



# Splunk 6.6 Fundamentals Part 2

# Course Prerequisites

- To be successful in this course, you should have completed:
  - Splunk Fundamentals Part 1

Note



In order to receive credit for this course, you must complete all lab exercises.

# Course Guidelines

---

- Hands-on lab exercises reinforce information presented in the lecture modules
- The lab exercises must be completed sequentially
  - Later lab exercises often depend on steps completed in previous lab exercises

# Course Goals

---

- Use transforming commands and visualizations
- Filter and format the results of a search
- Correlate events into transactions
- Create and manage Knowledge Objects
- Create & manage extracted fields, field aliases, calculated fields
- Create tags and event types
- Create and use macros and workflow objects
- Create and manage data models
- Use the Splunk Common Information Model (CIM)

Generated for Subbaiah Kandula ([s.venkata.kandula@accenture.com](mailto:s.venkata.kandula@accenture.com)) (C) Splunk Inc, not for distribution

# Course Outline

---

Module 2: Beyond Search Fundamentals

Module 3: Using Transforming Commands for Visualization

Module 4: Using Mapping and Single Value Commands

Module 5: Filtering and Formatting Results

Module 6: Correlating Events

Module 7: Introduction to Knowledge Objects

Module 8: Creating and Managing Fields

Module 9: Creating Field Aliases and Calculated Fields

Module 10: Creating Tags and Event Types

Module 11: Creating and Using Macros

Module 12: Creating and Using Workflow Actions

Module 13: Creating Data Models

Module 14: Using the Common Information Model (CIM) Add-On

Generated for Subbaiah Kandula ([s.venkata.kandula@accenture.com](mailto:s.venkata.kandula@accenture.com)) (C) Splunk Inc, not for distribution

# Callouts

- Scenarios

- Many of the examples in this course relate to a specific scenario
- For each example, a question is posed from a colleague or manager at Buttercup Games

- Notes & Tips

References for more information on a topic and tips for best practices

Scenario 

The online sales manager wants to see the action, productId, and status of customer interactions in the online store.

Note 

Lookups are discussed in the *Splunk Fundamentals Part 1* course.

# Course Scenario

---

- Use cases in this course are based on Buttercup Games, a gaming company
- Searches and reports are based on:
  - Business analytics from the web access logs and lookups
  - Internal operations information from mail and internal network data
  - Security operations information from internal network and badge reader data

# Buttercup Games, Inc.

---

Buttercup Games, Inc.

- Multinational company with 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



# Your Role at Buttercup Games

---

- You are a Splunk power user with a great understanding of all your company's data
- Your responsibilities are to provide information to users throughout the company and to create and manage Splunk knowledge objects for your stakeholders
- You implement best practices for naming conventions of all knowledge objects
- You gather data and statistics, and report on Security, IT Operations, Operational Intelligence, etc.

# Buttercup Games Network

Index	Description	Sourcetype	Host			
web	Online transactions	access_combined	www1			
			www2			
			www3			
security	Badge reader data	history_access	badgesv1			
	AD/DNS data	winauthentication_security	adldapsv1			
	Web login data	linux_secure	www1			
			www2			
			www3			
sales	Windows log data	win_audit	adldapsv1			
	Retail sales data	vendor_sales	vendorUS1			
	BI data	sales_entries	ecommsv1			
	Firewall data	cisco_firewall	cisco_router1			
network						
Email data	cisco_esa					
games	Web appliance data	cisco_wsa_squid	sim_cube_server			
	Game logs	simCubeBeta				

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Module 2: Beyond Search Fundamentals

Generated for Subbaiah Kandula ([s.venkata.kandula@accenture.com](mailto:s.venkata.kandula@accenture.com)) (C) Splunk Inc, not for distribution

# Module Objectives

---

- Review basic search commands
- Use case correctly in searches
- Describe Splunk's search process

# Basic Search Review

---

- **Keywords**

search for error, password

- **Booleans**

NOT, OR, AND; AND is implied; MUST be uppercase; can use ( )'s to force precedence

sourcetype=vendor\_sales OR (sourcetype=access\_combined action=purchase)

- **Phrases**

"web error" (different than web AND error)

- **Field searches**

status=404, user=admin

- **Wildcard (\*)**

- status=40\* matches 40, 40a, 404, etc.

- Starting keywords with a wildcard is very inefficient, e.g. \*dmin

- **Comparisons**

=, !=, <, <=, >=, > status>399, user!=admin

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Basic Search Review (cont.)

---

- **table**: returns table containing only specified fields in result set
- **rename**: renames a field in results
- **fields**: includes or excludes specified fields
- **dedup**: removes duplicates from results
- **sort**: sorts results by specified field
- **lookup**: adds field values from external source (e.g., csv files)

# Case Sensitivity – Sensitive

Case sensitive	Examples
Boolean operators (uppercase)	AND, OR, NOT (Boolean operators) and, or, not (literal keywords)
Field names	productId vs. productid eval cs_username = "Total Access"
Field values from lookup (default, but configurable)	product_name="Tulip Bouquet" vs. product_name="tulip bouquet"
Regular expressions	\d\d\d vs. \D\D\D
replace command	error vs. ERROR
eval and where commands	eval action;if(action=="view",...) where action="Purchase" stats count(eval(action="view")) as...
CASE() directive	CASE(Purchase)
Tags	tag=DMZ vs. tag=dmz

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Case Sensitivity – Insensitive

Case insensitive	Examples
Command names	STATS, stats, sTaTs
Command clauses and functions	AS used by stats, rename, . . . ; BY used by stats, chart, top, . . . ; WITH used by replace
Search terms	failed, FAILED, Failed
Statistical functions	avg, AVG, Avg used by stats, chart, ...
Field values	host=www1, host=WwW1 (unless coming from a lookup)

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# How Splunk Searches – Buckets

- As events come in, Splunk places them into an index's hot bucket (only writable bucket)
- As buckets age, they roll from the hot to warm to cold
- Each bucket has own index, earliest and latest time, and raw data
- Metadata files track source, sourcetype, and host
- Admins can add more



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# How Splunk Searches – Searching

- When you search, Splunk uses the time range to choose which buckets to search and then uses the bucket indexes to find qualifying events
- When you search for `index=web password fail*` during the last 24 hours:
  - Splunk identifies the buckets for the last 24 hours
  - And searches the indexes of those buckets for the search terms

Hot: Now to -3h	index	raw events
Hot: -3 to -6h	index	raw events
Hot: -5 to -8h	index	raw events
Warm: -9 to -12h	index	raw events
Warm: -12 to -15h	index	raw events
Warm: -14 to -17h	index	raw events
.....	index	raw events
Warm: -42 to -45h	index	raw events
Warm: -45 to -48h	index	raw events
Cold: -48 to -51h	index	raw events
Cold: -51 to -54h	index	raw events
Cold: -54 to -57h...	index	raw events

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# General Search Practices

---

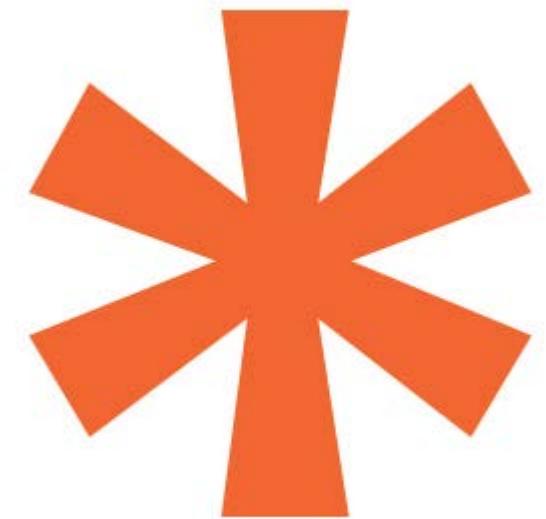
- As events are stored by time, time is the most efficient filter
- After time, most powerful keywords are host, source, sourcetype
- To make searches more efficient, include as many terms as possible
  - e.g., searching for sourcetype=x failure is better than failure
- Use the fields command to extract (discover) only fields you need
- Example: Search last 365 days, scans 566,720 events (in secs):

index=web sourcetype=access_combined	15.16
index=web sourcetype=access_combined   fields clientip bytes referrer	4.49

# General Search Practices – Wildcards

---

- Splunk only searches for whole words, but wildcards allowed
- Only *trailing* wildcards make efficient use of index
  - Wildcards at *beginning* of string scan all events within time frame
  - Wildcards in *middle* of string may return inconsistent results
  - So use fail\* (not \*fail or \*fail\* or f\*il)
- Wildcards tested after all other terms



# General Search Practices

---

- Inclusion is generally better than exclusion
  - Searching for "access denied" is faster than NOT "access granted"
- Filter as early in your search as possible
  - Removing duplicates then sorting is faster than sorting then removing duplicates
- Use the appropriate search mode
  - Fast - performance over completeness
  - Smart [default]
  - Verbose - completeness over performance

# Transforming Search Commands

---

- A transforming command:
  - Massages raw data into a data table
  - 'Transforms' specified cell values for each event into numerical values that you can use for statistical purposes
  - Is required to 'transform' search results into visualizations
- Transforming commands include:
  - top
  - rare
  - chart
  - timechart
  - stats
  - geostats

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Reviewing Search Mode – Fast Mode

- Emphasizes performance, returning only essential and required data
- For non-transforming searches:
  - ✓ Events – fields sidebar displays only those fields required for the search
  - ✓ Patterns
  - ✗ Statistics or visualizations
- For transforming searches:
  - ✗ Events
  - ✗ Patterns
  - ✓ Statistics or visualizations

index=web sourcetype=access\_combined

i	Time	Event
>	10/4/16 6:10:11.000 PM	108.65.113 SL6FF5ADFI tocart&ite (KHTML, 1: host = www1

index=web sourcetype=access\_combined  
| stats count by action

action	count
addtocart	25
changequantity	3
purchase	25

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Reviewing Search Mode – Smart Mode (Default)

- Designed to give you the best results for your search
- Combination of Fast and Verbose modes
- For non-transforming searches [Verbose]:
  - ✓ Events – fields sidebar displays all fields
  - ✓ Patterns
  - ✗ Statistics or visualizations
- For transforming searches:
  - ✗ Events
  - ✗ Patterns
  - ✓ Statistics or visualizations



The screenshot shows a Splunk search interface with the 'Statistics' tab selected. The results table has two columns: 'action' and 'count'. The data is as follows:

action	count
addtocart	20
changequantity	8
purchase	16
remove	3
view	20

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Reviewing Search Mode – Verbose Mode

- Emphasizes completeness by returning all possible field and event data
- For non-transforming searches:
  - ✓ Events – fields sidebar displays all fields
  - ✓ Patterns
  - ✗ Statistics or visualizations
- For transforming searches:
  - ✓ Events
  - ✓ Patterns
  - ✓ Statistics or visualizations

Events (147)		Patterns	Statistics (5)	Visual
Format Timeline ▾		List ▾	Format ▾	
< Hide Fields		All Fields	i Time	
Selected Fields				
a host	3			
# price	7			
# sale_price	6			
a source	3			
a sourcetype	1			
a user	1			
Interesting Fields				
a action	5			
# bytes	100+			
a categoryid	8			
a clientip	20			
# date_hour	2			
# date_mday	1			
# date_minute	42			
a date_month	1			
# date_second	51			
a date_wday	1			
# date_year	1			
a date_zone	1			
a eventtype	2			
a file	7			
a ident	1			
a index	1			
a itemid	14			
a JSESSIONID	23			
# linecount	1			
a method	2			
# other	100+			
a product_name	14			
a productid	15			
a punct	36			
a referer	72			
a referer_domain	4			
a req_time	100+			
a splunk_server	1			
a splunk_server_group	3			
# status	8			
# timeendpos	6			
# timestamppos	6			
a uri	100+			
a uri_path	7			
a uri_query	100+			
a useragent	16			
# version	1			
5 more fields				
+ Extract New Fields				

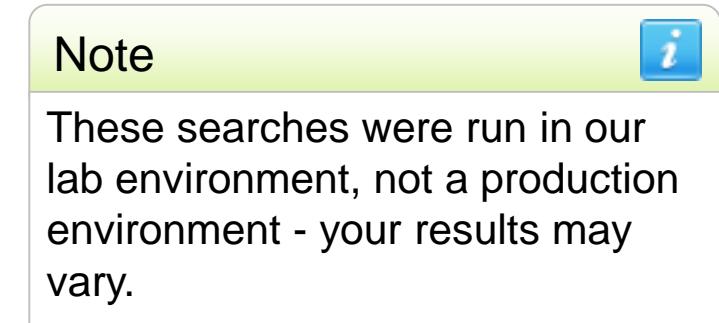
Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Search Performance – Modes

- Use the most appropriate search mode:

```
index=web sourcetype=access_combined  
| chart count by product_name
```

- Time range: last 365 days



<u>Mode</u>	<u>Returned Results</u>	<u>Events Scanned</u>	<u>Time</u>
Fast	14	566,731	1.82
Smart	14	566,731	1.91
Verbose	14	566,731	15.21

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Search Performance – Types of Searches

Search	Description	Indexer throughput
Dense	A large percentage of the data matches the search	Up to 50K matching EPS (Events per second) <i>CPU bound</i>
	Use Cases: computing stats, reporting	
	<code>index=web sourcetype=access_combined   timechart count</code>	
Sparse	A small percentage of data matches the search	Up to 5K matching EPS <i>CPU bound</i>
	Use Cases: troubleshooting, error analysis	
	<code>index=web sourcetype=access_combined status=404   timechart count</code>	
Super Sparse	Returns a small number of results from each index bucket matching the search	Up to 2 seconds per index bucket <i>I/O bound</i>
	I/O intensive as the indexer looks through all of an index's buckets	
	With a lot of data, with a lot of buckets, it can take a long time to finish	
Rare	The indexer checks all buckets to find results, but bloom filters eliminate those buckets that don't include search results	Up to 10-50 index buckets/second <i>I/O bound</i>
	Use Cases: user behavior tracking	
	<code>index=web sourcetype=access_combined sessionId=1234</code>	

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Search Job Inspector

- Tool allows you to examine:
  - Overall stats of search (e.g., records processed and returned, processing time)
  - How search was processed
  - Where Splunk spent its time
- Use to troubleshoot search's performance and understand impact of knowledge objects on processing (e.g., event types, tags, lookups)
- Any existing (i.e., not expired) search job can be inspected

Note

For more information, see:  
[docs.splunk.com/Documentation/Splunk/latest/Search/ViewsearchjobpropertieswiththeJobInspector](https://docs.splunk.com/Documentation/Splunk/latest/Search/ViewsearchjobpropertieswiththeJobInspector)

# Search Job Inspector – 3 Components

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

- Search bar: index=web sourcetype=access\_combined | stats count by action
- Job status: ✓ 650 events (10/4/16 2:29:00.000 PM to 10/4/16 6:29:41.000 PM) No Event Sampling
- Job dropdown menu:
  - Edit Job Settings...
  - Send Job to Background
  - Inspect Job** (highlighted with a green box)
  - Delete Job
- Navigation tabs: Events (650), Patterns, Statistics (5), Visualization
- Format Timeline dropdown
- List Format dropdown
- Results table:

i	Time	Event
<	10/4/16	27.96.128.0 - - [04/OCT/2016:10:20:19 +0000] GET /product

The screenshot shows the "Search job inspector" window with the following details:

- Header: Search job inspector
- Text: This search has completed and has returned 5 results by scanning 3,384 events in 0.515 seconds  
(SID: 1491239008.6) [search.log](#)
- Links:
  - > Execution costs
  - > Search job properties
- Text: Server info: Splunk 6.6.0, 34.223.247.197, Mon Apr 03 10:44:31 2017 User: student1

- Header
- Execution costs
- Search job properties

Generated for Subbaiah Kandula ([s.venkata.kandula@accenture.com](mailto:s.venkata.kandula@accenture.com)) (C) Splunk Inc, not for distribution

# Search Job Inspector – Header

## Search job inspector

This search has completed and has returned **5** results by scanning **650** events in **2.271** seconds

(SID: 1475605781.80) [search.log](#)

Top of Search job inspector provides basic information, including time to run and # of events scanned

# Search Job Inspector – Execution Costs

- Provides details on cost to retrieve results, such as:
  - command.search.index**  
Time to search the index for the location to read in rawdata files
  - command.search.filter**  
Time to filter out events that do not match
  - command.search.rawdata**  
Time to read events from the rawdata files

Duration (seconds)	Component	Invocations	Input count	Output count
0.01	command.addinfo	12	650	650
0.01	command.fields	12	650	650
0.01	command.prestats	12	650	39
0.02	command.remotetl	12	650	650
■ 0.17	command.search	12	-	650
0.02	command.search.expand_search	1	-	-
0.01	command.search.index	12	-	-
0.01	command.search.fieldalias	8	650	650
0.01	command.search.filter	8	-	-
0.00	command.search.calcfields	8	650	650
0.00	command.search.index.usec_1_8	282	-	-
■ 0.13	command.search.rawdata	8	-	-
0.02	command.search.typer	8	650	650
0.02	command.search.kv	8	-	-
0.01	command.search.lookups	8	650	650
0.01	command.search.tags	8	650	650
0.00	command.search.summary	12	-	-
0.01	command.stats	14	39	-
0.01	command.stats.execute_input	13	39	-
0.00	command.stats.execute_output	1	-	-

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Search Job Inspector – Search Job Properties

Example:



- Produces scanCount of **127,201** events
- Returns resultCount of **2,144** in 3.01 seconds
- To calculate performance:
  - Do **not** use resultCount/time  $2,144 / 3.01 = 712$  EPS\*
  - Rather, calculate scanCount/time  $127,201 / 3.01 = 40,892$  EPS
- Good performance: ~10K – 20K EPS

\* EPS= events per second

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Module 3: Using Transforming Commands for Visualizations

Generated for Subbaiah Kandula ([s.venkata.kandula@accenture.com](mailto:s.venkata.kandula@accenture.com)) (C) Splunk Inc, not for distribution

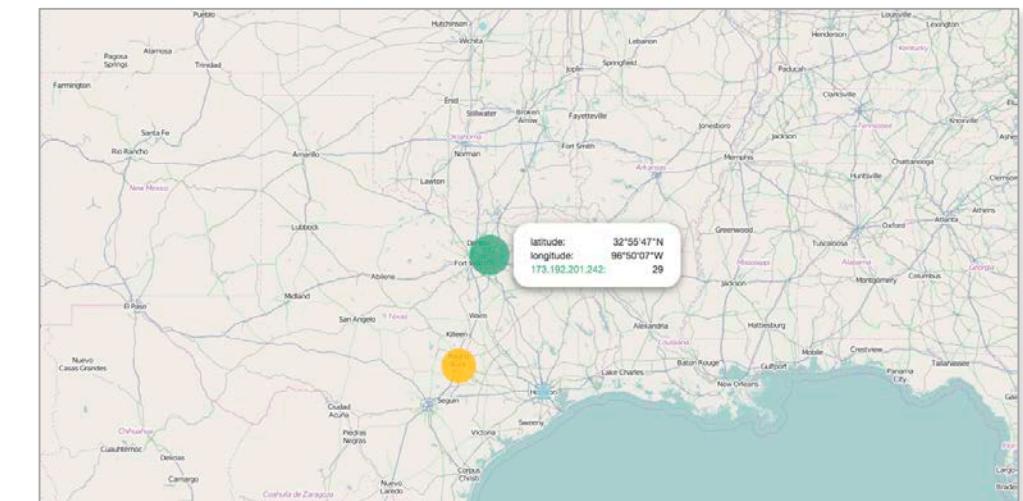
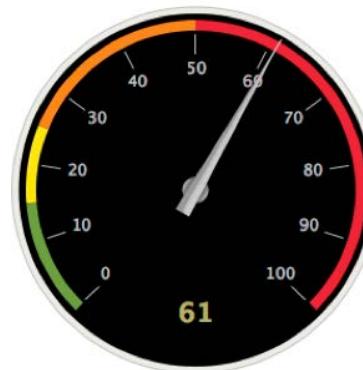
# Module Objectives

---

- Explore data structure requirements
- Explore visualization types
- Create and format charts
- Create and format timecharts
- Explain when to use each type of reporting command

# Visualization Types

- When a search returns statistical values, results can be viewed with a wide variety of visualization types
  - Statistics table
  - Charts: Line, column, pie, etc
  - Single value, Gauges
  - Maps
  - Many more



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc. not for distribution

# Viewing Results as a Visualization

- Not all searches can be visually represented
- A data series is a sequence of related data points that are plotted in a visualization
- Data series can generate any statistical or visualization results

New Search

index=web sourcetype=access\_combined ((404 OR 500 OR 503) OR (error OR fail\*))

Last 60 minutes

Events (13) Patterns Statistics Visualization

Your search isn't generating any statistic or visualization results. Here are some possible ways to get results.

**Pivot**  
Build tables and visualizations using multiple fields and metrics without writing searches.

**Quick Reports**  
Click on any field in the events tab for a list of quick reports like 'Top Referrers' and 'Top Referrers by time'.

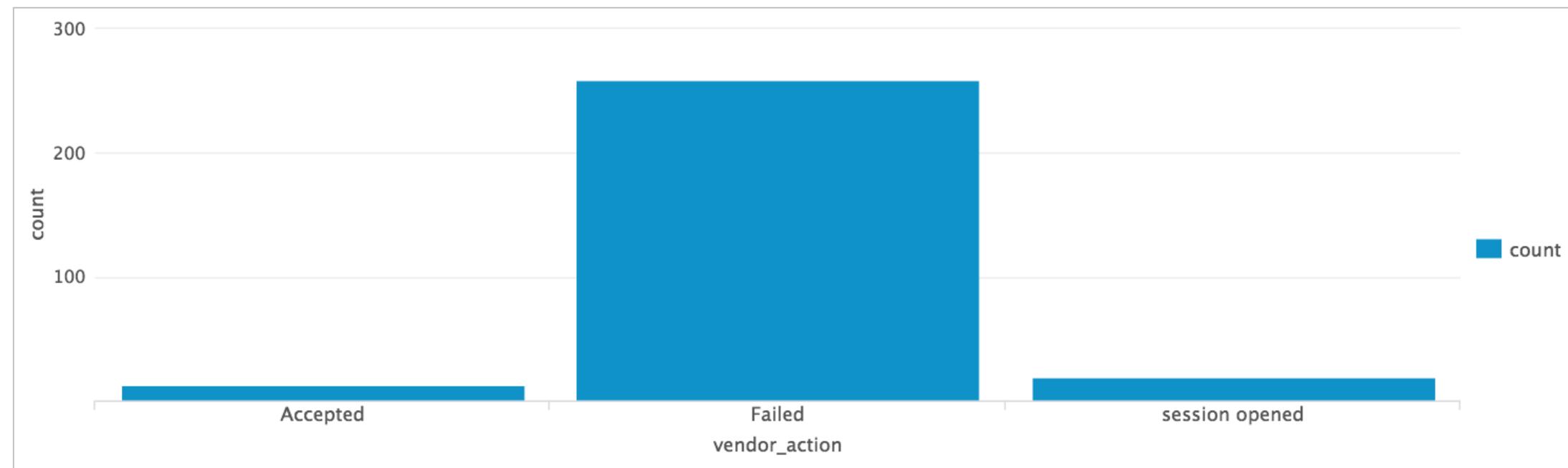
**Search Commands**  
Use a transforming search command, like timechart or stats, to summarize the data.

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Data Structure Requirements – Single Series

- Most visualizations require search results structured as tables, with at least two columns, a **single series**
  - Leftmost column** provides x-axis values
  - Subsequent columns** provide numeric y-axis values for each series in the chart

vendor_action	count
Accepted	13
Failed	259
session opened	19

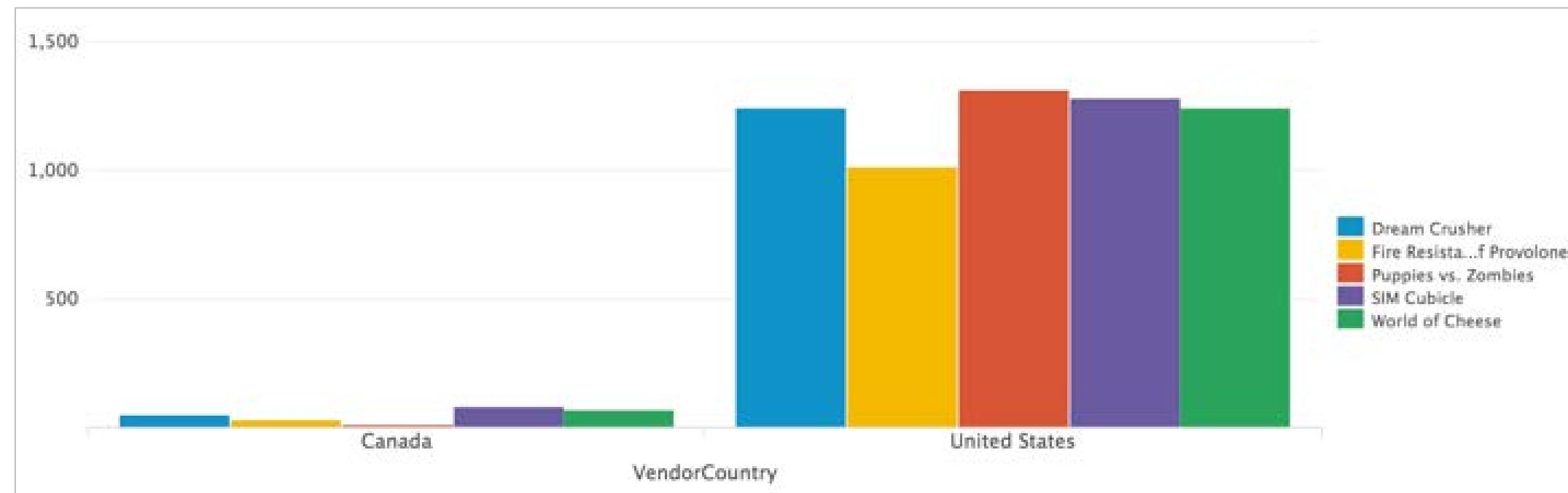


Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Data Structure Requirements – Multi-Series

To get **multi-series** tables, you need to set up the underlying search with reporting search commands like **chart** or **timechart**

VendorCountry	Dream Crusher	Fire Resistance Suit of Provolone	Puppies vs. Zombies	SIM Cubicle	World of Cheese
Canada	7	5	3	17	14
United States	236	192	239	241	212



```
index=sales sourcetype=vendor_sales VendorID<4000| chart count over VendorCountry by product_name limit=5  
useother=f
```

Last 30 days ▾

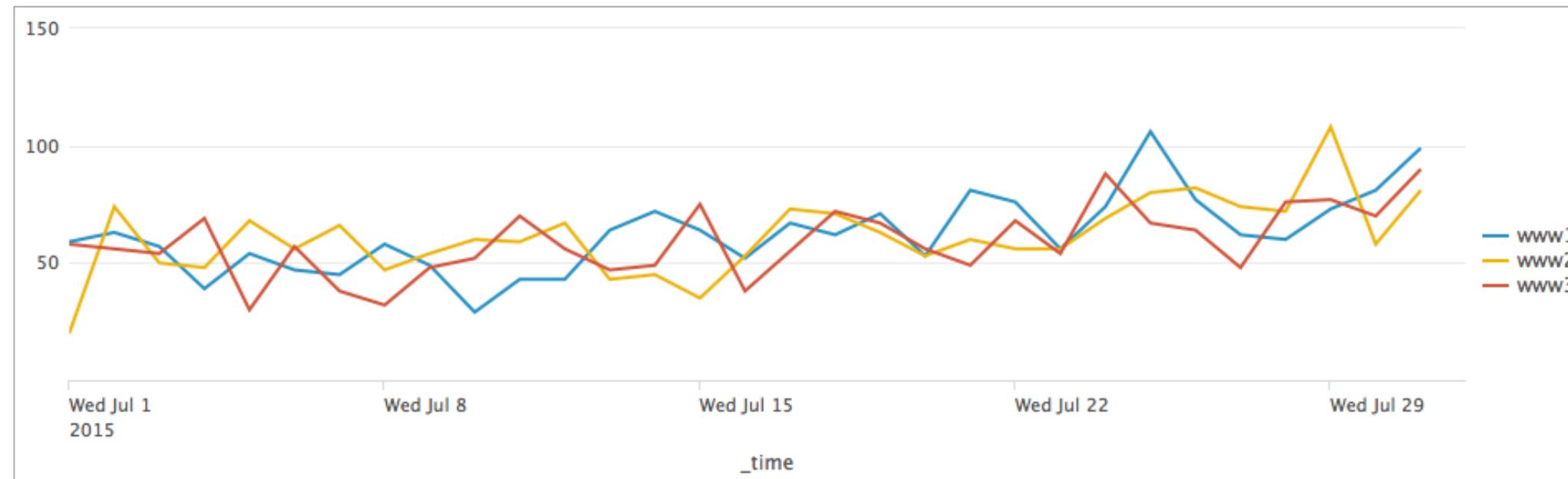


Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Data Structure Requirements – Time Series

- **Time series** displays statistical trends over time
- Can be single-series or multi-series

_time	www1	www2	www3
2016-07-01	131	168	180
2016-07-02	181	175	153
2016-07-03	137	185	184
2016-07-04	144	170	168
2016-07-05	166	168	130



```
index=web sourcetype=access_combined action=purchase status=200  
| timechart count by host
```

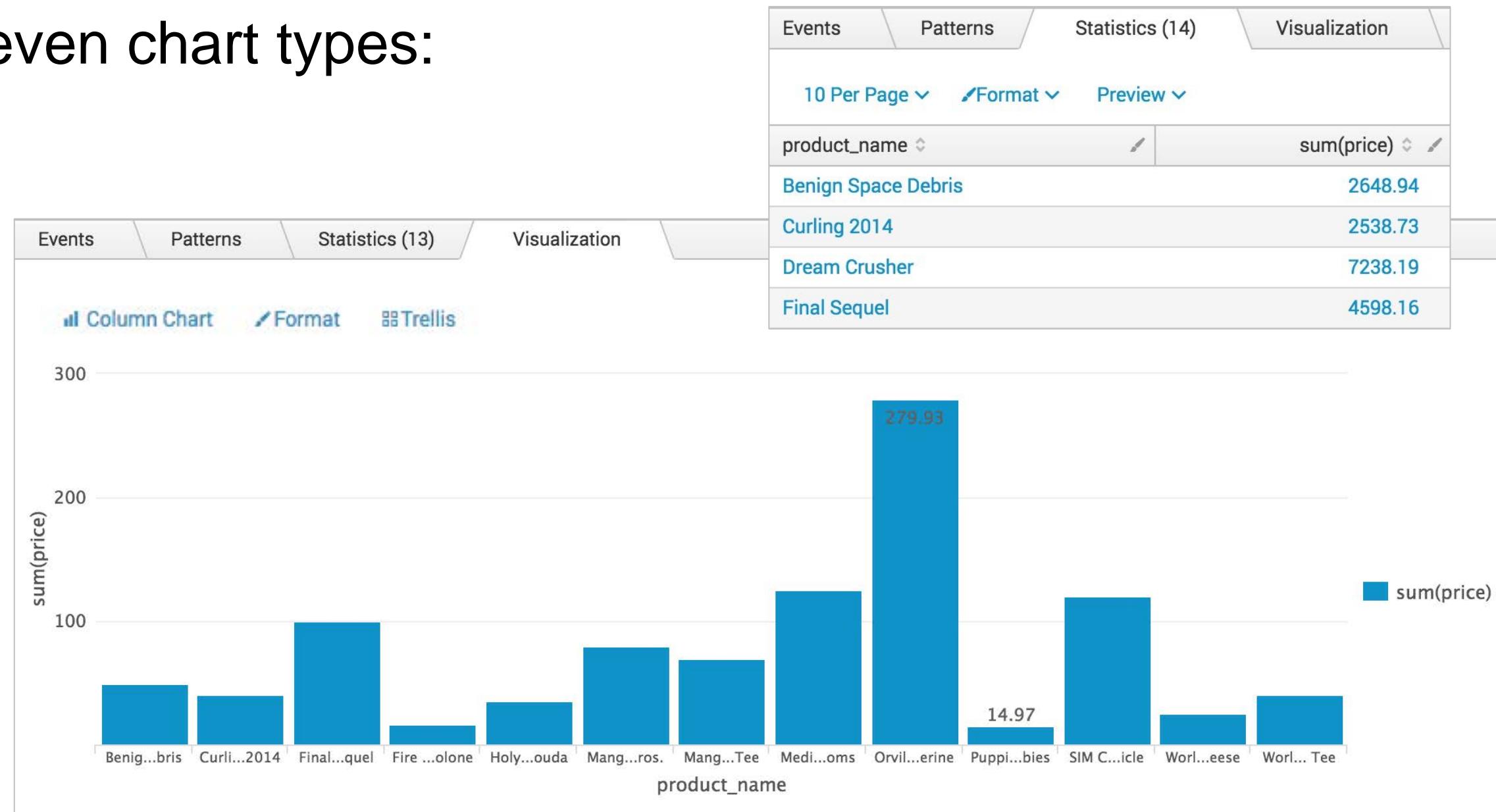
Previous month ▾



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Viewing Results as a Chart

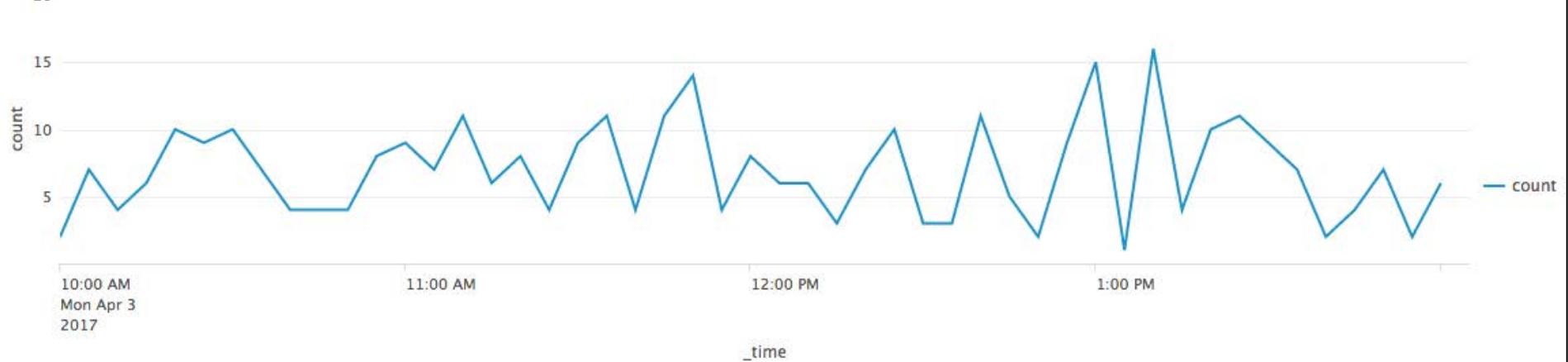
- There are seven chart types:
  - Line
  - Area
  - Column
  - Bar
  - Bubble
  - Scatter
  - Pie



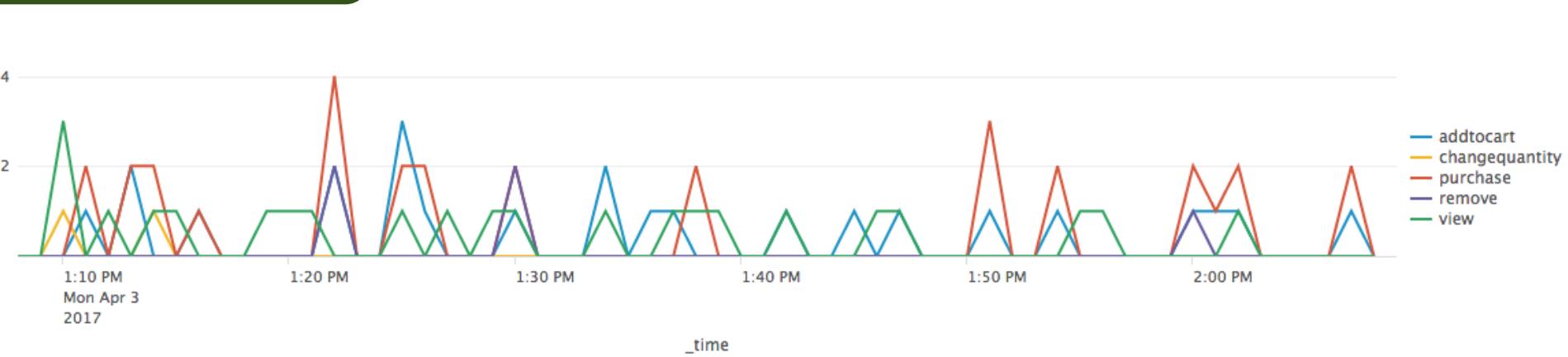
Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Charts – Line

```
index=web sourcetype=access_combined action=*
| timechart count
```



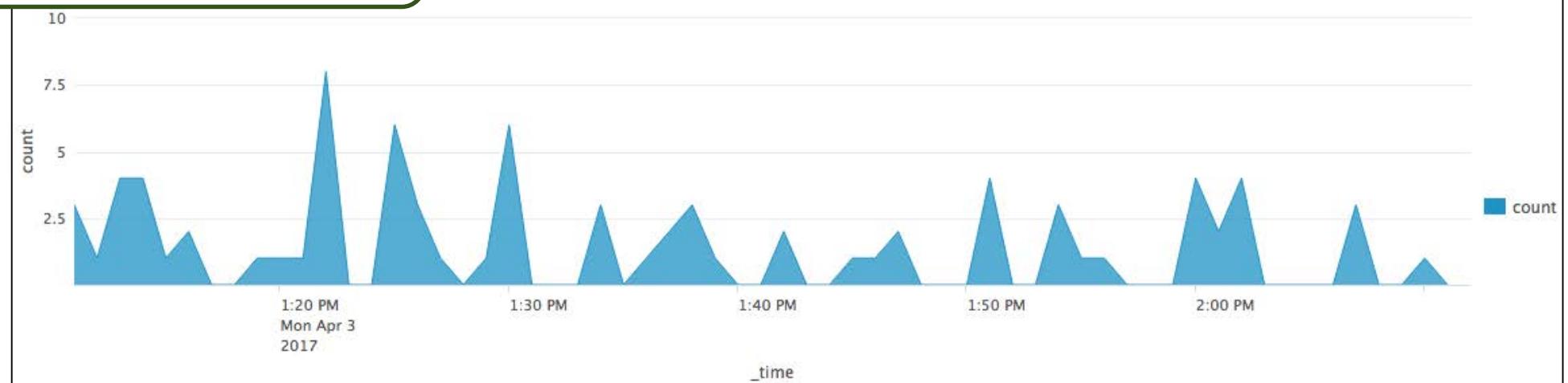
```
index=web sourcetype=access_combined action=*
| timechart count by action
```



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc. not for distribution

# Charts – Area

```
index=web sourcetype=access_combined action=*
| timechart count
```



```
index=web sourcetype=access_combined action=*
| timechart count by action
```



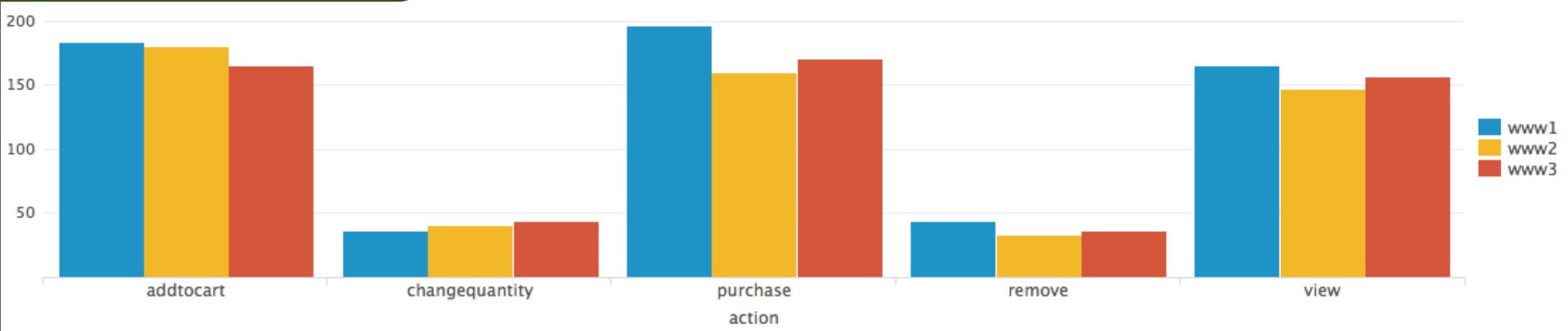
Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc. not for distribution

# Charts – Column

```
index=web sourcetype=access_combined action=*
| chart count over action
```



```
index=web sourcetype=access_combined action=*
| chart count over action by host
```



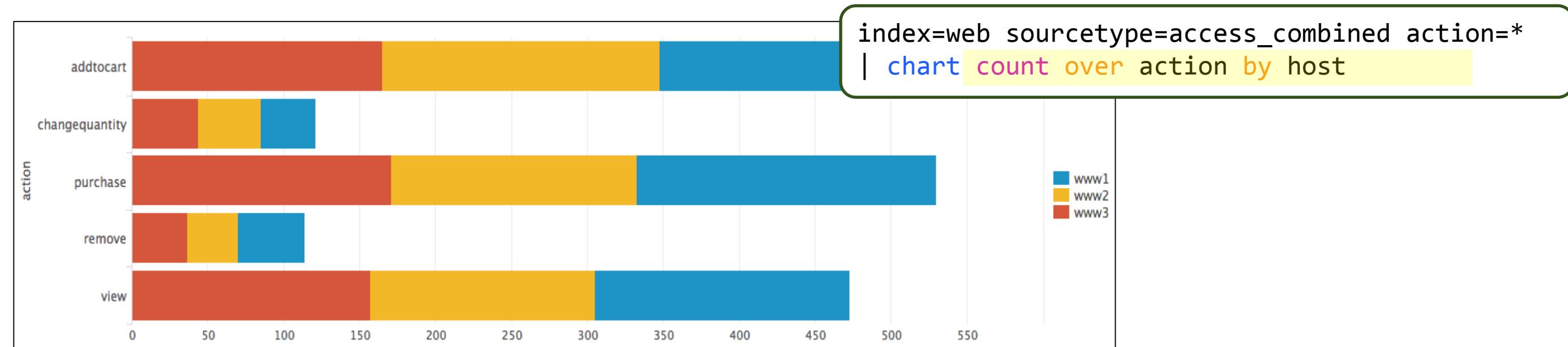
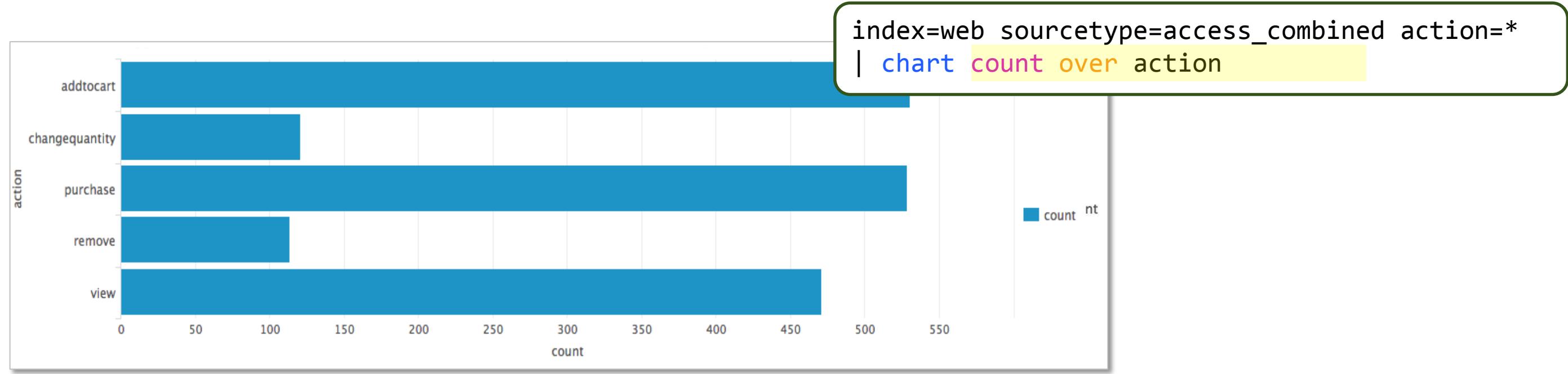
Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc. not for distribution

# Charts – Column (Formatted as Stacked)



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

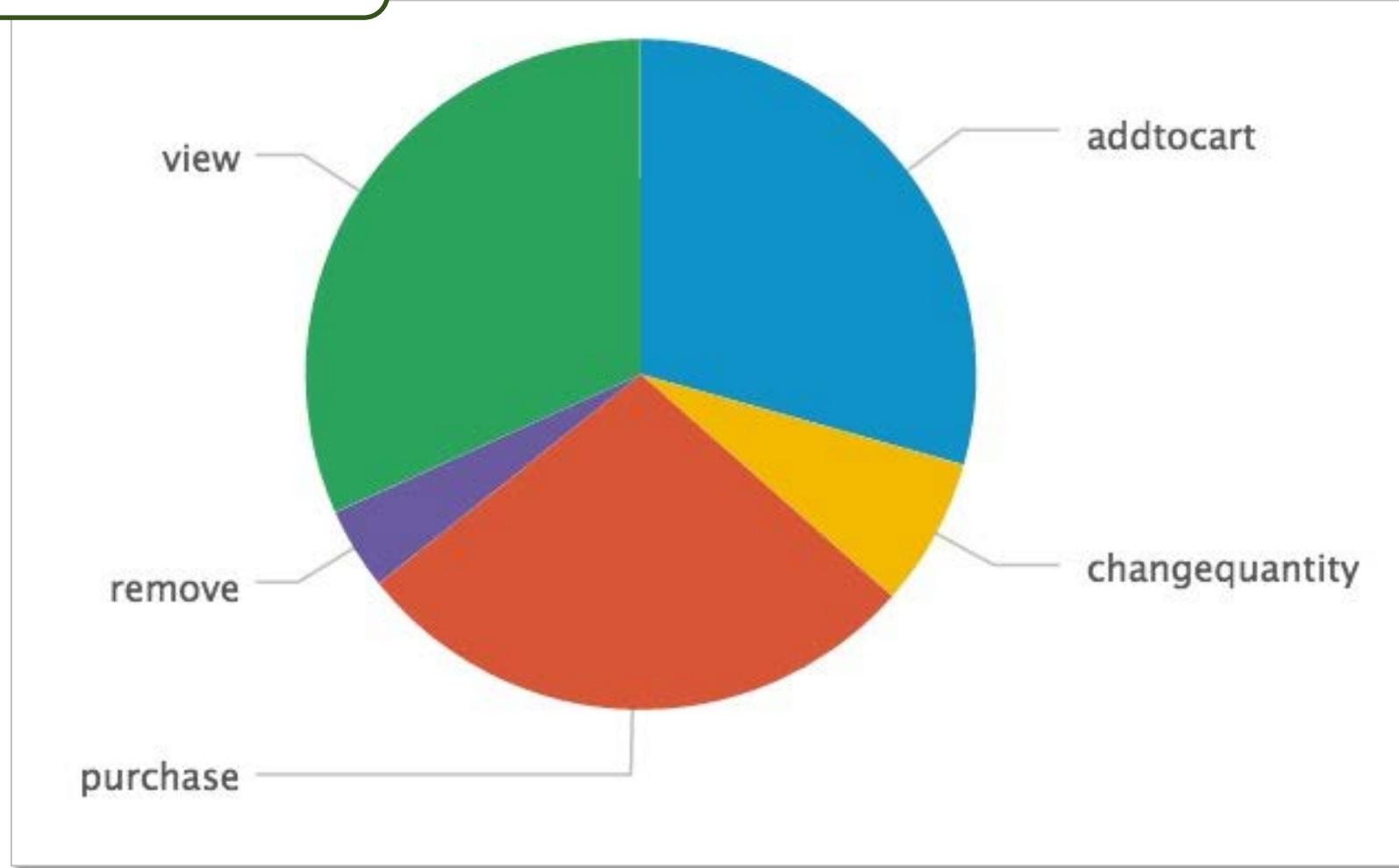
# Charts – Bar



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc. not for distribution

# Charts – Pie

```
index=web sourcetype=access_combined action=*  
| chart count over action
```



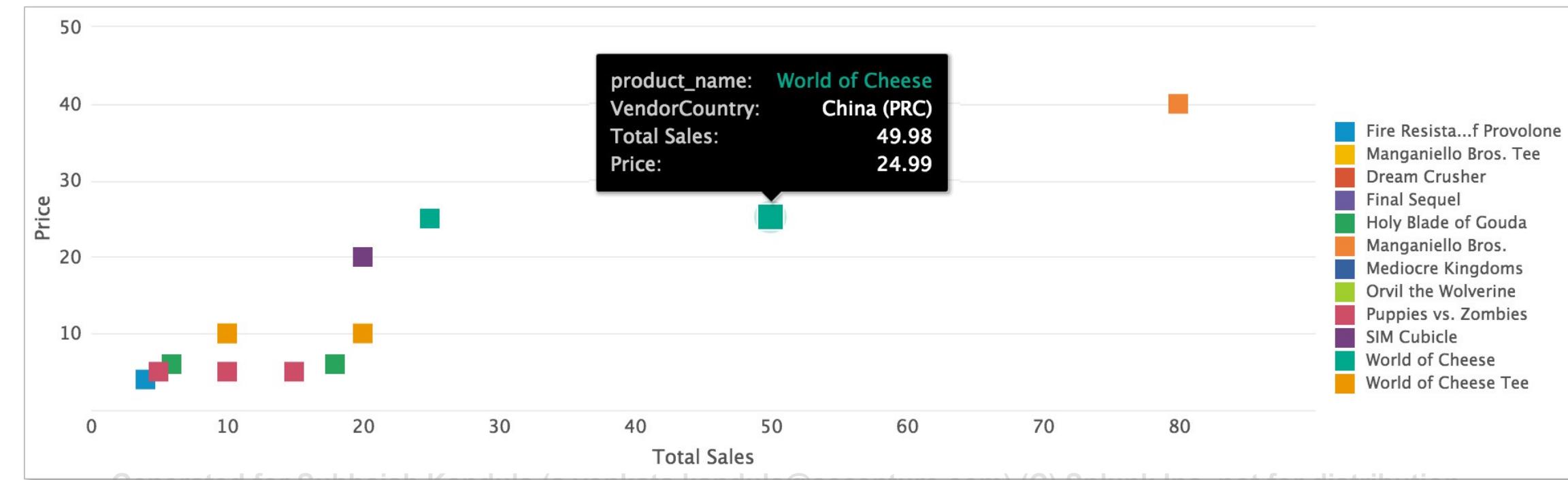
Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc. not for distribution

# Charts – Scatter

- Scatter chart shows trends in the relationships between discrete data values

```
index=sales sourcetype=vendor_sales  
VendorID >=7000 AND VendorID <=8999  
| stats sum(price) as "Total Sales",  
values(price) as "Price",  
count by VendorCountry, product_name
```

- Generally, it shows discrete values that do not occur at regular intervals or belong to a series

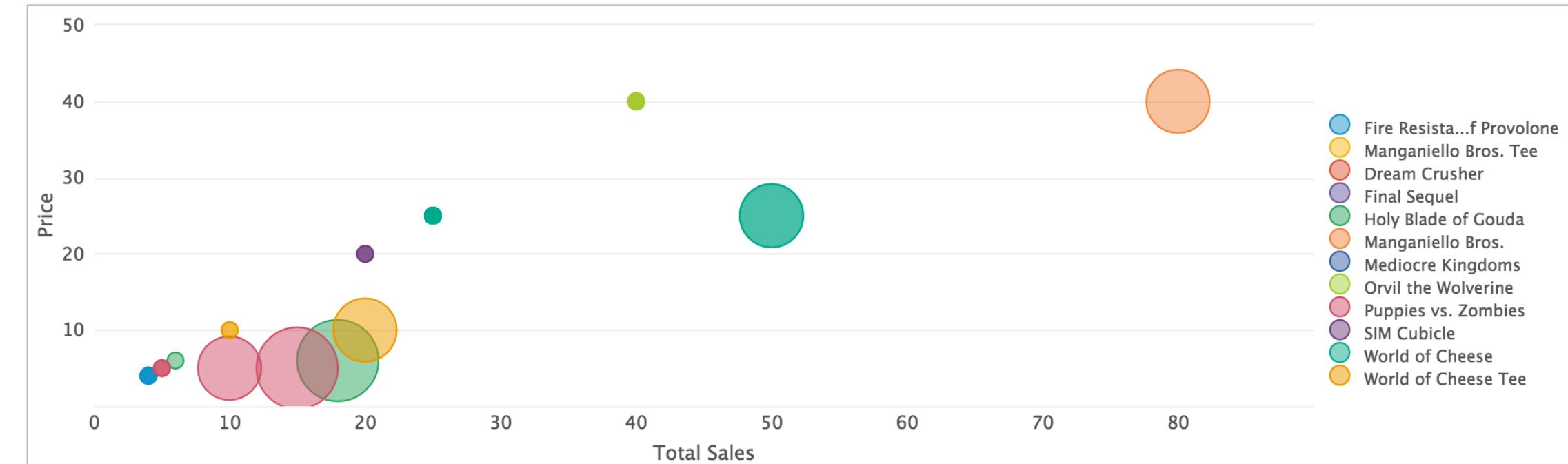


Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Charts – Bubble

- Bubble chart provides a visual way to view a three dimensional series
- Each bubble plots against two dimensions on the X and Y axes
- The size of the bubble represents the value for the third dimension

```
index=sales sourcetype=vendor_sales  
VendorID >=7000 AND VendorID <=8999  
| stats sum(price) as "Total Sales",  
values(price) as "Price",  
count by VendorCountry, product_name
```



