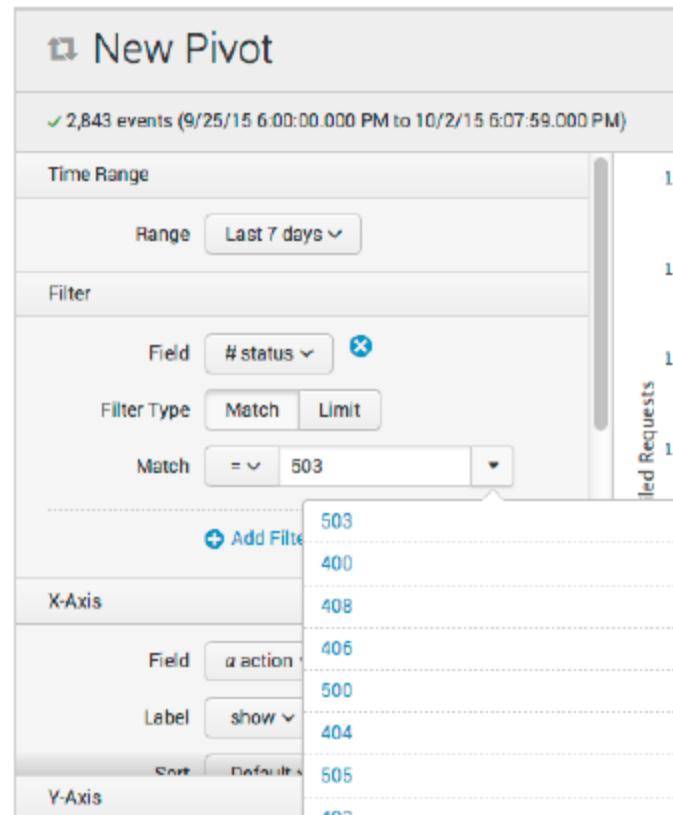
# Pivot – Using Attributes

- 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

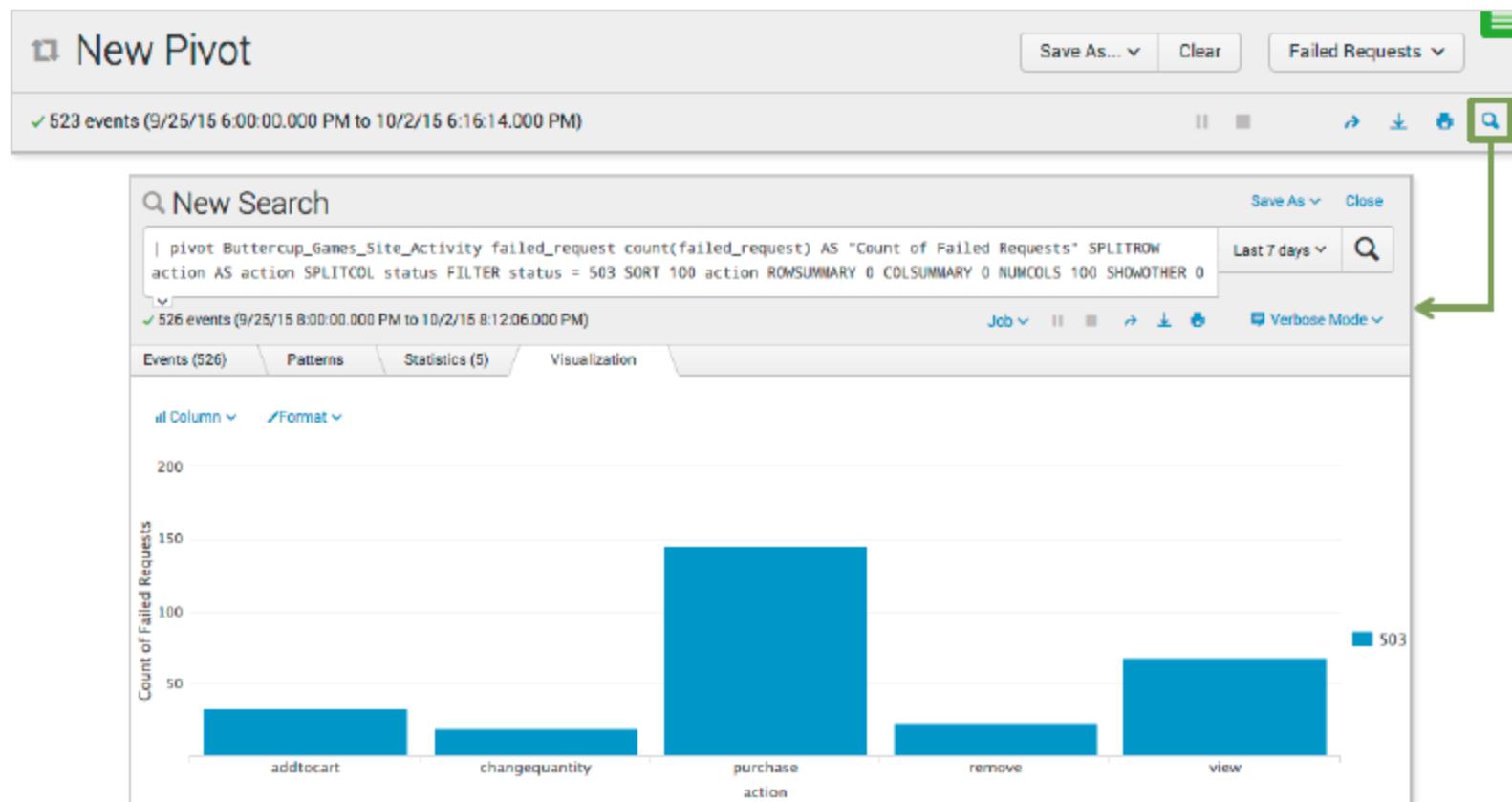


## Pivot – Using Attributes (cont.)

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



# Underlying Search



# 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 X

Data Model: Buttercup Games Site Activity

Owner: cfarrell

App: search

Display For: Owner App All Apps

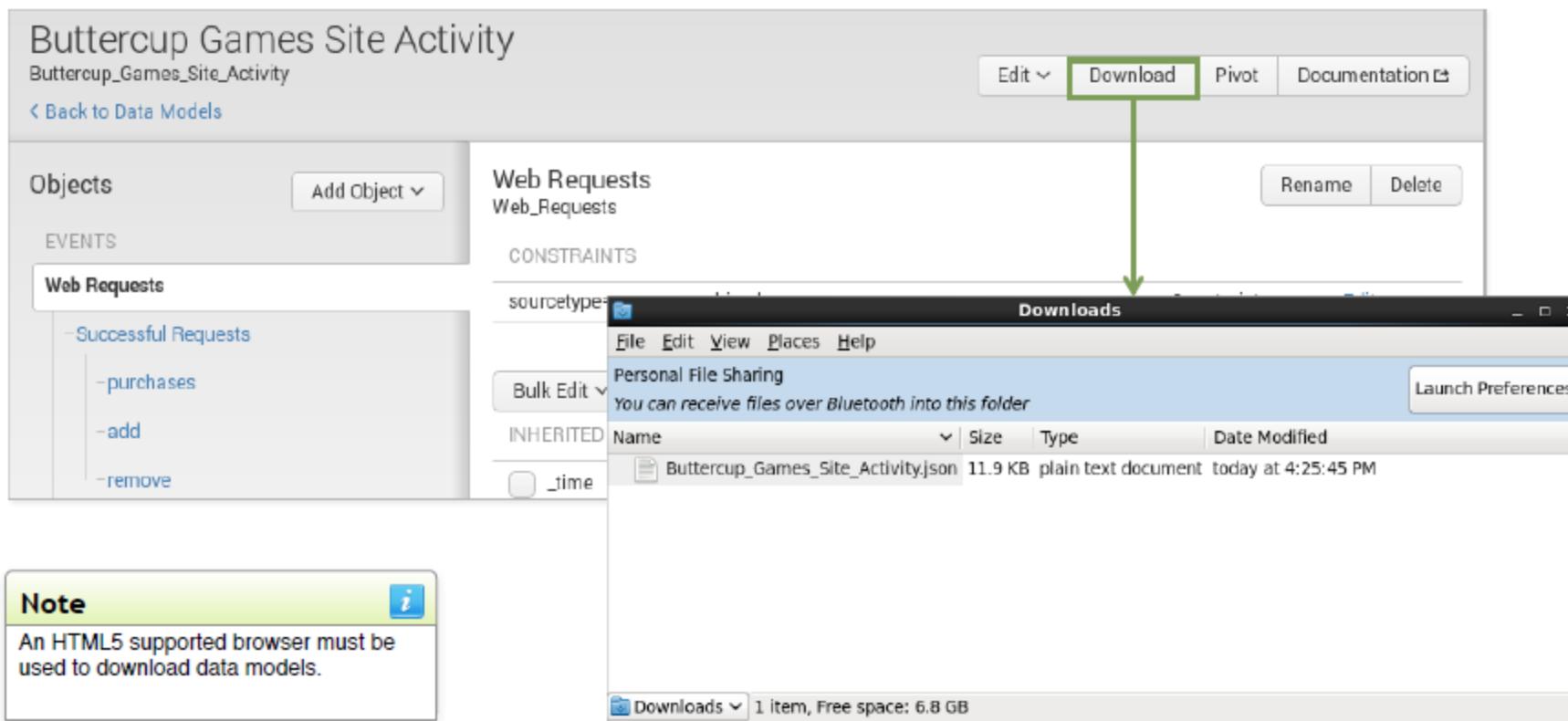
	Read	Write
Everyone	<input checked="" type="checkbox"/>	<input type="checkbox"/>
power	<input checked="" type="checkbox"/>	<input type="checkbox"/>
user	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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



# Uploading a Data Model

The screenshot illustrates the process of uploading a new data model in Splunk. It shows two windows: the main 'Data Models' list and a detailed view of a specific data model.

**Main Window (Data Models List):**

- Header: splunk > Apps >
- User: Lien Teng
- Toolbar: Messages, Settings, Activity, Help
- Section: Data Models