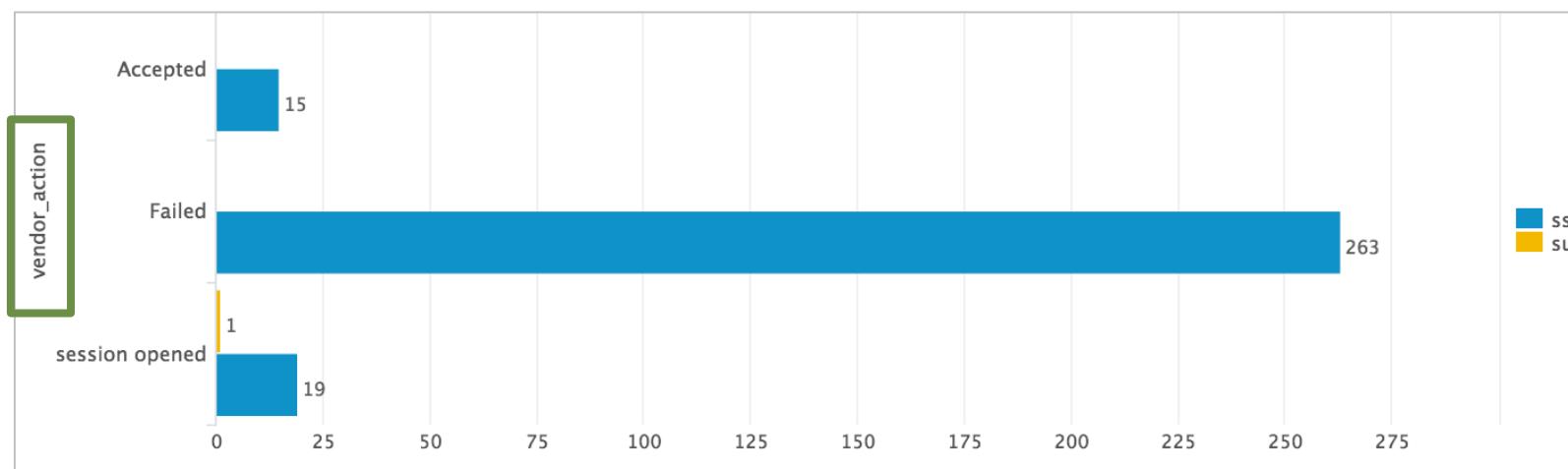
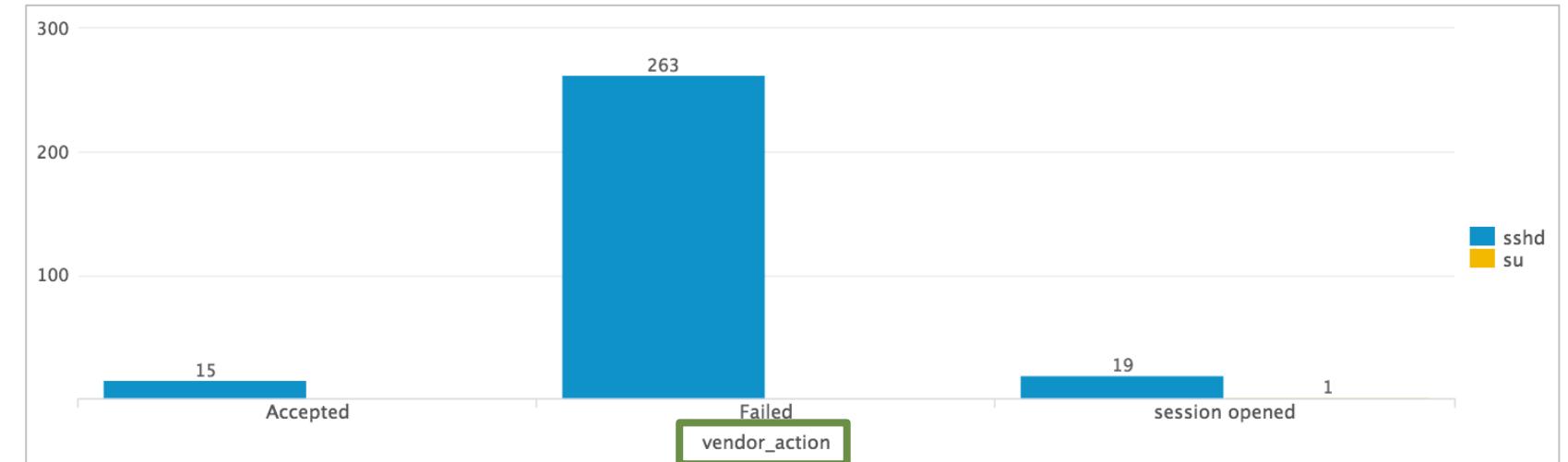
Generated for Subbaiah Kanadula (s.venkata.kanadula@accenture.com) (C) Splunk Inc. not for distribution

# Visualizations – x and y Axes

- For line, area, and column charts, the x axis is horizontal

```
index=security sourcetype=linux_secure  
| chart count over vendor_action by app
```

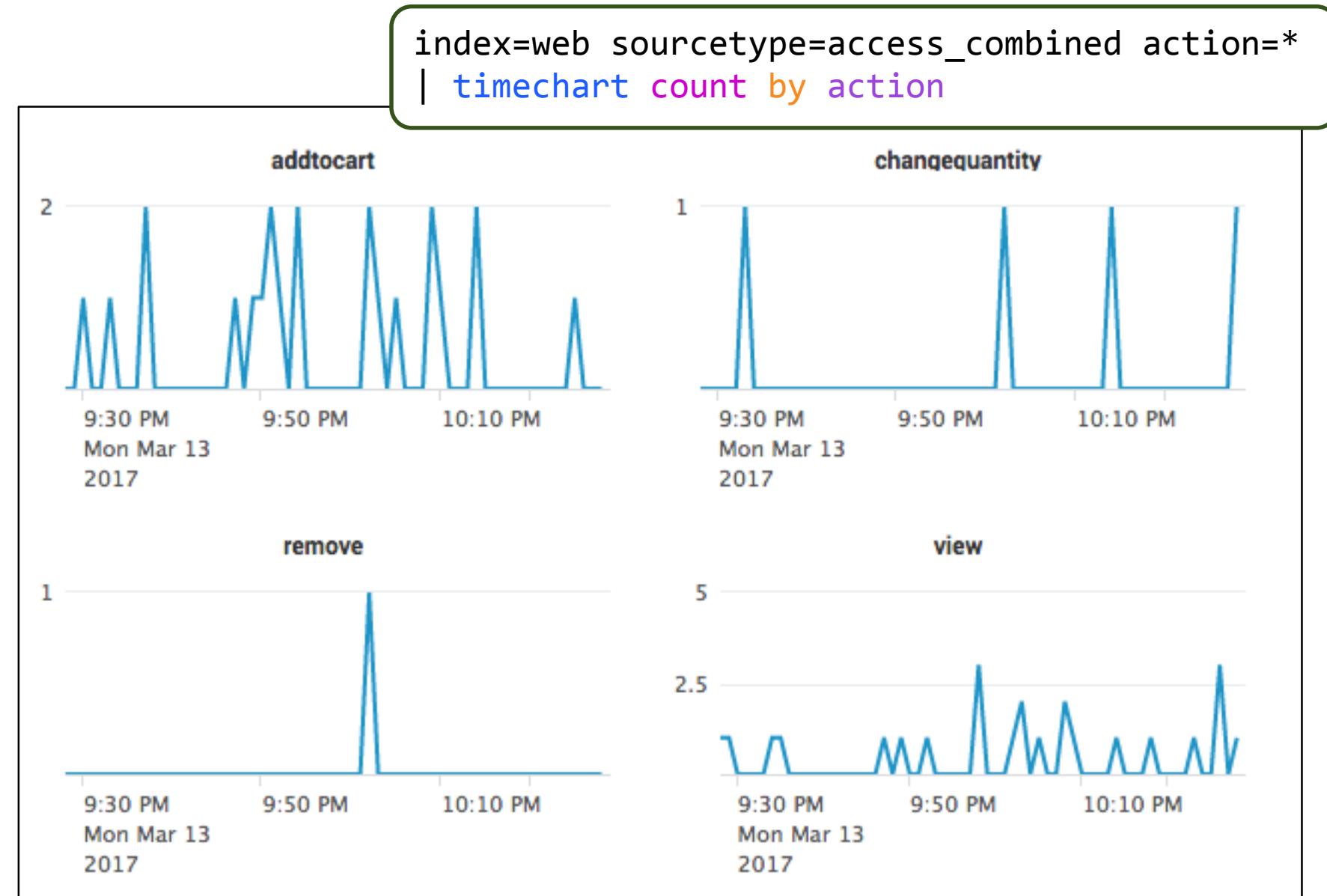
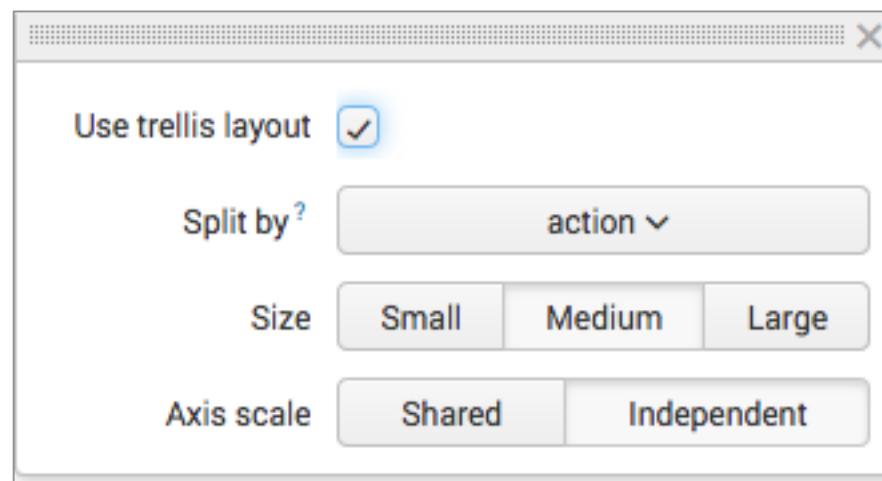
- For bar chart, the x axis is vertical



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Trellis Layout

- Display multiple charts based on one result set
- Allows visual comparison between different categories
- Data only fetched once



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# chart Command

---

- chart command can display any series of data that you want to plot
- You decide which field to plot on the x-axis
  - The function defines the value of the y-axis, therefore it should be numeric
  - The first field after the over clause is the x-axis
  - Using the over and by clauses divides the data into sub-groupings
    - The values from the by cause display in the legend

chart avg(bytes) over host

- The host values display over the x-axis

chart avg(bytes) over host by product\_name

- The host field is the x-axis and the series is further split by product\_name

# chart Command – over field

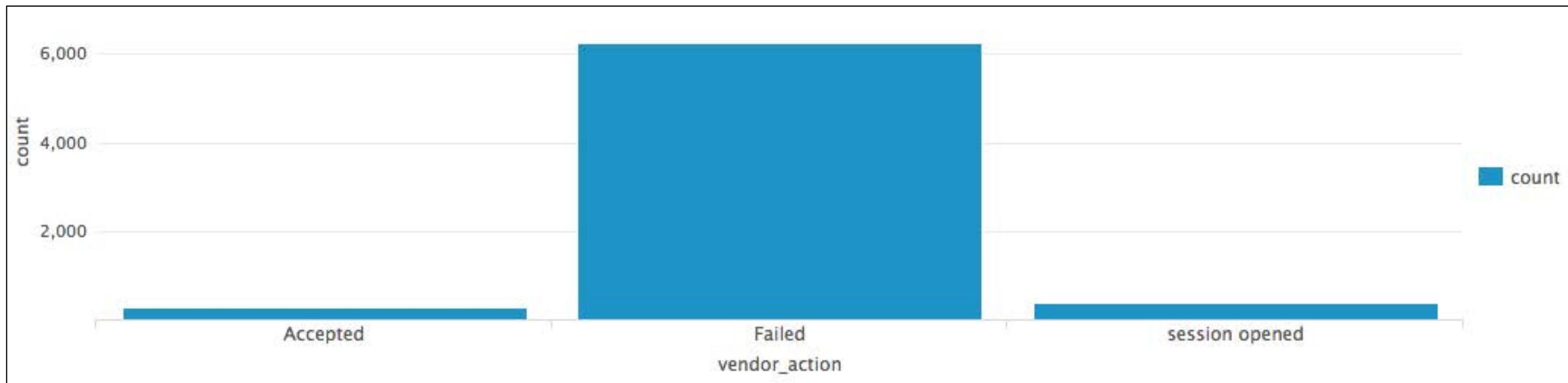
count function tallies the number of events for each value in the result set

Scenario



Display a count of vendor actions over the last 60 minutes.

```
index=security sourcetype=linux_secure  
| chart count over vendor_action
```



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# chart Command – over *field* by *field*

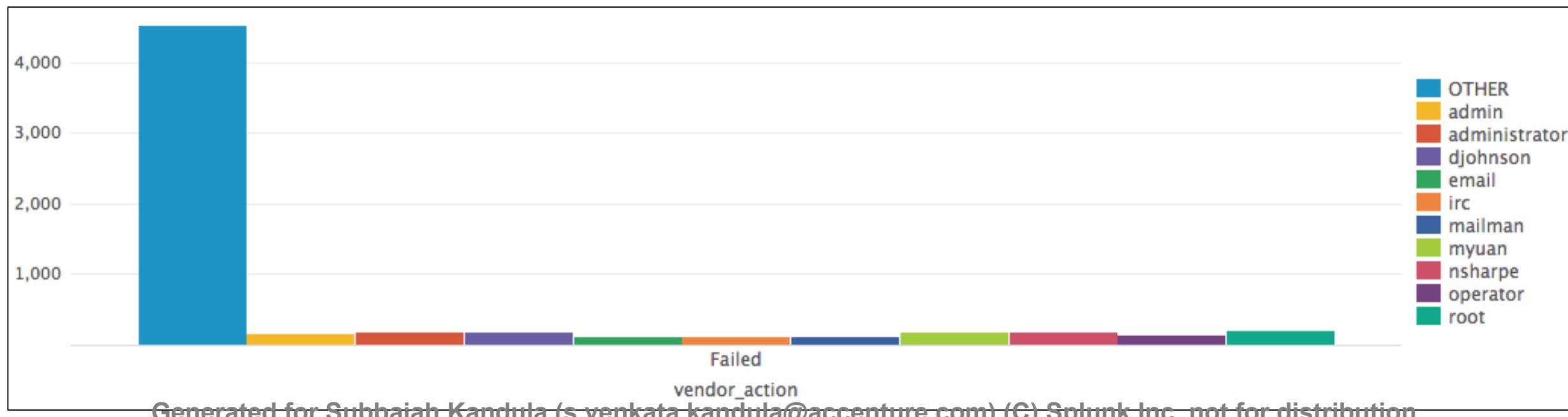
- You can use the **by** clause with the **over** clause to split results (over `vendor_action` by `user`)
- Alternatively, you can just use two **by** clauses (`by vendor_action, user`)
- You can only split chart results over TWO dimensions (unlike stats results)

## Scenario



Display a count of vendor actions **by user** over the last 60 minutes.

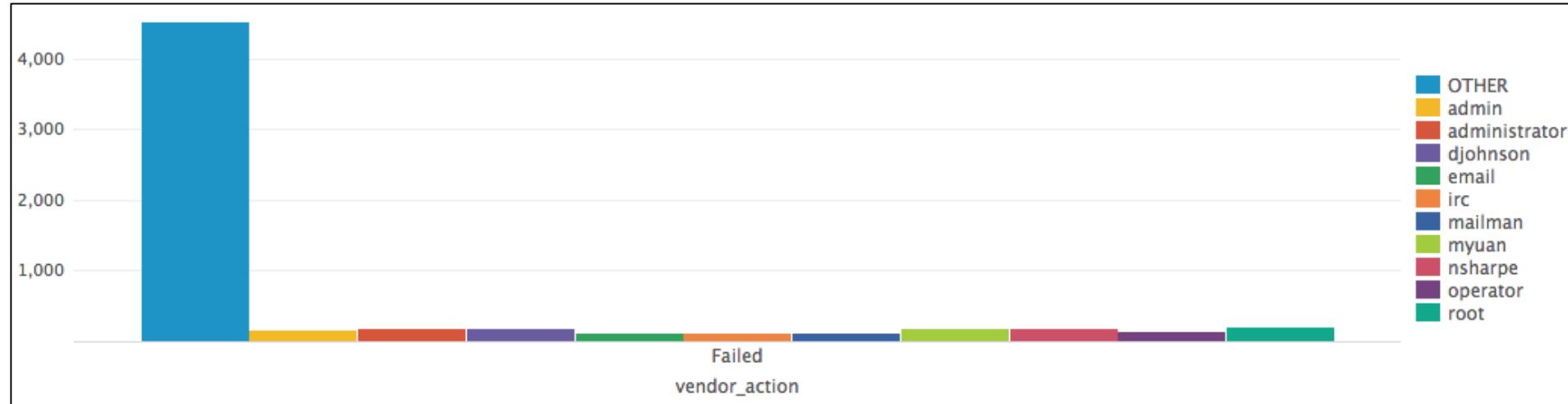
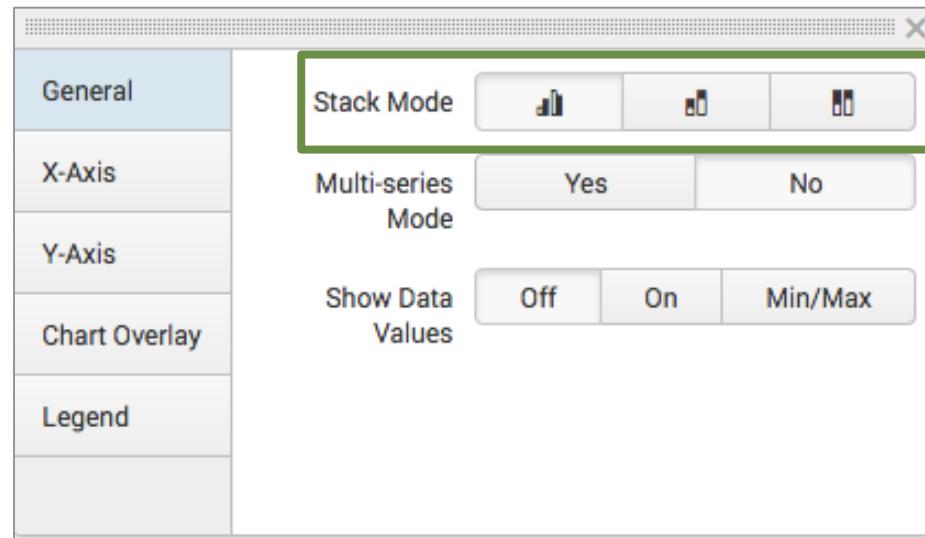
```
index=security sourcetype=linux_secure  
(invalid OR fail*)  
| chart count over vendor_action by user
```



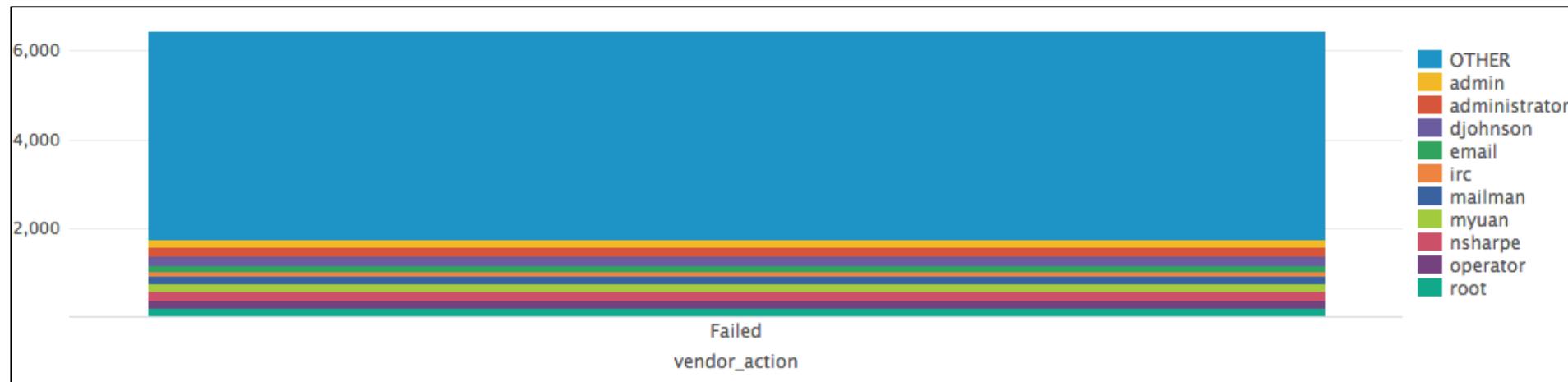
Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Stack Mode

## Stack Mode OFF



## Stack Mode ON



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Including NULL and OTHER Values

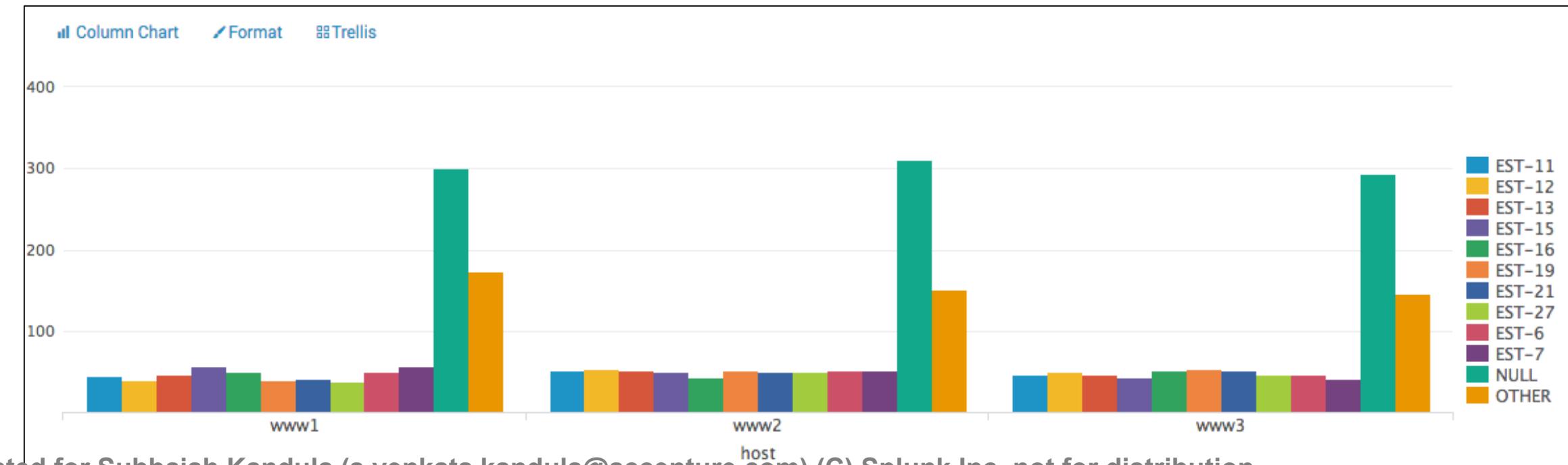
- chart and timechart commands automatically filter results to include the ten highest values
  - Surplus values are grouped into OTHER
- In this example, the results are skewed by NULL and OTHER
  - These values are shown by default

## Scenario



Display a count of unsuccessful web transactions by host for each item over the last 7 days.

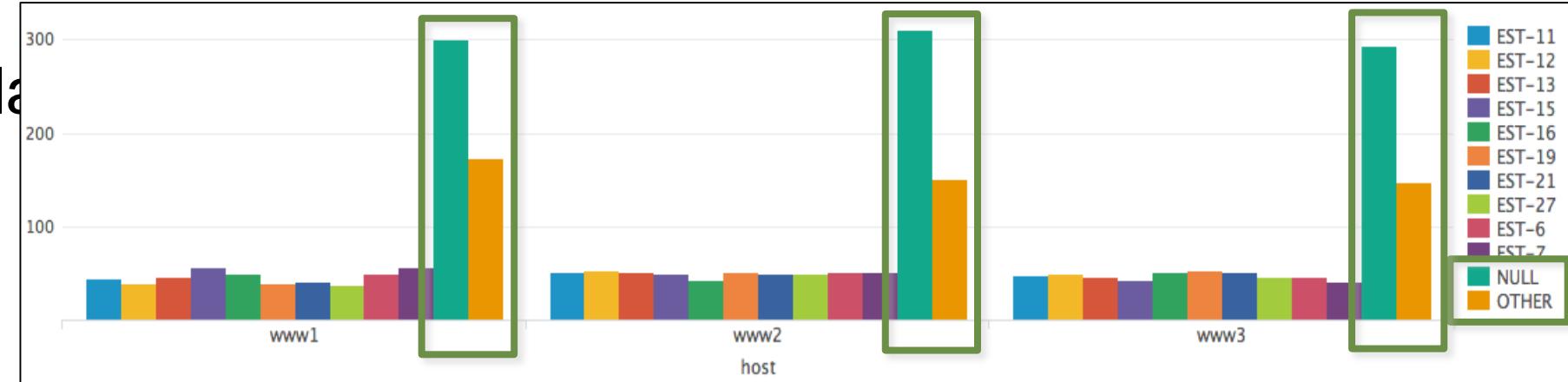
```
index=web sourcetype=access_combined  
status>399  
| chart count over host by itemId
```



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Omitting NULL and OTHER Values

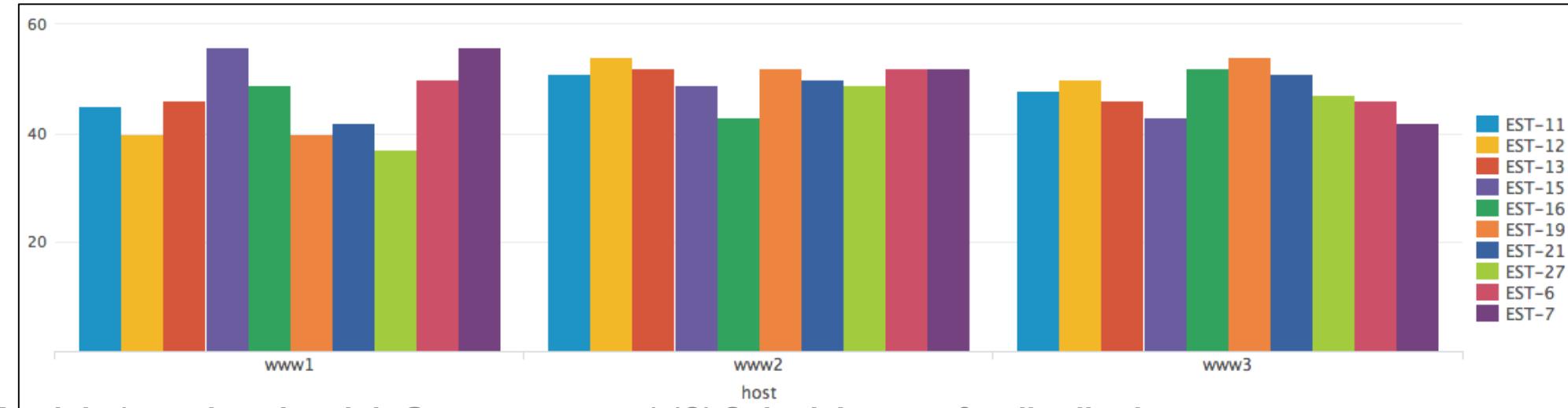
- To remove empty (NULL) and OTHER field values from the display, use these options:
  - useother=f
  - usenull=f



```
index=web sourcetype=access_combined status>399  
| chart count over host by itemId  
useother=f usenull=f
```

## Note

To remove null values, add itemId=\* to the base search.



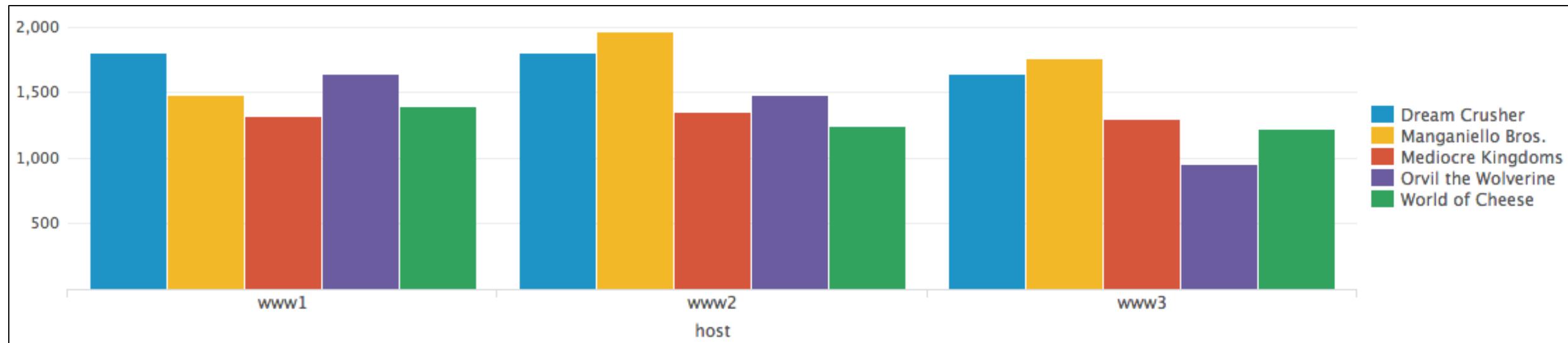
Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Limiting the Number of Values

- To adjust the number of plotted series, use the `limit` argument
- For unlimited values, use `limit=0`

Scenario ?  
Display sales per host for the top 5 best selling products over the last 7 days.

```
index=web sourcetype=access_combined  
action=purchase status=200  
| chart sum(price) over host  
by product_name limit=5 useother=f
```



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Visualization Formatting



# timechart Command – Overview

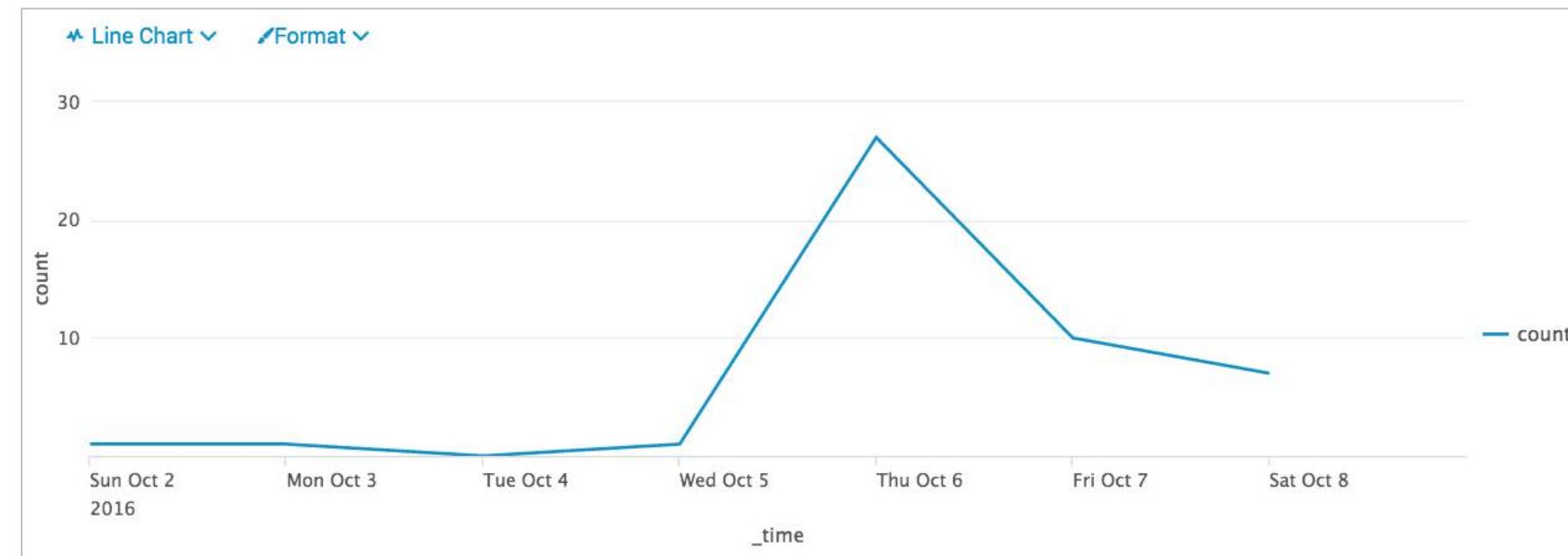
---

- timechart command performs statistical aggregations against time
- Plots and trends data over time
- `_time` is always the x-axis
- You can optionally split data using the `by` clause for one other field
  - Each distinct value of the split by field is a separate series in the chart
- Timecharts are best represented as line or area charts

# timechart Command – Example

Scenario ?  
How many usage violations have occurred during the last 7 days?

```
index=network sourcetype=cisco_wsa_squid usage=Violation  
| timechart count
```



Note i  
Functions and arguments used with stats and chart can also be used with timechart.

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

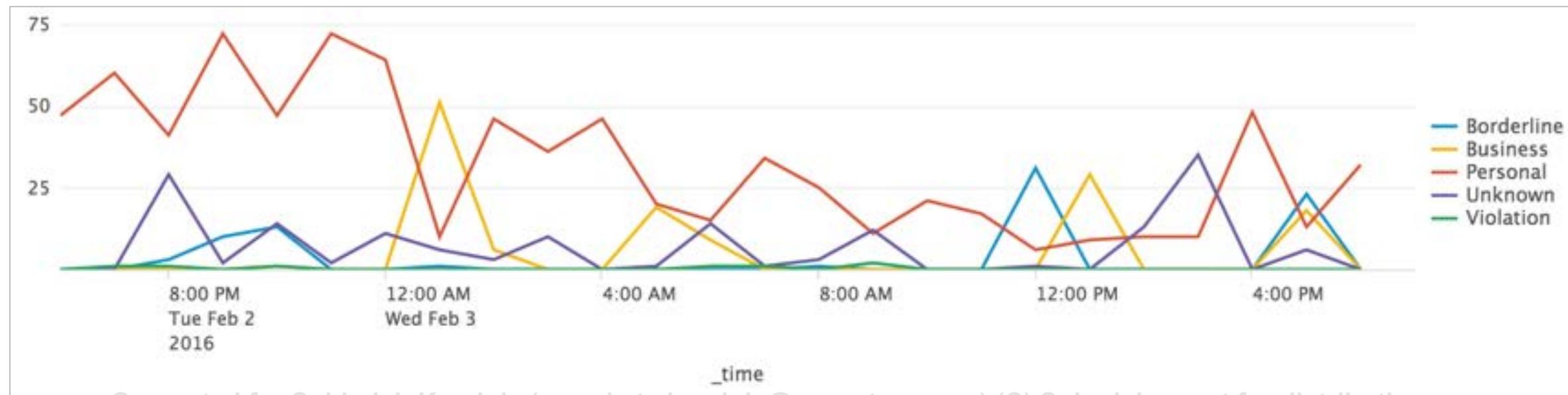
# timechart Command – Multiple Values

- Splitting by the usage field, each line represents a unique field value
  - Unlike stats, only ONE field can be specified after by
- y-axis represents the count for each field value

Scenario ?  
What is the overall usage trend  
for the last 24 hours?

index=network sourcetype=cisco\_wsa\_squid  
| timechart count by usage

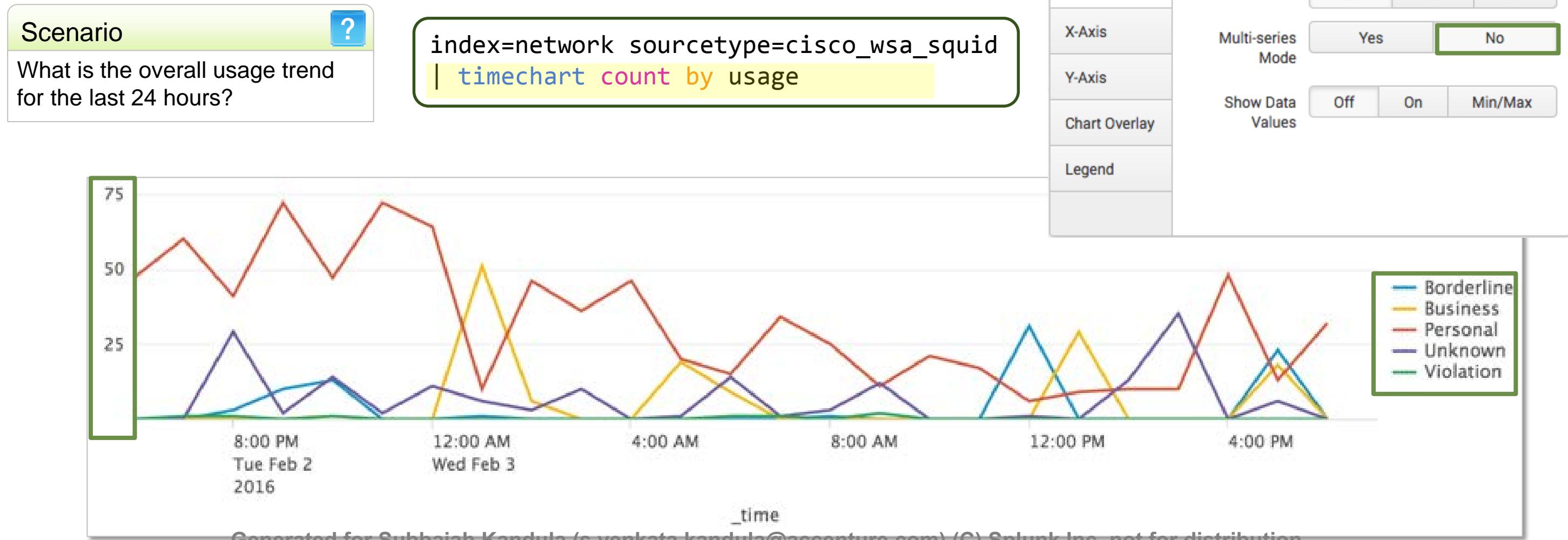
Note i  
Using timechart, you can split by  
a maximum of one field because  
\_time is the implied first by field.



Generated for Subbaiah Kandula (s.verikata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# timechart Command – Multi-series: No

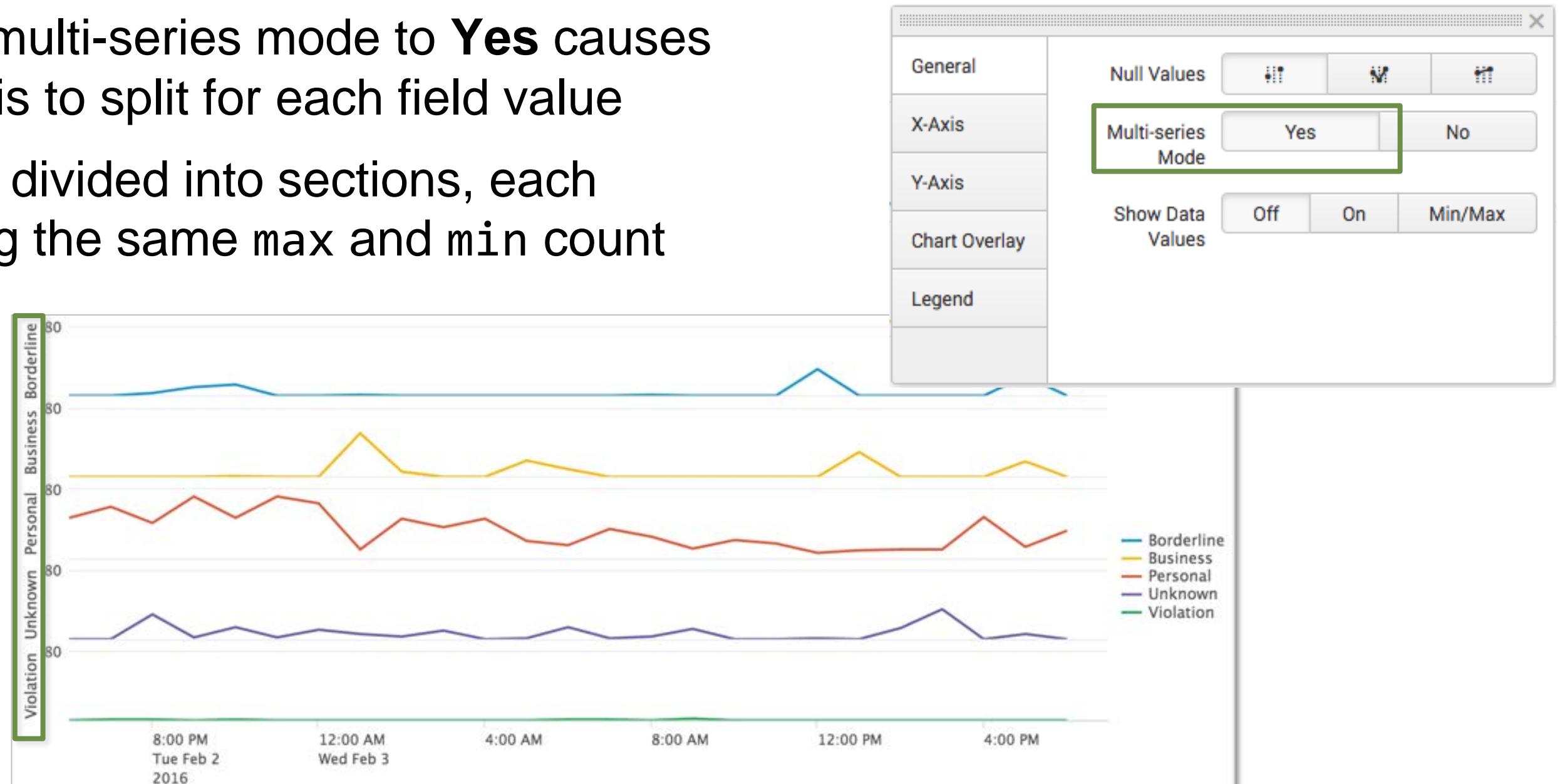
When the multi-series mode is set to **No**, all fields share the y-axis



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# timechart Command – Multi-series: Yes

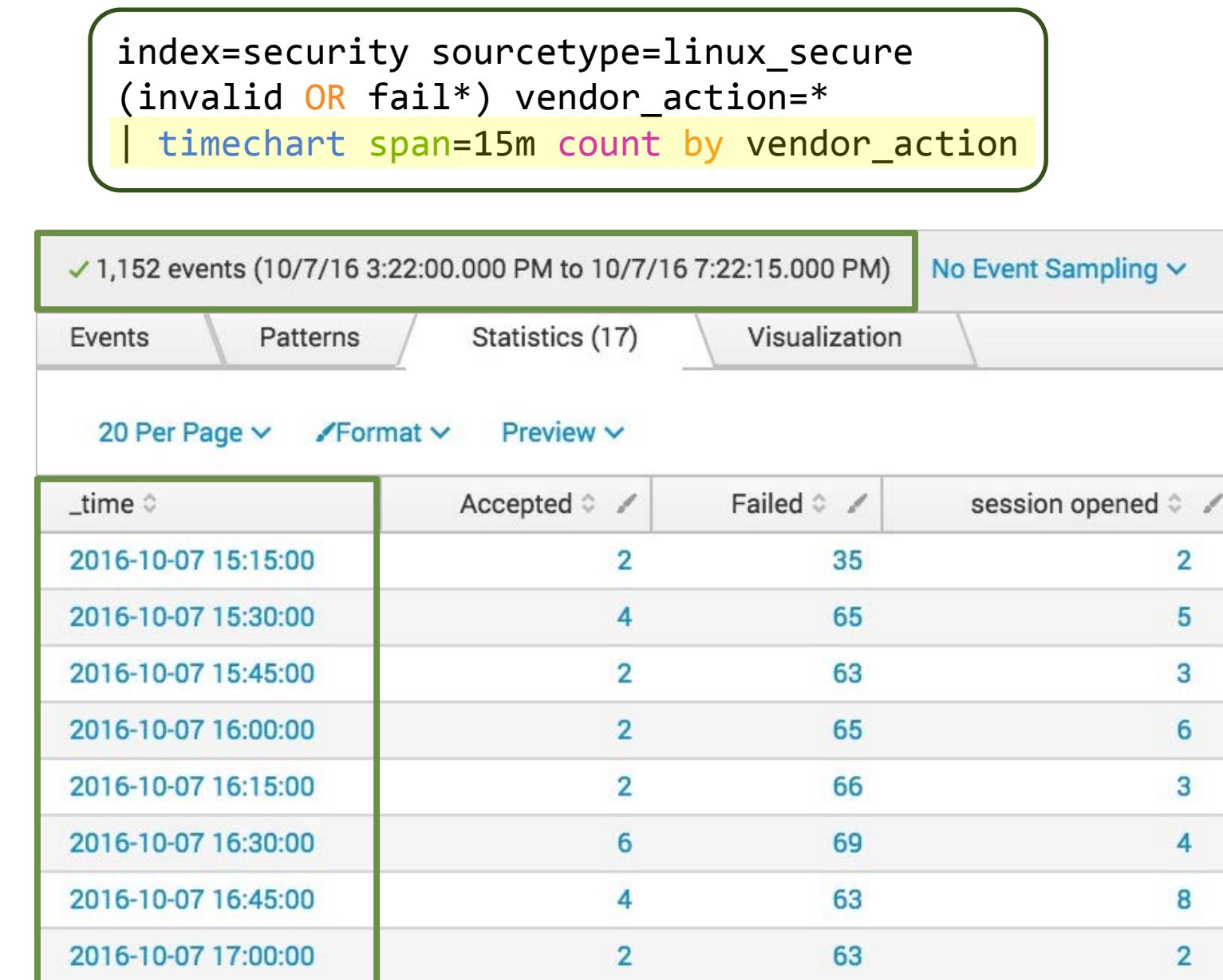
- Setting multi-series mode to **Yes** causes the y-axis to split for each field value
- y-axis is divided into sections, each spanning the same max and min count



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# timechart Command – Adjusting the Sampling Interval

- The timechart command "buckets" the values of the `_time` field
  - This provides dynamic sampling intervals, based upon the time range of the search
- Example defaults:
  - Last 60 minutes uses `span=1m`
  - Last 24 hours uses `span=30m`
- Adjust the interval using the `span` argument, e.g. `span=15m`



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# timechart Command – Statistical Functions

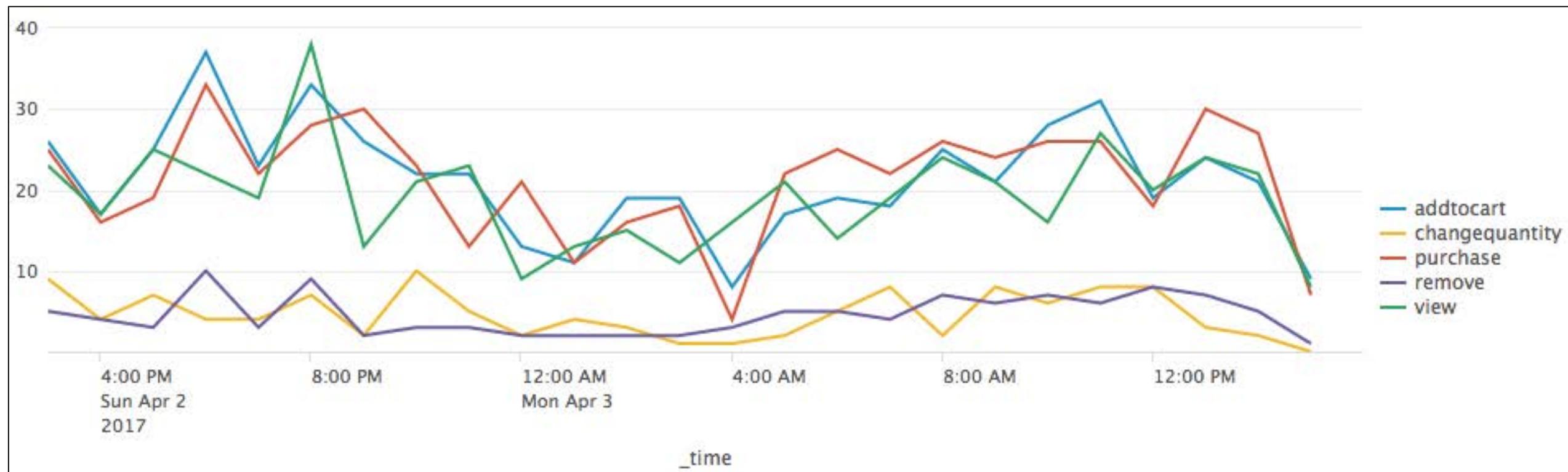
As with the stats and chart commands, you can apply statistical functions to the timechart command

## Scenario



How much Web activity of each type took place during the last 24 hours?

```
index=web sourcetype=access_combined action=*
| timechart span=1h count by action
```



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Formatting – Chart Overlay



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Transforming Command Summary

Feature	stats	chart	timechart
Multi-level breakdown [by clause]	Many	2	1
Limit # series shown	NA	<code>limit=n</code> <i>Default=10</i>	<code>limit=n</code> <i>Default=10</i>
Filter other series	NA	<code>useother=f</code>	<code>useother=f</code>
Filter null values	NA	<code>usenull=f</code>	<code>usenull=f</code>
Set time value on x axis	NA	NA	<code>span</code>

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Transforming Command Summary (cont.)

To count the frequency of a field(s), use top/rare

					index=security sourcetype=linux_secure   top src_ip, user, vendor_action, app		
src_ip	user	vendor_action	app		count	percent	
10.3.10.46	djohnson	Failed	sshd		41	3.713768	
10.2.10.163	nsharpe	Failed	sshd		36	3.260870	
10.3.10.46	djohnson	Accepted	sshd		34	3.079710	
10.1.10.172	myuan	Failed	sshd		30	2.717391	

					index=security sourcetype=linux_secure   rare src_ip, user, vendor_action, app		
src_ip	user	vendor_action	app		count	percent	
10.1.10.172	amavis	Failed	sshd		1	0.090090	
10.1.10.172	angel	Failed	sshd		1	0.090090	
10.1.10.172	appserver	Failed	sshd		1	0.090090	
10.1.10.172	bfsuser	Failed	sshd		1	0.090090	

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc. not for distribution

# Transforming Command Summary (cont.)

Use stats to calculate statistics for two or more by fields (non time-based)

```
index=security sourcetype=linux_secure  
| stats count by src_ip, user, vendor_action, app
```

src_ip	user	vendor_action	app	count
10.1.10.172	administrator	Failed	sshd	8
10.1.10.172	amavis	Failed	sshd	1
10.1.10.172	angel	Failed	sshd	1
10.1.10.172	apache	Failed	sshd	3
10.1.10.172	appserver	Failed	sshd	1
10.1.10.172	bfsuser	Failed	sshd	1
10.1.10.172	bin	Failed	sshd	2
10.1.10.172	brian	Failed	sshd	1
10.1.10.172	britany	Failed	sshd	1
10.1.10.172	cyrus	Failed	sshd	1

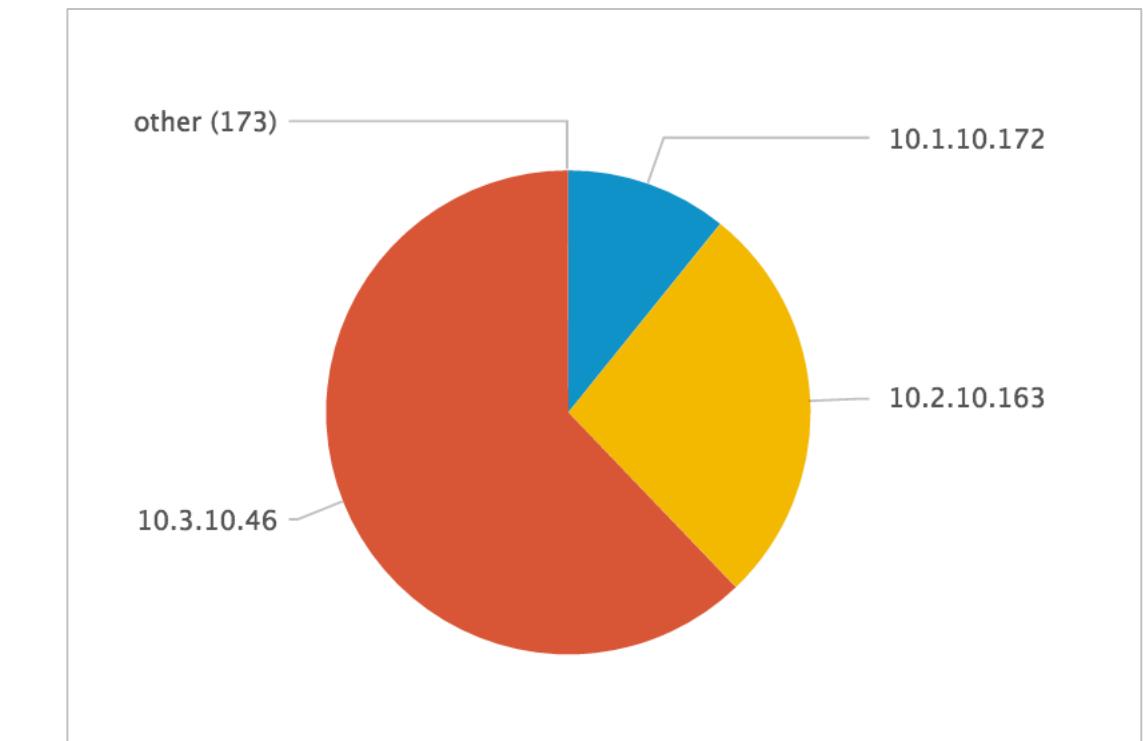
Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Transforming Command Summary (cont.)

- To calculate statistics with an arbitrary field as the x-axis (not `_time`), use `chart`
  - When you use a `by` field, the output is a table
  - Each column represents a distinct value of the split-by field

src_ip	Accepted	Failed
10.1.10.172	7	158
10.2.10.163	16	155
10.3.10.46	38	183
12.130.60.4	0	17

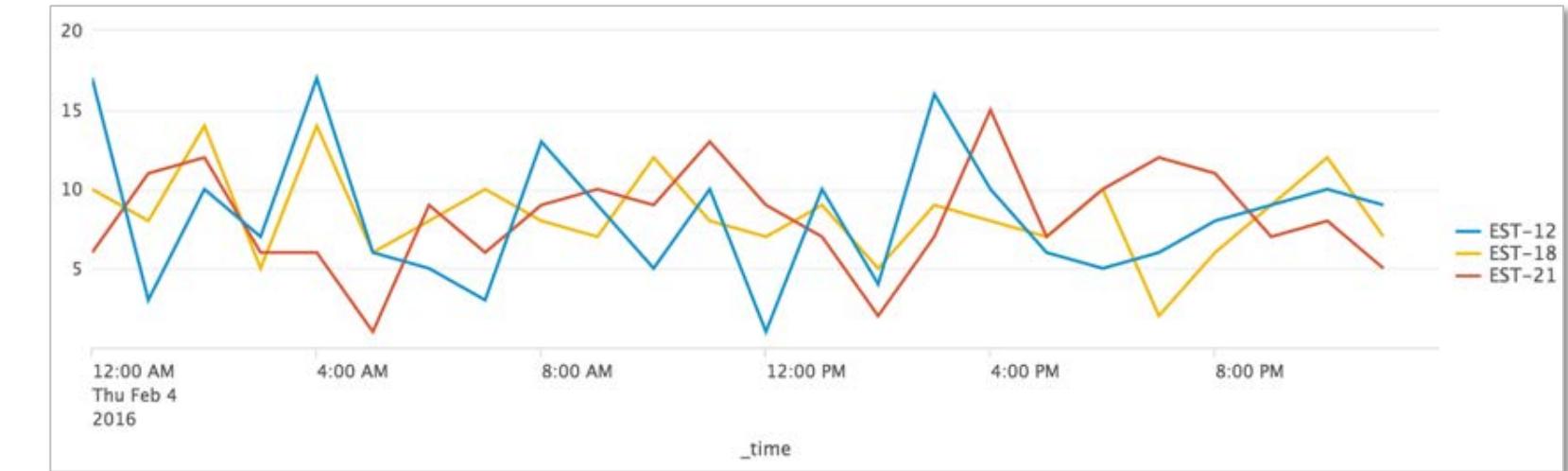
```
index=security sourcetype=linux_secure  
| chart count over src_ip  
by vendor_action
```



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Transforming Command Summary (cont.)

- Use timechart to calculate statistics with `_time` as the x-axis
- If a by field is used, the output is a table



- Each column represents a distinct value of the split-by field

```
... | timechart span=1h count by itemId limit=3 useother=f
```

_time	EST-17	EST-26	EST-6	NULL
2016-08-05 15:00	6	9	7	40
2016-08-05 16:00	16	5	8	47
2016-08-05 17:00	7	14	12	40
2016-08-05 18:00	12	12	8	46
2016-08-05 19:00	1	3	7	13

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Module 4: Using Trendlines, Mapping, and Single Value Commands

Generated for Subbaiah Kandula ([s.venkata.kandula@accenture.com](mailto:s.venkata.kandula@accenture.com)) (C) Splunk Inc, not for distribution

# Module Objectives

---

- Create a trendline
- Create maps
  - iplocation
  - geostats
  - geom
- Create and format single values
- Use the addtotals command

# trendline Command

---

- Allows you to overlay a computed moving average on a chart

- trendline computes the moving averages of a field

`trendline <trendtype><period>(field) [AS newfield]`

- *trendtype*:

- sma - simple moving average

- ema - exponential moving average

- wma - weighted moving average

# trendline Command (cont.)

- Must define the *period* over which to compute the trend
- *period* must be an integer between 2 and 10000
  - For example, `sma2(sales)` is valid
  - But `sma(sales)` would *fail* as it is missing an integer, the defining period

Scenario ?

Display total sales and sales trends over the past 24 hours.

New Search Save As ▾ Close

```
index=web sourcetype=access_combined action=purchase status=200
| timechart span=2h sum(price) as sales
| trendline sma(sales) as trend
```

Last 24 hours ?

! Error in 'trendline' command: command="trendline", Invalid trend period for argument 'sma(sales)'

Note i

Autocomplete displays functions in **purple**. Here however, since it does not recognize `sma` as a function, it is shown in black.

# trendline Command – Example

Scenario ?

Display total sales and sales trends over the past 24 hours.

```
index=web sourcetype=access_combined action=purchase status=200  
| timechart span=2h sum(price) as sales  
| trendline sma2(sales) as trend
```

General

Overlay  trend

X-Axis

Y-Axis

Chart Overlay

Legend

General

Stack Mode

X-Axis

Y-Axis

Multi-series Mode Yes  No

Chart Overlay

Show Data Values Off  On  Min/Max

The chart displays two series: 'sales' (blue area) and 'trend' (yellow line). The sales area shows significant fluctuations, peaking around 714.69 at approximately 8:00 AM on Friday. The trendline follows a smoother path, showing a general upward trend with some fluctuations.

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

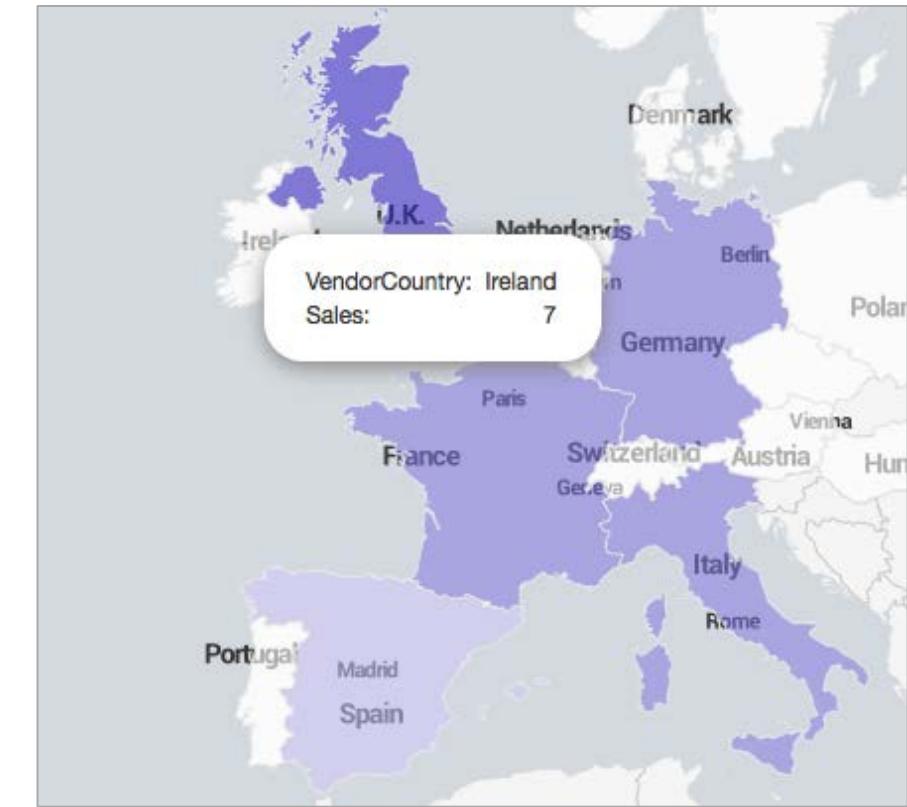
# Viewing Results as a Map

There are two map types:

## Cluster Map



## Choropleth Map



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# iplocation Command

## Scenario



Discover longitude and latitude data for src\_ip for the last 60 minutes.

```
index=security sourcetype=linux_secure (fail* OR invalid)
| iplocation src_ip
```

- Use iplocation to look up and add location information to an event
  - This information includes city, country, metro code, region, timezone, latitude and longitude
- Not all of the information is available for all ip address ranges
- Automatically defines the default lat and lon fields required by geostats

## Interesting Fields

a action 1

a app 2

a City 3

a Country 6

# date\_hour 1

# lat 6

# linecount 1

# lon 6

# pid 100+

a process 2

a punct 9

a Region 3

# geostats Command

---

- Use geostats to compute statistical functions and render a cluster map

```
geostats [latfield=string] [longfield=string] [stats-agg-term]* [by-clause]
```

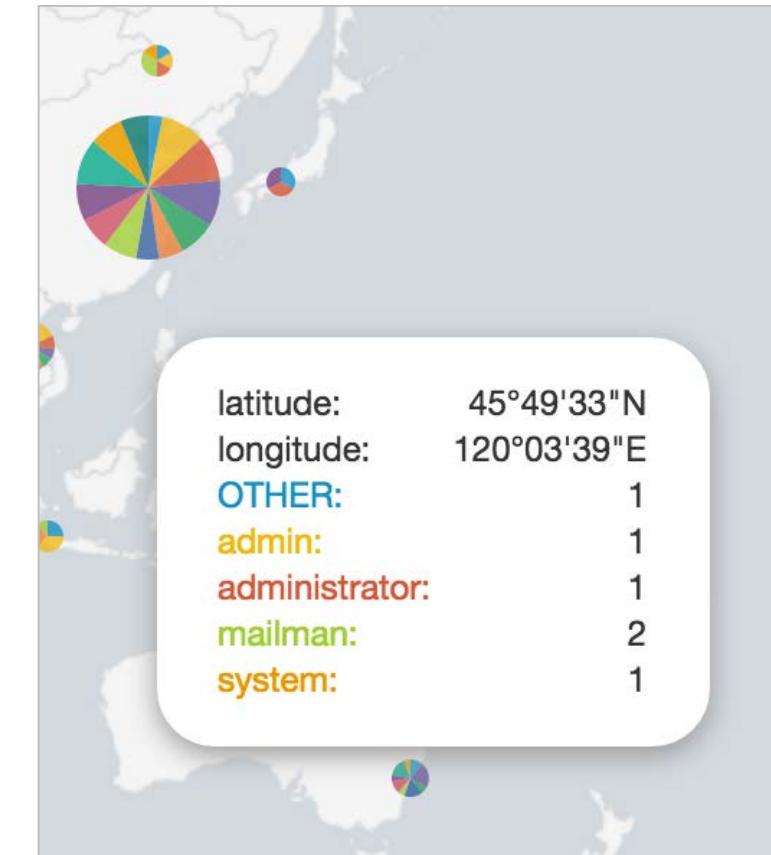
- Data must include latitude and longitude values
- Define the *Latfield* and *Longfield* only if they differ from the default lat and lon fields
- To control the column count:
  - On a global level, use the **globallimit** argument
  - On a local level, depending on where your focus is (i.e., where you've zoomed in), use the **locallimit** argument

# geostats Command – Example

Scenario ?

Map the users of failed actions on the network worldwide during the last 24 hours.

```
index=security sourcetype=linux_secure  
(fail* OR invalid)  
| iplocation src_ip  
| geostats globallimit=5 count by user
```

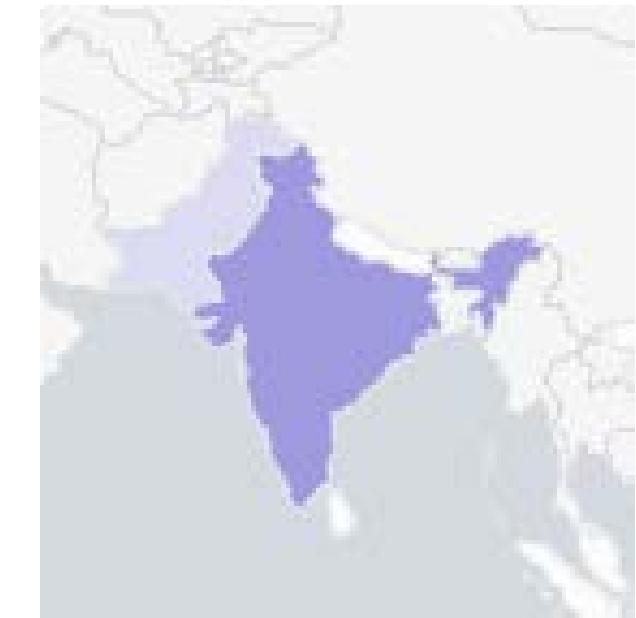


geobin	latitude	longitude	OTHER	admin	administrator	email	irc	jabber	mail	mailman
bin_id_zl_0_y_2_x_2	-28.09581	-57.44188	1	3		1		1	2	1
bin_id_zl_0_y_2_x_4	-29.00000	24.00000		1						1
bin_id_zl_0_y_2_x_6	-27.00000	133.00000	1		1			1	1	
bin_id_zl_0_y_2_x_7	-33.86660	151.20820	2			4	1		3	1

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Choropleth Map

- Uses shading to show relative metrics, such as sales, network intruders, etc., for predefined geographic regions
- To define regional boundaries, you must have either a:
  - KML (Keyhole Markup Language) file
  - KMZ (compressed Keyhole Markup Language) file
- Splunk ships with:
  - geo\_us\_states, United States
  - geo\_countries, countries of the world



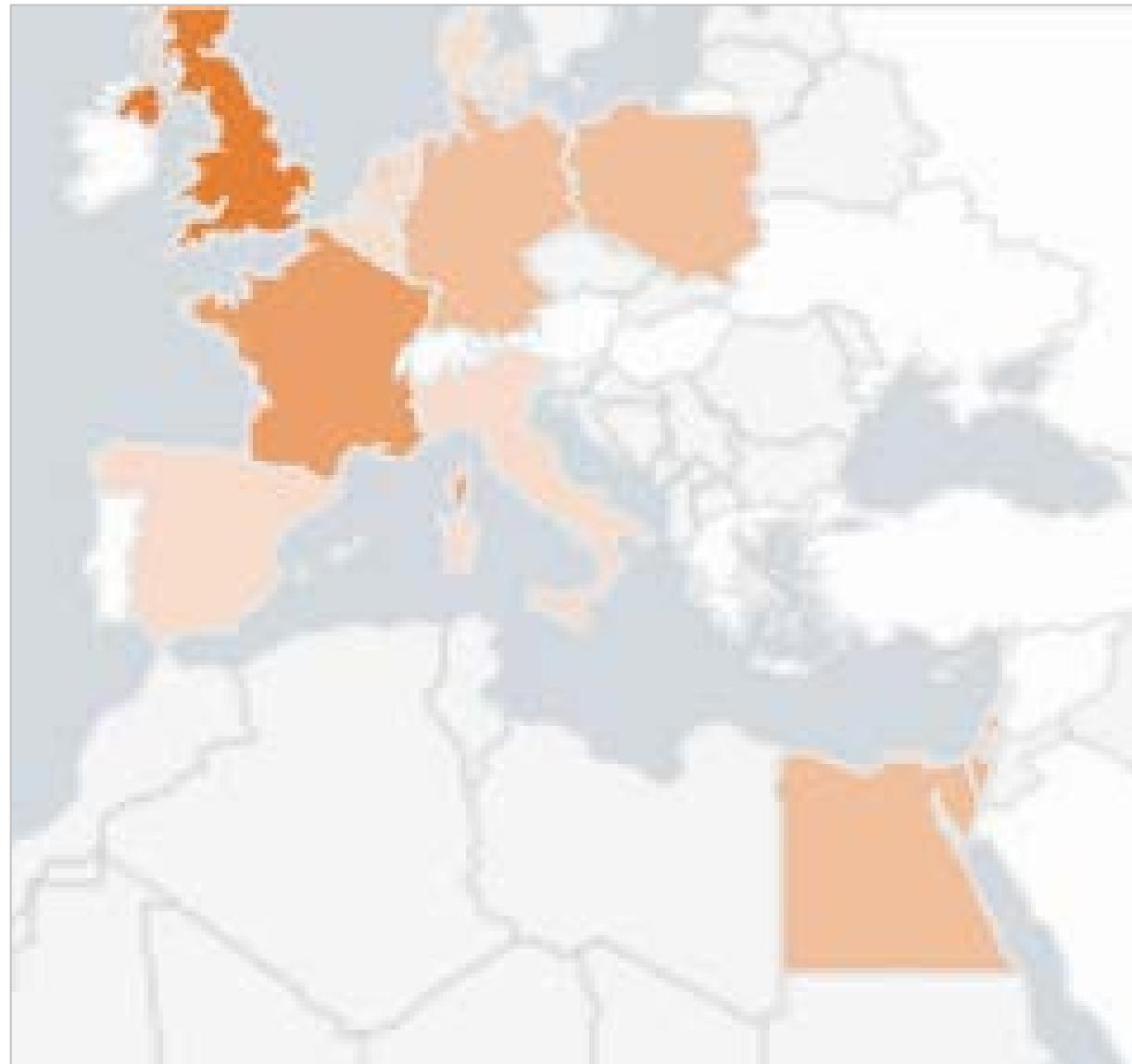
... | geom [*featureCollection*] [*featureIdField*=*string*]

Note

For more information, see Appendix D: Creating New Choropleth Maps

Generated for Subbaiah Kandula ([s.venkata.kandula@accenture.com](mailto:s.venkata.kandula@accenture.com)) (C) Splunk Inc, not for distribution

# geom Command

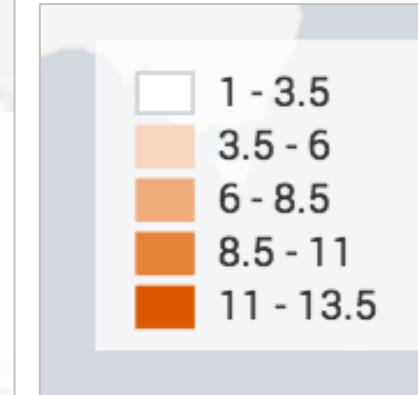


## Scenario



Display the previous week's retail sales in EMEA.

```
index=sales sourcetype=vendor_sales  
VendorID > 4999 AND VendorID < 6000  
| stats count as Sales by VendorCountry  
| geom geo_countries featureIdField=VendorCountry
```



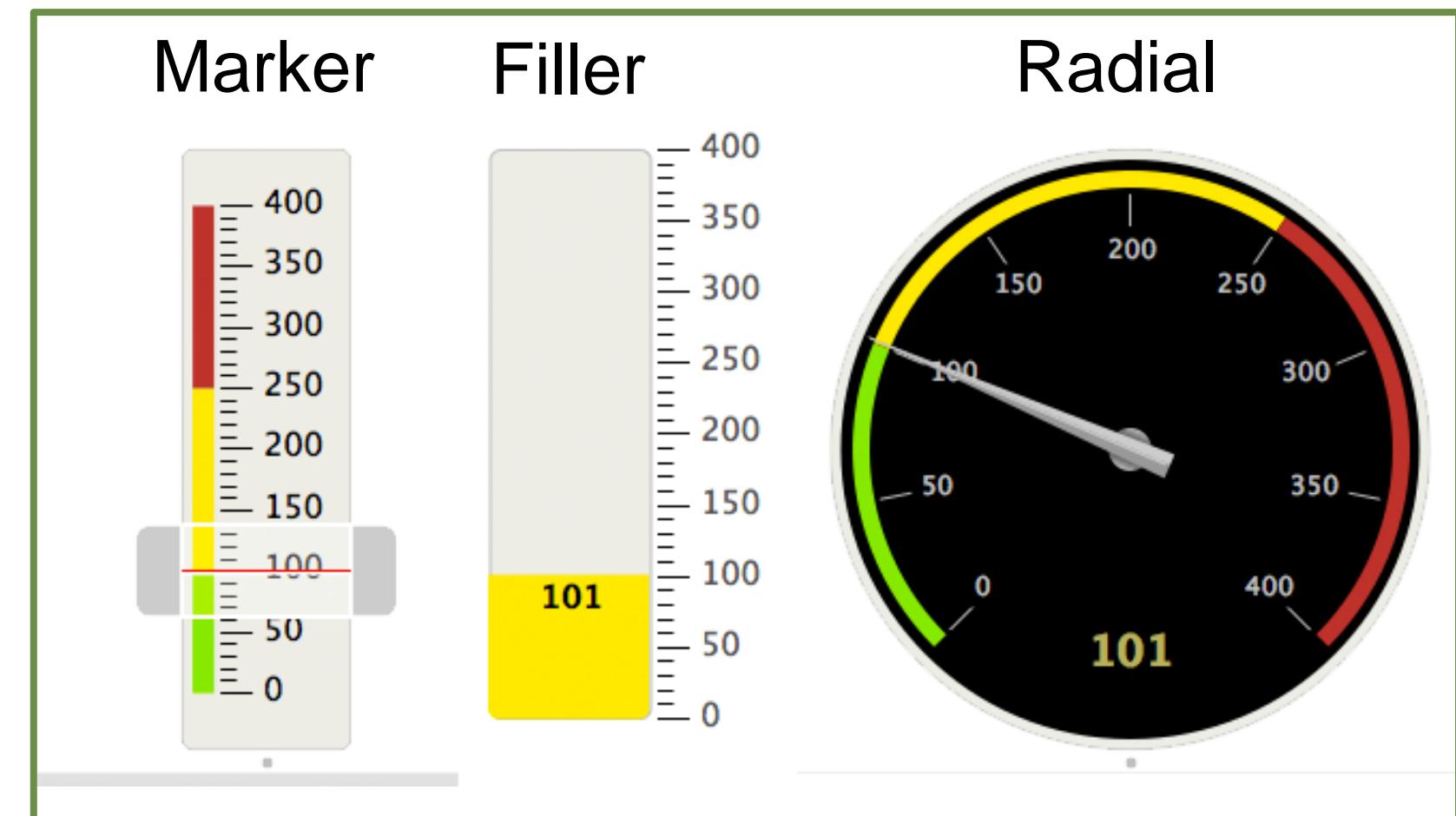
Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Viewing Results as a Single Value

Single value visualizations provide various formatting options

101

```
index=security sourcetype=linux_secure vendor_action=failed  
| stats count
```



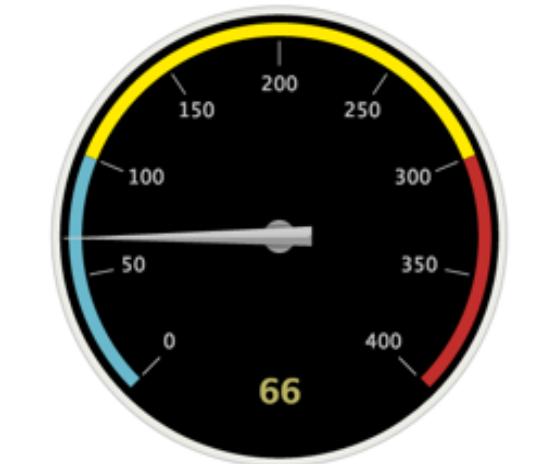
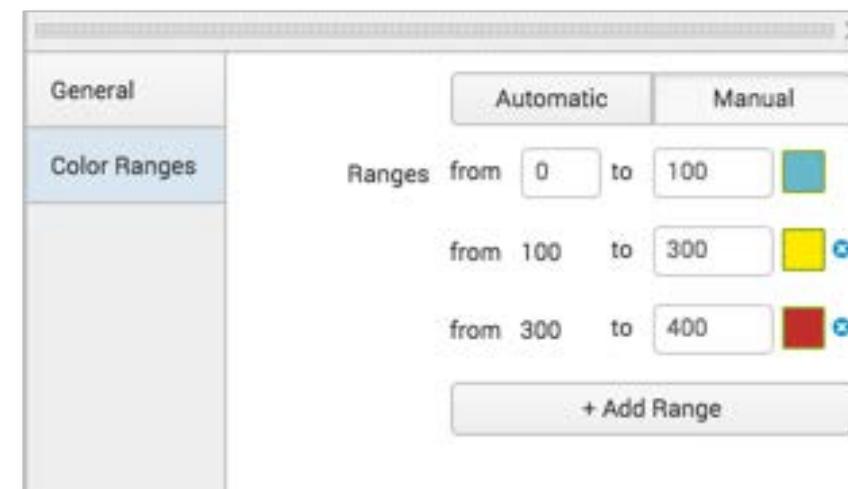
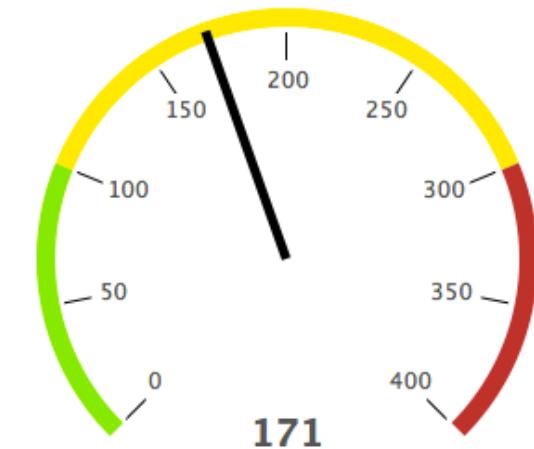
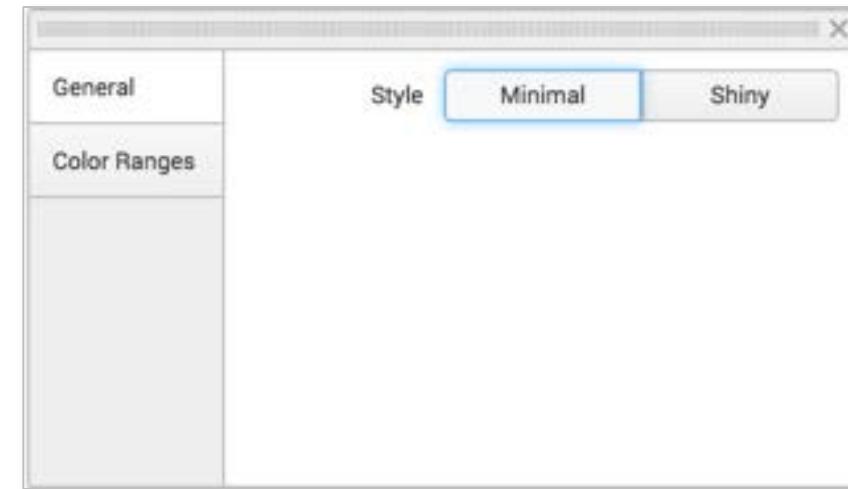
Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Single Value Visualizations: Formatting

Set color using UI or with the gauge command



```
sourcetype=access_combined action=purchase  
| stats sum(price) as count  
| gauge count 0 5000 10000 15000
```



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Single Value Visualizations: Formatting (cont.)

```
index=security sourcetype=linux_secure  
(fail* OR invalid)  
| stats count(vendor_action)
```

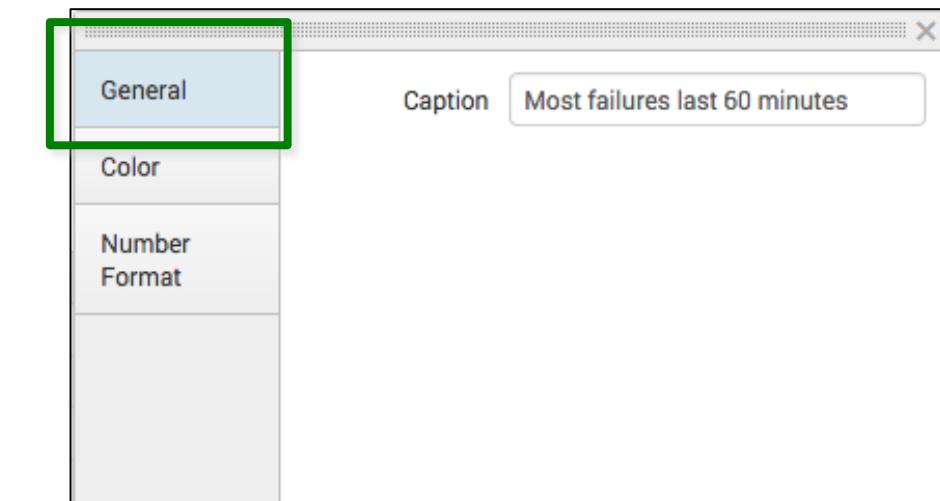
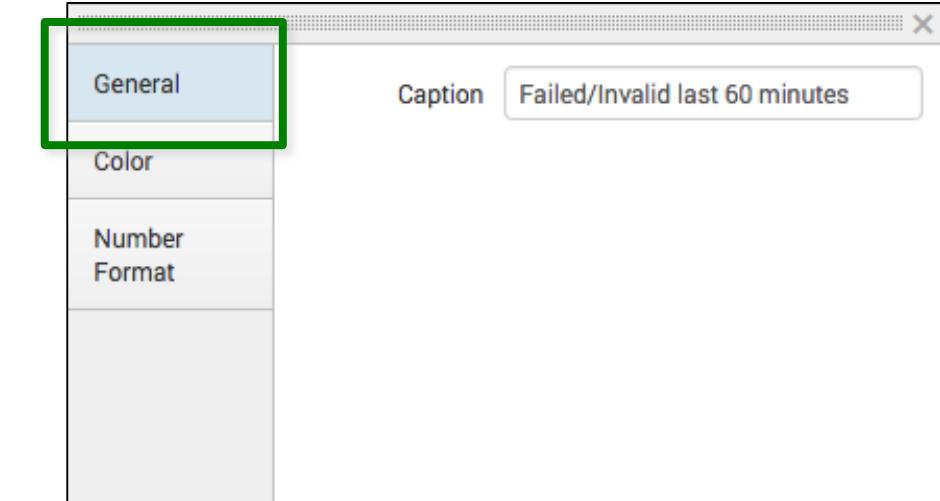
264

Failed/Invalid last 60 minutes

```
index=security sourcetype=linux_secure  
(fail* OR invalid)  
| chart count by src_ip  
| sort -count
```

10.1.10.172

Most failures last 60 minutes



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Single Value Visualizations: Formatting (cont.)

The screenshot shows the Splunk interface for configuring a Single Value visualization. On the left is the configuration pane with tabs for General, Color (highlighted with a green box), and Number Format. Under Color, settings include 'Use Colors' (Yes), 'Color by' (Value), and five color ranges from 0 to 100. On the right is the preview pane showing a large number '9' with the text 'Failed/invalid last 15 minutes' below it. A callout box highlights the search query: `index=security sourcetype=linux_secure (fail* OR invalid) stats count`. A green arrow points from the 'Color' tab in the config pane to the preview pane's title bar.

index=security sourcetype=linux\_secure  
(fail\* OR invalid)  
stats count

To resize the font,  
resize the pane

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Single Value Visualizations: Formatting (cont.)

Optionally, specify number format information for the single value on the **Number Format** tab

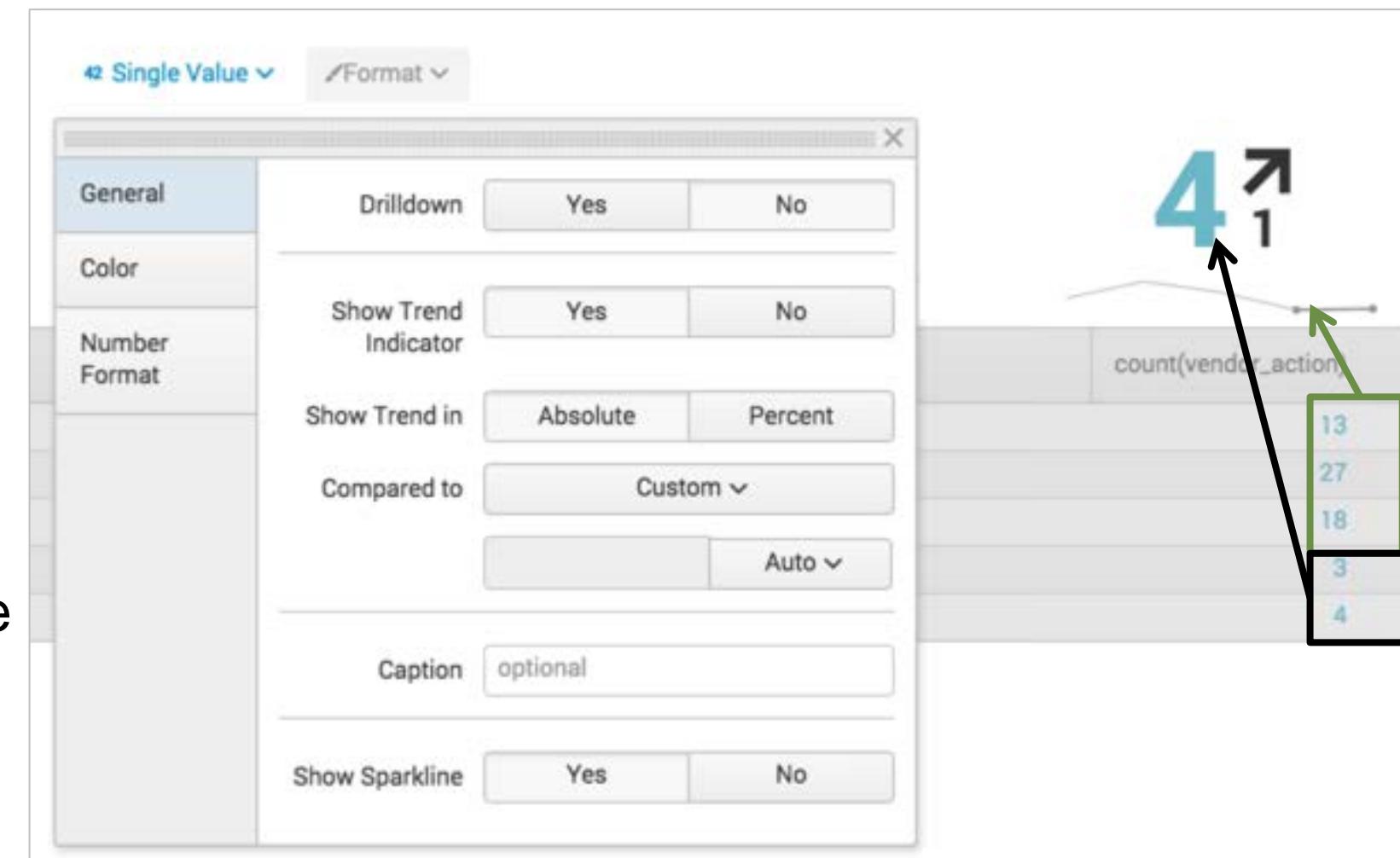
```
index=security sourcetype=linux_secure  
(fail* OR invalid)  
| stats count
```

The screenshot shows the configuration of a Single Value visualization. On the left, a configuration dialog box is open with the title 'Single Value' and a 'Format' dropdown. It contains tabs for 'General', 'Color', and 'Number Format'. The 'Number Format' tab is highlighted with a green border. Inside, there are settings for 'Precision' (set to 0), 'Use Thousand Separators' (set to Yes), 'Unit' (set to 'Events'), and 'Unit Position' (set to 'Before'). To the right of the dialog is a dashboard card titled '6 Events' with the subtitle 'Failed/Invalid last 15 minutes'.

# Single Value Visualizations: timechart

- With the **timechart** command, you can add a sparkline and a trend
- A **sparkline** is an inline chart
  - It is designed to display time-based trends associated with the primary key
- The **trend** shows the direction in which values are moving
  - It appears to the right of the single value

```
index=security sourcetype=linux_secure  
fail* OR invalid  
| timechart span=15m count(vendor_action)
```



# Adding Totals Using Format Options

- Automatically total every column using the Format options
- When using this approach, you:
  - Cannot indicate which column to total; all columns are always totaled
  - Cannot add labels

Scenario ?  
For the last 60 minutes, display the total number of events, with the total and average size (in bytes) by web server. Also, calculate the total bytes.

```
index=web sourcetype=access_combined  
| stats sum(bytes) as Bytes,  
avg(bytes) as avgBytes,  
count as totalEvents by host
```

host	Bytes	avgBytes	totalEvents
www1	268456714	2098.695347	127916
www2	268577676	2100.281333	127877
www3	270164063	2099.894781	128656

host	Bytes	avgBytes	totalEvents
www1	268456714	2098.695347	127916
www2	268577676	2100.281333	127877
www3	270164063	2099.894781	128656
807198453		6298.871461	384449

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

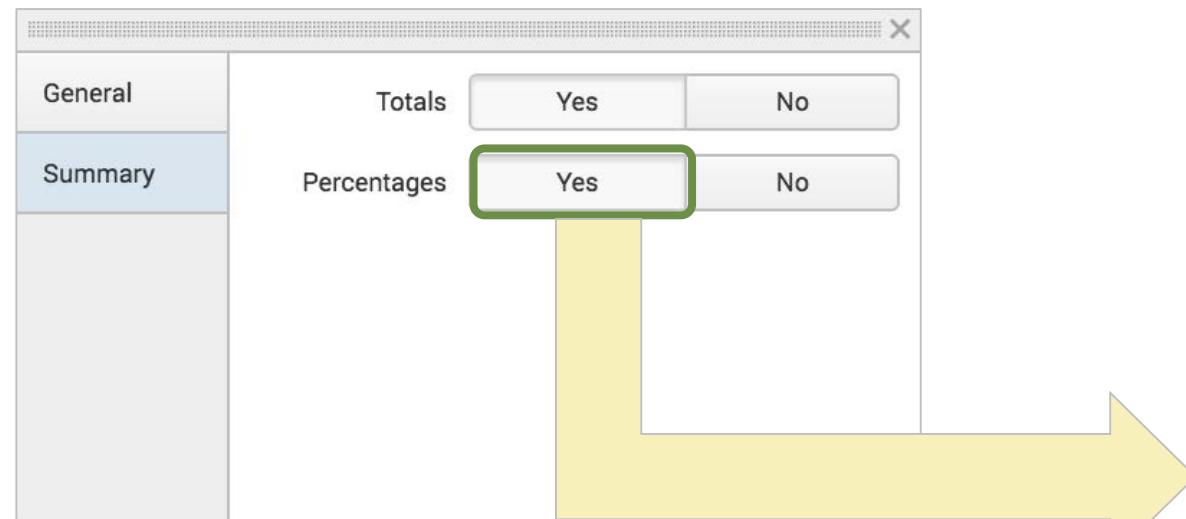
# Adding Totals Using Format Options (cont.)

- Using the **Summary** tab, you can add a % row to the end of the statistics table
- All columns are used to compute the percentage – i.e., all percentages from all columns combined will equal approximately 100%

Scenario ?

Display the retail products sold by country with totals by product and by country during the last 4 hours.

```
index=sales sourcetype=vendor_sales  
| chart count over product_name by VendorCountry
```



product_name	China (PRC)	Morocco	Spain	United States
Manganiello Bros.	0	0	1	0
Manganiello Bros. Tee	1	0	0	0
Mediocre Kingdoms	0	1	0	0
Puppies vs. Zombies	0	0	0	1
	1	1	1	1
	25%	25%	25%	25%

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Adding Totals Using addtotals Command

- Alternatively, use the `addtotals` command to:
  - Compute the sum of all **or selected** numeric fields for each column and place the total in the last row
  - Compute the sum of all **or selected** numeric fields for each **row** and place the total in the last column

product_name	Falkland Islands	United States	Total Per Product
Holy Blade of Gouda	0	1	1
Manganiello Bros. Tee	1	0	1
SIM Cubicle	0	1	1
<b>Total Per Country</b>	<b>1</b>	<b>2</b>	<b>3</b>

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# addtotals Command: Syntax

`addtotals [row=bool] [fieldname=field]  
[col=bool][labelfield=field] [label=string] field-list`

Row Options		Column Options	
<code>row=true/false (Default= true)</code>	A column is created that contains numeric totals for each row.	<code>col=true/false (Default= false)</code>	A row is created that contains numeric totals for each column.
<code>fieldname=<i>field</i> (Default=Total)</code>	Defines a string used to create a field name for the totals column.	<code>label=<i>string</i> (Default=Total)</code>	Defines a string used to name the totals row.
		<code>labelfield=<i>fieldname</i></code>	Defines where the label string is placed. (Generally, you should make this the first column.)

## General Options

`field-list=one or more numeric fields.  
(Default: all numeric fields)`

Defines the numeric fields to be totaled.

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# addtotals Command – Example 1

## Scenario



Calculate the total retail products sold by country totaled by product and by country during the last 60 minutes.

- `row=t` (default) counts the fields in each row under a column named "Total Per Product"
- `col=t` counts the fields in each row in a row named "Total Per Country"

```
index=sales sourcetype=vendor_sales  
| chart count over product_name by VendorCountry  
| addtotals  
  fieldname="Total Per Product" A  
  col=t B  
  label="Total Per Country" labelfield=product_name C
```

product_name	C	Falkland Islands	B	United States	A	Total Per Product
Holy Blade of Gouda		0		1		1
Manganiello Bros. Tee		1		0		1
SIM Cubicle		0		1		1
Total Per Country	C	1		B	2	3

# addtotals Command – Example 2

Scenario ?

For the last 60 minutes, display the total number of events with the total and average size (in bytes) by web server, and then total the bytes.

```
index=web sourcetype=access_combined  
| stats sum(bytes) as Bytes,  
avg(bytes) as avgBytes,  
count as totalEvents by host  
| addtotals row=f A col=t B label=totalBytes C  
labelfield=host D Bytes E
```

- A Do not total rows
- B Total columns
- C Add the label totalBytes
- D Place the label under the host column
- E Only total the Bytes column

D host	B Bytes	avgBytes	totalEvents
www1	108313	1934.160714	56
www2	50608	1946.461538	26
www3	142935	2507.631579	57
C totalBytes	E 301856		

# Module 5: Filtering and Formatting Results

Generated for Subbaiah Kandula ([s.venkata.kandula@accenture.com](mailto:s.venkata.kandula@accenture.com)) (C) Splunk Inc, not for distribution

# Module Objectives

---

- Use the eval command to:
  - Perform calculations
  - Convert values
  - Round values
  - Format values
  - Use conditional statements
- Use the search and where commands to filter calculated results
- Use fillnull command

# eval Command – Overview

---

- eval allows you to calculate and manipulate field values in your report

*eval fieldname = expression*

- Supports a variety of functions
- Results of eval written to either new or existing field you specify
  - If the destination field exists, the values of the field are replaced by the results of eval
  - Indexed data is not modified, and no new data is written into the index
  - Field values are treated in a case-sensitive manner

# eval Command

- The eval command allows you to:
  - Calculate expressions
  - Place the results in a field
  - Use that field in searches or other expressions

Type	Operators
Arithmetic	+ - * / %
Concatenation	+ .
Boolean	AND OR NOT XOR
Comparison	< > <= >= != = == LIKE

## eval

[Learn More ↗](#)

Calculates an expression and puts the resulting value into a field. You can specify to calculate more than one expression.

Example:

... | eval velocity=distance/time

# eval Command – Convert Values

- This example report displays the sum of bytes used for each usage category
- It is difficult to determine how much bandwidth is being used by looking at bytes
- First, use eval to convert the bytes value into megabytes

## Scenario

?

What types of websites used the most bandwidth in bytes during the previous month?

```
index=network sourcetype=cisco_wsa_squid  
| stats sum(sc_bytes) as Bytes by usage
```

usage	Bytes
Borderline	49124524
Business	65789246
Personal	311795818
Unknown	77118759
Violation	2937268

# eval Command – Convert Values (cont.)

- Results of eval must be set to a new or existing field
- In this example:
  - A Calculate the number of bytes for each usage type
  - B Create a new field named bandwidth
  - C Convert the values of the Bytes field into MB by dividing Bytes field values by  $(1024*1024)$

## Scenario



What types of websites used the most bandwidth in megabytes during the previous month?

```
index=network sourcetype=cisco_wsa_squid  
| stats sum(sc_bytes) as Bytes A by usage  
| eval bandwidth B = Bytes/(1024*1024) C
```

usage	A Bytes	B bandwidth
Borderline	49124524	46.848797 C
Business	65789246	62.741514
Personal	311795818	297.351664
Unknown	77118759	73.546180
Violation	2937268	2.801197

# eval Command – Round Values

- The results of Bandwidth are hard to read with so many decimal points
- `round(field/number, decimals)` function sets the value of a field to the number of decimals you specify
- In this example:
  - Divide the value of the Bytes field by  $(1024*1024)$
  - Round the result to two decimal points
  - If the number of decimals is unspecified, the result is a whole number

## Scenario



What types of websites used the most bandwidth in megabytes, rounded to 2 decimal places, during the previous month? Sort by bandwidth.

```
index=network sourcetype=cisco_wsa_squid
| stats sum(sc_bytes) as Bytes by usage
| eval bandwidth = round(Bytes/(1024*1024), 2) A
| sort -bandwidth
| rename bandwidth as "Bandwidth (MB)"
```

usage	Bytes	Bandwidth (MB)
Personal	311795818	297.35 A
Unknown	77118759	73.55
Business	65789246	62.74
Borderline	49124524	46.85
Violation	2937268	2.80

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Removing Fields

- The "Bandwidth (MB)" field has the data in the desired format
- The Bytes field is no longer needed
  - The Bytes field can be removed

## Scenario

What types of websites used the most bandwidth in megabytes, rounded to 2 decimal places, during the previous month? Sort by bandwidth.

```
index=network sourcetype=cisco_wsa_squid  
| stats sum(sc_bytes) as Bytes by usage  
| eval bandwidth = round(Bytes/(1024*1024), 2)  
| sort -bandwidth  
| rename bandwidth as "Bandwidth (MB)"  
| fields - Bytes A
```

usage	Bandwidth (MB)
Personal	297.35
Unknown	73.55
Business	62.74
Borderline	46.85
Violation	2.80

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# eval Command – Calculating Values

You can perform mathematical functions against fields with numeric field values

- A In this example, stats calculates the total list price and total sale price by product\_name
- B eval calculates the discount percentage and formats the discount field

## Scenario



Calculate total online sales for last week, include price, sales price, and discount percentage. Sort by descending discount value.

```
index=web sourcetype=access_combined product_name=*  
action=purchase  
A | stats sum(price) as tp, sum(sale_price) as tsp by product_name  
B | eval Discount = round(((tp - tsp)/ tp)*100)  
| sort -Discount  
| eval Discount = Discount.%"  
| rename tp as "Total List Price", tsp as "Total Sale Price",  
product_name as Product
```

Product	Total List Price	Total Sale Price	Discount
Puppies vs. Zombies	528.94	210.94	60%
Fire Resistance Suit of Provolone	686.28	342.28	50%
Holy Blade of Gouda	706.82	352.82	50%
Dream Crusher	6398.40	3998.40	38%
Manganiello Bros.	5598.60	3498.60	38%

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# eval Command – Calculating Values (cont.)

- C sort lists the highest discounted items first
- D eval converts Discount to a string and concatenates the % character
- E rename provides user friendly headings

## Scenario



Calculate total online sales for last week, include price, sales price, and discount percentage. Sort by descending discount value.

```
index=web sourcetype=access_combined product_name=*
action=purchase
stats sum(price) as tp, sum(sale_price) as tsp by product_name
eval Discount = round(((tp - tsp)/ tp)*100)
sort -Discount
eval Discount = Discount.,"%"
rename tp as "Total List Price", tsp as "Total Sale Price",
product_name as Product
```

C  
D  
E

Product	Total List Price	Total Sale Price	Discount
Puppies vs. Zombies	528.94	210.94	60%
Fire Resistance Suit of Provolone	686.28	342.28	50%
Holy Blade of Gouda	706.82	352.82	50%
Dream Crusher	6398.40	3998.40	38%
Manganiello Bros.	5598.60	3498.60	38%

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# eval Command – `tostring` Function

- `tostring` converts a numeric field value to a string

```
tostring(field, "option")
```

- Options:

- "commas": applies commas
  - › If the number includes decimals, it rounds to two decimal places
- "duration": formats the number as "hh:mm:ss"
- "hex": formats the number in hexadecimal

## Scenario

How much potential online sales revenue was lost during the previous week, due to 503 server errors?

```
index=web sourcetype=access_combined  
action=purchase status=503  
| stats count(price) as NumberOfLostSales, A  
    avg(price) as AverageLostSales,  
    sum(price) as TotalLostRevenue  
| eval AverageLostSales =  
    "$" + tostring(AverageLostSales, "commas") B  
| eval TotalLostRevenue =  
    "$" + tostring(TotalLostRevenue, "commas") C
```

NumberOfLostSales	AverageLostSales	TotalLostRevenue
A 124	\$22.35	B \$2,771.76 C

# tostring Function – duration Option

This example shows "duration" option of `tostring` function

- A stats calculates `sessionTime` for each session (`JSESSIONID`)
  - Use the `range` function to return the difference between the max and min values of `_time`
- B `sort 5` displays the top 5 most frequent values
- C The `duration` option formats the time as "hh:mm:ss"

## Scenario



Identify the five longest client sessions over the last 4 hours in HH:MM:SS format.

```
index=web sourcetype=access_combined  
| stats range(_time) as sessionTime by JSESSIONID A  
| sort 5 -sessionTime B  
| eval duration = tostring(sessionTime,"duration") C
```

A	JSESSIONID	A	sessionTime	duration
	SD9SL2FF8ADFF4961		145	00:02:25 C
	SD3SL1FF2ADFF4955		143	00:02:23
B	SD2SL6FF10ADFF4965		135	00:02:15
	SD1SL5FF10ADFF4954		134	00:02:14
	SD8SL5FF6ADFF4955		125	00:02:05

# Formatting and Sorting Values

- eval with added characters converts numeric field values to strings
- To order numerically, first sort, then use eval

```
index=web sourcetype=access_combined price=*
| stats values(price) as price by product_name
| eval price = "$".price
| sort -price
```

```
index=web sourcetype=access_combined price=*
| stats values(price) as price by product_name
| sort -price
| eval price = "$".price
```

product_name	price
Manganiello Bros. Tee	\$9.99
World of Cheese Tee	\$9.99
Holy Blade of Gouda	\$5.99
Puppies vs. Zombies	\$4.99
Dream Crusher	\$39.99
Manganiello Bros.	\$39.99
Orvil the Wolverine	\$39.99
Fire Resistance Suit of Provolone	\$3.99

Alpha

product_name	price
Dream Crusher	\$39.99
Manganiello Bros.	\$39.99
Orvil the Wolverine	\$39.99
Benign Space Debris	\$24.99
Final Sequel	\$24.99
Mediocre Kingdoms	\$24.99
World of Cheese	\$24.99
Curling 2014	\$19.99

Numeric

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Multiple eval Commands

Each subsequent command references the results of previous commands

- A Based on the values of `list_price` and `current_sale_price`, calculate the `current_discount` percentage
- B Calculate the `new_discount` value by subtracting 5 from `current_discount`
- C Calculate the `new_sale_price` by applying the `new_discount` percentage

## Scenario



Calculate a new sale price that is 5% less than the current discount percentage, for online sales data over the last hour.

```
index=web sourcetype=access_combined price=*
| stats values(price) as list_price, values(sale_price)
  as current_sale_price by product_name
| eval current_discount = round((list_price - current_sale_price)/list_price*100,2)
| eval new_discount = (current_discount - 5) A
| eval new_sale_price = list_price - (list_price * (new_discount/100)) B C
```

product_name	list_price	current_sale_price	current_discount	new_discount	new_sale_price
Benign Space Debris	24.99	19.99	20.01	15.01	21.24
Curling 2014	19.99	16.99	15.01	10.01	17.99
Dream Crusher	39.99	24.99	37.51	32.51	26.99
Final Sequel	24.99	16.99	32.01	27.01	18.24

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# eval Command – if Function Syntax

---

`if(X,Y,Z)`

- The `if` function takes three arguments
- The first argument, `X`, is a Boolean expression
  - If it evaluates to TRUE, the result evaluates to the second argument, `Y`
  - If it evaluates to FALSE, the result evaluates to the third argument, `Z`
- Non-numeric values must be enclosed in "double quotes"
- Field values are treated in a case-sensitive manner

# eval Command – if Function Example

## Scenario

Display retail sales for the previous week, broken down by Asia and the Rest of the World.

```
index=sales sourcetype=vendor_sales  
| eval SalesTerritory =  
| if((VendorID >= 7000 AND VendorID < 8000), "Asia", "Rest of the World")  
| stats sum(price) as TotalRevenue by SalesTerritory  
| eval TotalRevenue = "$" + tostring(TotalRevenue, "commas")
```

- Create a new field, **SalesTerritory**
- Evaluate **VendorID**
  - If  $\geq 7000$  AND  $< 8000$  is TRUE, set result to "Asia"
    - Remember, arguments must be enclosed in quotes
  - If it evaluates to FALSE, set result to "Rest of the World"

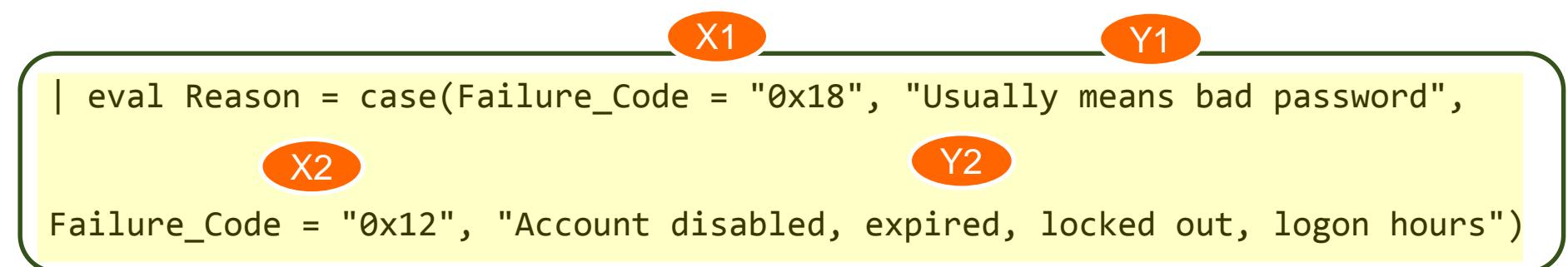
SalesTerritory	TotalRevenue
Asia	\$7,621.32
Rest of the World	\$82,045.11

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# eval Command – case Function

case(X1,Y1,X2,Y2...)