- Description: Data models enable users to easily create reports in the Pivot tool. [Learn More](#)
- Filter: App: Search & Reporting (search), Created in the App, Owner: Any
- Table:

#	Title ^	Actions	App	Owner	Shared
>	Splunks Internal Audit Logs - SAMPLE	Edit ▾ Pivot	search	nobody	Ap
>	Splunks Internal Server Logs - SAMPLE	Edit ▾ Pivot	search	nobody	Ap

**Modal Window (Upload New Data Model):**

- Header: Upload New Data Model
- File: Buttercup\_Games\_Site\_...
- File..
- ID: data\_model\_from\_Cerys (Can only contain letters, numbers and underscores.)
- App: Search & Reporting
- Dashboard Permissions: Private, Shared in App
- Buttons: Save (highlighted with a green arrow), Cancel

**Detail View (Buttercup Games Site Activity):**

- Header: splunk > App: Search & Reporting > Buttercup Games Site Activity
- User: Lien Teng
- Section: data\_model\_from\_Cerys
- Buttons: Back to Data Models, Rename, Delete
- Objects: Add Object ▾
- Events: Web Requests
- Web Requests: sourcetype=access\_combined
- Constraints: Constraint ▾ Edit
- Buttons: Bulk Edit ▾, Add Attribute ▾

# 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.