- The first argument,  $X_1$ , is a Boolean expression
- If it evaluates to TRUE, the result evaluates to  $Y_1$
- If it evaluates to FALSE, the next Boolean expression,  $X_2$ , is evaluated, etc.
- If you want an “otherwise” clause, just test for a condition you know is true at the end (e.g.,  $0=0$ )



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# eval function

- To count the number of events that contain a specific field value, use the count and eval functions
  - Used within a transforming command, such as stats
  - Requires an as clause
  - Double quotes are required for character field values
  - Field values are case-sensitive

## Scenario

Count the number of events that occurred yesterday where the vendor action was Accepted, Failed, or session opened.

```
index=security sourcetype=linux_secure vendor_action=*  
| stats  
count(eval(vendor_action="Accepted")) as Accepted, A  
count(eval(vendor_action="Failed")) as Failed, B  
count(eval(vendor_action="session opened")) as SessionOpened C
```

Accepted	Failed	SessionOpened
A 297	B 6237	C 404

# Filtering Results – search and where

---

- The search and where commands can be used at any point in the search pipeline to filter results
  - search
    - May be easier if you're familiar with basic search syntax
    - Treats field values in a case-insensitive manner
    - Allows searching on keyword
  - where
    - Can compare values from two different fields
    - Functions are available, such as `isnotnull()`
    - Field values are case-sensitive

# search Command

- To filter results, use search at any point in the search pipeline
- Behaves exactly like search strings before the first pipe
  - Uses the "\*" wildcard
  - Treats field values in a case-insensitive manner

## Scenario



Report which products during the last 24 hours have sold more than \$500 online.

```
index=web sourcetype=access_combined  
action=purchase status=200  
| stats sum(price) as sales by product_name  
| search sales>500 A  
| sort -sales  
| eval sales="$"+sales  
| rename sales as "Popular Products",  
product_name as "Product Name"
```

Product Name	Popular Products
Dream Crusher	\$839.79 A
World of Cheese	\$749.70
Mediocre Kingdoms	\$599.76

# where Command

*where eval-expression*

- Uses same expression syntax as eval command
- Uses boolean expressions to filter search results and only keeps results that are True
- Double quoted strings are interpreted as field values
  - Treats field values in a case-sensitive manner
- Unquoted or single-quoted strings are treated as fields

Note



To view all of the functions for where, see:

<http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Where?r=searchtip>

# where Command - Example

- Filters search results using eval expressions
- Used to compare two different fields

## Scenario



Report which days over the previous week have seen more remove actions than change quantity actions.

```
index=web sourcetype=access_combined  
| timechart count(eval(action="changequantity"))  
as changes, count(eval(action="remove")) as removals  
| where removals > changes A
```

_time	changes	removals
2016-07-27	115	A 124
2016-07-30	107	123

# where Command With like Operator

- Can do wildcard searches with where command
- Use (\_) for one character and (%) for multiple characters
- Must use the like operator with wildcards

## Scenario



Report the number of events over the past 24 hours by IP address for a specific range of addresses.

```
index=security sourcetype=linux_secure  
| stats count by src_ip  
| where src_ip like "10.%"
```

src_ip	count
10.1.10.172	1173
10.2.10.163	1038
10.3.10.46	1090

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# fillnull Command

- Use `fillnull` to replace null values in fields
- Use `value=string` to specify string you want displayed instead  
Example: `fillnull value=NULL`
- If no `value=` clause, default replacement value is 0
- Optionally, restrict which field(s) `fillnull` applies to by listing them at end of command  
Example: `fillnull VALUE="N/A" discount refund`

## fillnull

Replaces null values with a specified value.

Example:

`sourcetype="web" | timechart count by host | fillnull value=NULL`

[Learn More](#)

# fillnull Command – Examples

Scenario	?
Evaluate vendor sales by country for the last hour.	

```
index=sales sourcetype= vendor_sales  
| chart sum(price) over product_name by VendorCountry  
| fillnull
```

product_name	Oman	United States
Benign Space Debris	0	24.99
Curling 2014	0	19.99
Dream Crusher	0	39.99
Final Sequel	24.99	0
Fire Resistance Suit of Provolone	0	3.99

```
index=sales sourcetype= vendor_sales  
| chart sum(price) over product_name by VendorCountry  
| fillnull value="No Value"
```

product_name	Oman	United States
Benign Space Debris	No Value	24.99
Curling 2014	No Value	19.99
Dream Crusher	No Value	39.99
Final Sequel	24.99	No Value
Fire Resistance Suit of Provolone	No Value	3.99

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Module 6: Correlating Events

Generated for Subbaiah Kandula ([s.venkata.kandula@accenture.com](mailto:s.venkata.kandula@accenture.com)) (C) Splunk Inc, not for distribution

# Module Objectives

---

- Identify transactions
- Group events using fields
- Group events using fields and time
- Search with transactions
- Report on transactions
- Determine when to use transaction vs. stats

# What is a Transaction?

---

- A transaction is any group of related events that span time
- Events can come from multiple applications or hosts
  - Events related to a single purchase from an online store can span across an application server, database, and e-commerce engine
  - One email message can create multiple events as it travels through various queues
  - Each event in the network traffic logs represents a single user generating a single http request
  - Visiting a single website normally generates multiple http requests
    - HTML, JavaScript, CSS files
    - Flash, Images, etc.

Generated for Subbaiah Kandula ([s.venkata.kandula@accenture.com](mailto:s.venkata.kandula@accenture.com)) (C) Splunk Inc, not for distribution

# transaction Command

- **transaction *field-list***
  - *field-list* can be one field name or a list of field names
  - Events are grouped into transactions based on the values of these fields
  - If multiple fields are specified and a relationship exists between those fields, events with related field values will be grouped into a single transaction

- Common constraints:

maxspan      maxpause      startswith      endswith

**transaction**

Groups events into transactions.

Example:

... | transaction host cookie maxspan=30s maxpause=5s

[Learn More ↗](#)

# Events That Have the Same JSESSIONID

- The log shows a number of events that share the same JSESSIONID value (SD6SL10FF6ADFF4961)

- However, it is difficult to:
  - View the events as a group
  - Gain insight to what is happening with these events
  - Know if there are other events scattered in the results set

Scenario		?
Display customer transactions in the online store during the last 60 minutes.		
<code>index=web sourcetype=access_combined</code>		
>	4/24/16 11:58:25.000 PM	217.132.169.69 - - [24/Apr/2016:23:58:25] "GET /cart.do?action=remove&itemId=EST-17&productId=WC-SH-G04&JSESSIONID=SD6SL10FF6ADFF4961 HTTP 1.1" 200 1661 "http://www.buttercupgames.com/oldlink?itemId=EST-17" "Googlebot/2.1 ( http://www.googlebot.com/bot.html)" 613 <b>JSESSIONID = SD6SL10FF6ADFF4961</b>   host = www1   source = /opt/log/www1/access.log   sourcetype = access_combined
>	4/24/16 11:58:11.000 PM	217.132.169.69 - - [24/Apr/2016:23:58:11] "GET /oldlink?itemId=EST-19&JSESSIONID=SD6SL10FF6ADFF4961 HTTP 1.1" 200 660 "http://www.buttercupgames.com/cart.do?action=view&itemId=EST-19&productId=SC-MG-G10" "Googlebot/2.1 ( http://www.googlebot.com/bot.html)" 807 <b>JSESSIONID = SD6SL10FF6ADFF4961</b>   host = www1   source = /opt/log/www1/access.log   sourcetype = access_combined
>	4/24/16 11:58:03.000 PM	217.132.169.69 - - [24/Apr/2016:23:58:03] "GET /product.screen?productId=WC-SH-G04&JSESSIONID=SD6SL10FF6ADFF4961 HTTP 1.1" 200 1966 "http://www.google.com" "Googlebot/2.1 ( http://www.googlebot.com/bot.html)" 293 <b>JSESSIONID = SD6SL10FF6ADFF4961</b>   host = www1   source = /opt/log/www1/access.log   sourcetype = access_combined

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# transaction Command – Example 1

- The transaction command creates a single event from a group of events
  - The events must share the same value in a specified field
- Transactions can cross multiple tiers – such as web servers, application servers
- For example, you can easily view the events for JSESSIONID SD0SL6FF9ADFF4964

## Scenario



Group together Buttercup Games online store events based on the JSESSIONID value for the last 15 minutes.

```
index=web sourcetype=access_combined  
| transaction JSESSIONID
```

Time	Event
1/28/16 10:53:41.000 PM	87.194.216.51 - - [28/Jan/2016:22:53:41] "POST /oldlink?itemId=EST-19&JSESSIONID=SD0SL6FF9ADFF4964 HTTP/1.1" 200 1937 "http://www.yahoo.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 946
	87.194.216.51 - - [28/Jan/2016:22:53:54] "GET /oldlink?itemId=EST-12&JSESSIONID=SD0SL6FF9ADFF4964 HTTP/1.1" 200 2253 "http://www.buttercupgames.com/oldlink?itemId=EST-12" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 439
	87.194.216.51 - - [28/Jan/2016:22:54:08] "GET /product.screen?productId=SF-BVS-01&JSESSIONID=SD0SL6FF9ADFF4964 HTTP/1.1" 503 1162 "http://www.buttercupgames.com/cart.do?action=remove&itemId=EST-18" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 198
	host = www3   source = /opt/log/www3/access.log   sourcetype = access_combined

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc. not for distribution

# transaction Command – Example 2

- Use the search command at any point in the search pipeline to filter results
- Behaves exactly like search strings before the first pipe
  - search uses the "\*" wildcard and treats field values in a case-insensitive manner
  - status=404 finds the errors
  - highlight highlights the terms you specify

## Scenario



Display transactions that included a 404 error during the last 60 minutes.

```
index=web sourcetype=access_combined  
| transaction JSESSIONID A  
| search status=404  
| highlight JSESSIONID, 404 B
```

1/28/16 10:46:07.000 PM	141.146.8.66 - - [28/Jan/2016:22:46:07] "GET /oldlink?itemId=F4966 HTTP 1.1" 505 214 "http://www.buttercupgames.com" "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)" 410
	141.146.8.66 - - [28/Jan/2016:22:46:11] "GET /oldlink?itemId=F4966 HTTP 1.1" 200 1872 "http://www.buttercupgames.com/cart.action?remove&itemId=EST-7&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)" 840
	141.146.8.66 - - [28/Jan/2016:22:46:17] "GET /hidden/anna_nicole.hADFF4966 HTTP 1.1" 404 3258 "http://www.buttercupgames.com/product.screen?productId=SF-BV5-01" "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)" 555
	141.146.8.66 - - [28/Jan/2016:22:46:24] "GET /category.screen?categoryId=D55L4FF4ADFF4966 HTTP 1.1" 503 1731 "http://www.buttercupgames.com/oldlink?itemId=EST-14" "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)" 648
	host = www1   source = /opt/log/www1/access.log   sourcetype = access_combined

# transaction Command – Example 3

## Scenario

For failed network logins, display different users from the same IP during the last 60 minutes.



```
index=security sourcetype=linux_secure failed  
| transaction src_ip
```

#	Time	Event
>	2/9/16 7:37:58.000 PM	Feb 09 19:37:58 bcg-payroll sshd[17403]: Failed password for invalid user vpopmail from 175.45.176.98 port 52722 ssh2 Feb 09 19:46:57 bcg-payroll sshd[14883]: Failed password for invalid user guest from 175.45.176.98 port 34412 ssh2 host = www1   source = /opt/log/www1/auth.nix   sourcetype = linux_secure
>	2/9/16 7:16:24.000 PM	Feb 09 19:16:24 bcg-fileserver sshd[9974]: Failed password for invalid user brooke from 41.32.0.85 port 58580 ssh2 Feb 09 19:18:11 bcg-fileserver sshd[10033]: Failed password for invalid user bruno from 41.32.0.85 port 53132 ssh2 Feb 09 19:22:36 bcg-fileserver sshd[10049]: Failed password for invalid user ftp from 41.32.0.85 port 33206 ssh2 Feb 09 19:33:28 bcg-fileserver sshd[10053]: Failed password for invalid user angel from 41.32.0.85 port 33572 ssh2 Feb 09 19:42:09 bcg-fileserver sshd[7653]: Failed password for invalid user addicted from 41.32.0.85 port 35502 ssh2 host = www1 host = www2 host = www3   source = /opt/log/www1/auth.nix source = /opt/log/www2/auth.nix source = /opt/log/www3/auth.nix   sourcetype = linux_secure

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# transaction Command – Specific Fields

---

- The transaction command produces additional fields, such as:
  - duration – the difference between the timestamps for the first and last event in the transaction
  - eventcount – the number of events in the transaction

# transaction Command – maxspan/maxpause

- You can also define a max overall time span and max gap between events

- **maxspan=10m**

- ▶ Maximum total time between the *earliest* and *latest* events
  - ▶ If not specified, default is -1 (or no limit)

- **maxpause=1m**

- ▶ Maximum total time *between* events
  - ▶ If not specified, default is -1 (or no limit)

## Note

Assumptions: Transactions spanning more than 10 minutes with the same client IP are considered unrelated. Also, there can be no more than one minute between any two related events.

## Scenario

Display customer actions on the website during the last 4 hours.

```
index=web sourcetype=access_combined  
| transaction clientip maxspan=10m maxpause=1m  
| eval duration = tostring(duration,"duration")  
| sort -duration  
| table clientip duration action  
| rename clientip as "Client IP",  
| action as "Client Actions"
```

Client IP	duration	Client Actions
203.223.0.20	00:02:49	addtocart purchase remove view
198.228.212.52	00:02:41	addtocart view
195.2.240.99	00:02:35	addtocart purchase view

# transaction Command - startswith/endswith

- To form transactions based on terms, field values, or evaluations, use `startswith` and `endswith` options
- In this example:

- The first event in the transaction includes `addtocart`
- The last event includes `purchase`

## Scenario



Determine the length of time spent to do a purchase by customers in the online store, over the last 24 hours.

```
index=web sourcetype=access_combined  
| transaction clientip JSESSIONID  
  startswith=eval(action="addtocart")  
  endswith=eval(action="purchase")  
| table clientip, JSESSIONID, duration, eventcount
```

clientip	JSESSIONID	duration	eventcount
195.216.243.24	SD5SL8FF6ADFF4954	1	2
62.216.64.19	SD0SL7FF7ADFF4965	5	2
91.208.184.24	SD10SL1FF5ADFF4960	2	2
58.68.236.98	SD0SL9FF2ADFF4957	4	2

# Investigating with Transactions

- Transactions can be useful when a single event does not provide enough information
- This example searches email logs for the term “REJECT”
- Events that include the term do not provide much information about the rejection

## Scenario



Find emails that were rejected during the last 24 hours.

```
index=network sourcetype=cisco_esa REJECT
```

i	Time	Event
>	1/28/16 11:19:02.000 PM	Thu Jan 28 23:19:02 2016 Info: ICID 744005 REJECT SG BLACKLIST match sbrs[ 10.0: 3.0] SBRS 10.0 host = cisco_router1 source = /opt/log/cisco_router1/cisco_ironport_mail.log sourcetype = cisco_esa
>	1/28/16 10:53:41.000 PM	Thu Jan 28 22:53:41 2016 Info: ICID 744003 REJECT SG BLACKLIST match sbrs[ 10.0: 3.0] SBRS 10.0 host = cisco_router1 source = /opt/log/cisco_router1/cisco_ironport_mail.log sourcetype = cisco_esa
>	1/28/16 9:53:42.000 PM	Thu Jan 28 21:53:42 2016 Info: ICID 744001 REJECT SG BLACKLIST match sbrs[ 10.0: 3.0] SBRS 6.8 host = cisco_router1 source = /opt/log/cisco_router1/cisco_ironport_mail.log sourcetype = cisco_esa
>	1/28/16 9:33:28.000 PM	Thu Jan 28 21:33:28 2016 Info: ICID 743999 REJECT SG BLACKLIST match sbrs[ 10.0: 3.0] SBRS 10.0 host = cisco_router1 source = /opt/log/cisco_router1/cisco_ironport_mail.log sourcetype = cisco_esa

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Investigating with Transactions (cont.)

- By creating a transaction, you can then search and see additional events related to the rejection, such as:
  - IP address of sender
  - Reverse DNS lookup results
  - Action taken by the mail system following the rejection
- **mid** – Message ID
- **dcid** – Delivery Connection ID
- **icid** – Incoming Connection ID

## Scenario

Find emails that were rejected in the last 24 hours.

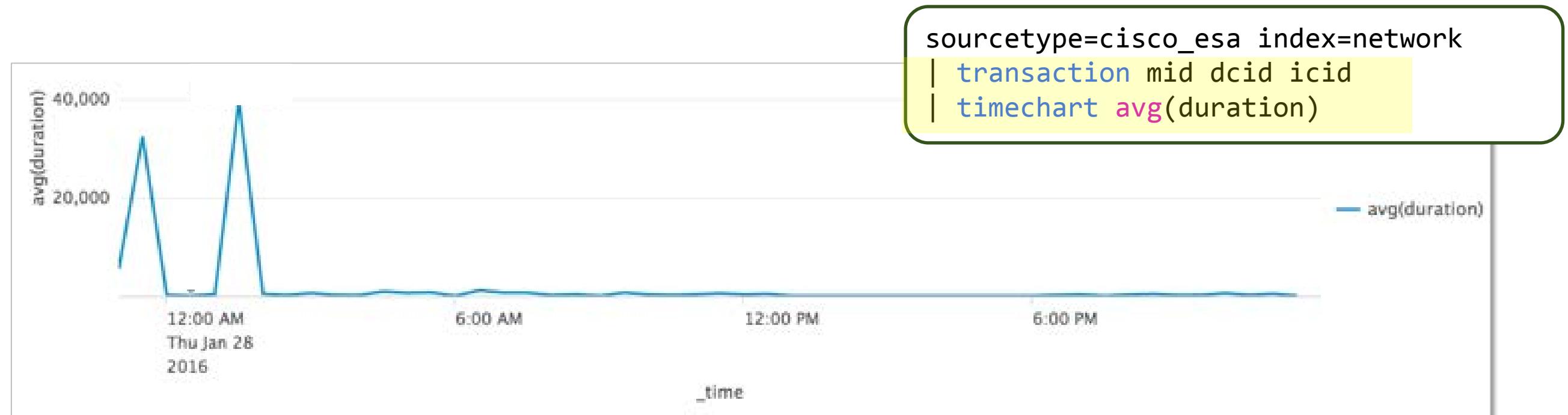
```
sourcetype=cisco_esa index=network  
| transaction mid dcid icid  
| search REJECT
```

I	Time	Event
>	1/27/16 11:24:37.000 PM	Wed Jan 27 23:35:55 2016 Info: New SMTP ICID 743914 interface Management (192.168.3.120) address 85.152.69.78 reverse dns host cm 85 152 69 78.telecable.es verified yes Wed Jan 27 23:36:00 2016 Info: ICID 743914 REJECT SG BLACKLIST match sbrs[ 10.0: 3.0] SBRS 10.0 Wed Jan 27 23:36:08 2016 Info: ICID 743914 close host = cisco_router1 : source = /opt/log/cisco_router1/cisco_ironport_mail.log sourcetype = cisco_esa
>	1/27/16 11:24:37.000 PM	Thu Jan 28 00:36:23 2016 Info: New SMTP ICID 743917 interface Management (192.168.3.120) address 216.102.155.100 reverse dns host adsl 216 102 155 100.dsl.1san03.pacbell.net verified yes Thu Jan 28 00:36:37 2016 Info: ICID 743917 REJECT SG BLACKLIST match sbrs[ 10.0: 3.0] SBRS 10.0 Thu Jan 28 00:36:49 2016 Info: ICID 743917 close host = cisco_router1 : source = /opt/log/cisco_router1/cisco_ironport_mail.log sourcetype = cisco_esa

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc. not for distribution

# Reporting on Transactions

- You can use statistics and reporting commands with transactions
- This example takes advantage of the duration field
  - It shows a trend of the mail queue slowing, then correcting, then slowing again
  - Adding events to the transaction from additional hosts or sources can uncover the cause of the slowdown



Generated for Subbarah Kanoula (s.venkata.kanoula@accenture.com) (C) Splunk Inc. not for distribution

# transaction vs. stats

---

- Use transaction when you:
  - Need to see events correlated together
  - Must define event grouping based on start/end values or chunk on time
  - Have fewer than 1,000 events for each correlated transaction
    - By default, transaction displays a maximum event count of 1,000
    - Admins can configure `max_events_per_bucket` in `limits.conf`
- Use stats when you:
  - Want to see the results of a calculation
  - Can group events based on a field value (e.g. "by `src_ip`")
  - Have more than 1,000 events for each grouped set of events
- When you have a choice, always use stats as it is faster and more efficient, especially in large Splunk environments

# transaction vs. stats: Example 1

A  
index=web  
sourcetype=access\_combined  
earliest=-1y@y latest=@y  
| transaction JSESSIONID  
| table JSESSIONID,  
  action, product\_name  
| sort JSESSIONID

B  
index=web  
sourcetype=access\_combined  
earliest=-1y@y latest=@y  
| stats values(action)  
  as "action",  
  values(product\_name)  
  as "product\_name"  
  by JSESSIONID  
| sort JSESSIONID

Scenario ?

Find online purchase transactions over the past year.

JSESSIONID	action	product_name
SD0SL10FF1ADFF4952		Manganiello Bros. Orvil the Wolverine
SD0SL10FF3ADFF4958	addtocart changequant	Benign Space Debris
SD0SL10FF4ADFF4962	addtocart changequant remove view	Dream Crusher Fire Resistance Suit of Provolone World of Cheese World of Cheese Tee
SD0SL10FF7ADFF4961	addtocart purchase	Puppies vs. Zombies SIM Cubicle World of Cheese

- Searches produce same result
- A took 23.381 seconds
- B took 2.077 seconds
- stats faster than transaction

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# transaction vs. stats: Example 2

A

```
index=security  
sourcetype=linux_secure failed  
| transaction src_ip  
| table src_ip, eventcount  
| sort - eventcount
```

Note

1. **transaction** has a limit of 1,000.
2. Count of transactions vs. count of IPs.

B

```
index=security  
sourcetype=linux_secure failed  
| stats count as eventcount  
| by src_ip  
| sort - eventcount
```

src_ip	eventcount
10.2.10.163	1000
10.3.10.46	991
10.1.10.172	866
87.194.216.51	132
10.2.10.163	81
95.163.78.227	79
88.12.32.208	63

- A took 6.163 seconds
- B took 4.643 seconds

src_ip	eventcount
10.2.10.163	1081
10.3.10.46	998
10.1.10.172	866
87.194.216.51	132
95.163.78.227	79
88.12.32.208	63
107.3.146.207	59

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Module 7: Introduction to Knowledge Objects

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Module Objectives

---

- Identify the categories of knowledge objects
- Define the role of a knowledge manager
- Identify naming conventions
- Review permissions
- Manage knowledge objects
- Describe the Splunk Common Information Model (CIM)

# What are Knowledge Objects?

- Knowledge objects are tools you use to discover and analyze various aspects of your data
  - **Data interpretation** – Fields and field extractions
  - **Data classification** – Event types
  - **Data enrichment** – Lookups and workflow actions
  - **Normalization** – Tags and field aliases
  - **Datasets** – Data models



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# What are Knowledge Objects? (cont.)

- **Shareable**
  - Can be shared between users
- **Reusable**
  - Persistent objects that can be used by multiple people or apps, such as macros and reports
- **Searchable**
  - Since the objects are persistent, they can be used in a search

Note

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

# What is a Knowledge Manager?

---

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

# Defining Naming Conventions

- This course uses simple names for lab exercises, but using a naming convention in your production environment is recommended. For example:
  - **Group:** Corresponds to the working group(s) of the user saving the object (examples: SEG. NEG. OPS. NOC)
  - **Object Type:** Indicates the type of object (alert, report, summary-index-populating) (examples: Alert, Report, Summary)
  - **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.
- So, for example: **SEG\_Alert\_WinEventlogFailures**

Note

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

# Reviewing Permissions

	Description	Create	Read	Edit (write)
<b>Private</b>	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
<b>This app only</b>	Object persists in the context of a specific app	Power Admin	User* Power* Admin	User* Power* Admin
<b>All apps</b>	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

# Reviewing Permissions (cont.)

- When an object is created, the permissions are set to **Keep private** by default
- When an object's permissions are set to **This app only** and **All apps**, all roles are given read permission. Write permission is reserved for admin and the object creator unless the creator edits permissions
- Only the admin role can promote an object to **All apps**

The screenshot shows two overlapping permission configuration windows for a field extraction named "linux\_secure : EXTRACT-src,port".

**Top Window (Admin permission options):**

- Object should appear in:
  - Keep private
  - This app only (search)
  - All apps
- Permissions table:

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

**Bottom Window (Power user permission options):**

- Object should appear in:
  - Keep private
  - This app only (search)
- Permissions table:

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

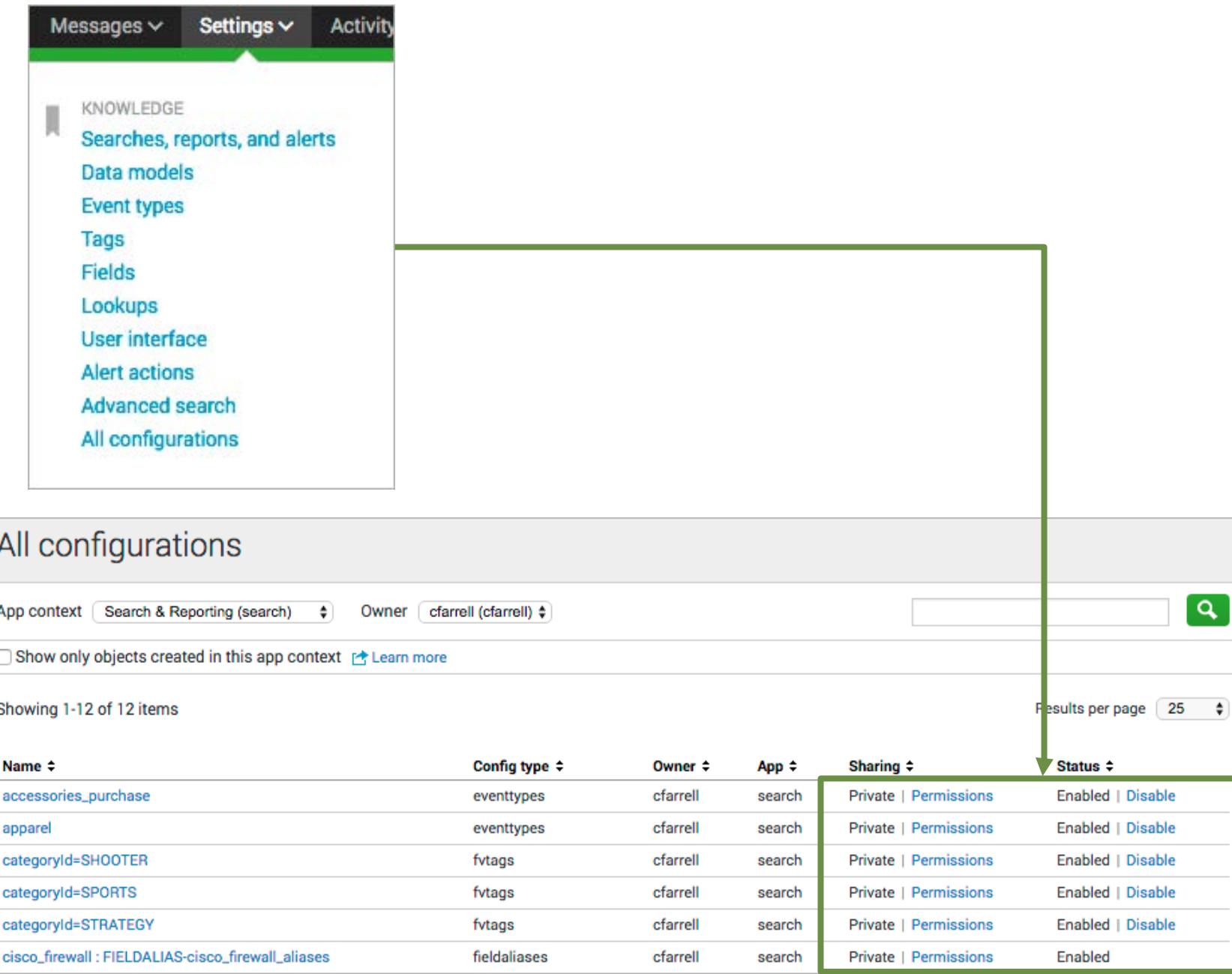
**Buttons:**

- Save button (in the bottom right corner of the bottom window)
- Cancel button (in the bottom left corner of the top window)

# Managing Knowledge Objects

- Knowledge objects are centrally managed from **Settings > Knowledge**
- Your role and permissions determine your ability to modify an object's settings

**Note**   
By default, objects for all owners are listed.



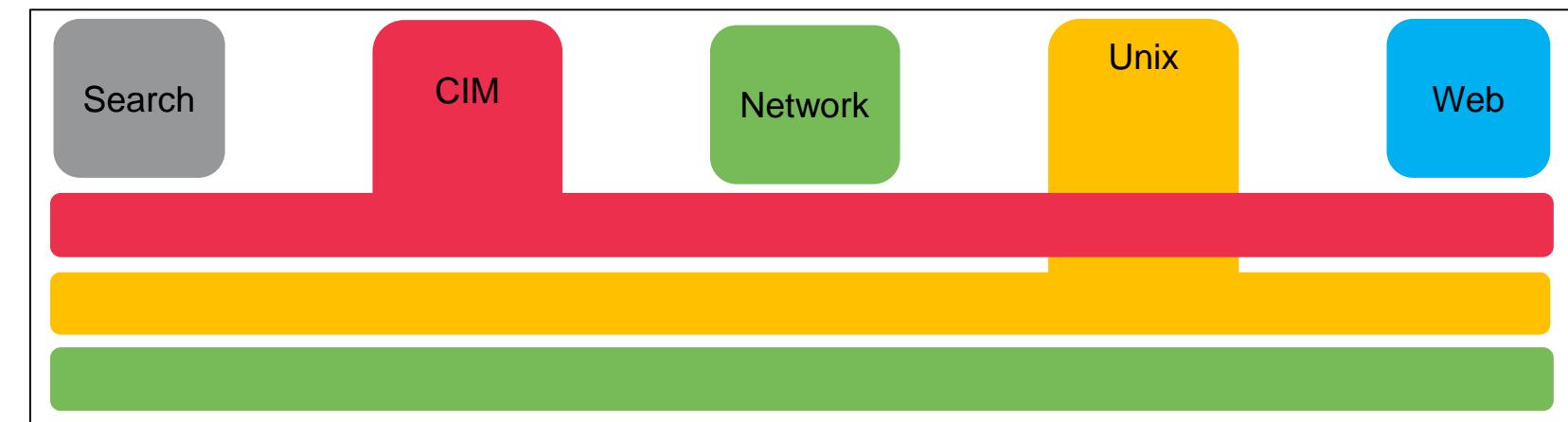
The screenshot shows the Splunk Settings > Knowledge interface. The left sidebar lists various knowledge objects: Searches, reports, and alerts; Data models; Event types; Tags; Fields; Lookups; User interface; Alert actions; Advanced search; and All configurations. The main pane displays the 'All configurations' page, which lists 12 items. The columns include Name, Config type, Owner, App, Sharing, and Status. A green box highlights the 'Sharing' and 'Status' columns. A green arrow points from the 'All configurations' heading down to the highlighted columns.

Name	Config type	Owner	App	Sharing	Status
accessories_purchase	eventtypes	cfarrell	search	Private   Permissions	Enabled   Disable
apparel	eventtypes	cfarrell	search	Private   Permissions	Enabled   Disable
categoryId=SHOOTER	fvtags	cfarrell	search	Private   Permissions	Enabled   Disable
categoryId=SPORTS	fvtags	cfarrell	search	Private   Permissions	Enabled   Disable
categoryId=STRATEGY	fvtags	cfarrell	search	Private   Permissions	Enabled   Disable
cisco_firewall : FIELDALIAS-cisco_firewall_aliases	fieldaliases	cfarrell	search	Private   Permissions	Enabled

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Using the Splunk Common Information Model (CIM)

- Methodology for normalizing data
- Easily correlate data from different sources and source types
- Leverage to create various objects discussed in this course—field extractions, field aliases, event types, tags
- More details discussed in Module 13



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Module 8: Creating and Managing Fields

Generated for Subbaiah Kandula ([s.venkata.kandula@accenture.com](mailto:s.venkata.kandula@accenture.com)) (C) Splunk Inc, not for distribution

# Module Objectives

---

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

Generated for Subbaiah Kandula ([s.venkata.kandula@accenture.com](mailto:s.venkata.kandula@accenture.com)) (C) Splunk Inc, not for distribution

# Field Auto-Extraction

---

- Splunk automatically discovers many fields based on source type and key/value pairs found in the data
- Prior to search time, some fields are already stored with the event in the index:
  - Meta fields, such as host, source, and sourcetype
  - Internal fields such as \_time and \_raw
- At search time, *field discovery* discovers fields directly related to the search's results
- Splunk may also extract other fields from raw event data that aren't directly related to the search

# Performing Field Extractions

- In addition to the many fields Splunk auto-extracts, you can also extract your own fields with the Field Extractor (FX)
- Use FX to extract fields that are static and that you use often in searches
  - Graphical UI
  - Extract fields from events using regex or delimiter
  - Extracted fields persist as knowledge objects
  - Can be shared and re-used in multiple searches
- Access FX via Settings, Fields Sidebar, or Event Actions menu

Note

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

# Field Extraction Methods

---

- **Regex**
  - Use this option when your event contains unstructured data like a system log file
  - FX attempts to extract 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 doesn't have headers and the fields must be separated by delimiters (spaces, commas, pipes, tabs, or other characters)

# Field Extraction Workflows - RegEx

Settings

The screenshot shows the Splunk Extract Fields workflow interface. It consists of four sequential steps:

- Select sample:** Shows a dropdown for "Data Type" set to "sourcetype" and a dropdown for "Source Type" with "Select Source Type" highlighted.
- Select method:** Shows a dropdown for "Source type" set to "linux\_secure". Below it, a blue box displays a log event: "Mon Jul 18 2016 17:08:46 www3 sshd[1392]: Failed password for invalid user susan from 10.1.10.172 port 3968 ssh2".
- Select fields:** Shows a "filter" input field and a "raw" dropdown.
- Save:** A "Next >" button.

On the right side of the interface, there are two circular icons with text descriptions:

- Regular Expression:** Represented by a circle containing "(.\*?)".

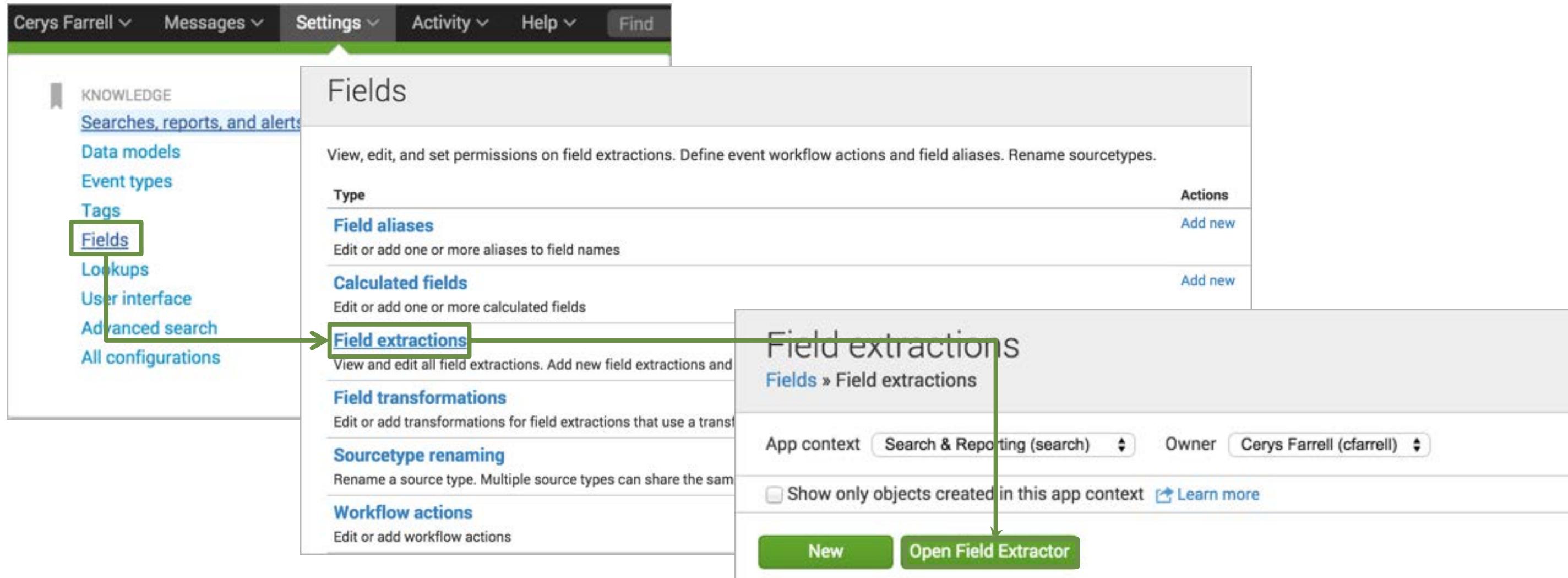
Splunk Enterprise will extract fields using a Regular Expression.
- Delimiters:** Represented by a circle containing "x|y|z".

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 Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Regex Field Extractions from Settings

Settings > Fields > Field extractions > Open Field Extractor



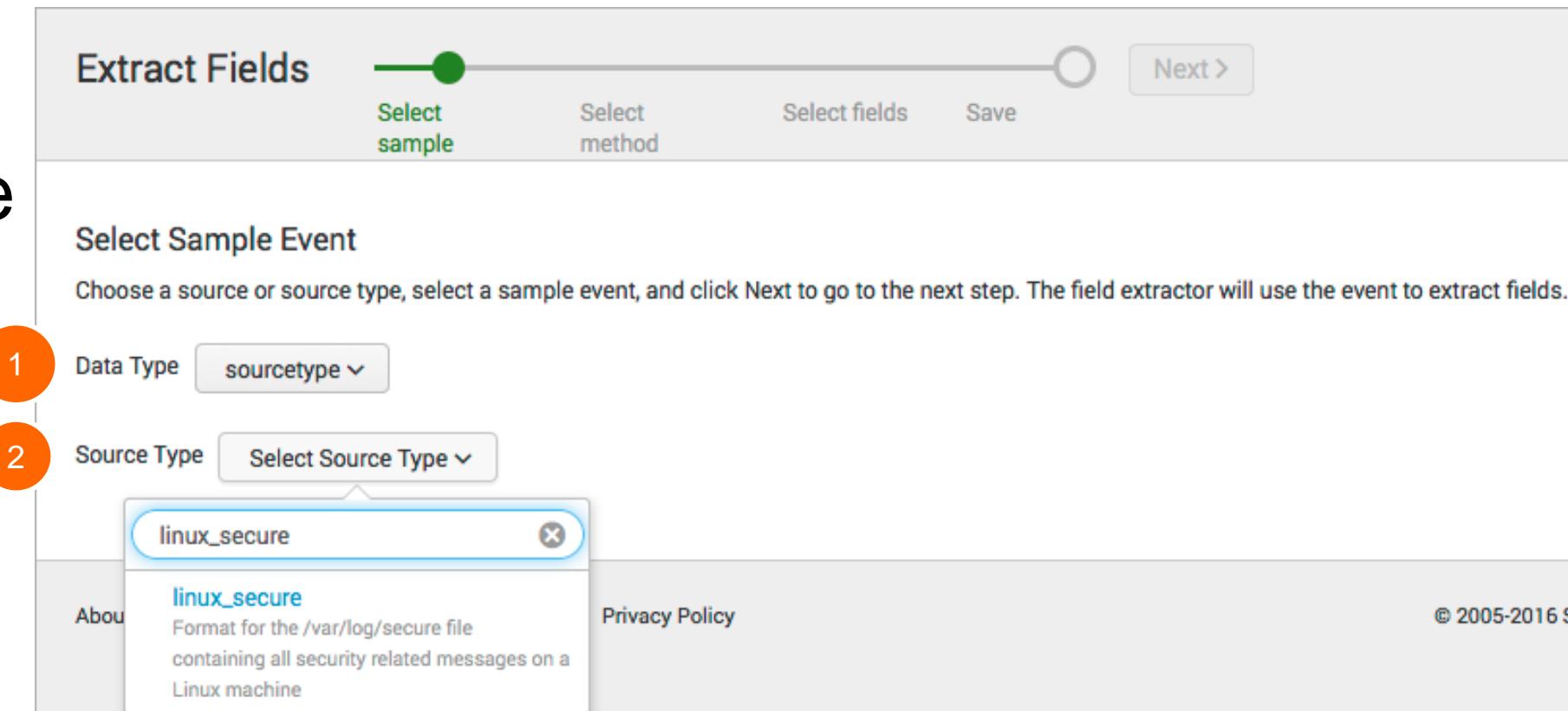
Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Regex Field Extractions from Settings (cont.)

## 1. Select the Data Type

- sourcetype
- source

## 2. Select the Source Type



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Regex Field Extractions from Settings – Select Sample

3. Select a sample event by clicking on it

4. Click **Next >**

The screenshot shows the 'Extract Fields' interface in Splunk. The top navigation bar has tabs: 'Select sample' (which is active and highlighted in green), 'Select method', 'Select fields', and 'Save'. A large orange button labeled 'Next >' is positioned to the right of the tabs. To the far right, there is a link 'Existing fields >'.  
  
The main area is titled 'Select Sample Event'. It contains instructions: '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.' Below this, there is a link 'I prefer to write the regular expression myself >'.  
  
There are two dropdown menus: 'Data Type' set to 'sourcetype' and 'Source Type' set to 'linux\_secure'.  
  
A list of events is displayed, with one event highlighted with a blue background and a white border. The highlighted event is: 'Wed Jul 20 2016 00:18:18 www3 sshd[3589]: Failed password for invalid user library from 199.15.234.66 port 1958 ssh2'. This event is circled with a red number '3'.  
  
Below the event list, there is a summary: '✓ 1,000 events (before 7/19/16 5:18:38.000 PM)'. To the right are buttons for '20 per page', 'Prev', and a page navigation bar showing pages 1 through 9. There are also buttons for 'filter', 'Apply', 'Sample: 1,000 events', and 'All events'.  
  
At the bottom of the event list, there is a section labeled '\_raw' containing three raw log entries:  
- 'Wed Jul 20 2016 00:18:37 www3 sshd[4421]: Failed password for invalid user mailman from 199.15.234.66 port 4809 ssh2'  
- 'Wed Jul 20 2016 00:18:24 www3 sshd[77825]: Accepted password for djohnson from 10.3.10.46 port 7627 ssh2'  
- 'Wed Jul 20 2016 00:18:18 www3 sshd[3589]: Failed password for invalid user library from 199.15.234.66 port 1958 ssh2'  
  
A red circle with the number '4' is drawn around the 'Next >' button.

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Regex Field Extractions from Settings – Select Method

## 5. Select Regular Expression

## 6. Click Next >

Extract Fields

6

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

Source type `linux_secure`

Wed Jul 20 2016 00:18:18 www3 sshd[3589]: Failed password for invalid user library from 199.15.234.66 port 1958 ssh2

5

(.\*?)

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).

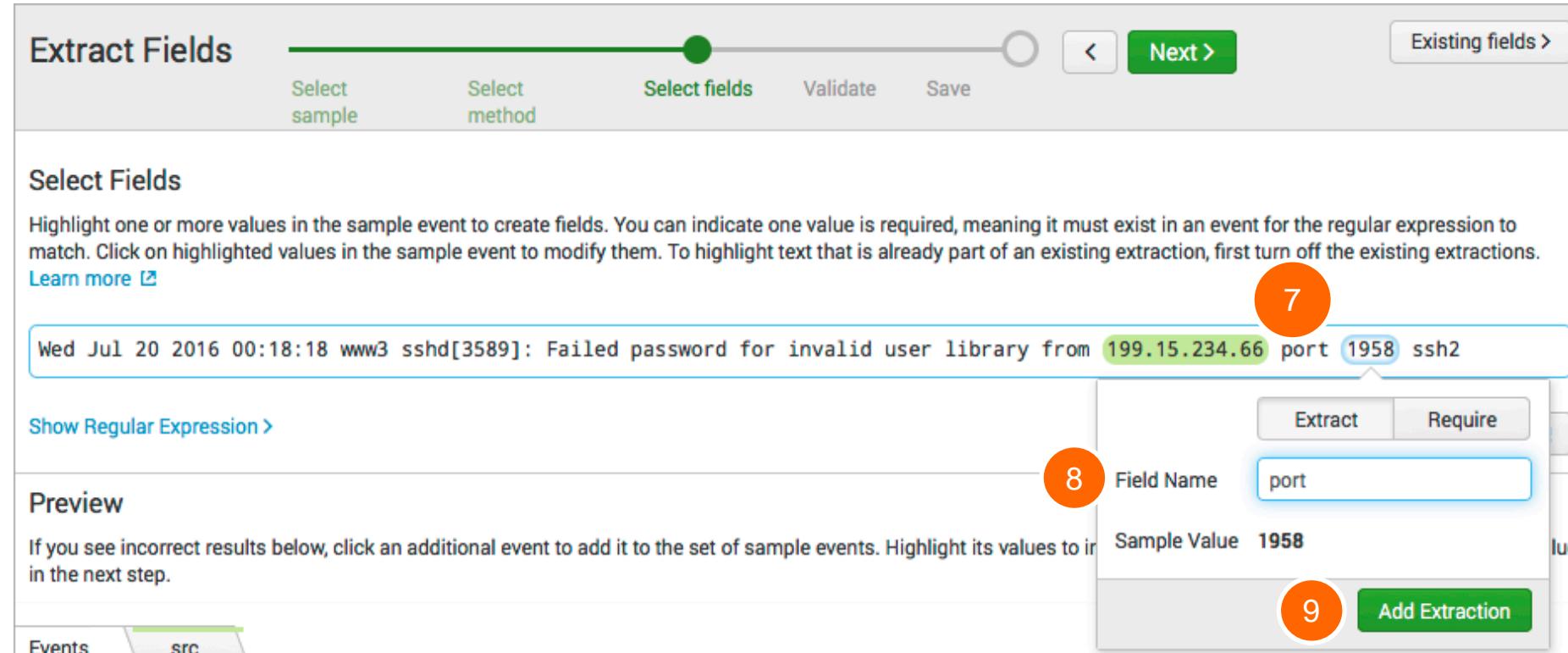
Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Regex Field Extractions from Settings – Select Values

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

**Note** 

Require option – only events with the highlighted string will be included in the extraction.



The screenshot shows the 'Extract Fields' wizard in Splunk. The current step is 'Select fields'. A sample event is displayed: 'Wed Jul 20 2016 00:18:18 www3 sshd[3589]: Failed password for invalid user library from 199.15.234.66 port 1958 ssh2'. The word 'port' is highlighted in green. To the right, there's a preview section and extraction settings. The 'Field Name' is set to 'port' and the 'Sample Value' is '1958'. At the bottom right is a green 'Add Extraction' button. Three orange circles with numbers 7, 8, and 9 are overlaid on the screenshot to indicate the steps in the list above.

# Regex Field Extractions from Settings – Preview

10. Preview the sample events

11. Click **Next**

The screenshot shows the 'Extract Fields' wizard in Splunk. The current step is 'Select fields'. The 'Select sample' and 'Select method' steps have been completed. The 'Select fields' step is highlighted with a green bar. The 'Validate' and 'Save' steps are shown as greyed-out options. An orange circle labeled '11' is positioned over the 'Next >' button.

**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 20 2016 00:18:18 www3 sshd[3589]: Failed password for invalid user library from 199.15.234.66 port 1958 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.

10

Events	src	port												
✓ 1,000 events (before 7/19/16 5:29:05.000 PM)	20 per page ▾	< Prev 1 2 3 4 5 6 7 8 9 ... Next >												
<input type="text" value="filter"/> <button>Apply</button>	<button>Sample: 1,000 events</button> <button>All events</button>	<button>All Events</button> <button>Matches</button> <button>Non-Matches</button>												
<table border="1"><thead><tr><th>_raw</th><th>src</th><th>port</th></tr></thead><tbody><tr><td>✓ Wed Jul 20 2016 00:29:02 mailsv1 sshd[3142]: Failed password for invalid user email from 223.205.219.198 port 4629 ssh2</td><td>223.205.219.198</td><td>4629</td></tr><tr><td>✓ Wed Jul 20 2016 00:28:44 mailsv1 sshd[5697]: Failed password for invalid user operator from 10.2.10.163 port 2888 ssh2</td><td>10.2.10.163</td><td>2888</td></tr><tr><td>✓ Wed Jul 20 2016 00:28:28 mailsv1 sshd[5012]: Failed password for invalid user library from 10.2.10.163 port 4233 ssh2</td><td>10.2.10.163</td><td>4233</td></tr></tbody></table>			_raw	src	port	✓ Wed Jul 20 2016 00:29:02 mailsv1 sshd[3142]: Failed password for invalid user email from 223.205.219.198 port 4629 ssh2	223.205.219.198	4629	✓ Wed Jul 20 2016 00:28:44 mailsv1 sshd[5697]: Failed password for invalid user operator from 10.2.10.163 port 2888 ssh2	10.2.10.163	2888	✓ Wed Jul 20 2016 00:28:28 mailsv1 sshd[5012]: Failed password for invalid user library from 10.2.10.163 port 4233 ssh2	10.2.10.163	4233
_raw	src	port												
✓ Wed Jul 20 2016 00:29:02 mailsv1 sshd[3142]: Failed password for invalid user email from 223.205.219.198 port 4629 ssh2	223.205.219.198	4629												
✓ Wed Jul 20 2016 00:28:44 mailsv1 sshd[5697]: Failed password for invalid user operator from 10.2.10.163 port 2888 ssh2	10.2.10.163	2888												
✓ Wed Jul 20 2016 00:28:28 mailsv1 sshd[5012]: Failed password for invalid user library from 10.2.10.163 port 4233 ssh2	10.2.10.163	4233												

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Regex Field Extractions from Settings – Validate

12. Validate the proper field values are extracted

13. Click Next

The screenshot shows the 'Extract Fields' interface in Splunk. The top navigation bar has tabs: 'Select sample', 'Select method', 'Select fields', 'Validate' (which is highlighted in green), and 'Save'. A progress bar indicates the current step is 'Validate'. A large orange circle highlights the number '13' next to the 'Next >' button. To the right of the button is a link 'Existing fields >'. Below the tabs, a section titled 'Validate' contains instructions: 'Validate your field extractions and remove values that are incorrectly highlighted in the Events tab. In the field tabs, inspect the extracted values for each field, and optionally click a value to apply it as a search filter to the Events tab event list.' There is a 'Show Regular Expression >' link and a 'View in Search' link. A navigation bar below shows tabs for 'Events', 'src', and 'port', with 'src' selected. It also shows '20 per page', page numbers 1-9, and a 'Next >' button. Below this are filters for 'filter' and 'Apply', and buttons for 'Sample: 1,000 events', 'All events', 'All Events', 'Matches', and 'Non-Matches'. The main area displays a table of event logs. The first event is highlighted with a green background for the 'src' field ('223.205.219.198') and an orange background for the 'port' field ('4629'). The event number '12' is circled in red. The table columns are '\_raw', 'src', and 'port'. The event details are: 'Wed Jul 20 2016 00:28:42 mailsrv1 sshd[3142]: Failed password for invalid user email from 223.205.219.198 port 4629 ssh2'. The table continues with other events, such as 'operator' and 'library' users.

_raw	src	port
✓ Wed Jul 20 2016 00:28:42 mailsrv1 sshd[3142]: Failed password for invalid user email from 223.205.219.198 port 4629 ssh2	223.205.219.198	4629
✓ Wed Jul 20 2016 00:28:44 mailsrv1 sshd[5697]: Failed password for invalid user operator from 10.2.10.163 port 2888 ssh2	10.2.10.163	2888
✓ Wed Jul 20 2016 00:28:28 mailsrv1 sshd[5012]: Failed password for invalid user library from 10.2.10.163 port 4233 ssh2	10.2.10.163	4233

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Regex Field Extractions from Settings – Save

14. Review the name for the newly extracted fields and set permissions

15. Click Finish

**Note** 

An extractions name is provided by default. However, this name can be changed.

**Extract Fields**

Save

Name the extraction and set permissions.

Extractions Name EXTRACT-src,port 14

Owner admin

App instructorinfo

Permissions Owner App All apps

Source type linux\_secure

Sample event Wed Jul 20 2016 00:18:18 www3 sshd[3589]: Failed password for invalid user library from 199.15.234.66 port 1958 ssh2

Fields src,port

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

15 Finish >

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Using the Extracted Fields

New Search Save As ▾ Close

```
1 index=security sourcetype=linux_secure  
2 | table src, port
```

Last 24 hours ▼ 🔍

✓ 7,458 events (3/14/17 10:00:00.000 PM to 3/15/17 10:09:43.000 PM) No Event Sampling ▾ Job ▾ II ■ ↗ ✚ ↓ 💡 Smart Mode ▾

Events Patterns Statistics (7,458) Visualization

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

src	port	Count
10.3.10.46		1956
10.3.10.46		4122
10.2.10.163		5035
10.3.10.46		3952
216.221.226.11		4989
216.221.226.11		2616
10.1.10.172		1969
10.1.10.172		4035
70.38.1.235		2232
70.38.1.235		3611

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (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'. A large orange circle labeled '2' is positioned over the 'Next >' button. On the right, there is a link 'Existing fields >'. Below the tabs, the title 'Select Method' is displayed with the instruction: 'Indicate the method you want to use to extract your field(s). [Learn more](#) | [I prefer to write the regular expression myself](#)'. The 'Source type' is set to 'linux\_secure'. A sample log entry is shown in a blue box: 'Tue Jul 26 2016 00:03:36 www3 sshd[2520]: Failed password for invalid user desktop from 87.240.128.18 port 2393 ssh2'. Two options 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 Subbaiah Kandula (s.venkata.kandula@accenture.com) (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/latest/Knowledge/AboutSplunkregularexpressions>

Extract Fields      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](#)

Tue Jul 26 2016 00:03:36 www3 sshd[2520]: Failed password for invalid user **desktop** 3 37.240.128.18 port 2393 ssh2

About    Support    File a Bug    Documentation    Privacy Policy    © 2005-2016 Splunk Inc. All rights reserved.

Field N 4 Extract    Require  
user

Sample Value desktop

5 Add Extraction

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (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 a 'Select Fields' step in a 'Extract Fields' workflow. The main window has tabs for 'Select method', 'Select fields' (which is active), 'Validate', and 'Save'. A green arrow points from the 'Show Regular Expression' button in the left sidebar to the regular expression editor in the bottom right of the main window. The regular expression is: `^\w+\s+\w+\s+\d+\s+\d+:\d+:\d+\s+\w+\d+\s+\w+\[\d+\]:\s+\w+\s+\w+\s+\w+\s+\w+\s+(?P<user>)\w+`. The bottom window shows the event `Tue Jul 26 2016 00:10:33 www1 sshd[5602]: Failed password for invalid user desktop from 74.82.57.172 port 4565 ssh2` with the word `desktop` highlighted.

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Editing Regex for Field Extractions – Modify RegEx

8. Update the regular expression

9. Click **Save**

## Warning



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

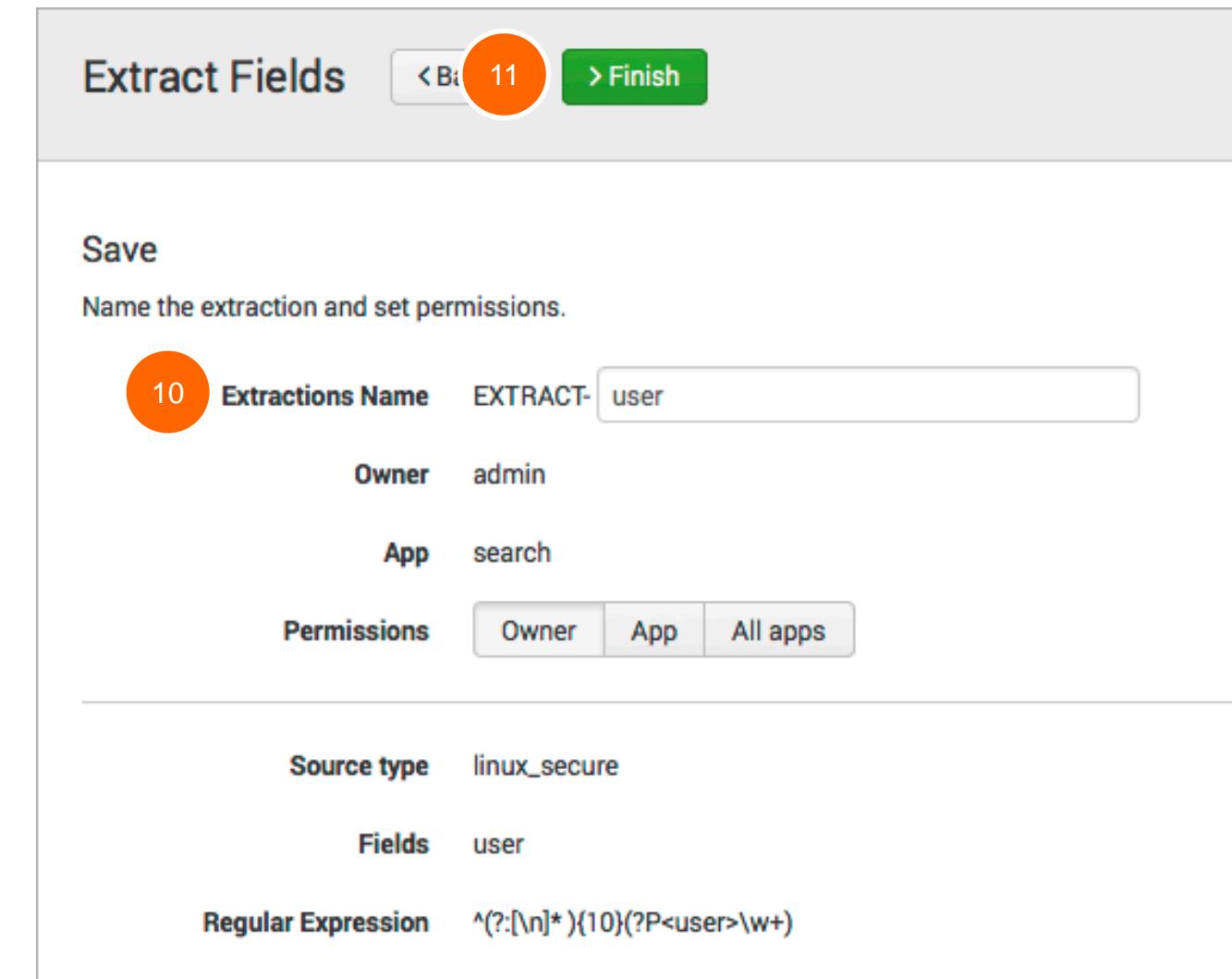
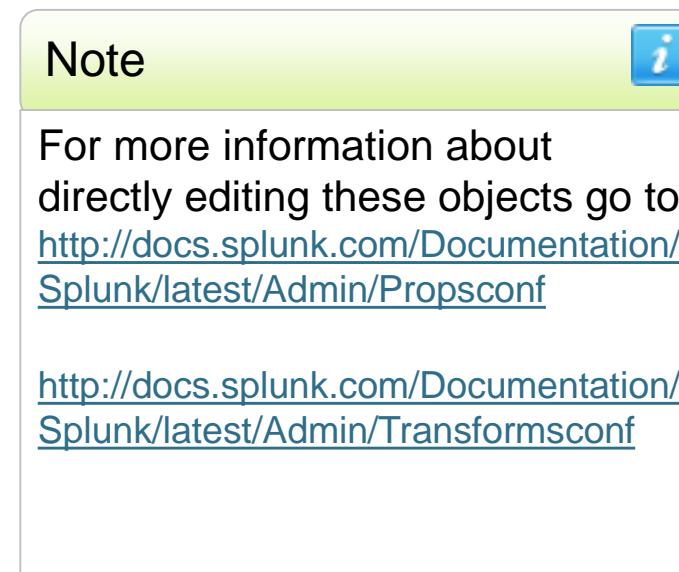
The screenshot shows the 'Extract Fields' interface. At the top, there are buttons for 'Extract Fields' (highlighted with a red circle labeled '8'), '< Back', and 'Existing fields >'. Below this, a warning message says: 'If you manually edit and then preview the regular expression below, you cannot return to the automatic field extraction workflow.' A note below it says: '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 for 'Regular Expression Reference' and 'View in Search'. At the bottom, there are tabs for 'Events' and 'user' (highlighted with a red circle labeled '9'). On the far right, there are 'Preview' and 'Save' buttons.

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (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 10 11 Finish

**Save**  
Name the extraction and set permissions.

**10** **Extractions Name** EXTRACT- **Owner** admin **App** search

**Permissions**

---

**Source type** linux\_secure  
**Fields** user  
**Regular Expression** ^(?:[\n]\*\r){10}(?P<user>\w+)

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Delimited 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

t	Time	Event
>	7/20/16 4:37:15.000 PM	"2016-07-20T12:37:15.000-0400",7036,4,Information,HOST0167,System,278584858 host = ip-10-222-134-157   source = /opt/log/adldapsv1/sysmonitor.log   sourcetype = win_audit
>	7/20/16 4:37:11.000 PM	"2016-07-20T12:37:11.000-0400",29,1,Error,HOST0167,System,502659790 host = ip-10-222-134-157   source = /opt/log/adldapsv1/sysmonitor.log   sourcetype = win_audit
>	7/20/16 4:37:10.000 PM	"2016-07-20T12:37:10.000-0400",29,1,Error,HOST0167,System,270875482 host = ip-10-222-134-157   source = /opt/log/adldapsv1/sysmonitor.log   sourcetype = win_audit

# Field Extraction Workflows - Delimiters

## Settings

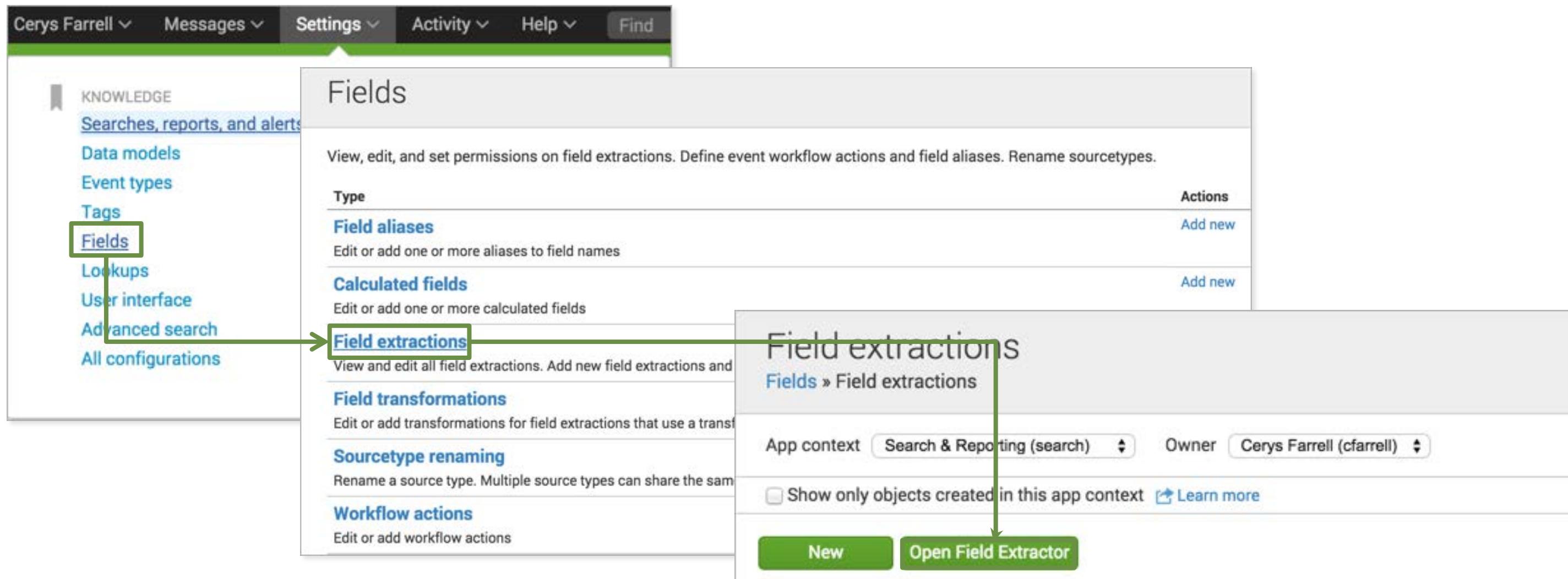
The screenshot illustrates the Splunk Extract Fields workflow, which consists of three main steps:

- Select sample**: This step is currently active. It includes fields for **Data Type** (set to `sourcetype`) and **Source Type** (with a dropdown menu). A **Select Sample Event** section shows a sample event: `"2016-07-18T19:35:09.000-0400",29,1,Error,HOST0167,System,24539140`. To the left is a **Fields Sidebar** containing sections for **Events**, **filter**, and **\_raw**.
- Select method**: This step follows the sample selection. It provides two options:
  - Regular Expression**: Represented by a green circle containing the pattern `(.*?)`.
  - Delimiters**: Represented by a blue square containing the pattern `x|y|z`.
- Select fields**: This step follows the method selection.

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Delimited Field Extractions from Settings

Settings > Fields > Field extractions > Open Field Extractor



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Delimited Field Extractions (Settings) – Select Sample

## 1. Select the Data Type

- sourcetype
- source

## 2. Select the Source Type

Extract Fields

— Select sample — Select method — Select fields — Save — Next >

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 1 event to train the field extractor.

Data Type sourcetype 1

Source Type Select Source Type 2

win\_audit

About win\_audit Privacy Policy

The screenshot shows the 'Extract Fields' interface with the 'Select sample' step highlighted. The 'Data Type' dropdown is set to 'sourcetype' (marked with a red circle 1). The 'Source Type' dropdown is set to 'Select Source Type' (marked with a red circle 2). A list of available source types includes 'win\_audit', which is currently selected. Other options like 'Abou' and 'Privacy Policy' are also visible.

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Delimited Field Extractions (Settings) – Select Event

3. Select a sample event

4. Click **Next >**

Extract Fields     4

Select sample    Select method    Select fields    Save

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

Data Type sourcetype

Source Type win\_audit

3

"2016-07-25T22:13:24.000-0400",628,8,SuccessAudit,"BUSDEV-007",Security,764138848

Events

✓ 1,000 events (before 7/25/16 4:06:19.000 PM)

filter    Apply    Sample: 1,000 events    All events

\_raw

"2016-07-25T22:13:37.000-0400",4689,0,Information,"BUSDEV-006",Security,451297152  
"2016-07-25T22:13:29.000-0400",4739,0,Information,"BUSDEV-006",Security,296723054  
"2016-07-25T22:13:24.000-0400",628,8,SuccessAudit,"BUSDEV-007",Security,764138848  
"2016-07-25T22:12:48.000-0400",29,1>Error,HOST0167,System,270124338  
"2016-07-25T22:12:45.000-0400",17,1>Error,HOST0167,System,792562577

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Delimited Field Extractions (Settings) – Select Method

## 5. Select Delimiters

## 6. Click Next >

Extract Fields

6

Select sample    Select method    Rename fields    Save    Next >

Select Method

Indicate the method you want to use to extract your field(s). [Learn more](#) | [I prefer to write the regular expression myself](#)

Source type `win_audit`

"2016-07-25T22:13:24.000-0400",628,8,SuccessAudit,"BUSDEV-007",Security,764138848

(.\*?)

Regular Expression

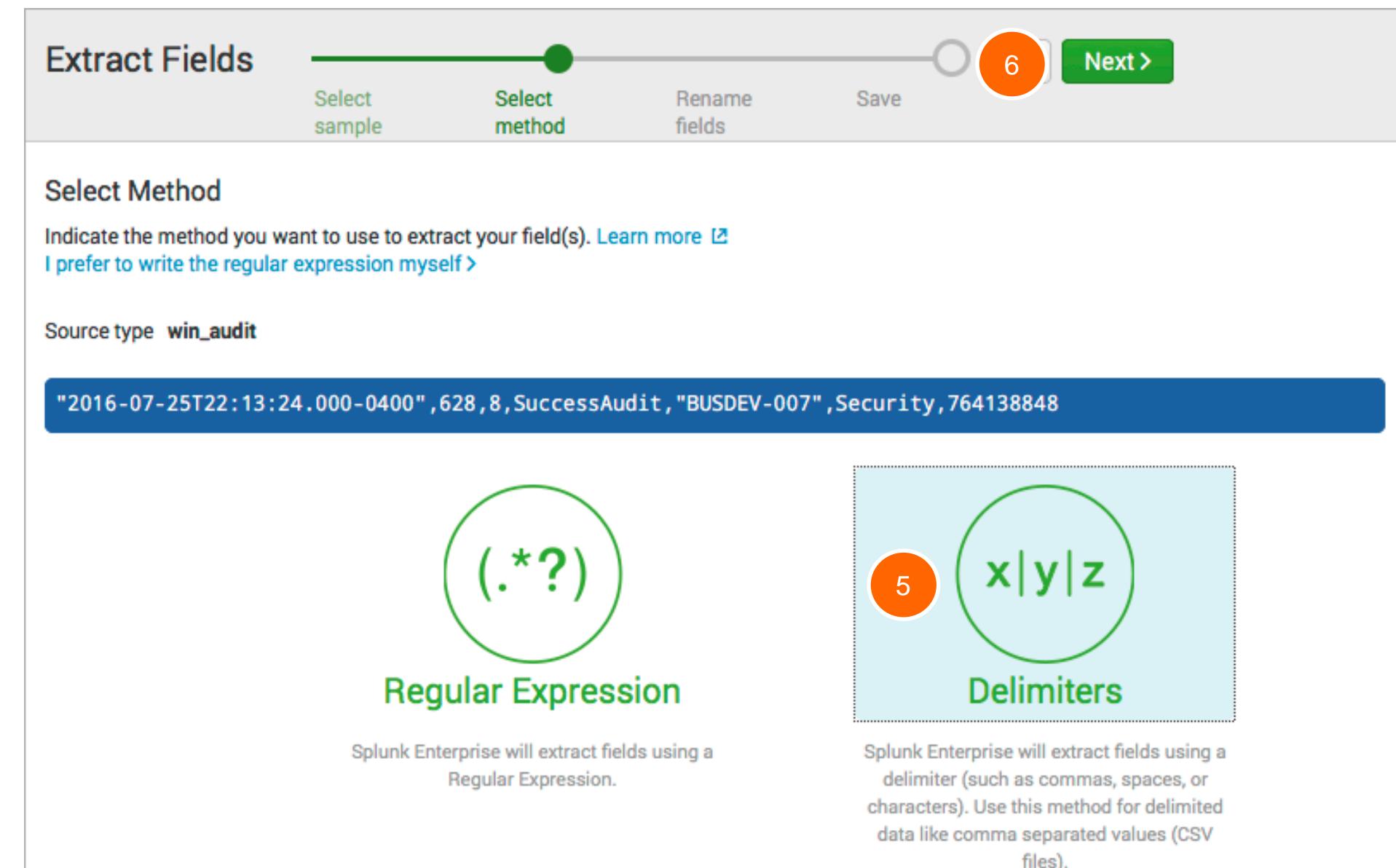
Splunk Enterprise will extract fields using a Regular Expression.

x|y|z

5

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).



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Delimited Field Extractions (Settings) - Select Delimiter

## 7. Select the Delimiter used in your event

7

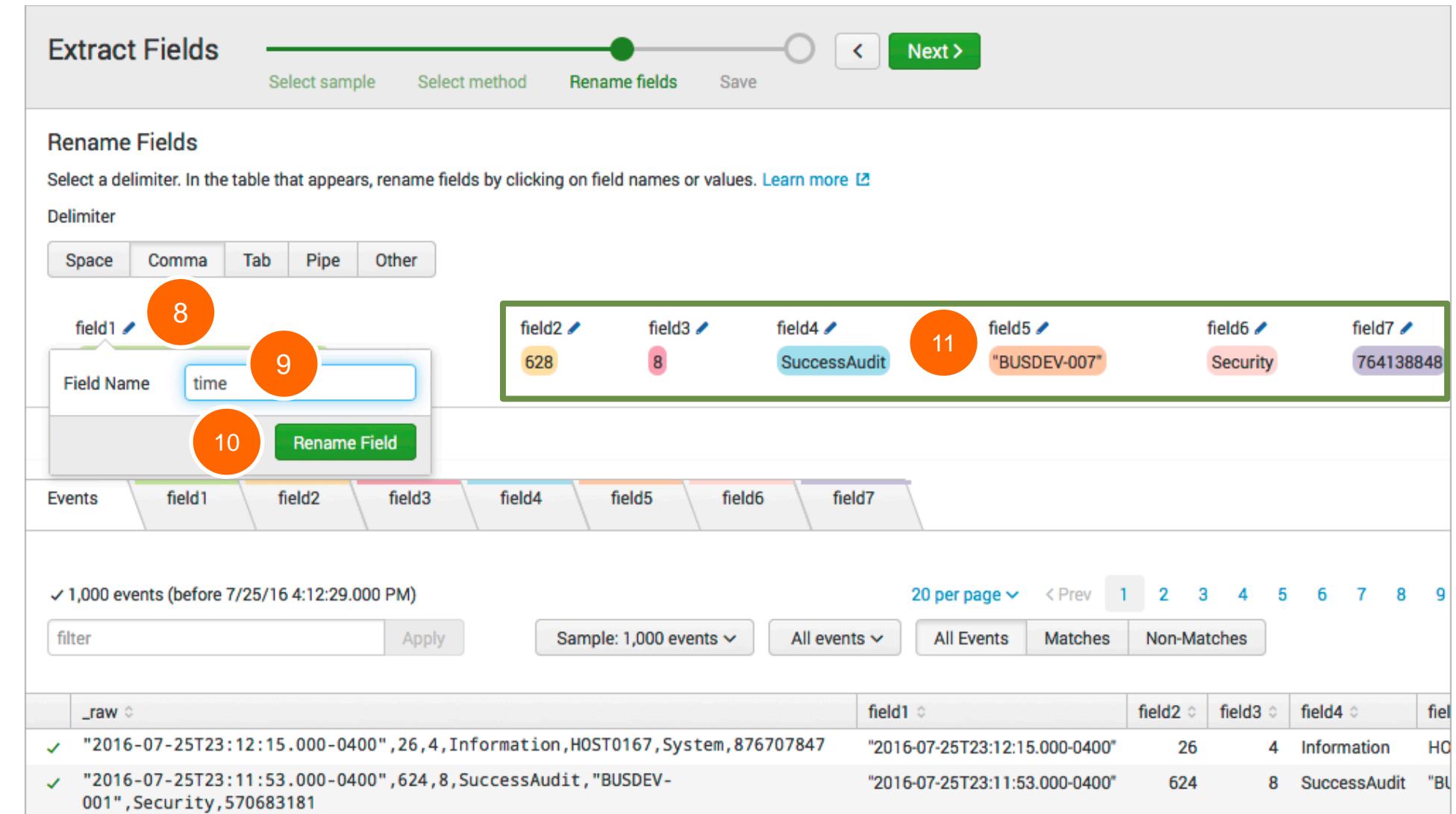
The screenshot shows the 'Extract Fields' interface in Splunk. The current step is 'Rename fields', indicated by a green dot on the progress bar. The interface includes tabs for 'Select sample', 'Select method', 'Rename fields' (which is active), and 'Save'. Below the tabs, there's a section titled 'Rename Fields' with instructions to select a delimiter and rename fields. A 'Delimiter' section has tabs for 'Space', 'Comma', 'Tab', 'Pipe', and 'Other'. The 'Other' tab is highlighted with a red circle. A preview section shows 7 fields: field1, field2, field3, field4, field5, field6, and field7. The first field, field1, contains the value '2016-07-25T22:13:24.000-0400'. At the bottom, there's a preview of 1,000 events, a filter input, and a table showing raw log data with columns for \_raw, field1, field2, field3, field4, and field5.

_raw	field1	field2	field3	field4	field5
"2016-07-25T23:12:15.000-0400",26,4,Information,HOST0167,System,876707847	"2016-07-25T23:12:15.000-0400"	26	4	Information	HOST0167
"2016-07-25T23:11:53.000-0400",624,8,SuccessAudit,"BUSDEV-001",Security,570683181	"2016-07-25T23:11:53.000-0400"	624	8	SuccessAudit	"BUSDEV-001"
"2016-07-25T23:11:31.000-0400",552,8,SuccessAudit,"BUSDEV-001",Security,505058881	"2016-07-25T23:11:31.000-0400"	552	8	SuccessAudit	"BUSDEV-001"

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Delimited Field Extractions (Settings) – Rename Field

8. Click the  icon next to the default field name
9. Enter a new field name
10. Click **Rename Field**
11. Repeat these steps for all fields



The screenshot shows the 'Extract Fields' interface in Splunk. The current step is 'Rename fields'. The 'Delimiter' is set to 'Comma'. In the 'Rename Fields' section, a table lists fields: field1 (time), field2 (628), field3 (8), field4 (SuccessAudit), field5 ("BUSDEV-007"), field6 (Security), and field7 (764138848). The 'field1' row has a green border. The 'field5' row is highlighted with a green box and circled with number 11. The 'Rename Field' button in the 'Field Name' row is circled with number 10. The 'Field Name' input field in the 'Field Name' row is circled with number 9. The 'field1' header is circled with number 8. At the bottom, there are pagination controls (1-9), a filter bar, and a results table showing two events.

_raw	field1	field2	field3	field4	field5	field6	field7
"2016-07-25T23:12:15.000-0400",26,4,Information,HOST0167,System,876707847	"2016-07-25T23:12:15.000-0400"	26	4	Information	HOST0167		
"2016-07-25T23:11:53.000-0400",624,8,SuccessAudit,"BUSDEV-001",Security,570683181	"2016-07-25T23:11:53.000-0400"	624	8	SuccessAudit	"BUSDEV-001"	Security	570683181

# Delimited Field Extractions (Settings) – Rename Field (cont.)

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

The screenshot shows the 'Extract Fields' interface in Splunk. The progress bar indicates step 12 of 12, with 'Rename fields' highlighted. The 'Rename Fields' section allows selecting a delimiter (Space, Comma, Tab, Pipe, Other) and renaming fields. A preview table shows fields like time, eventcode, eventtype, type, computername, logname, and recordnumber. Below the table, a preview section shows 7 fields: Events, time, eventcode, eventtype, type, computername, logname, and recordnumber. It also displays 1,000 events and a page navigation bar from 1 to 9. At the bottom, there's a table of raw event data with columns for \_raw, time, eventcode, eventtype, and type.

_raw	time	eventcode	eventtype	type
"2016-07-25T23:13:29.000-0400",17,1>Error,HOST0167,System,626225961	"2016-07-25T23:13:29.000-0400"	17	1	Error
"2016-07-25T23:13:29.000-0400",7036,4,Information,HOST0167,System,688575053	"2016-07-25T23:13:29.000-0400"	7036	4	Information

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Delimited Field Extractions (Settings) – Save

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

Extract Fields

13

Select sample Select method Rename fields Save

Save

Name the extraction and set permissions.

Extractions Name REPORT- sysmon

Owner admin

App search

Permissions Owner App All apps

---

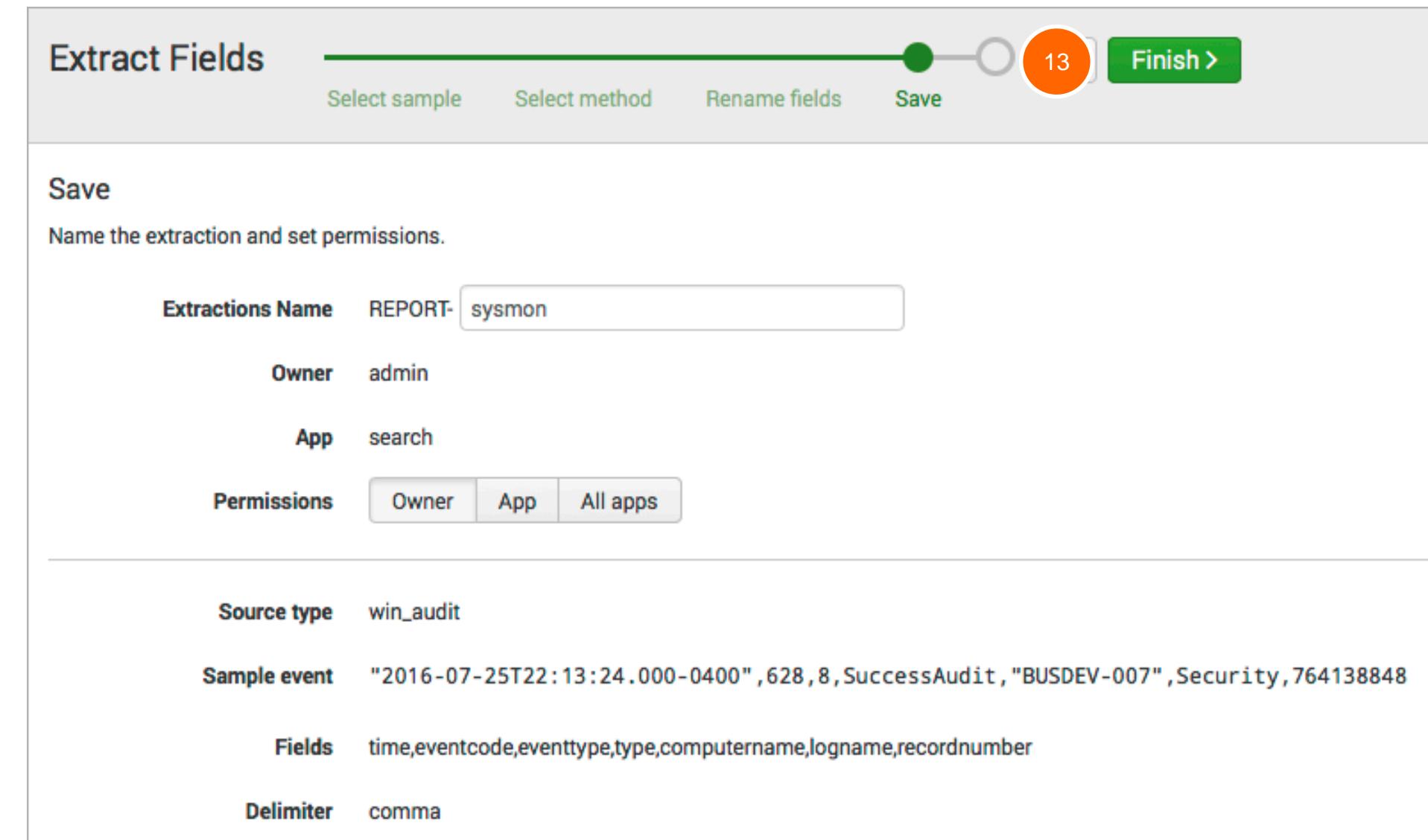
Source type win\_audit

Sample event "2016-07-25T22:13:24.000-0400",628,8,SuccessAudit,"BUSDEV-007",Security,764138848

Fields time,eventcode,eventtype,type,computername,logname,recordnumber

Delimiter comma

Finish >



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Using a Delimited Field Extraction

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

**Search Bar:** index=\_\* OR index=\* sourcetype=win\_audit type=failureaudit

**Time Range:** Last 24 hours

**Event Count:** 63 events (8/10/16 10:00:00.000 AM to 8/11/16 10:34:47.000 AM)

**Event Actions (Selected Fields):**

Type	Field	Value	Actions
Selected	host	adldapsv1	
	source	/opt/log/adldapsv1/sysmonitor.log	
	sourcetype	win_audit	
Event	computername	BUSDEV-005	
	eventcode	539	
	eventtype	nix-all-logs	
	logname	Security	
	recordnumber	894939433	
	time	2016-08-11T17:00:30.000-0400	
	type	FailureAudit	

**Event Timeline:** 8/11/16 10:00:30.000 AM

**Event List:**

Time	Event
8/11/16 10:00:30.000 AM	host = adldapsv1
8/11/16 9:59:01.000 AM	host = adldapsv1
8/11/16 9:03:08.000 AM	host = adldapsv1
8/11/16 9:02:37.000 AM	host = adldapsv1
8/11/16 8:05:23.000 AM	host = adldapsv1   source = /opt/log/adldapsv1/sysmonitor.log   sourcetype = win_audit
8/11/16 7:02:05.000 AM	host = adldapsv1   source = /opt/log/adldapsv1/sysmonitor.log   sourcetype = win_audit

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Module 9: Creating Field Aliases and Calculated Fields

Generated for Subbaiah Kandula ([s.venkata.kandula@accenture.com](mailto:s.venkata.kandula@accenture.com)) (C) Splunk Inc, not for distribution

# Module Objectives

---

- Create and use field aliases
- Create calculated fields

# Field Aliases

---

- A way to normalize data over any default field (host, source or sourcetype)
- 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

The screenshot shows three search results from a Splunk interface. Each result has a 'Selected' section on the left and an 'Event' section on the right.

- Event 1 (sourcetype=cisco\_firewall):** Shows a 'Username' field with value 'acurry'. A green box highlights this field, and an arrow points to it from a yellow box containing the query 'sourcetype=cisco\_firewall'.
- Event 2 (sourcetype=cisco\_wsa\_squid):** Shows a 'username' field with value 'acurry'. A green box highlights this field, and an arrow points to it from a yellow box containing the query 'sourcetype=cisco\_wsa\_squid'.
- Event 3 (sourcetype=winauthentication\_security):** Shows a 'User' field with value 'acurry'. A green box highlights this field, and an arrow points to it from a yellow box containing the query 'sourcetype=winauthentication\_security'.

Selected	Event
<input checked="" type="checkbox"/> host ✓ <input checked="" type="checkbox"/> source ✓ <input checked="" type="checkbox"/> sourcetype ✓	cisco_router1 /opt/log/cisco_router1/cisco_firewall.log
<input type="checkbox"/> Duration ✓ <input type="checkbox"/> Group ✓ <input type="checkbox"/> IP ✓ <input type="checkbox"/> Username ✓ <input type="checkbox"/> bcg_ip ✓ <input type="checkbox"/> bcg_workstation ✓	0h:0m:0s buttercupgame 10.1.10.246 acurry 10.1.10.246 BG01-acurry
	<input checked="" type="checkbox"/> sourcetype ✓ <input type="checkbox"/> action ✓ <input type="checkbox"/> bytes_in ✓ <input type="checkbox"/> c_ip ✓ <input type="checkbox"/> cs_method ✓ <input type="checkbox"/> cs_mime_type ✓ <input type="checkbox"/> cs_url ✓ <input type="checkbox"/> username ✓ <input type="checkbox"/> x_webcat_code_abbr ✓ <input type="checkbox"/> x_webcat_code_full ✓ <input type="checkbox"/> x_webroot_threat_name ✓
	cisco_wsa_squid TCP_MISS 798 59.36.99.70 GET image/gif http://www.creditreport.com/AP acurry IW_fnnc Finance -
	<input type="checkbox"/> ComputerName ✓ <input type="checkbox"/> EventCode ✓ <input type="checkbox"/> EventType ✓ <input type="checkbox"/> LogName ✓ <input type="checkbox"/> Message ✓ <input type="checkbox"/> RecordNumber ✓ <input type="checkbox"/> Sid ✓ <input type="checkbox"/> SidType ✓ <input type="checkbox"/> SourceName ✓ <input type="checkbox"/> Type ✓ <input type="checkbox"/> User ✓
	BG01-acurry 4634 8 Security Successful 9658 S-1-5-21-57989841-920026266-725345543-6444 1 Security Success acurry

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (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

The screenshot shows the 'Add new' dialog for creating a field alias in Splunk. The steps are numbered 1 through 4:

1. Destination app: search
2. Name: cisco\_firewall\_aliases
3. Apply to: sourcetype (selected) and named: cisco\_firewall
4. Field aliases: Username = user

Annotations explain the 'Field aliases' section:

- An arrow points to 'Username' with the label 'existing field name'.
- An arrow points to 'user' with the label 'new field alias'.

# 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 sequential screenshots of the Splunk 'Add new Field aliases' interface, showing the creation of three separate field aliases for different sourcetypes.

**Screenshot 1:** Creating a field alias for 'cisco\_firewall\_aliases'. The 'Destination app' is set to 'search', 'Name' is 'cisco\_firewall\_aliases', 'Apply to' is 'sourcetype' (selected), and 'named' is 'cisco\_firewall'. Under 'Field aliases', 'Username' is mapped to 'user'. A 'Cancel' button is at the bottom left.

**Screenshot 2:** Creating a field alias for 'cisco\_wsa\_squid\_aliases'. The 'Destination app' is set to 'search', 'Name' is 'cisco\_wsa\_squid\_aliases', 'Apply to' is 'sourcetype' (selected), and 'named' is 'cisco\_wsa\_squid'. Under 'Field aliases', 'cs\_username' is mapped to 'user'. A 'Cancel' button is at the bottom left.

**Screenshot 3:** Creating a field alias for 'winauthentication\_security\_aliases'. The 'Destination app' is set to 'search', 'Name' is 'winauthentication\_security\_aliases', 'Apply to' is 'sourcetype' (selected), and 'named' is 'winauthentication'. Under 'Field aliases', 'User' is mapped to 'user'. A 'Delete' link is next to the 'user' mapping, and a 'Save' button is at the bottom right.

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Testing the Field Alias

After the field alias is created, perform a search using the new field alias

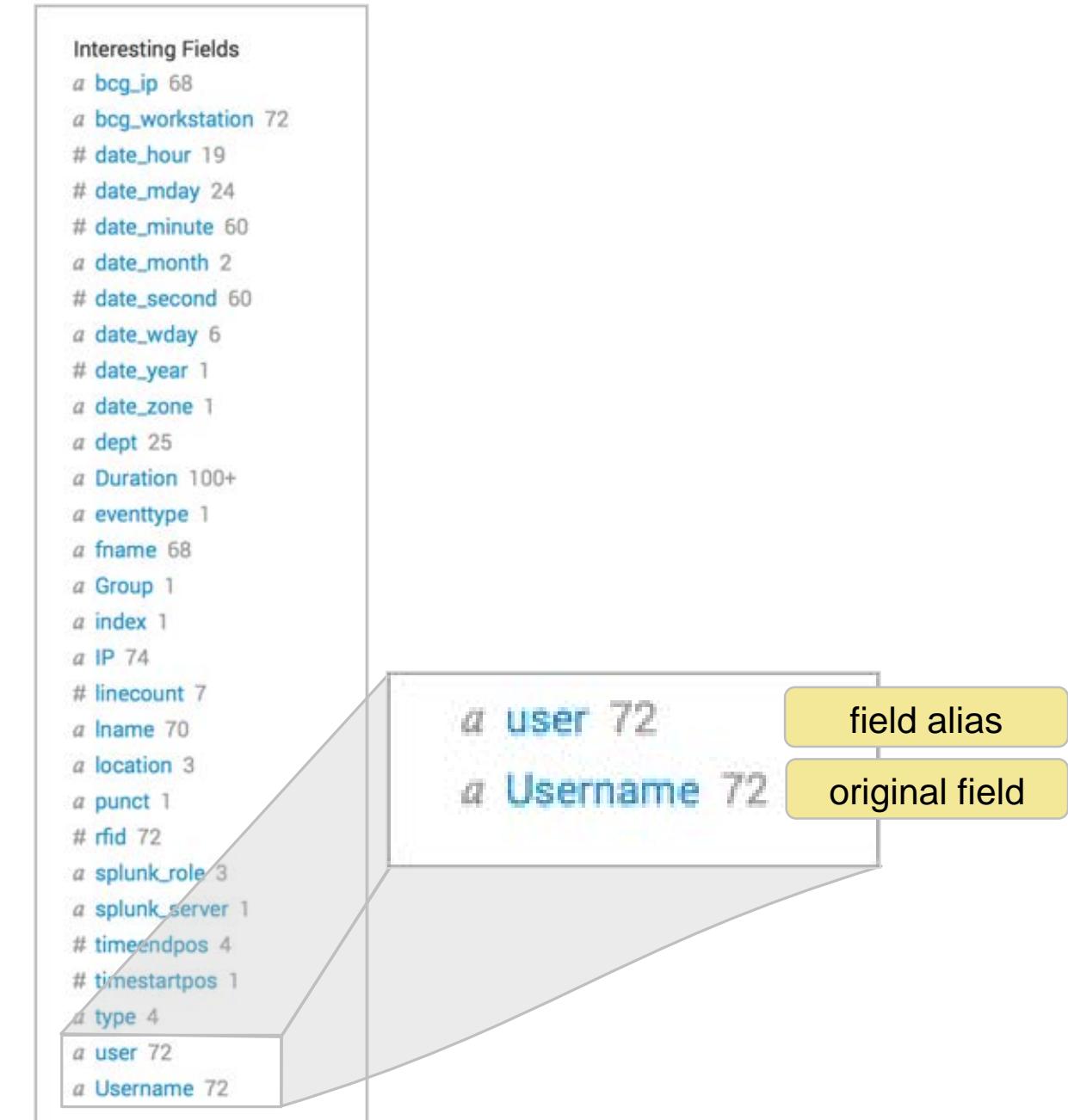
The screenshot shows the Splunk search interface. At the top, a search bar contains the query `user=acurry*`. Below the search bar, it says `99 events (7/13/16 9:00:00.000 PM to 7/14/16 9:25:58.000 PM)` and `No Event Sampling`. The timeline below shows event distribution over time. The main view displays a table for the `sourcetype` field. The table shows three values: `winauthentication_security` (Count: 96, %: 96.97%), `cisco_wsasquid` (Count: 2, %: 2.02%), and `cisco_firewall` (Count: 1, %: 1.01%). A green box highlights the `sourcetype` table, and a green arrow points from the `sourcetype` field in the Selected Fields list to the `sourcetype` table.

Values	Count	%
winauthentication_security	96	96.97%
cisco_wsasquid	2	2.02%
cisco_firewall	1	1.01%

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (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 appear in the All Fields and Interesting Fields lists, if they appear in at least 20% of events



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Field Aliases and Lookups

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

The screenshot shows the Splunk interface for defining field aliases. On the left, under 'Fields > Field aliases > cisco\_firewall : FIELDALIAS-cisco\_firewall', there is a table for 'Field aliases'. One entry shows 'Username' mapped to 'user'. A green box highlights the 'user' field in both the alias table and the CSV file on the right. An arrow points from the highlighted 'user' in the alias table to the highlighted 'user' in the CSV file.

Field aliases	
Username	= user
	=

**cisco\_firewall : FIELDALIAS-cisco\_firewall**

Fields » Field aliases » cisco\_firewall : FIELDALIAS-cisco\_firewall

employee.csv

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	iwing@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 Subbaiah Kandula (s.venkata.kandula@accenture.com) (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

The screenshot shows a Splunk search interface. The search bar contains the following command:

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

The search results section displays 39,548 events from October 1, 2016, to October 31, 2016. The results are grouped by usage (Personal, Unknown, Business, Borderline, Violation) and sorted by Bandwidth (MB) in descending order. The bandwidth values are as follows:

usage	Bandwidth (MB)
Personal	320.626208
Unknown	77.558703
Business	67.661781
Borderline	52.038978
Violation	2.811679

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (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 class\_Fund2

Apply to \*

2 sourcetype named \*

cisco\_wsa\_squic

Name \*

3 megabytes

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

# 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. The search bar contains the command: `index=network sourcetype=cisco_wsa_squid | stats sum(bandwidth) as "Bandwidth (MB)" by usage | sort -"Bandwidth (MB)"`. The term `sum(bandwidth)` is highlighted with a green box. Below the search bar, the results summary is shown: 39,553 events (10/1/16 12:00:00.000 AM to 10/31/16 8:57:54.000 PM), No Event Sampling, Last 30 days, and a magnifying glass icon. The visualization tab is selected, showing a table with two columns: `usage` and `Bandwidth (MB)`. The data rows are:

usage	Bandwidth (MB)
Personal	320.629846
Unknown	77.569352
Business	67.661781
Borderline	52.038978
Violation	2.811679

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Module 10: Working with Tags and Event Types

Generated for Subbaiah Kandula ([s.venkata.kandula@accenture.com](mailto:s.venkata.kandula@accenture.com)) (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
- 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 shows the Splunk interface for creating tags. At the top, there is a log entry: "Tue Aug 16 2016 20:42:41 www1 sshd[4719]: Failed password for root from 81.11.191.113 port 1382 ssh2". Below it is a "Event Actions" panel with dropdown menus for "Type" (Selected: host, source, sourcetype), "Event" (Selected: eventtype), "Time" (Selected: \_time), and "Default" (Selected: index, tag). A green box highlights the "Edit Tags" button in the "Default" section, with a red circle labeled "3" above it. A modal window titled "Create Tags" is open, containing a "Field Value" input field with "user=root" and a "Tag" input field with "privileged", separated by a comma. A red circle labeled "4" is positioned next to the "privileged" tag. The bottom right of the modal has a "Save" button.

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Viewing Tags

When tagged field/value pairs are selected, the tags appear:

- In the results as tags A
- In parentheses next to the associated field/value pairs B

The screenshot shows a Splunk search interface. At the top, a log entry is displayed with several field/value pairs. A green box highlights the 'tag' field, which contains 'authentication tag = error tag = privileged'. An orange circle labeled 'A' is positioned to the left of this highlighted area. Below the log entry is a detailed view of the event fields. The 'tag' field is expanded, showing its values: 'authentication', 'error', and 'privileged'. An orange circle labeled 'A' is placed next to the checkbox for 'authentication'. At the bottom of the event details, the 'user' field is also expanded, showing its value: 'root (privileged)'. An orange circle labeled 'B' is placed next to the checkbox for 'user'.

Field	Value
sourcetype	linux_secure
tag	authentication error privileged
Event	action Failed pid 4219 process sshd src 91.205.189.15 user root (privileged)

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Using Tags

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

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

- Search Bar:** index=web sourcetype=linux\_secure tag=priv\* src!=NULL | stats count by src, port
- Time Range:** Last 24 hours
- Event Count:** 198 events (8/16/16 1:00:00.000 PM to 8/17/16 1:42:37.000 PM)
- Sampling:** No Event Sampling
- Visualizations:** Job, II, III, ▶, 🔍, ⌂, Verbose Mode
- Table Headers:** Events (198), Patterns, Statistics (198), Visualization
- Table Options:** 20 Per Page, Format, Preview
- Table Data:** A table showing the top ports from which traffic originated, ordered by count. The columns are src, port, and count.

src	port	count
88.12.32.208	1489	1
88.12.32.208	2302	1
88.191.83.82	1250	1
88.191.83.82	2259	1
89.106.20.218	1907	1
91.205.189.15	2983	1
91.205.189.15	3526	1
91.205.189.27	1560	1
91.205.40.22	2739	1

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Searching for Tags

- To search for a tag associated with a value:

- tag=<tagname>

```
tag=privileged
```

Note

Tag names are case-sensitive.



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

- tag::<field>=<tagname>

```
tag::user=privileged
```

- To search for a tag using a partial field value:

- Use (\*) wildcard

```
tag=p*
```

# Managing Tags – List by Field Value Pair

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**

Field value pair	Tag name	App	Sharing	Status	Actions
User=Administrator	privileged	search	Private   Permissions	Enabled   Disable all tags for pair	Clone   Move   Delete
user=root	privileged	search	Private   Permissions	Enabled   Disable all tags for pair	Clone   Move   Delete

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (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 UI for managing tags. On the left, the 'List by field value pair' page is displayed. It includes filters for 'App context' (Search & Reporting), 'Owner' (cfarrell), and a checkbox for 'Show only objects created in this app context'. A green 'New' button is visible. The table lists two items: 'User=Administrator' and 'user=root', each with a 'Tag name' of 'privileged', 'App' of 'search', and 'Sharing' set to 'Private | Permissions'. A green arrow points from the 'User=Administrator' row to a modal window on the right. The modal is titled 'User=Administrator' and shows the 'Tag name' field containing 'privileged'. It also has a 'Delete' link and a 'Save' button. Below the tag name field, there is an 'Add another field' link.

Field value pair	Tag name	App	Sharing
User=Administrator	privileged	search	Private   Permissions
user=root	privileged	search	Private   Permissions

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (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 illustrates the process of managing field value pairs for a specific tag. On the left, the 'List by tag name' page for the tag 'privileged' is shown. The 'Tag name' dropdown is set to 'privileged'. The table displays one item: 'User=Administrator, user=root'. A green arrow points from the 'privileged' tag in the list to the 'Field value pair' section of the detailed view on the right. The right-hand panel shows the 'Field value pair' configuration for the 'privileged' tag. It lists two entries: 'User=Administrator' and 'user=root', each with a 'Delete' link. Below these entries is a button labeled 'Add another field'. At the bottom of the panel are 'Cancel' and 'Save' buttons.

Tag name	Field value pair	Owner
privileged	User=Administrator, user=root	cfarrell

privileged  
Tags » List by tag name » privileged

Field value pair  
*example: host=splunk.com*

User=Administrator Delete

user=root Delete

Add another field

Cancel Save

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Describing Event Types

---

- 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

# Creating an Event Type from the Search Page

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 shows the Splunk search interface. On the left, a search bar contains the query `index=* status>499`. Below the search bar, it says "180 events (8/16/16 2:00:00.000 PM to 8/17/16 2:53:23.000 PM) No Event Sampling". A context menu is open at the top right, with the "Event Type" option highlighted. To the right of the search interface is a "Save As Event Type" dialog box.

**Save As Event Type**

- Name: web\_error
- Tags: Optional
- Color: yellow
- Priority: 1 (Highest)

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

Cancel Save

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Using the Event Type Builder

## 1. From the event details, select **Event Actions > Build Event Type**

The screenshot shows a Splunk search interface for the query `index=* status>499`. The search results show 180 events from August 16, 2016, to August 17, 2016. The 'Events (180)' tab is selected. In the bottom right corner of the event details area, there is a dropdown menu labeled 'Event Actions'. This menu has three options: 'Build Event Type' (which is highlighted with a green border), 'Extract Fields', and 'Show Source'. The rest of the interface includes a timeline, search bar, and various navigation and configuration buttons.

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Using the Event Type Builder (cont.)

2. Refine the criteria for your event type such as:
  - Search string
  - Field values
  - Tags

3. Verify your selections and click **Save**

The screenshot shows the Splunk Event Type Builder interface. At the top, it displays a "Generated event type" with the search criteria: `(index=** status>499)`. Below this are three buttons: "Edit", "Test", and "Save".

The main area is divided into two sections: "Suggested field values" on the left and "Sample events" on the right.

**Suggested field values:**

- eventtype:**  nix-all-logs
- ident:**  -
- linecount:**  1
- user:**  -
- version:**  1.1
- index:**  web
- network
- method:**  POST
- GET
- sourcetype:**  access\_combined
- cisco\_wsa\_squid
- file:**  product.screen
- cart.do
- category.screen
- oldlink
- host:**  www1
- cisco\_router1
- www2
- www3
- referer\_domain:**  http://www.buttercupgames.com
- http://www.bing.com
- http://www.google.com
- http://www.yahoo.com

**Sample events:**

Note: Sample events match the current event type search.

Event ID	Time	Event Details
176.212.0.44	[17/Aug/2016:21:47:03]	"POST /product.screen?productId=EST-15&category=1.1 HTTP/1.1"
91.210.104.143	[17/Aug/2016:21:25:04]	"GET /oldlink?itemId=EST-15&category=1.1 HTTP/1.1"
1471468198.356	48949 69.72.161.186 NONE/503 1878 GET http://startdowntime.com/oldlink?itemId=EST-15&category=1.1	
67.170.226.218	[17/Aug/2016:21:06:03]	"GET /cart.do?action=changequantity&id=141.146.8.66 HTTP/1.1"
202.201.1.233	[17/Aug/2016:21:02:23]	"GET /category.screen?category=1.1 HTTP/1.1"
81.11.191.113	[17/Aug/2016:20:58:35]	"POST /cart.do?action=purchase&id=141.146.8.66 HTTP/1.1"
91.217.178.210	[17/Aug/2016:20:51:22]	"GET /cart.do?action=view&id=141.146.8.66 HTTP/1.1"
91.210.104.143	[17/Aug/2016:20:44:15]	"GET /oldlink?itemId=EST-11&category=1.1 HTTP/1.1"
1471465685.572	144 195.2.240.99 NONE/503 1875 GET http://pcguardscan.com/oldlink?itemId=EST-11&category=1.1	
50.23.124.50	[17/Aug/2016:20:24:33]	"GET /product.screen?productId=EST-11&category=1.1 HTTP/1.1"
141.146.8.66	[17/Aug/2016:20:04:59]	"GET /product.screen?productId=EST-11&category=1.1 HTTP/1.1"
1471463990.853	48915 70.38.1.235 NONE/503 1872 GET http://scan4fast.info/oldlink?itemId=EST-11&category=1.1	
128.241.220.82	[17/Aug/2016:19:50:44]	"GET /oldlink?itemId=EST-19&category=1.1 HTTP/1.1"
216.221.226.11	[17/Aug/2016:19:46:21]	"GET /cart.do?action=purchase&id=141.146.8.66 HTTP/1.1"
176.212.0.44	[17/Aug/2016:19:36:12]	"POST /oldlink?itemId=EST-18&category=1.1 HTTP/1.1"
89.11.192.18	[17/Aug/2016:19:32:33]	"GET /product.screen?productId=EST-18&category=1.1 HTTP/1.1"
195.2.240.99	[17/Aug/2016:19:24:09]	"POST /category.screen?category=1.1 HTTP/1.1"
188.173.152.100	[17/Aug/2016:19:22:12]	"GET /oldlink?itemId=EST-13&category=1.1 HTTP/1.1"
201.122.42.235	[17/Aug/2016:19:17:20]	"GET /oldlink?itemId=EST-13&category=1.1 HTTP/1.1"
1471460699.599	3743 59.36.99.70 NONE/503 1899 GET http://www.raisethebar.com/oldlink?itemId=EST-13&category=1.1	
188.138.40.166	[17/Aug/2016:19:04:47]	"GET /oldlink?itemId=EST-7&category=1.1 HTTP/1.1"
1471460533.894	31 81.18.148.190 NONE/503 1875 GET http://loading-nso.net/oldlink?itemId=EST-7&category=1.1	
90.205.111.169	[17/Aug/2016:19:00:12]	"GET /cart.do?action=changequantity&id=141.146.8.66 HTTP/1.1"
203.92.58.136	[17/Aug/2016:18:55:58]	"POST /cart.do?action=view&id=141.146.8.66 HTTP/1.1"
203.92.58.136	[17/Aug/2016:18:55:16]	"GET /oldlink?itemId=EST-26&category=1.1 HTTP/1.1"

**Generated event type**  
`(index=** status>499)`

**Suggested field values**

Check the below field values, to build up your new event type. **Blue field values** are from your selected event; other values are from other events.

**eventtype:**  nix-all-logs  
**ident:**  -  
**linecount:**  1  
**user:**  -  
**version:**  1.1  
**index:**  web  
 network  
**method:**  POST  
 GET  
**sourcetype:**  access\_combined  
 cisco\_wsa\_squid  
**file:**  product.screen  
 cart.do  
 category.screen  
 oldlink  
**host:**  www1  
 cisco\_router1  
 www2  
 www3  
**referer\_domain:**  http://www.buttercupgames.com  
 http://www.bing.com  
 http://www.google.com  
 http://www.yahoo.com

**Generated event type**  
`(index=** status>499)`

**Suggested field values**

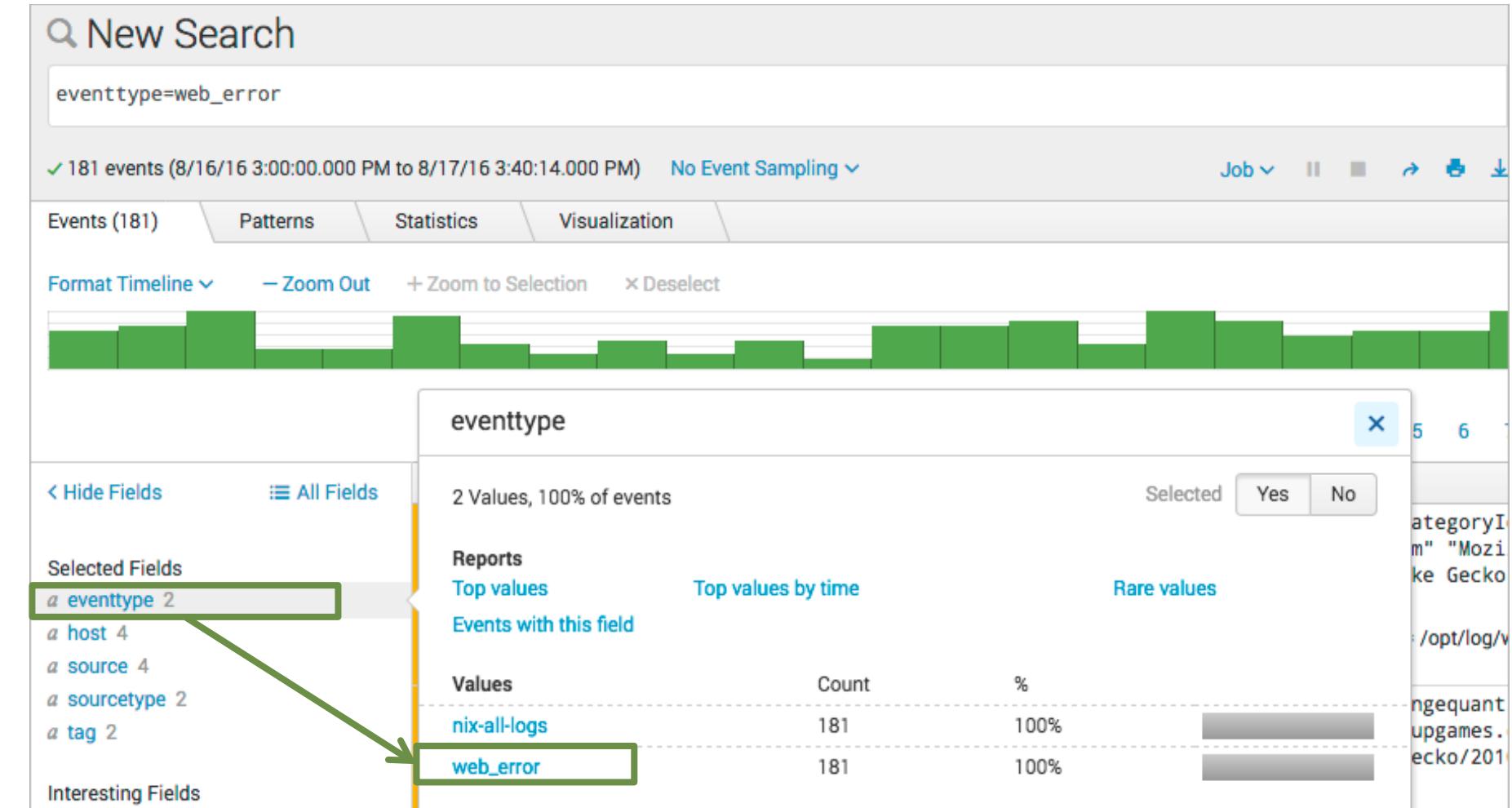
Check the below field values, to build up your new event type. **Blue field values** are from your selected event; other values are from other events.

**eventtype:**  nix-all-logs  
**ident:**  -  
**linecount:**  1  
**user:**  -  
**version:**  1.1  
**index:**  web  
 network  
**method:**  POST  
 GET  
**sourcetype:**  access\_combined  
 cisco\_wsa\_squid  
**file:**  product.screen  
 cart.do  
 category.screen  
 oldlink  
**host:**  www1  
 cisco\_router1  
 www2  
 www3  
**referer\_domain:**  http://www.buttercupgames.com  
 http://www.bing.com  
 http://www.google.com  
 http://www.yahoo.com

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Using Event Types

- To verify the event type, search for `eventtype=web_error`
- ‘`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 Subbaiah Kandula (s.venkata.kandula@accenture.com) (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, 'Field' is selected. Under 'Selected', 'eventtype' is checked. The 'Value' column shows 'web\_error ( error web )' and 'nix-all-logs'. In the 'Actions' column, there is a button labeled 'Edit Tags'. A green box highlights this button. Below it, a modal window titled 'Create Tags' is open. It has a 'Field Value' input field containing 'eventtype=web\_error' and a 'Tag(s)' input field containing 'error, web'. A green arrow points from the 'Edit Tags' button down to the 'Tag(s)' input field in the 'Create Tags' modal.

The screenshot shows the configuration of the 'web\_error' event type. The 'Search string' is set to 'index==\* status>499'. In the 'Tag(s)' section, 'error web' is listed. In the 'Color' section, 'yellow' is selected. In the 'Priority' section, '1 (Highest)' is selected. A note below states: 'Highest priority shows up first in a result.' A green box highlights the 'Tag(s)' input field. A yellow callout box at the bottom right states: 'Priority determines which event type color displays for an event'. A green arrow points from the 'Save' button in the 'Create Tags' modal up to the 'Priority' dropdown in this window.

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Event Types vs. Saved Reports

---

- 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
- Can be shared with Splunk users and added to dashboards

# Module 11:

# Creating and Using

# Macros

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (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

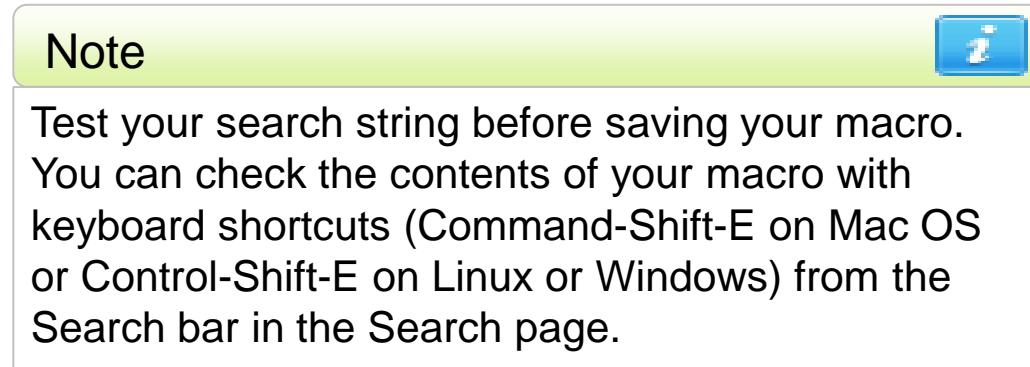
---

- 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 search segment
  - Pass parameter values to macro at execution time
  - Macro uses values to resolve search string

# 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

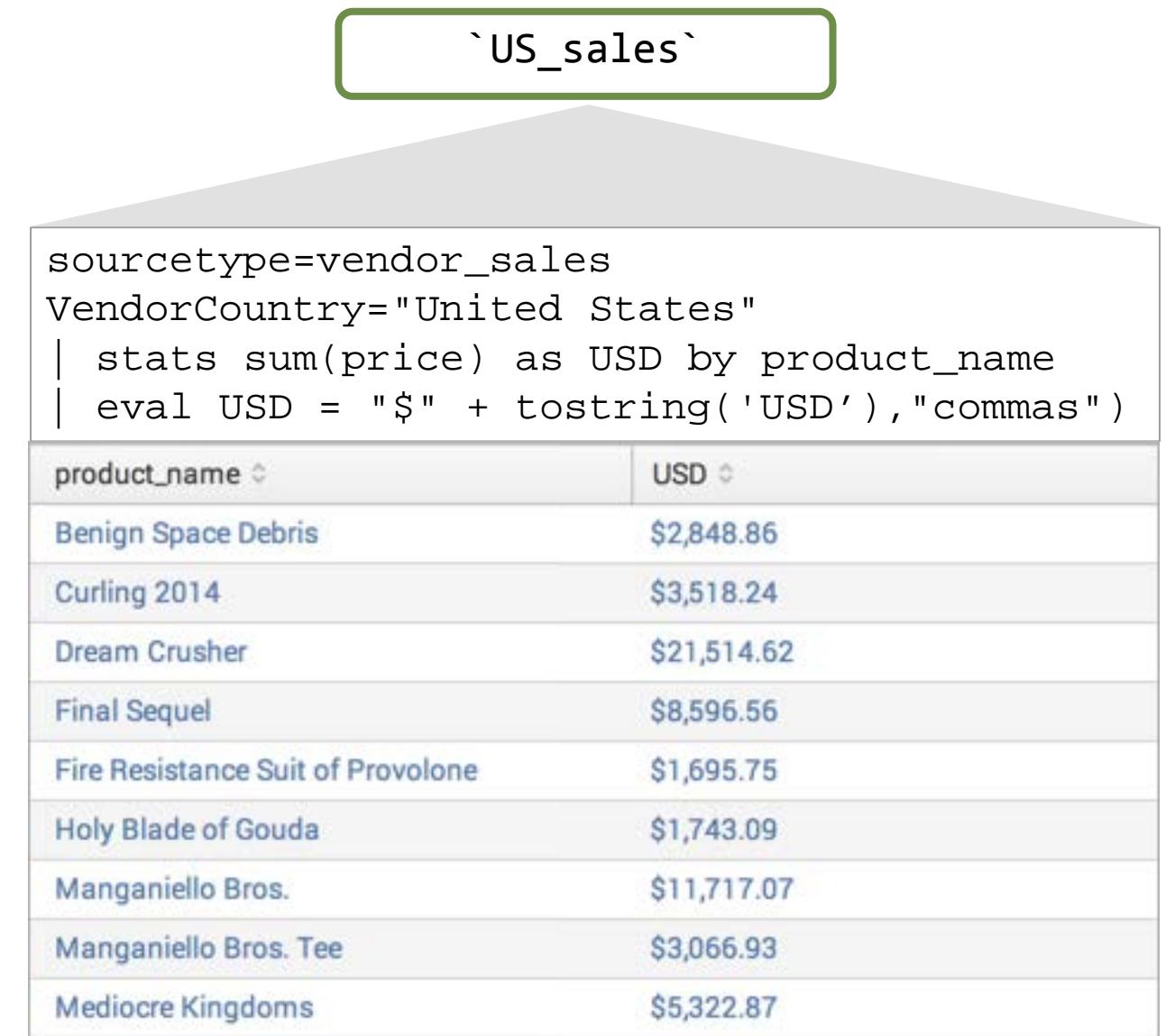
Definition \*

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('USD', "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 Splunk search interface. At the top, a green box highlights the macro name `US\_sales`. Below it, a search command is displayed:

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

Below the command is a table of sales data:

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
- Be sure to pass in the arguments in the same order as you defined them

```
sourcetype=vendor_sales VendorCountry=Germany  
OR VendorCountry=France OR VendorCountry=Italy  
`monthly_sales(euro,€,0.79)`
```

```
sourcetype=vendor_sales VendorCountry=Germany OR  
VendorCountry=France OR VendorCountry=Italy  
| stats sum(price) as USD by product_name  
| eval euro = "€" + tostring(USD*0.79, "commas")  
| eval USD = "$" + tostring(USD, "commas")
```



product_name	USD	euro
Benign Space Debris	\$649.74	€513.29
Curling 2014	\$559.72	€442.18
Dream Crusher	\$399.90	€315.92
Final Sequel	\$224.91	€177.68
Fire Resistance Suit of Provolone	\$131.67	€104.02
Holy Blade of Gouda	\$161.73	€127.77
Manganiello Bros.	\$1,239.69	€979.36
Manganiello Bros. Tee	\$419.58	€331.47
Mediocre Kingdoms	\$724.71	€572.52
Orvil the Wolverine	\$1,119.72	€884.58
Puppies vs. Zombies	\$29.94	€23.65
SIM Cubicle	\$979.51	€773.81
World of Cheese	\$1,124.55	€888.39
World of Cheese Tee	\$369.63	€292.01

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Validating Macros

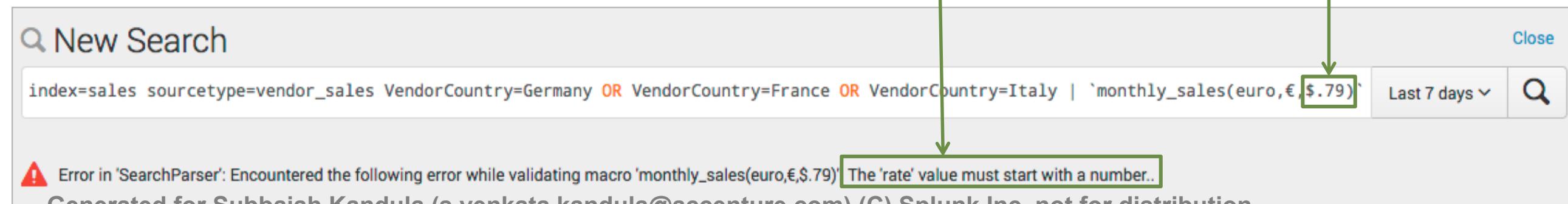
- You can validate the argument values in your macro
  - Validation Expression
    - You can enter an expression for each argument
  - Validation Error Message
    - Message that appears when you run the macro

**Note**  Don't create macros with leading pipes—someone may put a pipe in front of the macro when using it in the actual search string.

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 Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Module 12: Creating and Using Workflow Actions

Generated for Subbaiah Kandula ([s.venkata.kandula@accenture.com](mailto:s.venkata.kandula@accenture.com)) (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

The screenshot shows the Splunk interface for executing workflow actions. At the top, there is a log entry:

```
10/31/16 Mon Oct 31 2016 21:09:32 mailsv1 sshd[5752]: Failed password for invalid user mantis  
9:09:32.000 PM from 195.216.243.24 port 2973 ssh2
```

Below the log entry is a "Event Actions" button. A dropdown menu is open, showing the following options:

- Build Event Type
- Get info for IP:195.216.243.24 (highlighted with a green border)
- Extract Fields
- Show Source

To the right of the dropdown is a table showing field values and their corresponding actions:

Value	Actions
mailsv1	▼
/opt/log/mailsv1/secure.log	▼
linux_secure	▼
authentication	▼
error	▼
remote	▼
errOr ( error )	▼
failed_login	▼
sshd_authentication ( authentication remote )	▼
nix-all-logs	▼

At the bottom left of the interface, there is a "Event" button with a radio input and the text "eventtype".

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (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.*

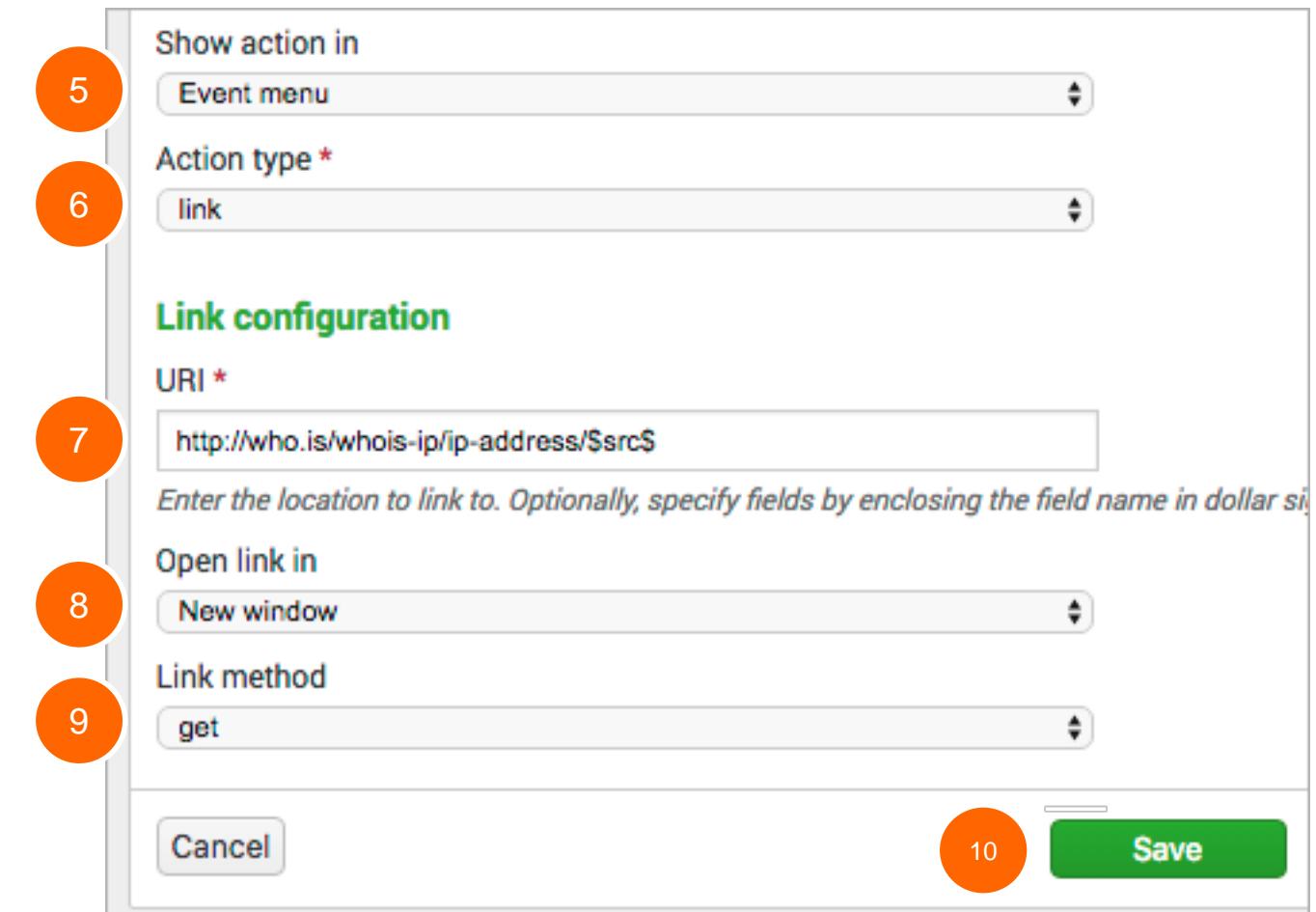
Label \*  
3 Get info for IP:\$src\$  
*Enter the label that appears for this action. Optionally, incorporate a field's value by enclosing the value in \$field\$.*

Apply only to the following fields  
4 src  
*Specify a comma-separated list of fields that must be present in an event for the workflow action menus for those fields; otherwise it appears in all field menus.*

Apply only to the following event types  
4  
*Specify a comma-separated list of event types that an event must be associated with for the workflow action to appear in its menu.*

# 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



# Testing the GET Workflow Action

The screenshot shows a Splunk search results page. On the left, a search result is displayed with the following details:

- Date: 8/17/16
- Time: Thu Aug 18 2016 00:29:24
- User: www3
- Process: sshd[3672]
- Message: Failed password for invalid user git from 10.2.10.163 port 1435 ssh2

Below the search result is a "Event Actions" dropdown menu. One item in the menu, "Get info for IP:10.2.10.163", is highlighted with a green box and has a green arrow pointing to it from the bottom right.

On the right, a modal window titled "10.2.10.163 address profile" is open. It contains two tabs: "Whois" (selected) and "Diagnostics". The "Whois" tab displays the following information:

IP Whois	
NetRange:	10.0.0.0 – 10.255.255.255
CIDR:	10.0.0.0/8
NetName:	PRIVATE-ADDRESS-ABLK-RFC1918-IANA-RESERVED
NetHandle:	NET-10-0-0-0-1
Parent:	( )
NetType:	IANA Special Use
OriginAS:	
Organization:	Internet Assigned Numbers Authority (IANA)
RegDate:	
Updated:	2013-08-30
Comment:	These addresses are in use by many millions of independently operated networks.
Comment:	
Comment:	These addresses can be used by anyone without any need to coordinate with IANA.
Comment:	
Comment:	These addresses were assigned by the IETF, the organization that develops Internet standards.
Comment:	<a href="http://datatracker.ietf.org/doc/rfc1918">http://datatracker.ietf.org/doc/rfc1918</a>
Ref:	<a href="https://whois.arin.net/rest/net/NET-10-0-0-0-1">https://whois.arin.net/rest/net/NET-10-0-0-0-1</a>

A note at the top right of the Whois section states: "cache expires in 10 hours, 35 minutes and 3 seconds".

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (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

The screenshot shows the 'Add new' workflow action configuration page. The steps are numbered as follows:

1. Destination app: search
2. Name \*: multiple\_attempts\_to\_open\_ports
3. Label \*: Create ticket - multiple attempts to port:\$port\$
4. Apply only to the following fields: port
5. Show action in: Event menu
6. Action type \*: link

The 'Name' field has a note: "Enter a unique name without spaces or special characters. This is used for identifying your workflow action." The 'Label' field has a note: "Enter the label that appears for this action. Optionally, incorporate a field's value by enclosing it in \$field\$." The 'Apply only to the following fields' field has a note: "Specify a comma-separated list of fields that must be present in an event for the workflow action to appear in the field menus for those fields; otherwise it appears in all field menus." The 'Show action in' field has a note: "Specify a comma-separated list of event types that an event must be associated with for the workflow action to appear in the event menu." The 'Action type' field has a note: "Select the type of action to perform when the user selects this item from the menu." The 'Link' option is selected.

# 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 \*

Enter the location to link to. Optionally, specify fields by enclosing the field name in dollar signs (\$). For example, \$port\$.

Open link in

New window

Link method

post

Post arguments

title	=	Multiple attempts to open\$port\$	<a href="#">Delete</a>
description	=	\$_raw\$	<a href="#">Delete</a>

Add another field

Cancel

Save

11

7

8

9

10

# 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' workflow action configuration page. The 'Action type' dropdown at the bottom is set to 'search'. The following fields are filled out:

- Destination app:** search
- Name \***: search\_login\_by\_IP
- Label \***: Search failed login from IP:\$src\$
- Apply only to the following fields:** src
- Apply only to the following event types:** (empty)
- Show action in:** Event menu
- Action type \***: search (highlighted with a green border)

Step numbers 1 through 6 are overlaid on the form fields:

- Destination app
- Name \*
- Label \*
- Apply only to the following fields
- Show action in
- Action type \*

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (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 \*

index=security sourcetype=linux\_secure failed src=\$src\$

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

Run in app

search

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

Open in view

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

Run search in

New window

Time range

Earliest time      Latest time

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

Cancel

Save

The screenshot shows the 'Search configuration' dialog box. Step 7 is highlighted in orange around the 'Search string' field containing the search query. Step 8 is highlighted around the 'Run in app' dropdown set to 'search'. Step 9 is highlighted around the 'Run search in' dropdown set to 'New window'. Step 10 is highlighted around the 'Earliest time' and 'Latest time' fields. Step 11 is highlighted around the 'Use the same time range as the search that created the field listing' checkbox. Step 12 is highlighted around the 'Save' button at the bottom right.

# Testing the Search Workflow Action

The screenshot shows the Splunk interface with a search workflow action open. On the left, there's a sidebar with 'Event Actions' dropdown, 'Build Event Type' section (Get info for IP:125.7.55.180), 'Extract Fields' section (Search failed login from IP:125.7.55.180), and 'Show Source' section (host: www1 port: 2911). A green box highlights the 'Search failed login from IP:125.7.55.180' button. To its right is a list of values: errOr (error), failed\_login, sshd\_authentication, nix-all-logs, nix\_errors (error), www1, and 2911. A green arrow points from the 'Search failed login from IP:125.7.55.180' button to the search bar in the main panel. The main panel shows a 'New Search' dialog with the query 'index=security sourcetype=linux\_secure failed src=125.7.55.180'. Below it, a search results table displays two events:

	i	Time	Event
>	8/17/16 6:00:24.000 PM	Thu Aug 18 2016 01:00:24 www1 sshd[4090]: Failed password for invalid user sys tem from 125.7.55.180 port 4603 ssh2 eventtype = errOr error eventtype = failed_login eventtype = sshd_authentication authentication remote eventtype = nix-all-logs eventtype = nix_errors error host = www1   port = 4603   source = /opt/log/www1/secure.log   sourcetype = linux_secure   tag = authentication tag = error tag = remote	
>	8/17/16 6:00:08.000 PM	Thu Aug 18 2016 01:00:08 www1 sshd[1116]: Failed password for invalid user zab ix from 125.7.55.180 port 4603 ssh2 eventtype = errOr error eventtype = failed_login eventtype = sshd_authentication authentication remote eventtype = nix-all-logs eventtype = nix_errors error host = www1   port = 4603   source = /opt/log/www1/secure.log   sourcetype = linux_secure   tag = authentication tag = error tag = remote	

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Module 13:

# Creating Data Models

Generated for Subbaiah Kandula ([s.venkata.kandula@accenture.com](mailto:s.venkata.kandula@accenture.com)) (C) Splunk Inc, not for distribution

# Objectives

---

- Describe the relationship between data models and Pivot
- Identify data model datasets
- Identify dataset fields
- Create a data model
- Use a data model in Pivot

# Reviewing Pivot

- Used for creating reports and dashboards (discussed in Fundamentals 1)
- As a knowledge manager, you're responsible for building the data model that provides the datasets for Pivot

The image shows two screenshots from the Splunk interface. On the left is the 'Datasets' page, which lists 60 datasets. One dataset, 'Buttercup Games Site Activity > Web Requests', has its 'Pivot' button highlighted with a green box. On the right is the 'New Pivot' interface, showing a summary of 38,475 events from July 10, 2016, to August 9, 2016. The pivot table includes 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, Orvil the Wolverine, Puppies vs. Zombies, SIM Cubicle, and a count of web requests. The 'product\_name' column is also visible.

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	SIM Cubicle
addtocart	280	271	385	387	425	377	391	382	465	275	312	481
changequantity	60	65	95	94	88	80	88	97	88	72	65	87
purchase	151	157	218	223	221	204	218	201	262	136	164	272
remove	59	44	102	81	80	75	94	68	103	72	60	113
view	238	247	381	328	366	294	378	344	405	265	325	407

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Overview of Data Models

- Hierarchically structured datasets that generate searches and drive Pivot
  - Pivot reports are created based on datasets
  - Each event, search or transaction is saved as a separate dataset

The screenshot shows the Splunk Data Model Editor interface. The title bar reads "splunk > App: Search & Reporting > Buttercup Games Site Activity". The main area is titled "Buttercup\_Games\_Site\_Activity". On the left, there's a sidebar with sections for "Datasets", "EVENTS", "SEARCHES", and "TRANSACTIONS". Under "EVENTS", the "Web Requests" dataset is selected, showing its structure. It includes "Successful Requests" (purchases, addtocart, remove) and "Failed Requests" (failed purchases, failed addtocart, failed remove). On the right, the "Web Requests" dataset is detailed with fields like "\_time" (Time), "host" (String), "source" (String), "sourcetype" (String), "action" (String), "bytes" (Number), "categoryId" (String), "change\_type" (String), "clientip" (IPv4), and "cookie" (String). Each field has an "Edit" button and an "Override" link.

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Data Model Dataset Types

- Data models consist of 3 types of datasets

1. Events
2. Searches
3. Transactions

Buttercup Games Site Activity  
Buttercup\_Games\_Site\_Activity  
< All Data Models

Datasets Add Dataset ▾

EVENTS

Web Requests

Successful Requests

- purchases
- addtocart
- remove

Failed Requests

- failed purchases
- failed addtocart
- failed remove

SEARCHES

User

TRANSACTIONS

visit duration

CONSTRAINTS

index=web sourcetype=access\_combined

Bulk Edit ▾

INHERITED

- \_time Time
- host String
- source String
- sourcetype String

EXTRACTED

- action String
- bytes Number
- categoryid String
- change\_type String
- clientip String
- cookie String
- date\_hour Number

Rename Delete

Constraint Edit

Add Field ▾

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

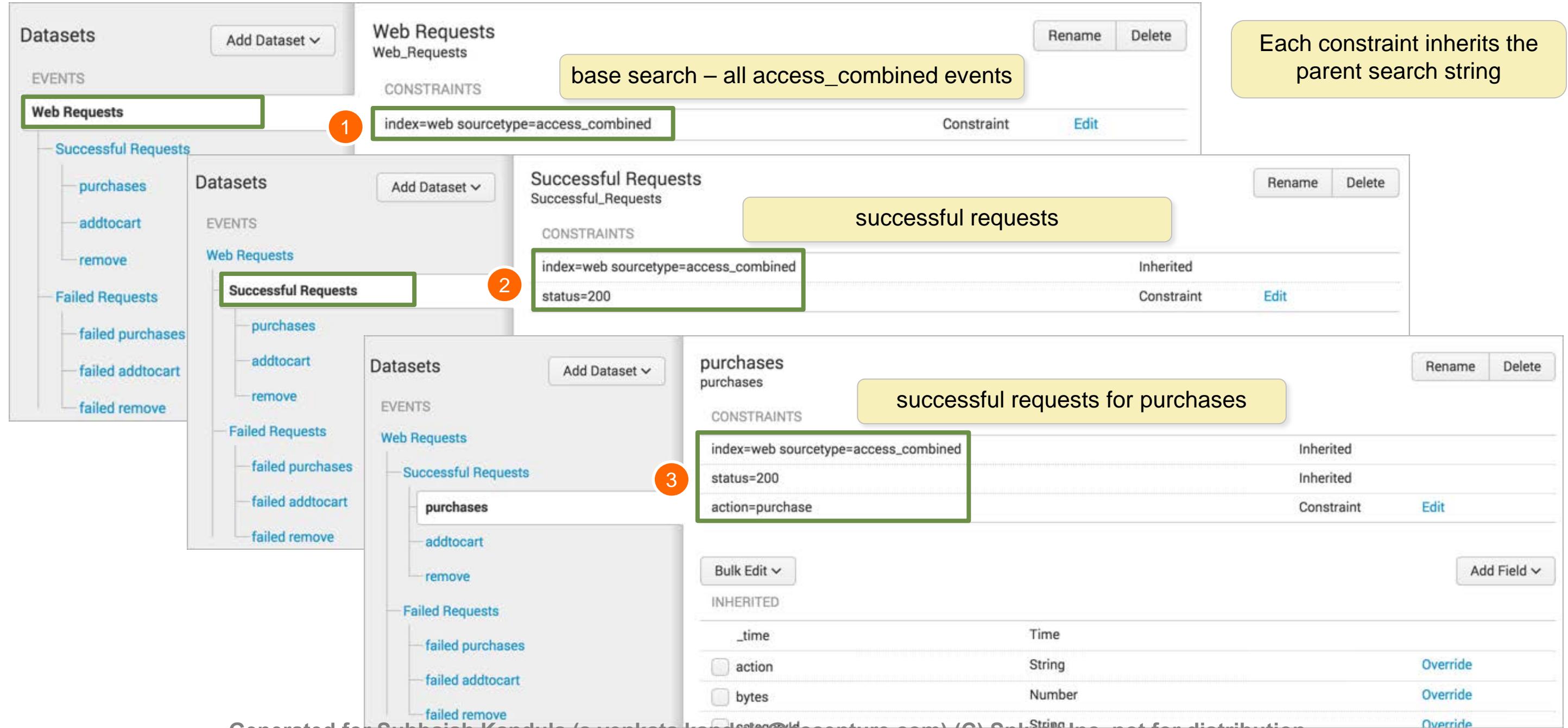
# Data Model Events

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

The screenshot shows the Splunk Data Model Editor interface. On the left, under 'DATASETS', there is a list of datasets. The 'Web Requests' dataset is selected, shown in the main pane. The 'EVENTS' section contains a tree view of event types: 'Successful Requests' (with sub-events like 'purchases', 'addtocart', 'remove') and 'Failed Requests' (with sub-events like 'failed purchases', 'failed addtocart', 'failed remove'). Below these are sections for 'SEARCHES' (User) and 'TRANSACTIONS' (visit duration). On the right, the 'CONSTRAINTS' section displays a search string: 'index=web sourcetype=access\_combined'. This string is highlighted with a yellow box labeled 'base search'. Below the constraints, the 'FIELDS' section lists various fields with their types and edit options. Fields include '\_time' (Time), 'host' (String, Override), 'source' (String, Override), 'sourcetype' (String, Override), 'action' (String, Edit), 'bytes' (Number, Edit), 'categoryId' (String, Edit), 'change\_type' (String, Edit), 'clientip' (String, Edit), 'cookie' (String, Edit), and 'date\_hour' (Number, Edit). A yellow box highlights the 'fields' section.

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Event Object Hierarchy and Constraints



# Dataset Fields

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

The screenshot shows the 'Web Requests' dataset configuration page. At the top, there are 'Rename' and 'Delete' buttons. Below that, the title 'Web Requests' and the identifier 'Web\_Requests' are displayed, along with a 'CONSTRAINTS' section containing the query 'index=web sourcetype=access\_combined'. To the right of the query are 'Constraint' and 'Edit' buttons. A green box highlights the 'INHERITED' and 'EXTRACTED' sections. In the 'INHERITED' section, fields like '\_time', 'host', 'source', and 'sourcetype' are listed with their types (Time, String, String, String) and 'Override' links. In the 'EXTRACTED' section, fields like 'action', 'bytes', 'categoryid', 'change\_type', 'clientip', 'cookie', 'date\_hour', 'date\_mday', 'date\_minute', 'date\_month', and 'date\_second' are listed with their types (String, Number, String, String, String, String, Number, Number, Number, String, Number) and 'Edit' links.

INHERITED		
_time	Time	
<input type="checkbox"/> host	String	<a href="#">Override</a>
<input type="checkbox"/> source	String	<a href="#">Override</a>
<input type="checkbox"/> sourcetype	String	<a href="#">Override</a>

EXTRACTED		
<input type="checkbox"/> action	String	<a href="#">Edit</a>
<input type="checkbox"/> bytes	Number	<a href="#">Edit</a>
<input type="checkbox"/> categoryid	String	<a href="#">Edit</a>
<input type="checkbox"/> change_type	String	<a href="#">Edit</a>
<input type="checkbox"/> clientip	String	<a href="#">Edit</a>
<input type="checkbox"/> cookie	String	<a href="#">Edit</a>
<input type="checkbox"/> date_hour	Number	<a href="#">Edit</a>
<input type="checkbox"/> date_mday	Number	<a href="#">Edit</a>
<input type="checkbox"/> date_minute	Number	<a href="#">Edit</a>
<input type="checkbox"/> date_month	String	<a href="#">Edit</a>
<input type="checkbox"/> date_second	Number	<a href="#">Edit</a>

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Dataset Fields (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 Splunk UI for managing dataset fields. At the top, it says "Web Requests" and "Web\_Requests". Below that is a "CONSTRAINTS" section with the query "index=web sourcetype=access\_combined". To the right are "Constraint" and "Edit" buttons. On the far right, there are "Rename" and "Delete" buttons. A "Bulk Edit" dropdown is open. The main area is divided into "INHERITED" and "EXTRACTED" sections. The "INHERITED" section lists fields: \_time (Time), host (String), source (String), and sourcetype (String). The "EXTRACTED" section lists fields: action (String), bytes (Number), categoryId (String), change\_type (String), clientip (String), cookie (String), date\_hour (Number), date\_mday (Number), date\_minute (Number), date\_month (String), and date\_second (Number). Each field entry has an "Edit" link to its right. On the far right, a sidebar lists "Auto-Extracted", "Eval Expression", "Lookup", "Regular Expression", and "Geo IP", with "Auto-Extracted" highlighted by a green box.

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Data Model Search Datasets

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

The screenshot shows the Splunk Data Model Editor interface. On the left, there's a sidebar with 'Buttercup Games Site Activity' under 'All Data Models'. The main area shows a search definition:

```
_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 the search definition, there's a 'User' section with 'User' selected. Under 'BASE SEARCH', the same search command is shown again. To the right, there's a 'Bulk Edit' section with a dropdown menu open, showing options like 'Auto-Extracted', 'Eval Expression', 'Lookup', 'Regular Expression', and 'Geo IP'. At the bottom, it says: 'Calculated fields are processed in the order above, so ensure any dependent fields are defined first. Drag to rearrange.'

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Data Model Transaction Datasets

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

Buttercup Games Site Activity  
Buttercup\_Games\_Site\_Activity

< All Data Models

Datasets Add Dataset ▾

EVENTS

Web Requests

- Successful Requests
  - purchases
  - addtocart
  - remove
- Failed Requests
  - failed purchases
  - failed addtocart
  - failed remove

SEARCHES

User

TRANSACTIONS

visit duration

visit duration visit\_duration

CONSTRAINTS

Group Datasets Web\_Requests Transaction Edit

Group By clientip

Max Pause 10s

Max Span

Bulk Edit ▾ Add Field ▾

INHERITED

Field	Type	Required	Action
_time	Time	Required	
duration	Number	Required	Override
eventcount	Number	Required	Override
host	String		Override
source	String		Override
sourcetype	String		Override

EXTRACTED

Field	Type	Action
action	String	Edit
bytes	Number	Edit
categoryid	String	Edit
change_type	String	Edit

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Search and Transaction Dataset Considerations

---

- There must be at least one event or search dataset before adding a transaction dataset
- Search and Transaction datasets 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 datasets?
- 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 web interface for managing data models. At the top, there's a navigation bar with links like 'splunk>', 'App: Search & R...', 'cfarrell', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. Below the navigation is a header titled 'Data Models' with a sub-instruction: 'Data models enable users to easily create reports in the Pivot tool. [Learn More](#)'. On the left, a table lists three existing data models: 'Splunk's Internal Audit Logs - SAMPLE' and 'Splunk's Internal Server Logs - SAMPLE', both categorized under 'App: Search & Reporting (search)'. To the right of the table is a 'New Data Model' dialog box. The dialog has fields for 'Title' (set to 'Buttercup Games Site Activity'), 'ID' (set to 'Buttercup\_Games\_Site\_Activity' with a note about allowed characters), 'App' (set to 'Search & Reporting'), and 'Description' (set to 'optional'). There are 'Cancel' and 'Create' buttons at the bottom. A green arrow points from the 'New Data Model' button in the header to the dialog box. Two yellow callout boxes provide additional information: one pointing to the 'Title' field with the text 'ID is automatically populated from Title, but can be overridden', and another pointing to the 'App' field with the text 'Choose app context'.

Generated for Subbaiah Kandula ([s.venkata.kandula@accenture.com](mailto:s.venkata.kandula@accenture.com)) (C) Splunk Inc, not for distribution

# Adding a Root Event

The screenshot illustrates the process of adding a root event dataset in Splunk. It shows three main windows:

- Left Window (Buttercup Games Site Activity):** Shows the 'Root Event' and 'Root Search' options highlighted with a green box. A green arrow points from this window to the 'Add Event Dataset' window.
- Middle Window (Add Event Dataset):** Titled 'Add Event Dataset' with 'Data Model: Buttercup Games Site Activity'. It contains fields for 'Dataset Name' (Web Requests) and 'Constraints' (index=web sourcetype=access\_combined). A yellow callout box says: "Constraints are essentially search terms – add child events (discussed later in this section) to further "narrow" your search".
- Right Window (Preview):** Shows the results of the constraint 'index=web sourcetype=access\_combined'. It displays 1,000 events from August 9, 2016, at 10:05:41 AM. A yellow callout box says: "Click Preview to view the events that the constraint returns". A green arrow points from the 'Preview' button to the callout.

**Event Preview Sample:**

- 203.223.0.20 - - [09/Aug/2016:17:05:25] "GET /category.screen?categoryId=NULL&JSESSIONID=SD8SL7FF4ADFF4959 HTTP 1.1" 503 1474 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-01" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 358
- 203.223.0.20 - - [09/Aug/2016:17:05:15] "GET /cart.do?action=changequantity&itemId=EST-17&productId=FS-SG-G03&JSESSIONID=SD8SL7FF4ADFF4959 HTTP 1.1" 200 2036 "http://www.buttercupgames.com/category.screen?categoryId=STRATEGY" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 525
- 203.223.0.20 - - [09/Aug/2016:17:05:02] "GET /category.screen?categoryId=ARCADE&JSESSIONID=SD8SL7FF4ADFF4959 HTTP 1.1" 200 3814 "http://www.buttercupgames.com/oldlink?itemId=EST-17" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 608

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (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 Field > Auto-Extracted** to add more fields

Buttercup Games Site Activity  
Buttercup\_Games\_Site\_Activity

< All Data Models

Edit Download Pivot Documentation

Datasets Add Dataset ▾

Web Request Web\_Request Rename Delete

EVENTS

Web Request

CONSTRAINTS

index=web sourcetype=access\_combined Constraint Edit

Bulk Edit ▾

INHERITED

	Type	
_time	Time	
host	String	
source	String	
sourcetype	String	

Add Field ▾

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

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

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Adding Fields – Auto-Extracted

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

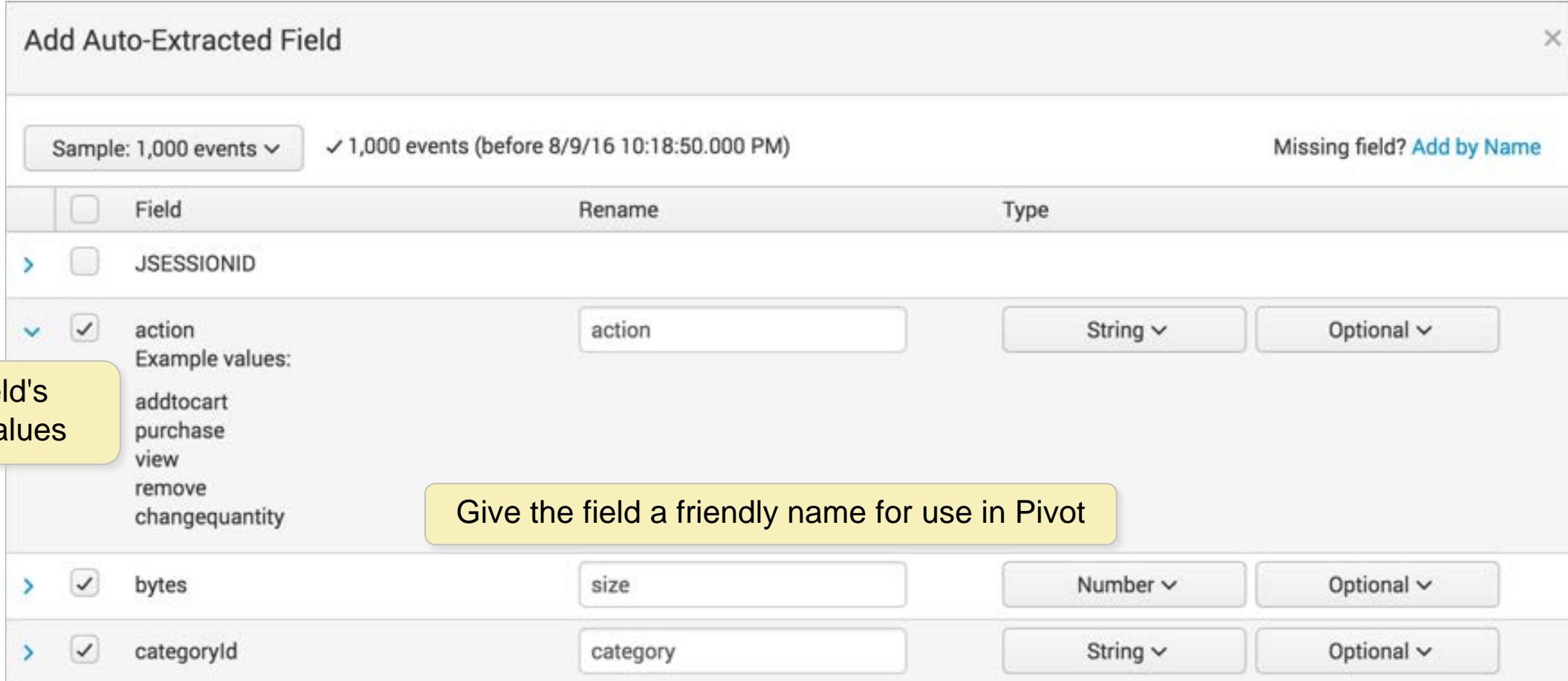
Add Auto-Extracted Field

Sample: 1,000 events ✓ 1,000 events (before 8/9/16 10:18:50.000 PM) Missing field? Add by Name

Field	Rename	Type	
> JSESSIONID			
✓ action Example values: addtocart purchase view remove changequantity	action	String	Optional
> ✓ bytes	size	Number	Optional
> ✓ categoryId	category	String	Optional

View a field's example values

Give the field a friendly name for use in Pivot



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

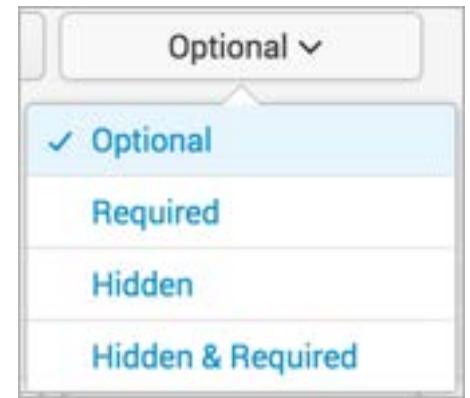
# Field Types

- **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



# Field Flags

- **Optional:** This field doesn't have to appear in every event
- **Required:** Only events that contain this field are returned in Pivot
- **Hidden:** This field is not displayed to Pivot users when they select the dataset in Pivot
  - Use for fields that are only being used to define another field, 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 Fields – Eval Expressions

- You can define a new field using an eval expression
  - In this example, you create a field named Error Reason that evaluates the value of the status field

Add Fields with an Eval Expression  
Data Model: Buttercup Games Site Activity   Dataset: Web Requests

**Eval Expression**

```
if(status>399, "Web error", "OK")
```

**Field**

Field Name:  Display Name:  Type:

Flags:

Click Preview to verify your eval expression returns events

Cancel  Save

Events	Values											
✓ 1,000 events (before 8/9/16 3:34:11.000 PM)	10 per page ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >											
Sample: 1,000 events ▾												
_time	errorReason	host	source	sourcetype	action	bytes	categoryid	change_type	clientip	cookie	date_hour	date_
2016-08-09 15:28:31	OK	www1	/opt/log/www1/access.log	access_combined		3721			27.101.11.11		22	
2016-08-09 15:28:31	OK	www1	/opt/log/www1/access.log	access_combined		3721			27.101.11.11		22	
2016-08-09 15:28:31	OK	www1	/opt/log/www1/access.log	access_combined		3721			27.101.11.11		22	
2016-08-09 15:28:31	OK	www1	/opt/log/www1/access.log	access_combined		3721			27.101.11.11		22	

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Adding Fields – 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 Fields with a Lookup  
Data Model: Buttercup Games Site Activity   Dataset: Web Requests

Documentation

Lookup Table  
http\_status\_lookup

Input  
Field in Lookup: Field in Dataset:  
code = status Remove

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

Cancel Preview Save

Auto-Extracted  
Eval Expression  
Lookup  
Regular Expression  
Geo IP

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Adding Fields – Lookups (cont.)

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

Add Fields with a Lookup  
Data Model: Buttercup Games Site Activity   Dataset: Web Requests

Documentation

Lookup Table  
http\_status\_lookup

Input  
Field in Lookup: Field in Dataset:  
code = status Remove

Add New Output  
Field in Lookup: Field in Dataset:  
 code code  
 description description

Events Values

✓ 1,000 events (before 8/9/16 3:46:04.000 PM)  
Sample: 1,000 events

20 per page

Values Count %

Values	Count	%
OK.	887	88.700
Service Unavailable.	20	2.000
Bad Request.	19	1.900
Not Found.	19	1.900
Not Acceptable.	15	1.500
Internal Server Error.	14	1.400
Request Timeout.	11	1.100
HTTP Version Not Supported.	8	0.800
Forbidden.	7	0.700

Events Values

✓ 1,000 events (before 8/9/16 3:46:04.000 PM)  
Sample: 1,000 events

Values OK. Service Unavailable. Bad Request. Not Found. Not Acceptable. Internal Server Error. Request Timeout. HTTP Version Not Supported. Forbidden.

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Adding Fields – Regular Expression

You can define a new field using a regular expression

Add Fields with a Regular Expression

Data Model: Buttercup Games Site Activity   Dataset: Web Requests

Extract From: \_raw

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

Example: From: (?<from>.\* ) To: (?<to>.\* )

Learn More ↗

Field(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 8/9/16 4:13:39.000 PM)

20 per page ▾

Cancel Preview Save

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

\_raw

27.101.11.11 - - [09/Aug/2016:22:28:31] "GET /product.screen?productId=WC-SH-A02&JSESSIONID=SD9SL2FF7ADFF4965 HTTP 1.1" 200 3721 "http://www.buttercupgames.com/product.screen?productId=WC-SH-A02" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 297

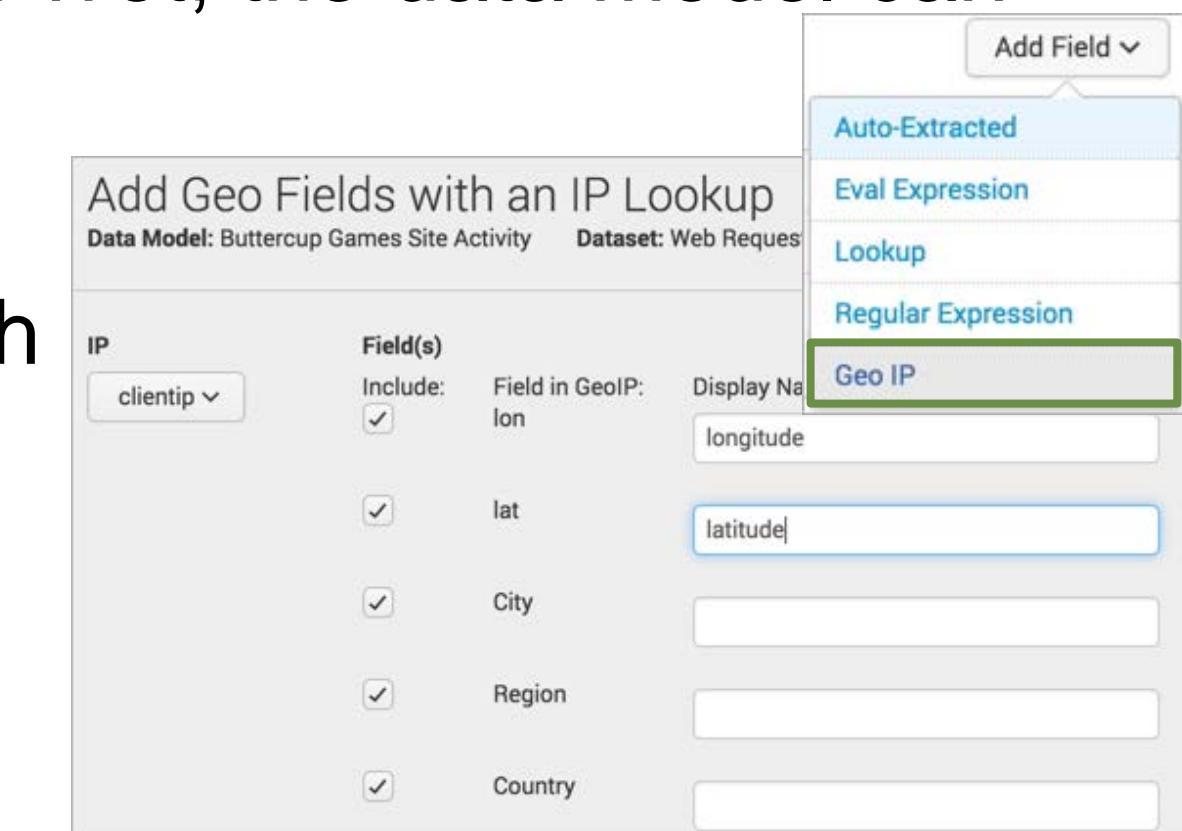
27.101.11.11 - - [09/Aug/2016:22:28:31] "GET /product.screen?productId=WC-SH-A02&JSESSIONID=SD9SL2FF7ADFF4965 HTTP 1.1" 200 3721 "http://www.buttercupgames.com/product.screen?productId=WC-SH-A02" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 297

27.101.11.11 - - [09/Aug/2016:22:28:31] "GET /product.screen?productId=WC-SH-A02&JSESSIONID=SD9SL2FF7ADFF4965 HTTP 1.1" 200 3721 "http://www.buttercupgames.com/product.screen?productId=WC-SH-A02" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 297

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Adding Fields - 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



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Adding Child Datasets

When you create a new child dataset, you give it one or more additional constraints

The screenshot shows the 'Buttercup Games Site Activity' data model interface. On the left, under 'Datasets', there is a tree view with 'Root Event' (selected), 'Root Transaction', 'Root Search', and 'Child'. A green box highlights the 'Child' node, and a green arrow points from it to the 'Add Child Dataset' dialog on the right. The dialog has the following fields:

- Data Model:** Buttercup Games Site Activity
- Dataset Name:** Successful Requests
- Dataset ID:** Successful\_Requests
- Inherit From:** Web Requests
- Additional Constraints:** status<400

A yellow callout box next to the 'status<400' constraint provides the description: "All events that have a status less than 400 (successful http request)". Below the constraint field, examples of search terms are shown: "uri=\"\*.php\*\" OR uri=\"\*.py\*\"", "NOT (referer=null OR referer=\"-\")".

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Adding Child Datasets (cont.)

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

The screenshot shows the Splunk Data Model Editor interface for a child dataset named "Successful Requests" (Successful\_Requests). At the top right are "Rename" and "Delete" buttons. Below the name is a "CONSTRAINTS" section containing two entries: "index=web sourcetype=access\_combined" and "status<400". The "status<400" entry is highlighted with a green border and has "Inherited" and "Constraint" labels next to it. An "Edit" button is also present in this row.

Below the constraints is a "Bulk Edit" dropdown menu. To its right is a "Add Field" dropdown menu with options: Auto-Extracted, Eval Expression (which is selected and highlighted in blue), Lookup, Regular Expression, and Geo IP. There are "Override" buttons for each of these options.

The main table lists fields with their types and inheritance status. The first column is labeled "INHERITED" and contains checkboxes for fields: \_time, action, bytes, categoryid, change\_type, clientip, cookie, and date\_hour. The second column lists the field names, and the third column lists their types. The "date\_hour" field is explicitly listed as "Number" instead of being inherited.

INHERITED	Field	Type
<input type="checkbox"/>	_time	Time
<input type="checkbox"/>	action	String
<input type="checkbox"/>	bytes	Number
<input type="checkbox"/>	categoryid	String
<input type="checkbox"/>	change_type	String
<input type="checkbox"/>	clientip	String
<input type="checkbox"/>	cookie	String
<input type="checkbox"/>	date_hour	Number

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Adding a Transaction

- You can add a transaction to the data model
- The transaction dataset below would equate to the search:  
**sourcetype=access\_\*** | **transaction clientip maxpause=10s**

Add Transaction Dataset  
Data Model: Buttercup Games Site Activity

You must specify at least one of the optional fields.

Select a dataset from the data model to base the transaction on

Dataset Name: visit duration

Dataset ID?: visit\_duration

Can only contain letters, numbers and underscores.

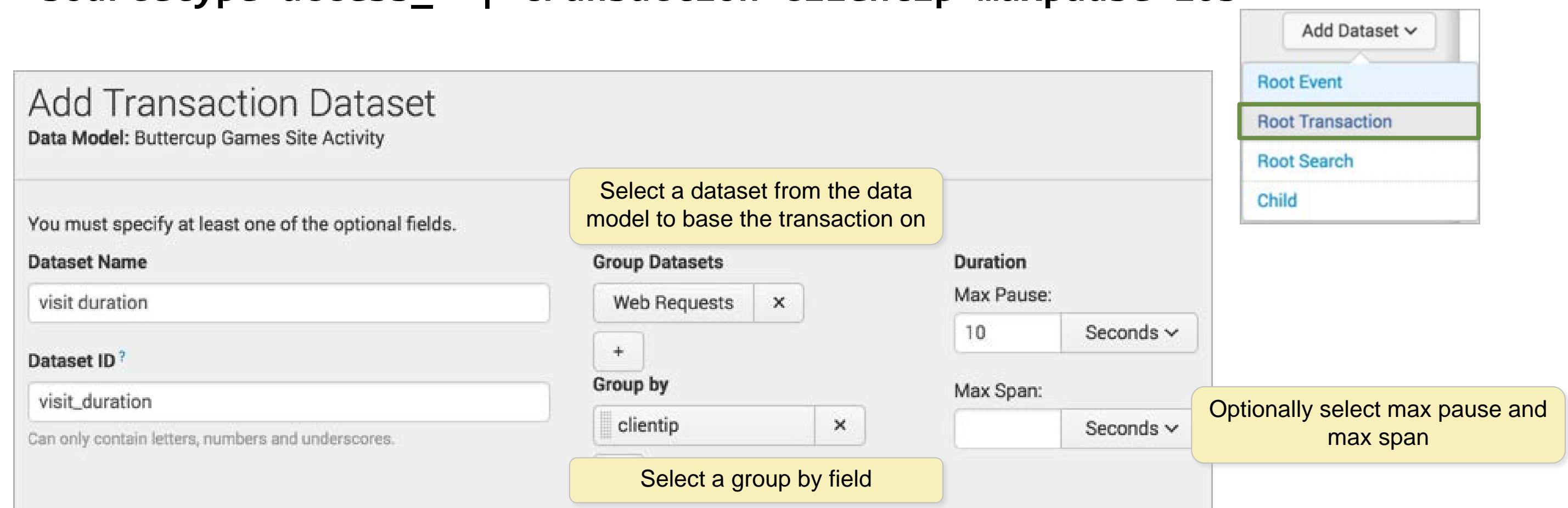
Group Datasets: Web Requests

Group by: clientip

Duration: Max Pause: 10 Seconds

Max Span:

Optional: Optionally select max pause and max span



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Adding a Transaction (cont.)

- You can then add an eval expression or any other field 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

The screenshot shows two overlapping UI components. The top component is a 'visit duration' transaction configuration in the Data Model Editor. It includes fields for Group Datasets (Web\_Requests), Group By (clientip), Max Pause (10s), and Max Span. The bottom component is a 'visit duration' dataset configuration under 'Add Fields with an Eval Expression'. It shows an 'Eval Expression' field containing 'duration/60' with a green arrow pointing to it from the left. A dropdown menu on the right lists 'Auto-Extracted', 'Eval Expression' (which is selected and highlighted in green), 'Lookup', 'Regular Expression', and 'Geo IP'. The 'Field' section on the right shows 'Field Name: visitDuration', 'Display Name: visitDuration', 'Type: Number', and 'Flags: Optional'.

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Testing the Data Model

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

Buttercup Games Site Activity  
Buttercup\_Games\_Site\_Activity

< All Data Models

Edit Download **Pivot** Documentation

Datasets Add Dataset ▾

EVENTS

**Web Requests**

Web\_Requests

CONSTRAINTS

index=web sourcetype=access\_combined

Constraint

**Successful Requests**

- purchases
- addtocart
- remove

**Failed Requests**

- failed purchases
- failed addtocart
- failed remove

Bulk Edit ▾

INHERITED

\_time Time

host String

source String

sourcetype String

EXTRACTED

Select a Dataset

i 10 Objects in Buttercup Games Site Activity

> Web Requests

> Successful Requests

> purchases

> addtocart

> remove

> Failed Requests

> failed purchases

> failed addtocart

> failed remove

> visit duration

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Using the Data Model in Pivot

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

The screenshot shows the Splunk New Pivot interface. On the left, the main pane displays a summary: "1,208 events (8/2/16 10:00:00.000 AM to 8/9/16 10:44:41.000 AM)" and a "Filters" section with a "Last 7 days" button. On the right, there's a "Select a Dataset" sidebar and a table view.

**Select a Dataset:**

- 10 Objects in Buttercup Games Site Activity
- Web Requests
- Successful Requests
- purchases
- addtocart
- remove
- Failed Requests** (highlighted with a green box)
- failed purchases
- failed addtocart
- failed remove
- visit duration

**Data Model:**

Count of Failed Requests: 1208

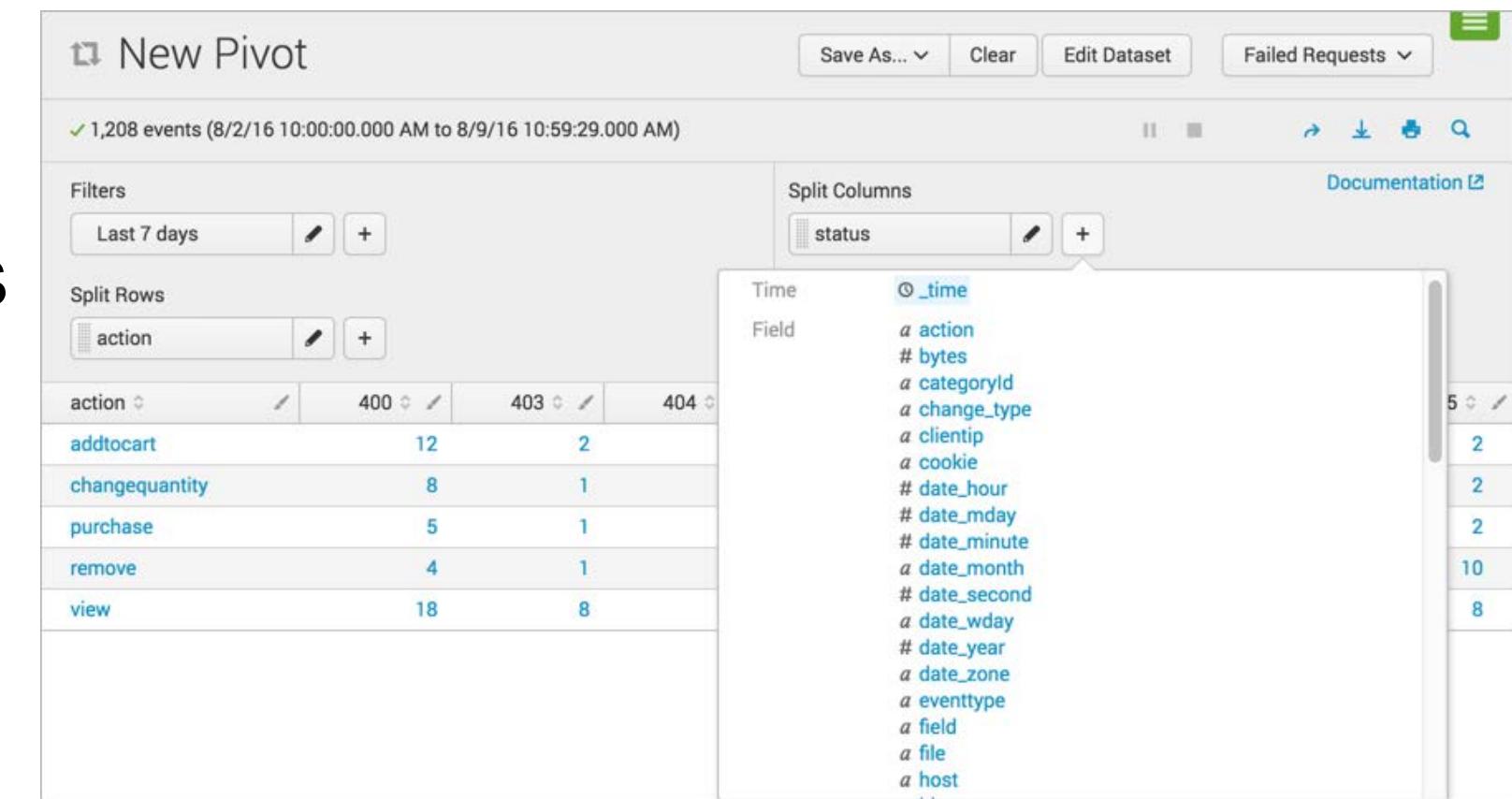
Split Columns: +

Column Values: Count of Failed Re... (with a green arrow pointing to it)

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

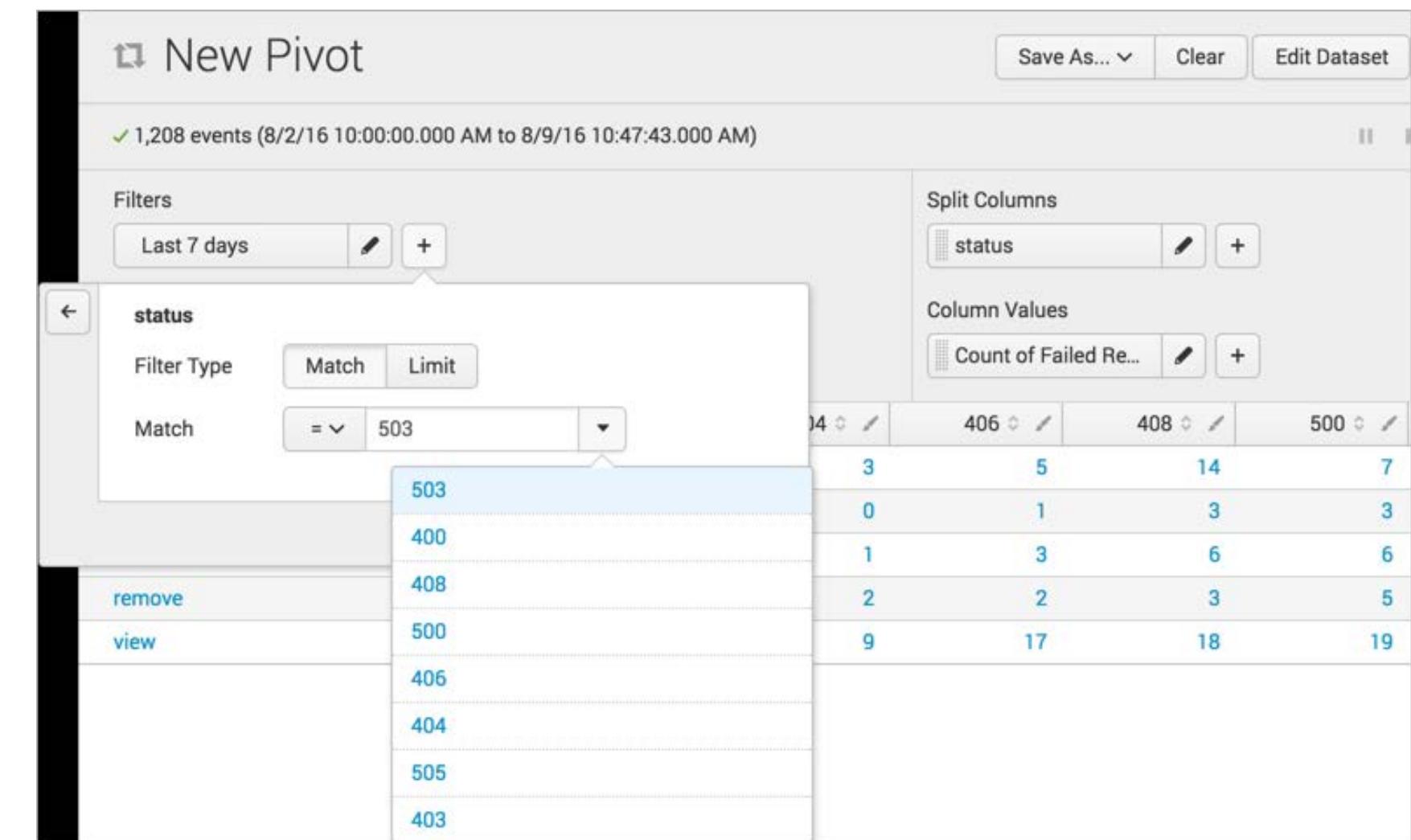
# Pivot – Using Fields

- The fields associated with each dataset 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 Fields (cont.)

- Fields can also be used to filter events in the Pivot interface
- In this example, the Pivot report is filtered to only return results where status=503



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Underlying Search

The screenshot shows the Splunk interface with two main windows. The top window is titled "New Pivot" and displays a search bar with the text "313 events (8/2/16 10:00:00.000 AM to 8/9/16 10:52:31.000 AM)". Below the search bar are several buttons: "Save As...", "Clear", "Edit Dataset", and "Failed Requests". A green box highlights the search icon in the top right corner of the search bar. The bottom window is titled "New Search" and contains a search command: `| pivot Buttercup_Games_Site_Activity Failed_Requests count(Failed_Requests) 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`. To the right of the command is a search bar with the placeholder "Last 7 days" and a magnifying glass icon. A green arrow points from the "Failed Requests" button in the top window to the magnifying glass icon in the bottom window. The bottom window also features a "Save As" button, a "Close" button, and a "Smart Mode" button. Below the search command, there are tabs for "Events", "Patterns", "Statistics (5)", and "Visualization", with "Events" selected. The "Events" tab displays a table with the following data:

Action	Count
action	503
addtocart	12
changequantity	5
purchase	146
remove	5
view	13

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Underlying Search (cont.)

Data model name

Object name

```
| pivot Buttercup_Games_Site_Activity failed_request  
count(failed_request) AS "Count of Failed requests"
```

Split row field (or attribute)

```
SPLITROW action AS action TOP 100  
count(failed_request)
```

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

```
SPLITCOL status  
FILTER status = 503
```

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (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

The screenshot shows the Splunk interface for managing data models. The main title is "Buttercup Games Site Activity" under the dataset "Buttercup\_Games\_Site\_Activity". The top navigation bar includes "Edit", "Download" (which is highlighted with a green box and a downward arrow), "Pivot", and "Documentation". Below the title, there's a link to "All Data Models".

The left sidebar shows "Datasets" and an "Add Dataset" button. Under "EVENTS", the "Web Requests" dataset is selected. The "Web Requests" section contains a "CONSTRAINTS" section with the query "index=web sourcetype=access\_combined".

The "Successful Requests" section lists categories: "purchases", "addtocart", "remove", and "Failed Requests" which includes "failed purchases".

A "Note" box states: "An HTML 5 supported browser must be used to download data models." with an information icon.

The "Downloads" window is overlaid on the interface, showing a file named "Buttercup\_Games\_Site\_Activity.json" in the "Downloads" folder. The file is 11.9 KB, a plain text document, and was modified today at 4:25:45 PM. The window also displays "1 item, Free space: 6.8 GB".

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Uploading a Data Model

The screenshot shows the Splunk Data Models interface. On the left, a list of existing data models is displayed, including "Buttercup Games Site Activity", "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 "New Data Model" tab in a modal window. The modal window is titled "Upload New Data Model" and contains fields for "File" (set to "Buttercup\_Games\_Site..."), "ID" (set to "Buttercup\_Games\_Site\_Activity\_AC"), "App" (set to "Search & Reporting"), and "Permissions" (set to "Private"). A green arrow points from the "Upload" button in the modal to the "Successful Requests" dataset under the "Web Requests" section of the main data model page.

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

3 Data Models App: Search & Reporting (search) Created in the App Owner: Any filter

i	Title ^	Type	Actions	App	Owner
>	Buttercup Games Site Activity	data model	Edit ▾ Pivot	search	cfarrell
>	Splunk's Internal Audit Logs - SAMPLE	data model	Edit ▾ Pivot	search	nobody
>	Splunk's Internal Server Logs - SAMPLE	data model	Edit ▾ Pivot	search	nobody

**Buttercup Games Site Activity**  
Buttercup\_Games\_Site\_Activity\_AC  
[All Data Models](#)

**Datasets** Add Dataset ▾

EVENTS

Web Requests Web\_Requests

CONSTRAINTS

index=web sourcetype=access\_combined Constraint Edit

Bulk Edit ▾ Add Field ▾

INHERITED

**Successful Requests**

- purchases
- addtocart

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Data Model Acceleration

- Uses automatically created summaries to speed completion times for pivots
- Takes the form of inverted time-series index files (`tsidx`) that have been optimized for speed
- Discussed in more detail in *Advanced Searching and Reporting*

Note

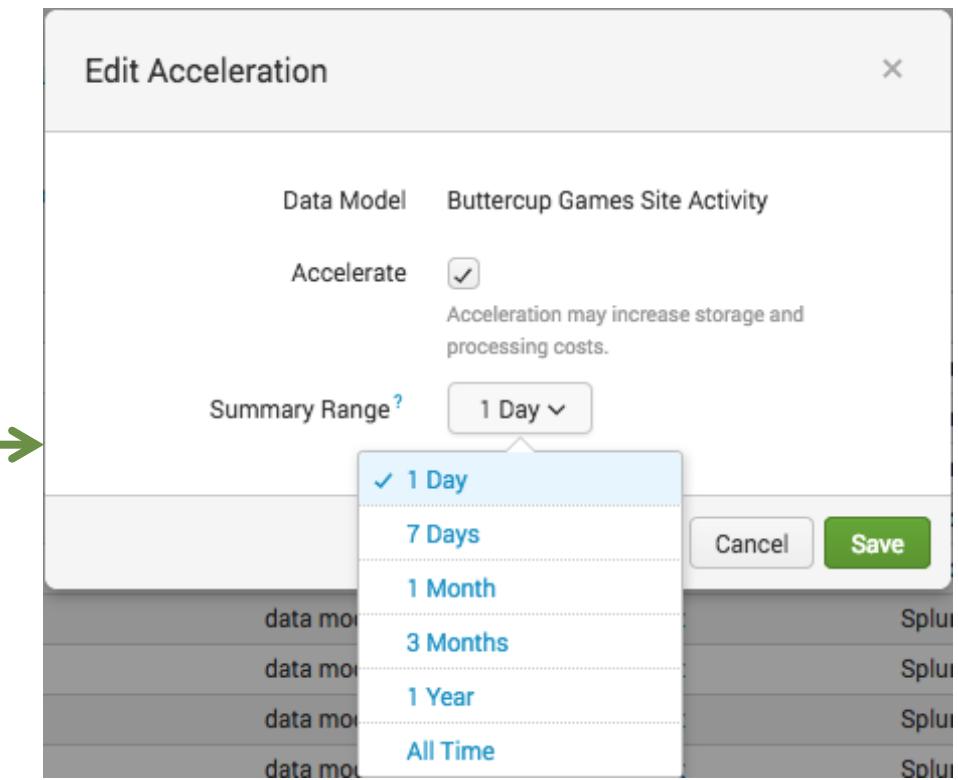


Reports can also be accelerated, as discussed in Appendix B.

# Accelerating a Data Model

- With persistent data model acceleration, all fields in the model become "indexed" fields
- 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 'Data Models' list. There is one data model named 'Buttercup Games Site Activity'. A context menu is open over this data model, with the 'Edit Acceleration' option highlighted and a green arrow pointing to the corresponding option in the 'Edit Acceleration' dialog.

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Module 14: Using the Common Information Model (CIM) Add-On

Generated for Subbaiah Kandula ([s.venkata.kandula@accenture.com](mailto:s.venkata.kandula@accenture.com)) (C) Splunk Inc, not for distribution

# Objectives

---

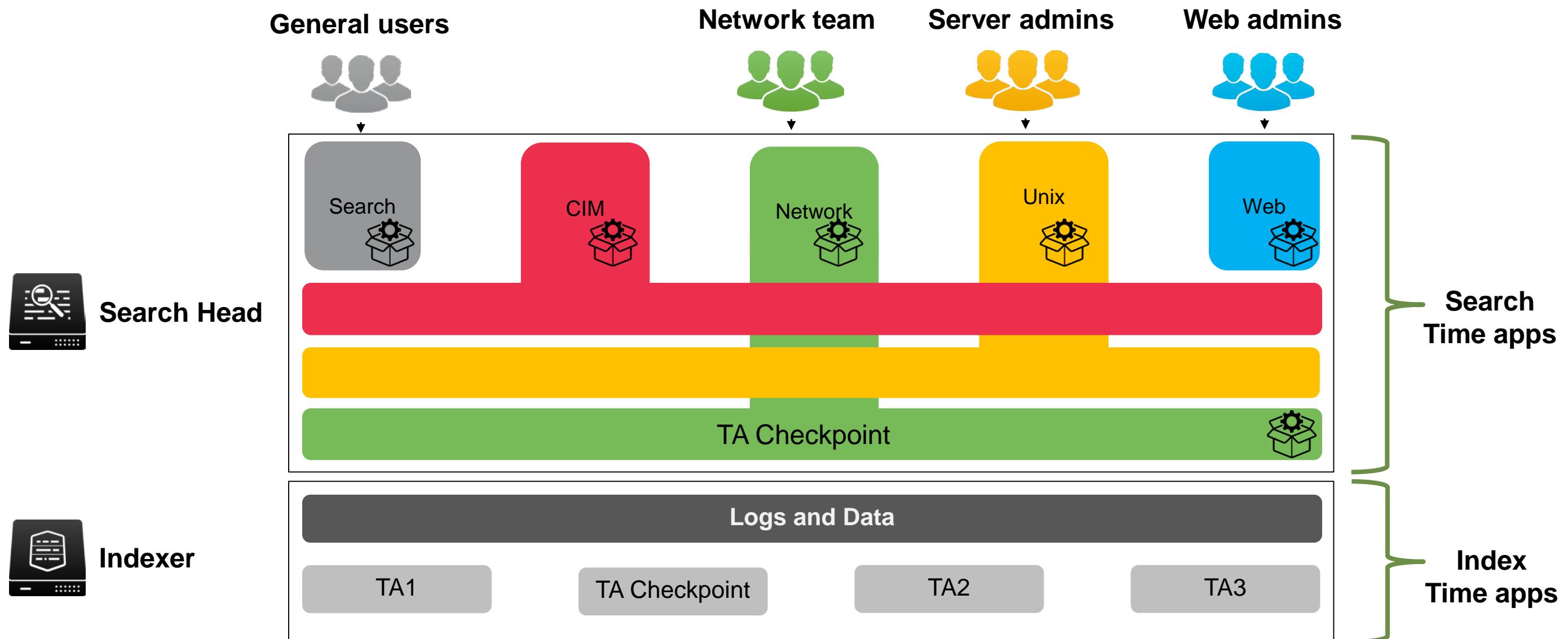
- Describe the Splunk Common Information Model
- List the knowledge objects included with the Splunk CIM Add-On
- Use the CIM Add-On to normalize data

# 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, field aliases, 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

# How the Splunk CIM Works



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# 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 <a href="#">aliased</a> from more specific fields such as src_host, src, or src_name.	

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (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 <a href="#">aliased</a> from more specific fields such as src_host, src, or src_name.	

Generated for Subbaiah Kandula ([s.venkata.kandula@accenture.com](mailto:s.venkata.kandula@accenture.com)) (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 Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Splunk CIM Add-on

- Set of 22 pre-configured data models
  - Fields and event category tags
  - Least common denominator of a domain of interest
- Leverage the CIM so that knowledge objects in multiple apps can co-exist on a single Splunk deployment
- Available on splunkbase:
  - <https://splunkbase.splunk.com/app/1621/>
- Use the CIM Reference Tables
  - <https://docs.splunk.com/Documentation/CIM/latest/User/Howtousethesreferencetables>

Splunk CIM Add-On Data Models	
<a href="#">Alerts</a>	<a href="#">Java Virtual Machines (JVM)</a>
<a href="#">Application State</a>	<a href="#">Malware</a>
<a href="#">Authentication</a>	<a href="#">Network Resolution (DNS)</a>
<a href="#">Certificates</a>	<a href="#">Network Sessions</a>
<a href="#">Change Analysis</a>	<a href="#">Network Traffic</a>
<a href="#">CIM Validation (S.o.S)</a>	<a href="#">Performance</a>
<a href="#">Databases</a>	<a href="#">Splunk Audit Logs</a>
<a href="#">Email</a>	<a href="#">Ticket Management</a>
<a href="#">Interprocess Messaging</a>	<a href="#">Updates</a>
<a href="#">Intrusion Detection</a>	<a href="#">Vulnerabilities</a>
<a href="#">Inventory</a>	<a href="#">Web</a>

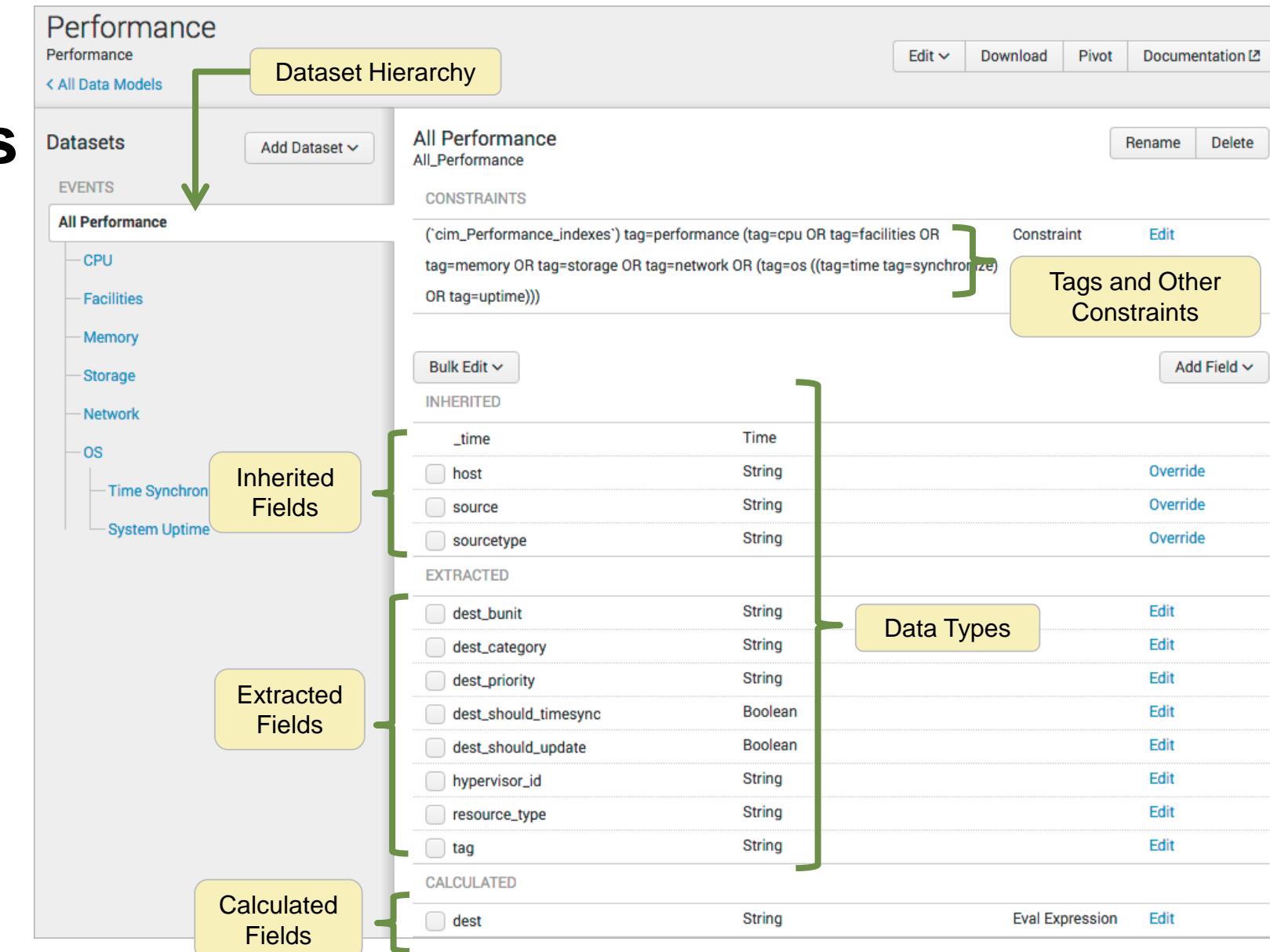
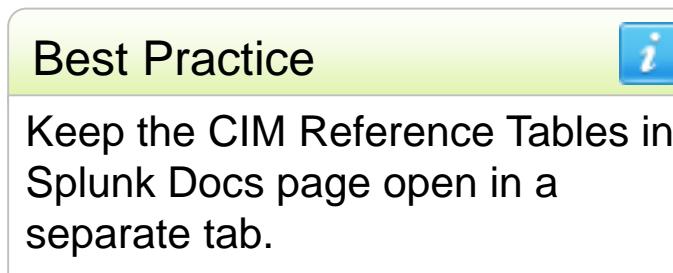
## Note

The data models included in the CIM add-on are configured with data model acceleration turned off.

# Using the CIM Add-on

## 1. Examine your data

- Go to **Settings > Data Models**
- Identify a data model relevant to your dataset



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Using the CIM Add-on (cont.)

## 2. Create event types & tags

- Identify the CIM datasets relevant to your events
- Observe which tags are required for that dataset or any parent datasets
- Apply those tags to your events using event types

The screenshot shows the Splunk interface for creating a new event type. The main window is titled "Add new Event types » Add new". It has fields for "Destination App" (set to "search"), "Name" (set to "bcg\_online\_sales"), and "Search string" (set to "index=web sourcetype=access\_combined action='\*'"). On the left, there's a sidebar with "Tag(s)" (set to "web"), "Color" (set to "blue"), and "Priority" (set to "5"). A tooltip for "Priority" explains that it determines which style wins when an event has more than one event type. A "Save As Event Type" dialog box is open in the foreground, mirroring the main window's settings: "Name" is "bcg\_online\_sales", "Tags" is "web", "Color" is "blue", and "Priority" is "5". Both dialogs have "Cancel" and "Save" buttons.

# Using the CIM Add-on (cont.)

## 3. Create field aliases

- Determine whether any existing fields in your data have different names than the names expected by the data models
- Define field aliases to capture the differently named field in your original data and map it to the field name that the CIM expects

Add new  
Fields > Field aliases > Add new

Destination app: search

Name \*: access\_combined\_aliases

Apply to: sourcetype

named \*: access\_combine

Field aliases:

Field name in your data	=	Field name in CIM object
clientip	=	src
host	=	dest
useragent	=	http_user_agent

[Add another field](#)

[Cancel](#) [Save](#)

The diagram shows a screenshot of the Splunk interface for creating a new field alias. It highlights two specific fields with yellow boxes: 'Field name in your data' (containing 'clientip', 'host', and 'useragent') and 'Field name in CIM object' (containing 'src', 'dest', and 'http\_user\_agent'). A green arrow points from the 'Field name in CIM object' box down to the 'Field name in your data' box, indicating the mapping process.

# Using the CIM Add-on (cont.)

## 4. Add missing fields

- Create field extractions
- Write lookups to add fields and normalize field values

## 5. Validate against data model

- Use the datamodel command
- Use Pivot in Splunk Web

### Note

For more information, see the *Common Information Model Add-on Manual*:  
<http://docs.splunk.com/Documentation/CIM/latest/User/Overview>

Add new  
Lookups » Automatic lookups » Add new

Destination app \* search Extract Fields  
Name \* Action Select sample Select method Select fields Save  
Next >

Lookup table \* cim\_access\_action\_lookup

Apply to \* named \*  
sourcetype sav

Lookup input fields LI\_ACTION = action\_taken

Add another field

Lookup output fields action\_primary = action Delete

Add another field

Overwrite field values

Cancel Save

1	2
1	LI_ACTION1 action_primary
2	1 Quarantine
3	2 Rename
4	3 Delete
5	4 Leave alone
6	5 Clean
7	6 Clean or delete macros

# datamodel Command

- Search against a specified data model object
- Return a description of all or a specified data model and its objects
- Is a generating command and should be the first command in the pipeline

**datamodel**    [Help](#)    [More »](#)  
Allows user to examine data models and run the search for a datamodel object.

**Examples**

Example usage  
| datamodel

**Important**



The object name and `search` keyword aren't valid unless preceded by the data model name. The keyword `search` cannot be substituted with a search string or name.

# datamodel Command – Example

```
| datamodel Web Web search | fields Web*
```

A      B      C      D      E

- A** Command
- B** Data model name
- C** Data model dataset name
- D** Keyword
- E** Find field names with Web prefix

Dataset name  
prepended to field  
names in your data

## Note



When using the datamodel command, the data model name and object name are case-sensitive.

Interesting Fields

- a Web.action 5
- # Web.bytes 100+
- a Web.dest 1
- a Web.http\_content\_type 1
- a Web.http\_method 1
- a Web.http\_referrer 1
- a Web.http\_user\_agent 1
- # Web.http\_user\_agent\_length 1
- # Web.is\_not\_Proxy 1
- # Web.is\_Proxy 1
- a Web.src 1
- # Web.status 7
- a Web.tag 2
- a Web.uri\_path 6
- a Web.uri\_query 100+
- a Web.url 1
- # Web.url\_length 1
- a Web.user 1
- a Web.vendor\_product 1

# Additional CIM Resources

---

- Understand and use the CIM Add-on

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

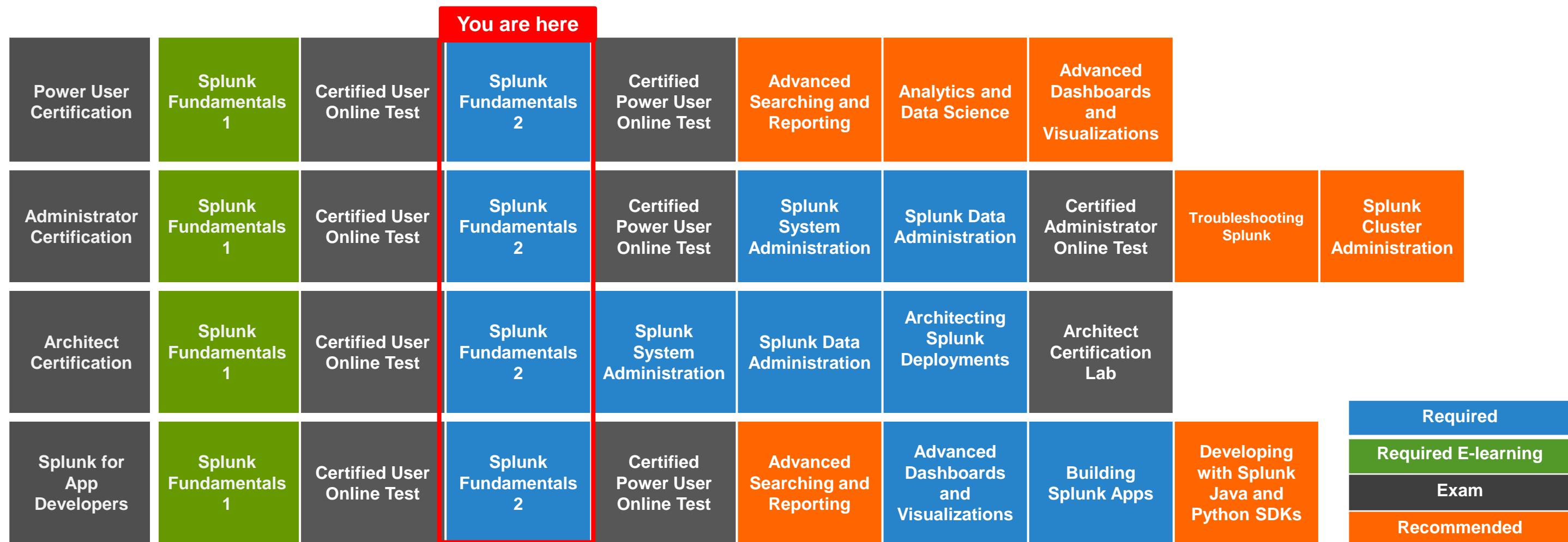
- Overview of the Splunk CIM

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

- Use the CIM to normalize data at search time

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

# What's Next?



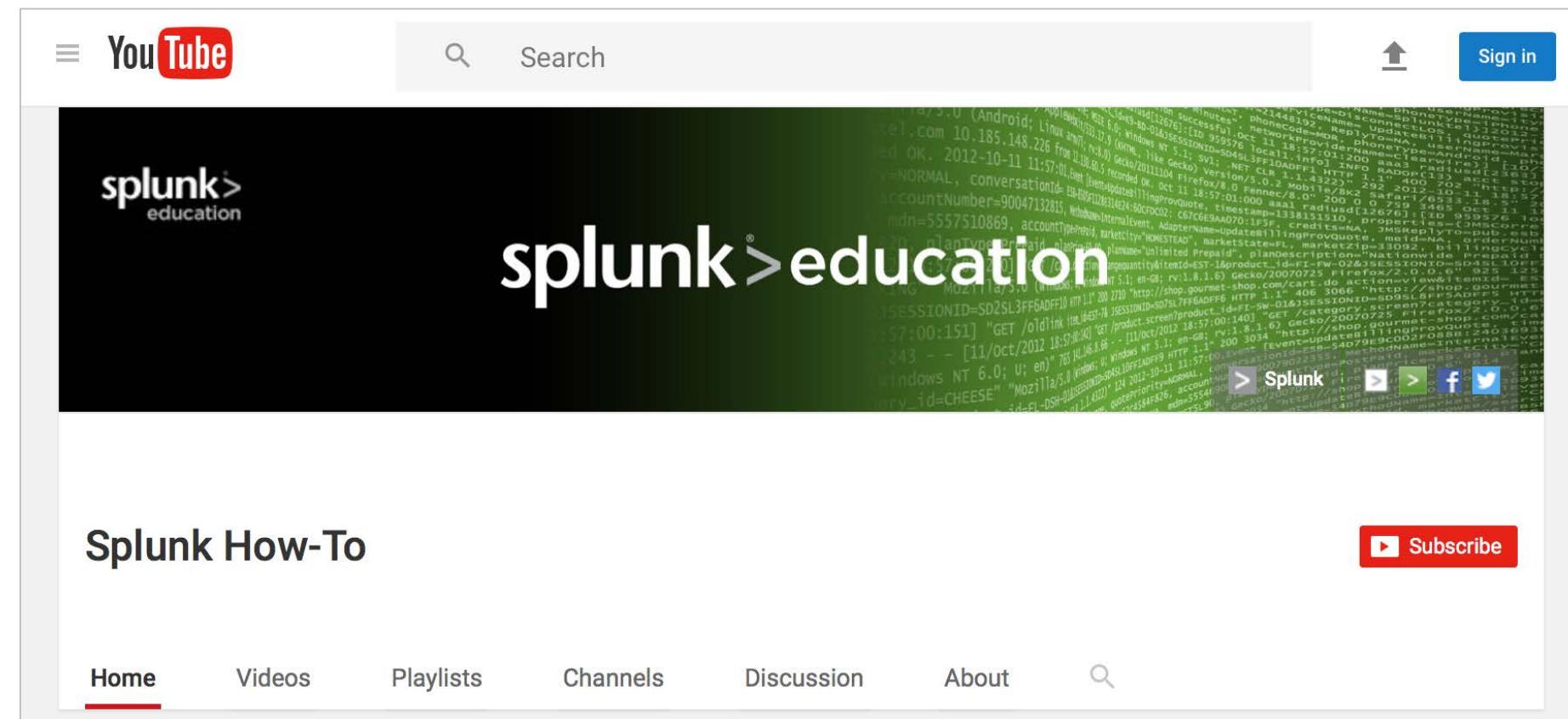
For detailed course and certification information go to: <http://splk.it/g8q>

If you have further questions, send an email to: [certification@splunk.com](mailto:certification@splunk.com)

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# YouTube: The Splunk How-To Channel

- In addition to our roster of training courses, check out the Splunk Education How-To channel: <http://www.youtube.com/c/SplunkHowTo>
- This site provides useful, short videos on a variety of Splunk topics



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Other Resources

---

- Splunk App Repository  
<https://splunkbase.splunk.com/>
- Splunk Answers  
<http://answers.splunk.com/>
- Splunk Blogs  
<http://blogs.splunk.com/>
- Splunk Wiki  
<http://wiki.splunk.com/>
- Splunk Docs  
<http://docs.splunk.com/Documentation/SplunkCloud/latest>
- Splunk User Groups  
<http://usergroups.splunk.com/>
- Splunk Slack User Group sign up page  
<splunk-usergroups.signup.team>

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Appendix A: erex, rex, multikv Commands

Generated for Subbaiah Kandula ([s.venkata.kandula@accenture.com](mailto:s.venkata.kandula@accenture.com)) (C) Splunk Inc, not for distribution

# Fields Extraction Commands

---

- **erex command**

- You do not know the regular expression to use
- You have example values in your retrieved events

- **rex command**

- NO UI; you must write regex
- Only persists for the duration of the search
- Does not persist as a knowledge object
- Good for rarely used fields

# erex Command

- Instead of using regex, the erex command allows you to extract a field at search time by providing examples
- **examples=erex-examples** comma-separated list of example values for the information to be extracted and saved into a new field

[✓ Auto Open](#)

**erex**    [Help](#)    [More »](#)

Automatically extracts field values similar to the example values.

**Examples**

Extracts out values like "7/01", putting them into the "monthday" attribute.  
... | erex monthday examples="7/01"

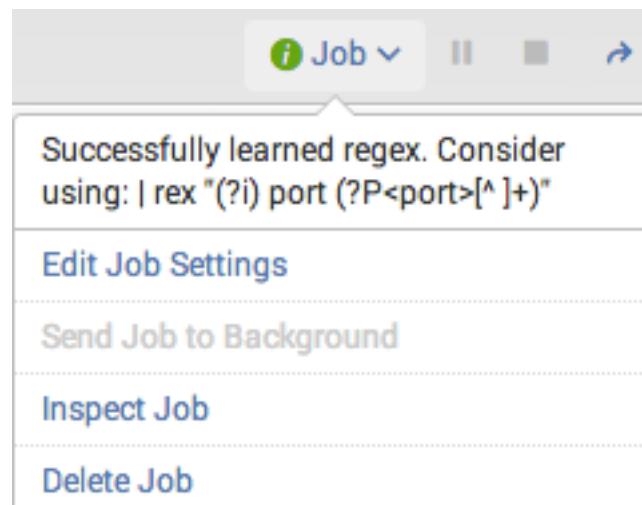
Extracts out values like "7/01" and "7/02", but not patterns like "99/2", putting extractions into the "monthday" attribute.  
... | erex monthday examples="7/01, 07/02" counterexamples="99/2"

## Note

The examples used must be in the returned results. For example, first run sourcetype=linux\_secure port and use some of the resulting ports as examples. Then, run the erex command.

# erex Command – Example

- A Creates a new field called, port
- B Extracts values using the examples, which exist in the data
  - 4987, 4549
- To view the regex generated by your search, click the Job dropdown



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

## Scenario



Display the IP address and port of potential attackers.

```
sourcetype=linux_secure port "failed password"
| erex port A examples="4945,3761" B
| table src_ip, port
```

src_ip	port
66.69.195.226	1605
66.69.195.226	2143
10.3.10.46	4945 B
10.3.10.46	3136 B
10.3.10.46	4707
10.3.10.46	3883
10.3.10.46	3475
10.3.10.46	4945 B

# rex Command

- The rex command allows you to extract fields at search time
- Matches the value of the field against unanchored regex
  - Defaults to `field=_raw`
- `regex` specifies both the match and a named capture that creates the new field

✓ Auto Open

**rex** Help More »

Specifies a Perl regular expression named groups to extract fields while you search.

**Examples**

Extract "from" and "to" fields using regular expressions. If a raw event contains "From: Susan To: Bob", then from=Susan and to=Bob.

```
... | rex field=_raw "From: (?<from>.*?) To: (?<to>.*?)"
```

**Example usage**

```
... | rex mode=sed "s/(\\d{4})\\{3}/XXXX-XXXX-XXXX-/g"
```

# rex Command – Example 1

## Scenario

Display the user name of potential email attackers.



```
index=network sourcetype=cisco_esa  
mailfrom=*  
| rex "\<(?<potentialAttacker>.*@)"  
| table potentialAttacker
```

- The Cisco router server contains the email addresses of those sending email to the company
- mailfrom contains the entire address
- Use rex to extract just the user name at search time

potentialAttacker	
OSGIMR5CJLB220KK5SVWVNDD7NH0746JAQ.1.7	
saver	
saver	

t	Time	Event
>	2/7/16 11:08:11.000 PM	Sun Feb 07 23:08:11 2016 Info: MID 245461 ICID 744500 From: <OSGIMR5CJLB220KK5SVWVNDD7NH0746JAQ.1.7@b. mypoints.com> host = cisco_router1   source = /opt/log/cisco_router1/cisco_ironport_mail.log   sourcetype = cisco_esa
>	2/7/16 10:00:37.000 PM	Sun Feb 07 22:00:37 2016 Info: MID 245459 ICID 0 From: <saver@ingdirect.com> host = cisco_router1   source = /opt/log/cisco_router1/cisco_ironport_mail.log   sourcetype = cisco_esa
>	2/7/16 9:59:10.000 PM	Sun Feb 07 21:59:10 2016 Info: MID 245458 ICID 744497 From: <saver@ingdirect.com> host = cisco_router1   source = /opt/log/cisco_router1/cisco_ironport_mail.log   sourcetype = cisco_esa

Generated for Subbaiah Kandula (s.y Venkata.Kandula@accenture.com) (C) Splunk Inc. not for distribution

# rex Command – Example 2

## Scenario

Display the user name and mail domains from which the employees are receiving email.

```
index=network sourcetype=cisco_esa mailfrom=*
| rex "\<(?<potentialAttacker>.*)@(?<domain>.*)\>"
| table mailfrom, potentialAttacker, domain
```

- Email domain is not extracted as a separate field, but as part of **mailfrom**
- Use **rex** to extract it at search time
- Can perform multiple extractions

## Note

To limit the scope of the **rex** command, use the **field=mailfrom** argument. This can significantly reduce the complexity of your regex code.

i	Time	Event
>	2/8/16 11:58:40.000 PM	Mon Feb 08 23:58:40 2016 Info: MID 245509 ICID 744601 From: <camron@akinsbrox.com> host = cisco_router1   source = /opt/log/cisco_router1/cisco_ironport_mail.log   sourcetype = cisco_esa
>	2/8/16 9:38:08.000 PM	Mon Feb 08 21:38:08 2016 Info: MID 245508 ICID 744595 From: <daily_headlines@ms3.1ga2.nytimes.com> host = cisco_router1   source = /opt/log/cisco_router1/cisco_ironport_mail.log   sourcetype = cisco_esa

mailfrom	potentialAttacker	domain
notification+ocpgree@facebookmail.com	notification+ocpgree	facebookmail.com
prvs=5481054b2=automated@ecoupons.com	prvs=5481054b2=automated	ecoupons.com
slickdeals@slickdeals.net	slickdeals	slickdeals.net

# erex vs. rex – Example

```
index=security  
sourcetype=linux_secure  
port "failed password"  
| erex port examples="3890,3761"  
| table src_ip, port
```

Scenario ?

Display IP addresses and ports of potential attackers.

```
index=security  
sourcetype=linux_secure port  
"failed password"  
| rex "port\s(?<port>\d+)"  
| table src_ip, port
```

## erex

- Easier to use  
(Do not have to know regex)
- Provides regex code
- Must constantly provide examples
- Should not use in saved reports

src_ip	port
117.21.246.164	4925
117.21.246.164	4210
117.21.246.164	1786
117.21.246.164	4596
117.21.246.164	1568

## rex

- More difficult to use  
(Must know regex)
- Do not have to provide examples
- Can use regex from erex
- Can use in saved reports

# Extracting Fields from a Table-Formatted Event

- Many data types are formatted as large single events in a table
- Each event contains titles with tabular values
  - Fieldnames are derived from the title row, A ; all other rows represent values B

i	Time	Event	index=os sourcetype=ps													
>	2/7/16 11:59:34.000 PM	USER root root root root	A	PID	PSR	pctCPU	CPUTIME	pctMEM	RSZ_KB	VSZ_KB	TTY	S	ELAPSED	COMMAND	ARGS	
			B	1	2	0.0	00:00:01	0.0	2572	19644	?	S	6-08:30:06	init	<noArgs>	
				2	0	0.0	00:00:00	0.0	0	0	?	S	6-08:30:06	[kthreadd]	<noArgs>	
				3	0	0.0	00:00:00	0.0	0	0	?	S	6-08:30:06	[ksoftirqd/0]	<noArgs>	
				5	0	0.0	00:00:00	0.0	0	0	?	S	6-08:30:06	[kworker/0:0H]	<noArgs>	
Show all 138 lines																
host = splunk1   source = ps   sourcetype = ps																
>	2/7/16 11:59:04.000 PM	USER root root root root	A	PID	PSR	pctCPU	CPUTIME	pctMEM	RSZ_KB	VSZ_KB	TTY	S	ELAPSED	COMMAND	ARGS	
			B	1	2	0.0	00:00:01	0.0	2572	19644	?	S	6-08:29:36	init	<noArgs>	
				2	0	0.0	00:00:00	0.0	0	0	?	S	6-08:29:36	[kthreadd]	<noArgs>	
				3	0	0.0	00:00:00	0.0	0	0	?	S	6-08:29:36	[ksoftirqd/0]	<noArgs>	
				5	0	0.0	00:00:00	0.0	0	0	?	S	6-08:29:36	[kworker/0:0H]	<noArgs>	
Show all 138 lines																
host = splunk1   source = ps   sourcetype = ps																
>	2/7/16 11:58:34.000 PM	USER root root root root	A	PID	PSR	pctCPU	CPUTIME	pctMEM	RSZ_KB	VSZ_KB	TTY	S	ELAPSED	COMMAND	ARGS	
			B	1	2	0.0	00:00:01	0.0	2572	19644	?	S	6-08:29:06	init	<noArgs>	
				2	0	0.0	00:00:00	0.0	0	0	?	S	6-08:29:06	[kthreadd]	<noArgs>	
				3	0	0.0	00:00:00	0.0	0	0	?	S	6-08:29:06	[ksoftirqd/0]	<noArgs>	
				5	0	0.0	00:00:00	0.0	0	0	?	S	6-08:29:06	[kworker/0:0H]	<noArgs>	
Show all 138 lines																
host = splunk1   source = ps   sourcetype = ps																

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# multikv Command

- For table-formatted events, multikv creates an event for each row
- Field names are from the first row of each event



Interesting Fields														
a ARGS 72														
a COMMAND 98														
a CPUTIME 100+														
a ELAPSED 100+														
a eventtype 3														
# pctCPU 100+														
# pctMEM 10														
# PID 100+														
# PSR 4														
a punct 1														
# RSZ_KB 100+														
a S 4														
a tag 8														
a tag::eventtype 8														
a timestamp 1														
a TTY 9														
a USER 7														
# VSZ_KB 100+														

i	Time	Event	index=os sourcetype=ps											
>	4/29/15 11:59:41.000 PM	USER root root root root	1	3	0.0	00:00:00	0.0	1604	19488	?	S	07:53:36	init	ARGS <noArgs>
			2	2	0.0	00:00:00	0.0	0	0	?	S	07:53:36	[kthreadd]	<noArgs>
			3	0	0.0	00:00:00	0.0	0	0	?	S	07:53:36	[ksoftirqd/0]	<noArgs>
			5	0	0.0	00:00:00	0.0	0	0	?	S	07:53:36	[kworker/0:0H]	<noArgs>
			Show all 106 lines											
			host = splunk1   index = main   linecount = 107   source = ps   sourcetype = ps   splunk_server = ip-10-222-134-157											
index=os sourcetype=ps   multikv														
i	Time	Event	1	3	0.0	00:00:00	0.0	1604	19488	?	S	07:53:36	init	<noArgs>
>	4/29/15 11:59:41.000 PM	root	1	3	0.0	00:00:00	0.0	1604	19488	?	S	07:53:36	init	<noArgs>
			host = splunk1   index = main   linecount = 1   source = ps   sourcetype = ps   splunk_server = ip-10-222-134-157											
>	4/29/15 11:59:41.000 PM	root	2	2	0.0	00:00:00	0.0	0	0	?	S	07:53:36	[kthreadd]	<noArgs>
			host = splunk1   index = main   linecount = 1   source = ps   sourcetype = ps   splunk_server = ip-10-222-134-157											
>	4/29/15 11:59:41.000 PM	root	3	0	0.0	00:00:00	0.0	0	0	?	S	07:53:36	[ksoftirqd/0]	<noArgs>
			host = splunk1   index = main   linecount = 1   source = ps   sourcetype = ps   splunk_server = ip-10-222-134-157											
>	4/29/15 11:59:41.000 PM	root	5	0	0.0	00:00:00	0.0	0	0	?	S	07:53:36	[kworker/0:0H]	<noArgs>
			host = splunk1   index = main   linecount = 1   source = ps   sourcetype = ps   splunk_server = ip-10-222-134-157											

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# multikv Command – fields

- To make the fields easier to read, this example pipes to the table command
- Use the fields option to limit the fields returned in the table
  - Only fields in this option are included
    - All others are ignored

```
index=os sourcetype=ps
| multikv fields USER pctCPU COMMAND
| table USER, pctCPU, COMMAND
```

USER	pctCPU	COMMAND
root	0.0	init
root	0.0	[kthreadd]
root	0.0	[ksoftirqd/0]
root	0.0	[kworker/0:0H]
root	0.0	[kworker/u30:0]

# Appendix B: Accelerating Reports

Generated for Subbaiah Kandula ([s.venkata.kandula@accenture.com](mailto:s.venkata.kandula@accenture.com)) (C) Splunk Inc, not for distribution

# Module Objectives

---

- Describe report acceleration
- Create summaries
- Search against summaries

# Comparison of Data Summary Creation Methods

Report Acceleration	<ul style="list-style-type: none"><li>• Uses automatically created summaries to speed completion times for qualified reports</li><li>• Easier to create than summary indexes and backfill automatically</li><li>• Depending on the defined time span, periodically ages out data</li><li>• Can correct gaps and overlaps from the UI 'rebuild' feature</li><li>• Cannot create a "data-cube" and report on smaller subsets</li></ul>
Summary Indexing	<ul style="list-style-type: none"><li>• Useful for speeding up searches that don't qualify for report acceleration</li><li>• Can persist after underlying events have been frozen by controlling retention period or index size</li><li>• Backfill is a manual (scripted) process</li></ul>
Data Model Acceleration	<ul style="list-style-type: none"><li>• Uses automatically created summaries to speed completion times for pivots</li><li>• Takes the form of time-series index files</li></ul>

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Report Acceleration – Overview

---

- Reports that span a large volume of data can:
  - Take a long time to complete
  - Consume a great deal of system resources
- You can ‘accelerate’ a qualifying report when you:
  - Save it
  - Create a dashboard panel based on it
  - Edit a qualifying saved report

# Report Acceleration – Conditions

---

You

- Your role has the schedule search capability
- You have write permissions for the report you want to accelerate

The report

- The report was not created via Pivot
- The search that the report is based upon is qualified for acceleration

Search Mode

- You can accelerate a qualified report if the underlying search uses verbose mode
  - Note that Splunk automatically changes the search mode to smart or fast
- You cannot change search mode of an accelerated report to verbose

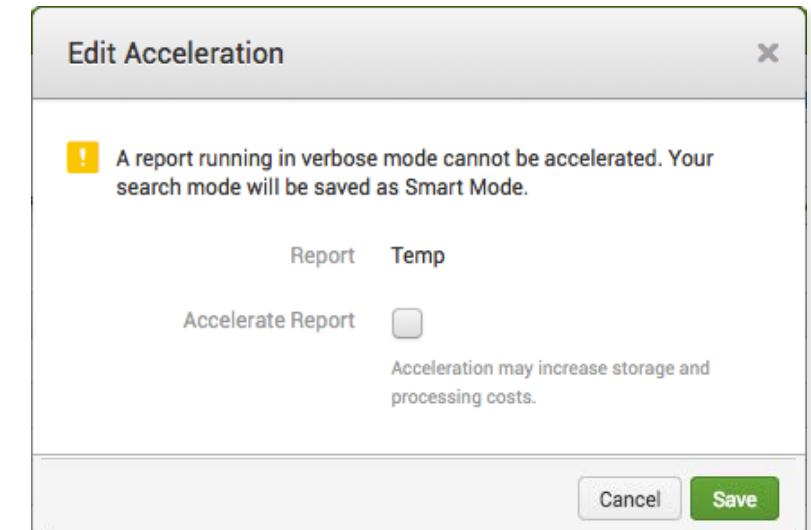
# Report Acceleration – Common Use Cases

---

- Common use cases include:
  - More efficiently run reports for large datasets over long time ranges
    - ▶ Show the number of page views and visitors for each of your websites over the past 30 days, broken out by site
  - A rolling report that shows aggregated statistics over long periods of time
    - ▶ Display a running count of downloads for a specific file on a website
    - ▶ Calculate the average amount spent per purchase over a year

# Report Acceleration – Acceleration Summaries

- To accelerate a report, Splunk creates an acceleration summary
- Acceleration summaries
  - Efficiently report on large volumes of data
  - Qualify future searches against the summary
- To accelerate a report, search mode must be set to either smart or fast
  - If in verbose mode, the report is saved with smart mode
  - Neither the timeline, nor the Fields sidebar displays
- By default, only power users can accelerate reports
- If you delete all the searches that use a summary, the summary is deleted
- If an acceleration summary is created from a shared report, reports that can use it, will use it



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Populating Search Requirements

---

- Qualifying searches
  - Search must include a reporting command
    - › For example: chart, timechart, stats, top, and rare
  - Any command before the reporting command must be a streaming command; that is, a command that applies a transformation to each event returned by the search
    - › For example: eval, fields, multikv, rex, rename, and replace

# Search Examples

---

- Qualifying search examples:

```
index=web sourcetype=access_combined action=purchase status=200  
| stats sum(price) as revenue by productId  
| eval revenue="$" + revenue
```

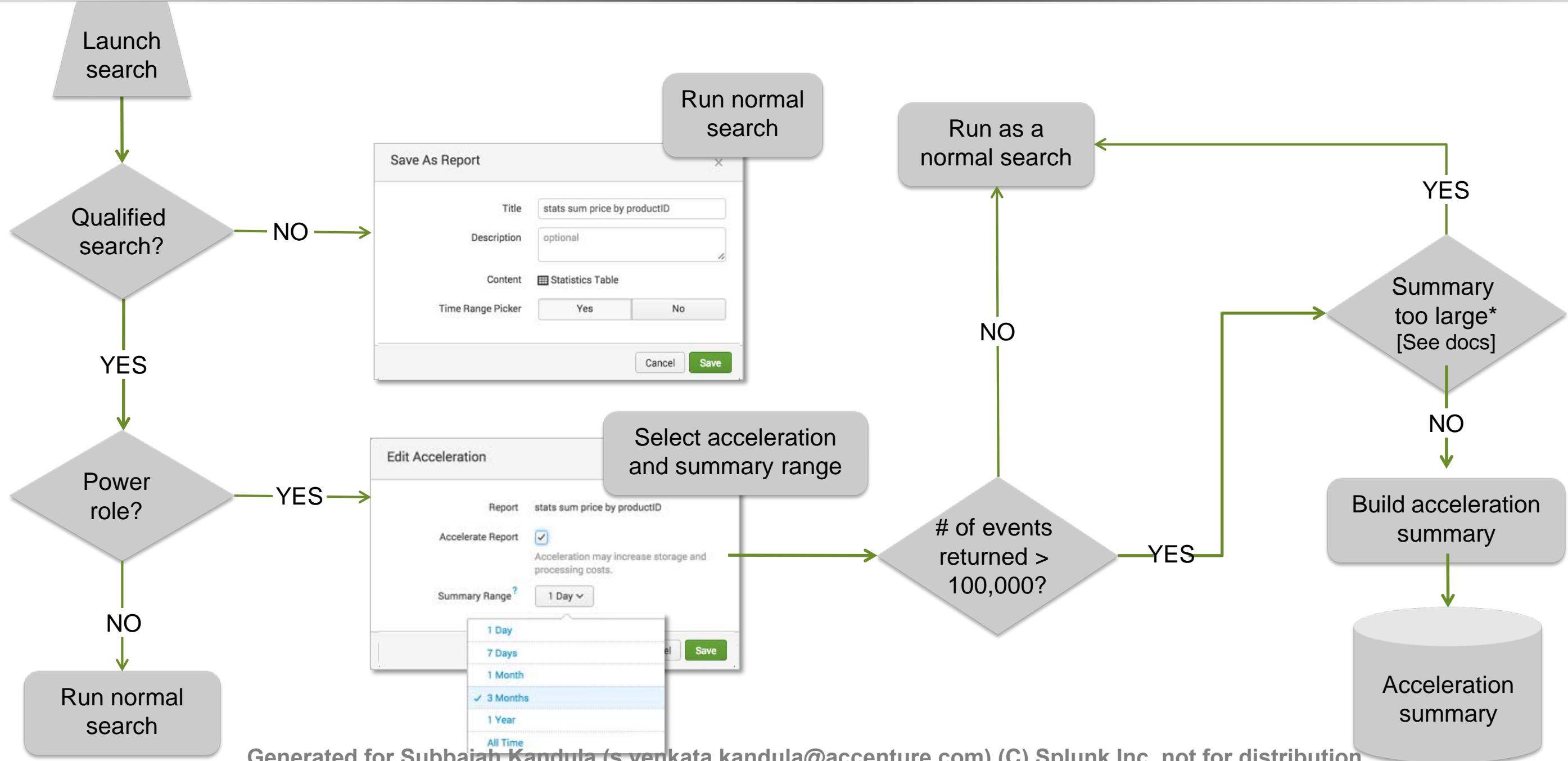
```
index=web sourcetype=access*  
| fields price action host  
| chart sum(price) over action by host
```

- Non-qualifying search examples

```
index=web sourcetype=access_combined action=purchase status=404 [No reporting  
command]
```

```
index=web sourcetype=access_combined [Transaction is not a streaming command]  
| transaction startswith="view" endswith="purchase"  
| stats avg(duration)
```

# Creating Acceleration Summaries



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

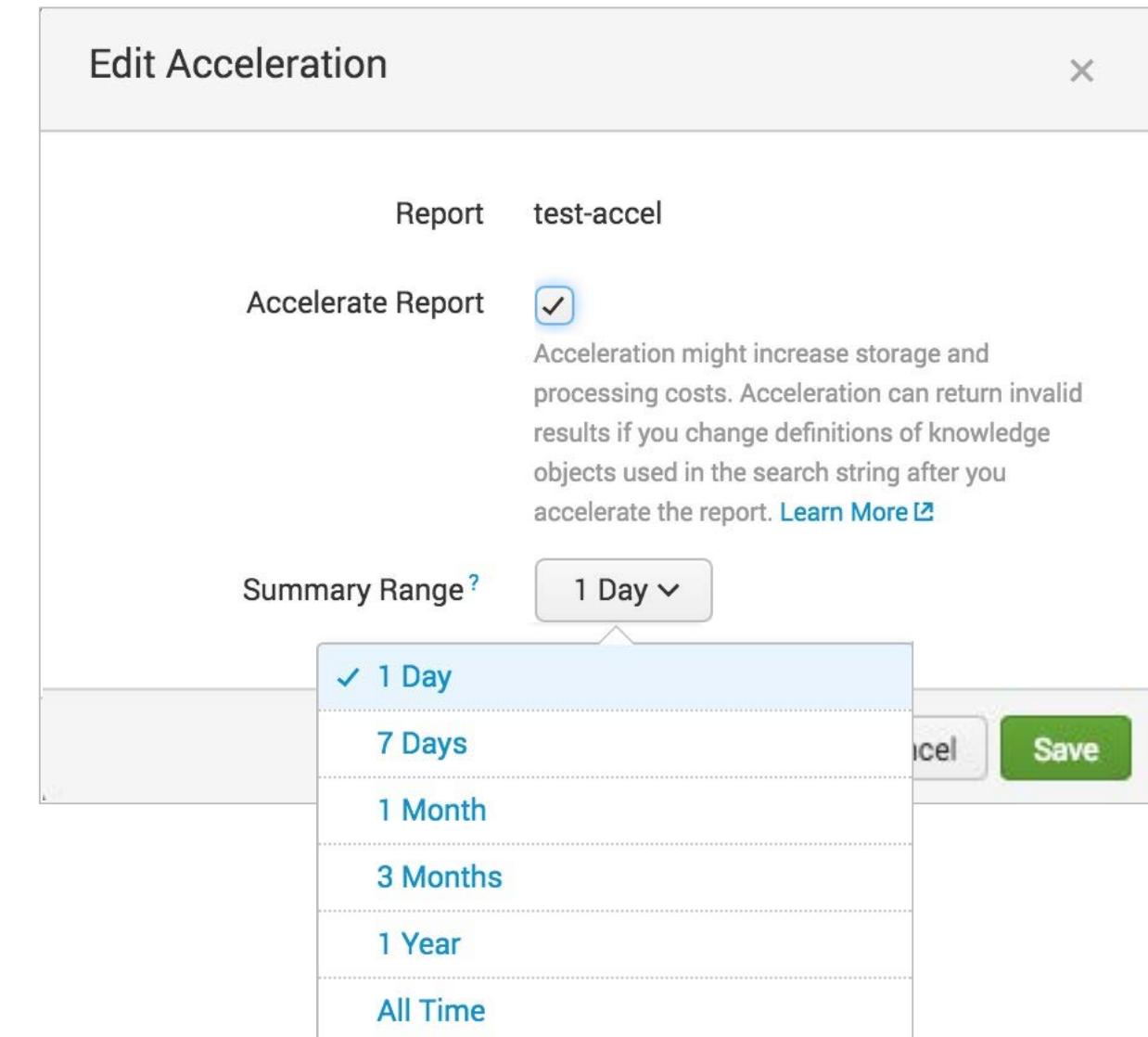
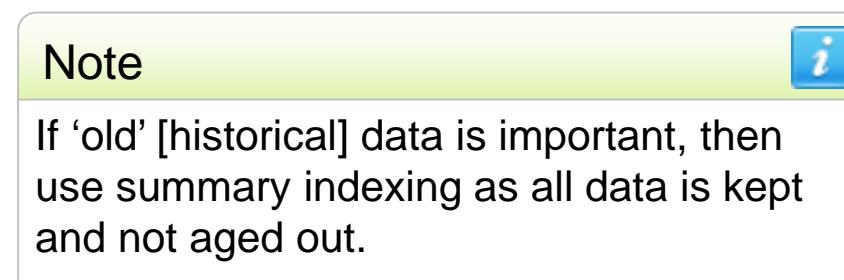
# When Splunk Does NOT Build a Summary

---

- There are cases where Splunk allows you to "accelerate" a search, but a summary won't be created
- Splunk knows what's most efficient and *generally* will not generate a summary if:
  - There are fewer than 100K events in the summary range –  
**It's faster executing the search without a summary**
  - Summary size is projected to be too large –  
**It's faster executing the search because the main index is smaller**
- If a summary is defined and not created for the above reasons, Splunk continues to check periodically, then automatically creates a summary after it meets the requirements

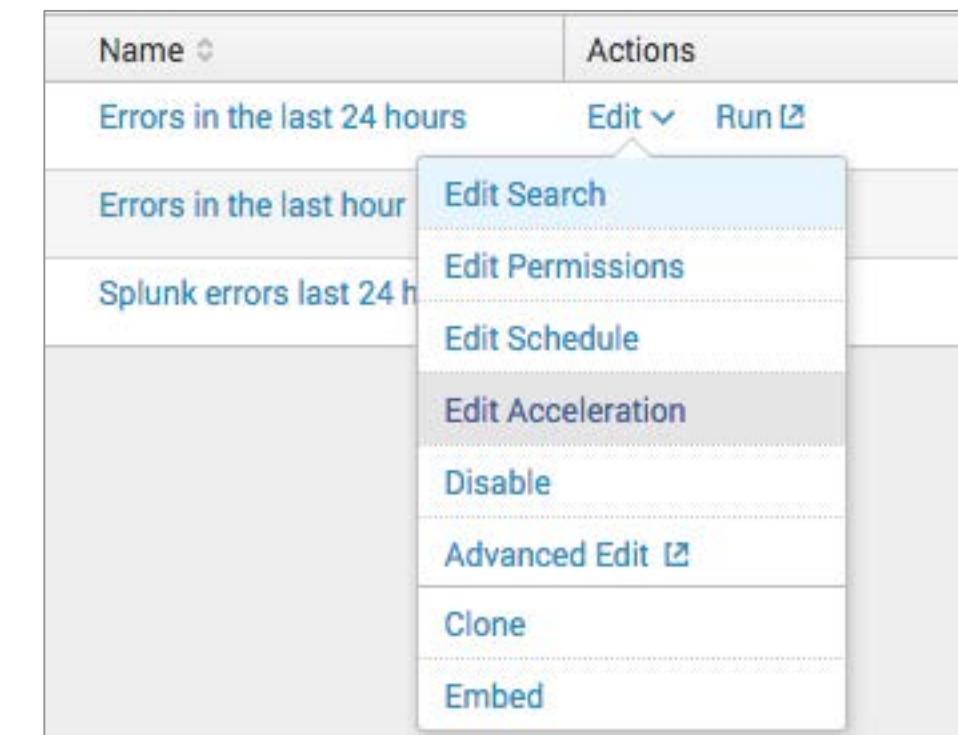
# Acceleration Summary Time Ranges

- Summary spans the specified range, relative to now
- Periodically removes older summary data that ages out of the range



# Accelerating a Saved Report

- From Settings > Searches, Reports and Alerts, select a saved report
- The Accelerate option is always available, whether the search qualifies or not
  - Splunk determines if it can be accelerated when you click Save
- If you try to accelerate an unqualified search, an error message displays:



Name	Actions
Errors in the last 24 hours	Edit Run
Errors in the last hour	
Splunk errors last 24 h	

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Searching Against a Summary

---

- In addition to saved accelerated reports, ad-hoc searches can use the summary when:
  - Search criteria matches the populating saved search
  - The time span is greater than or equal to the summary span
    - ▶ For time spans that are greater than the span of the summary, Splunk uses as much of the summary as it can
- You can also append the search string with additional reporting commands, for example:
  - Populating search –

```
index=web sourcetype=access_combined | stats count by price
```
  - Ad hoc search –

```
index=web sourcetype=access_combined | stats count by price | eval discount = price/2
```

# Appendix C: Table Formatting

Generated for Subbaiah Kandula ([s.venkata.kandula@accenture.com](mailto:s.venkata.kandula@accenture.com)) (C) Splunk Inc, not for distribution

# Overview: Color Coding

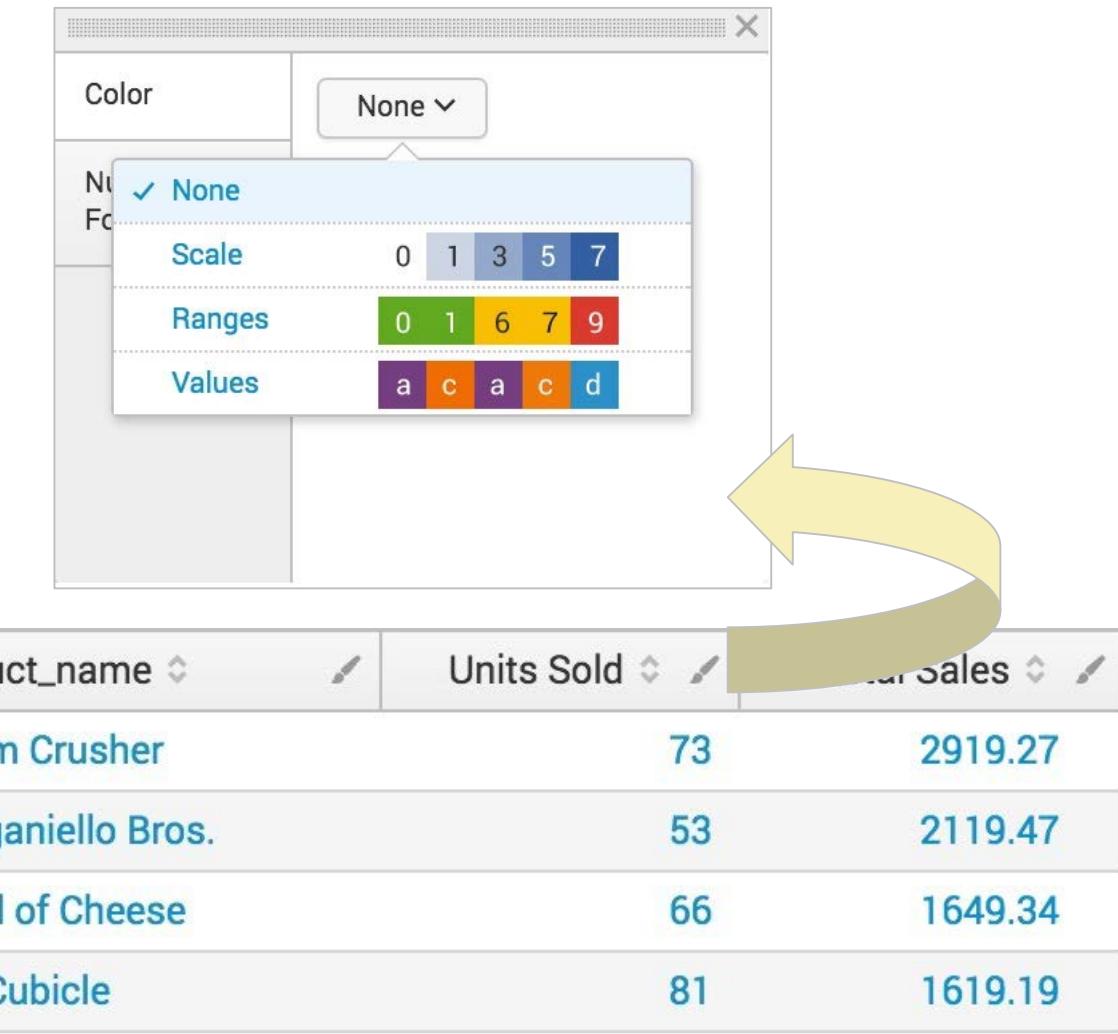
- Color coding enables you to color the data cells in a particular column
- User defines the rules that determine the color of a data cell

product_name	Units Sold	Total Sales
Manganiello Bros.	18	719.82
Dream Crusher	17	679.83
World of Cheese	16	399.84
Mediocre Kingdoms	10	249.90
SIM Cubicle	11	219.89
Final Sequel	7	174.93

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Color Coding Schemes

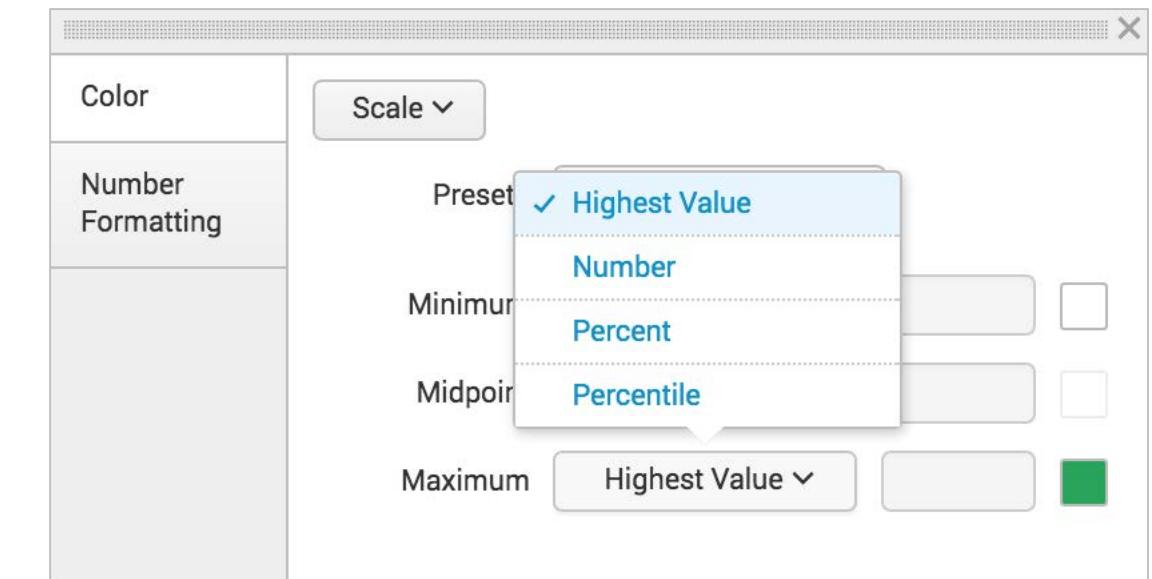
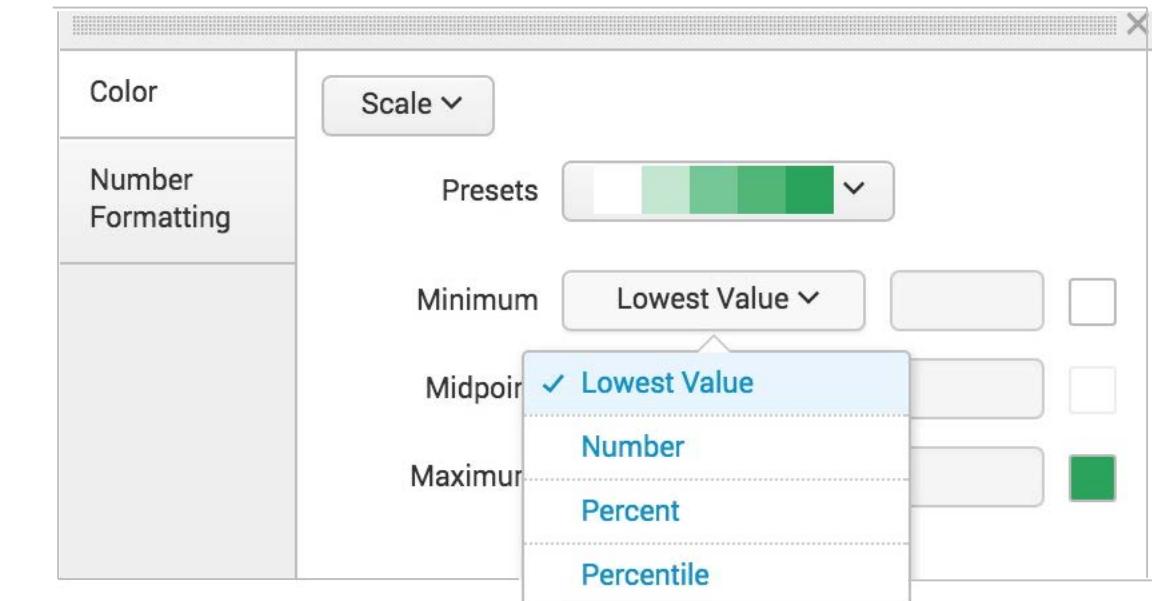
- Color coding is configured on the **Color** tab, using the pull-down button
- Select from:
  - **None**: no color coding (default)
  - **Scale**: cell color changes as the data values rise, based on a scale you define (numeric data)
  - **Ranges**: cell color changes based on a set range that you define (numeric data)
  - **Values**: cell colors change based on values that you configure (numeric and non-numeric data)



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

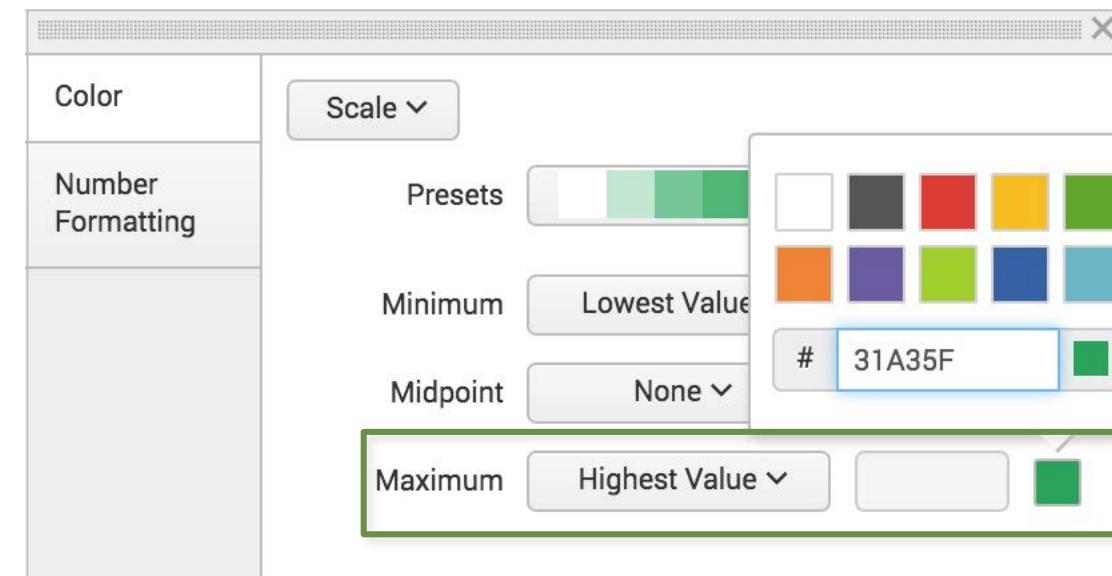
# Setting Color Using a Scale

- Preset values for scale and color can be selected from the **Presets** pull-down
- If desired, change values from a preset to create the desired scale and color range for the **Minimum**, **Midpoint**, or **Maximum**
- The scale can be defined based on the:
  - **Lowest Value/Highest Value** for this data field
  - **Number**
  - **Percent**
  - **Percentile**



# Setting Color Using a Scale (cont.)

- If desired, change the color for the **Minimum**, **Midpoint**, and **Maximum** by clicking in the color box to the right
- For example, to change the **Maximum**:
  1. To the far right of **Maximum**, click the color box
  2. Select a color OR enter its BCG value in hexadecimal

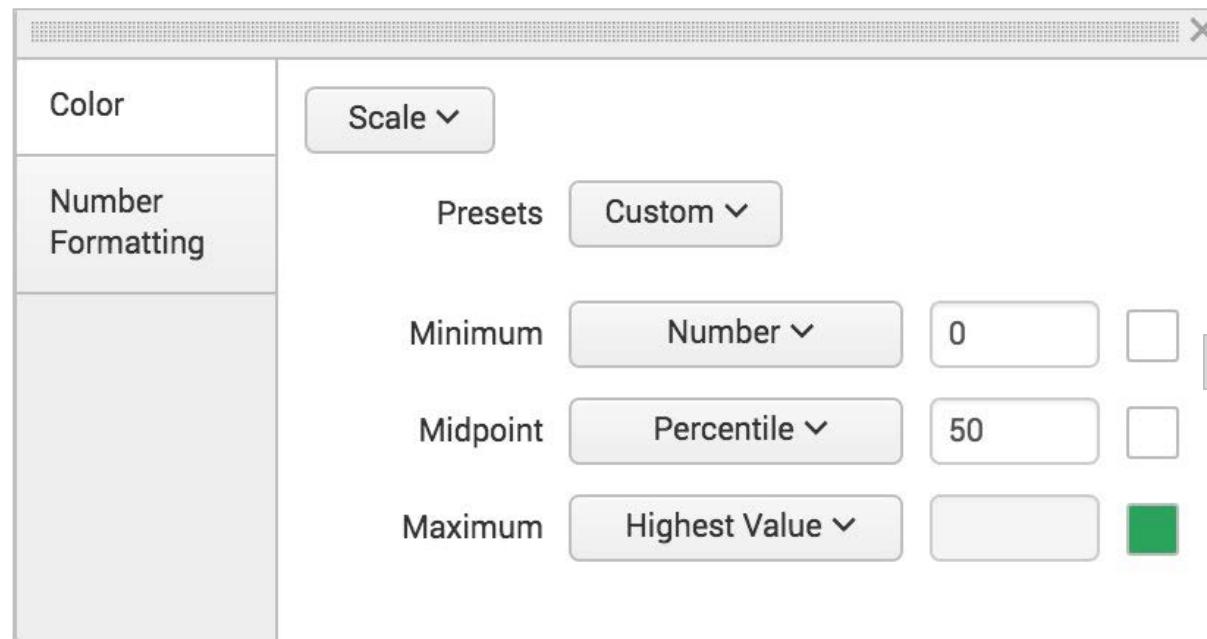


Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Example: Setting Color Using a Scale

- This dialog...

...produces this result



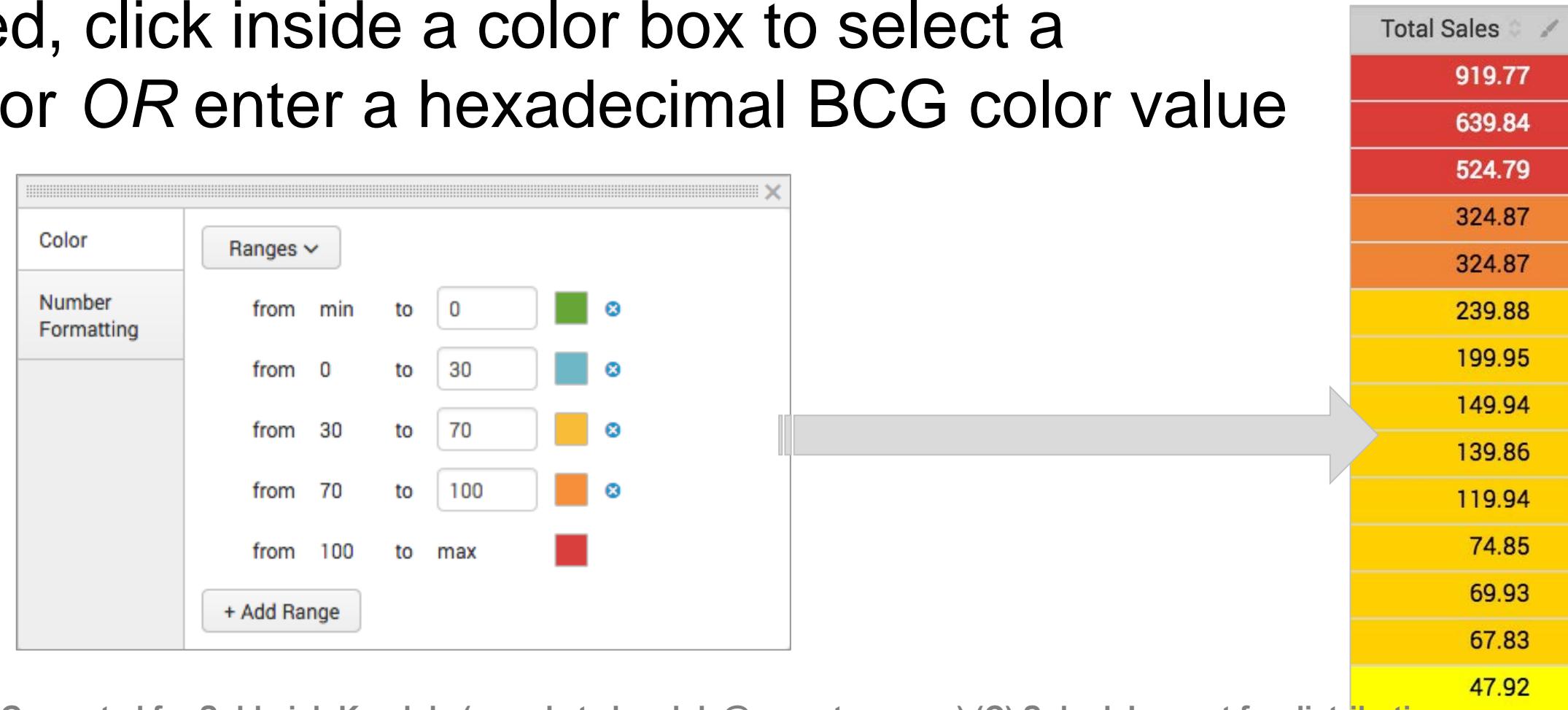
product_name	Units Sold	Total Sales
Dream Crusher	75	2999.25
Manganiello Bros.	47	1879.53
World of Cheese	68	1699.32
SIM Cubicle	79	1579.21
Final Sequel	56	1399.44
Orvil the Wolverine	32	1279.68
Mediocre Kingdoms	48	1199.52
Benign Space Debris	30	749.70
Curling 2014	32	639.68
World of Cheese Tee	54	539.46
Manganiello Bros. Tee	39	389.61
Puppies vs. Zombies	66	329.34
Fire Resistance Suit of Provolone	72	287.28
Holy Blade of Gouda	47	281.53

- Try different settings to finetune your results

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Setting Color Using a Range

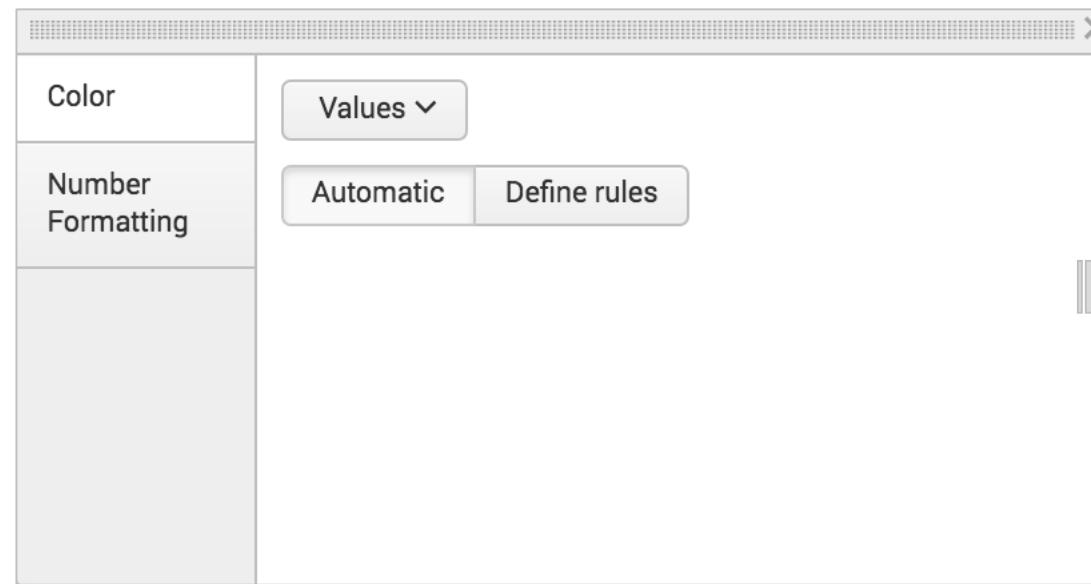
- Define the numerical ranges as desired
- Map each range to a color
- If desired, click inside a color box to select a new color OR enter a hexadecimal BCG color value



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Setting Color Using a Value

- This setting works with both numeric and string values
- The **Automatic** setting has no manual controls
  - Use this setting when you want to vary the color for each row, but the specific color scheme is not important



product_name
Dream Crusher
Manganiello Bros.
World of Cheese
Final Sequel
Mediocre Kingdoms
SIM Cubicle
Orvil the Wolverine
Benign Space Debris
Manganiello Bros. Tee
Curling 2014
Puppies vs. Zombies
World of Cheese Tee
Fire Resistance Suit of Provolone
Holy Blade of Gouda

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Setting Color Using a Value (cont.)

- Using **Define rules**, specify the values and colors to use
  - Values can be numeric or string
  - Not all values must be colored
- If desired, click inside a color box to select a new color *OR* enter a hexadecimal BCG color value

The screenshot illustrates the configuration of color mapping rules and their application to a list of products. On the left, a 'Color' configuration dialog is open, showing three defined rules:

- Cell value is Orvil the Wolverine (Color: Red)
- Cell value is Puppies vs. Zombies (Color: Red)
- Cell value is World of Cheese (Color: Yellow)

An arrow points from this dialog to a list of products on the right, where the items corresponding to the defined rules are colored according to the specified colors.

product_name
Dream Crusher
Manganiello Bros.
World of Cheese
Final Sequel
Mediocre Kingdoms
SIM Cubicle
Orvil the Wolverine
Benign Space Debris
Manganiello Bros. Tee
Curling 2014
Puppies vs. Zombies

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

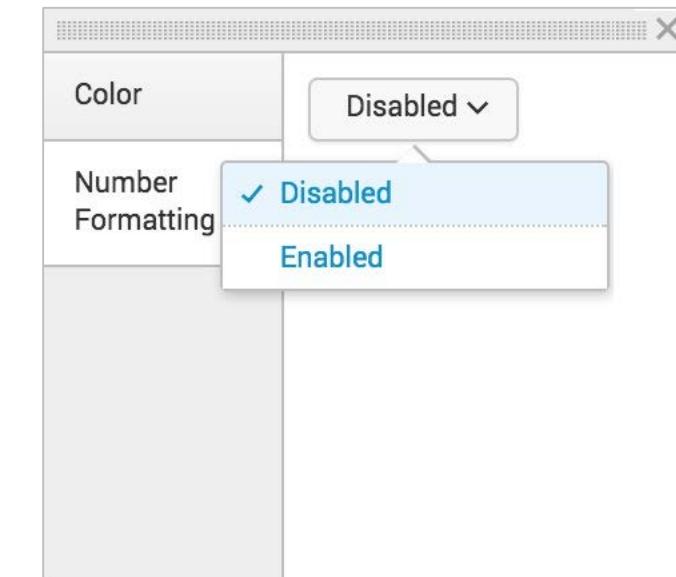
# Overview: Number Formatting

---

- Number formatting enables you to customize how numbers in the data are displayed
- Number formatting includes the ability to
  - Specify numeric precision, from 0 to 4 decimal places
  - Thousands separators
  - Add currency symbols

# Number Formatting

- To enable number formatting:
  1. Select the **Number Formatting** tab
  2. Click the dropdown button
  3. Select **Enabled**
- With number formatting enabled, set the options as desired



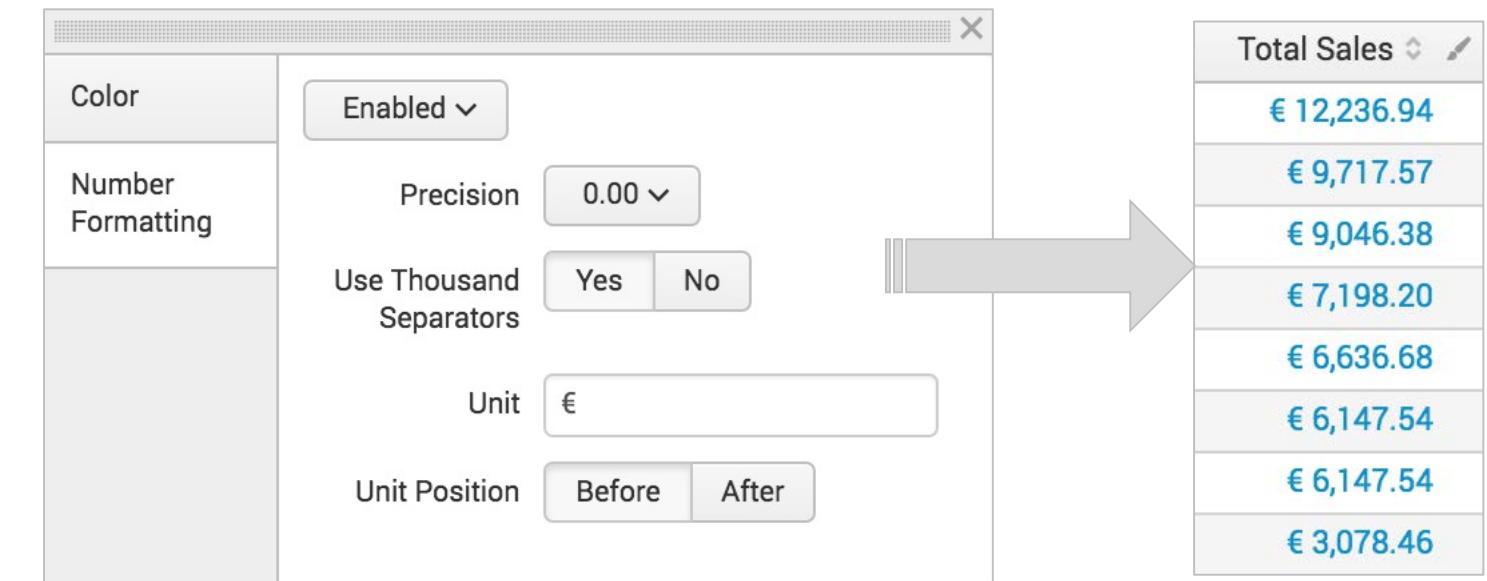
A screenshot of the 'Number Formatting' configuration dialog. The 'Color' tab is selected. The 'Number Formatting' tab is selected and highlighted with a blue border. The 'Precision' dropdown is set to '0.00'. The 'Use Thousand Separators' section has 'Yes' selected. The 'Unit' input field is empty. The 'Unit Position' section has 'Before' selected.

A screenshot of the 'Number Formatting' configuration dialog. The 'Color' tab is selected. The 'Number Formatting' tab is selected and highlighted with a blue border. The 'Precision' dropdown is set to '0.00'. The 'Use Thousand Separators' section has 'Yes' selected. A dropdown menu is open over the 'Unit' input field, showing five options: '0', '0.0', '✓ 0.00' (selected, indicated by a checkmark and blue outline), '0.000', and '0.0000'.

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Number Formatting (cont.)

- **Use Thousands Separators** embeds one or more commas into the number
  - For example, 100000000 would become 1,000,000
- **Unit** refers to currency
  - Copy desired currency indicator
  - In **Unit Position**, specify if the currency indicator goes **Before** or **After**

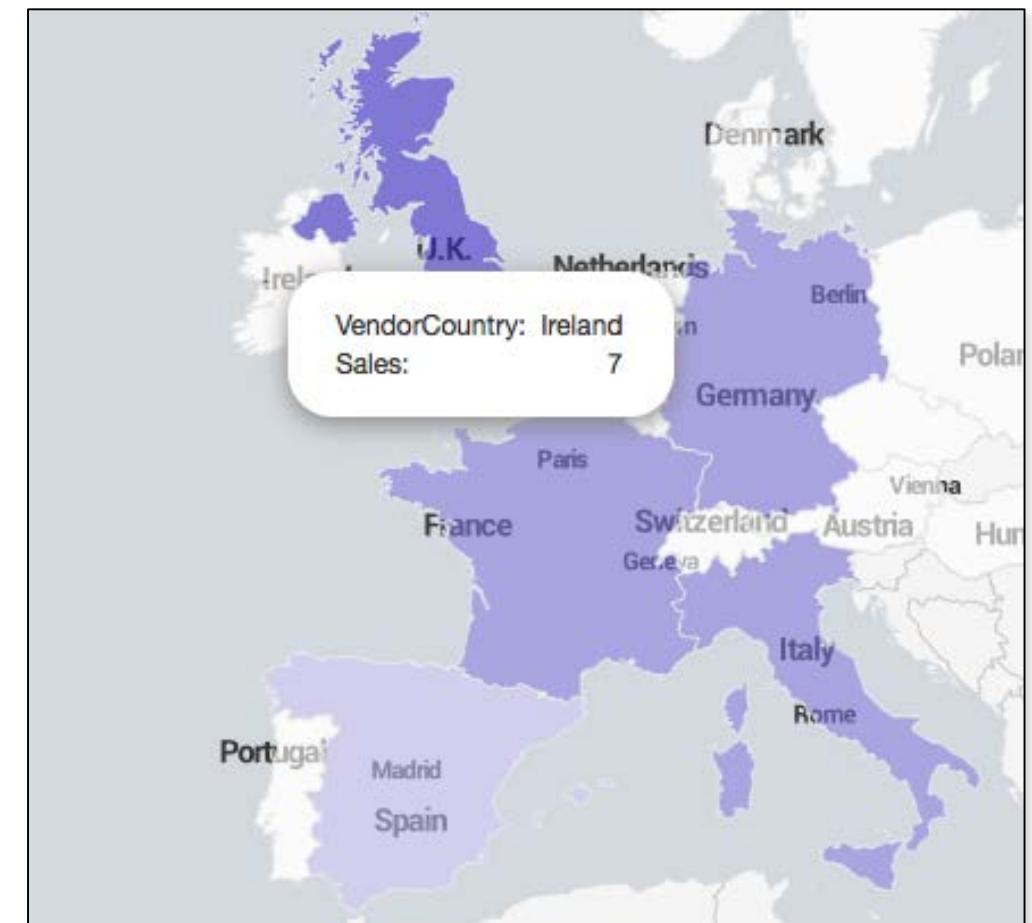


# Appendix D: Creating New Choropleth Maps

Generated for Subbaiah Kandula ([s.venkata.kandula@accenture.com](mailto:s.venkata.kandula@accenture.com)) (C) Splunk Inc, not for distribution

# Choropleth Maps

- Uses shading to show relative metrics for predefined geographic regions
- Splunk ships with two:
  - geo\_us\_states, United States
  - geo\_countries, countries of the world
- You can import other choropleth maps or create your own



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

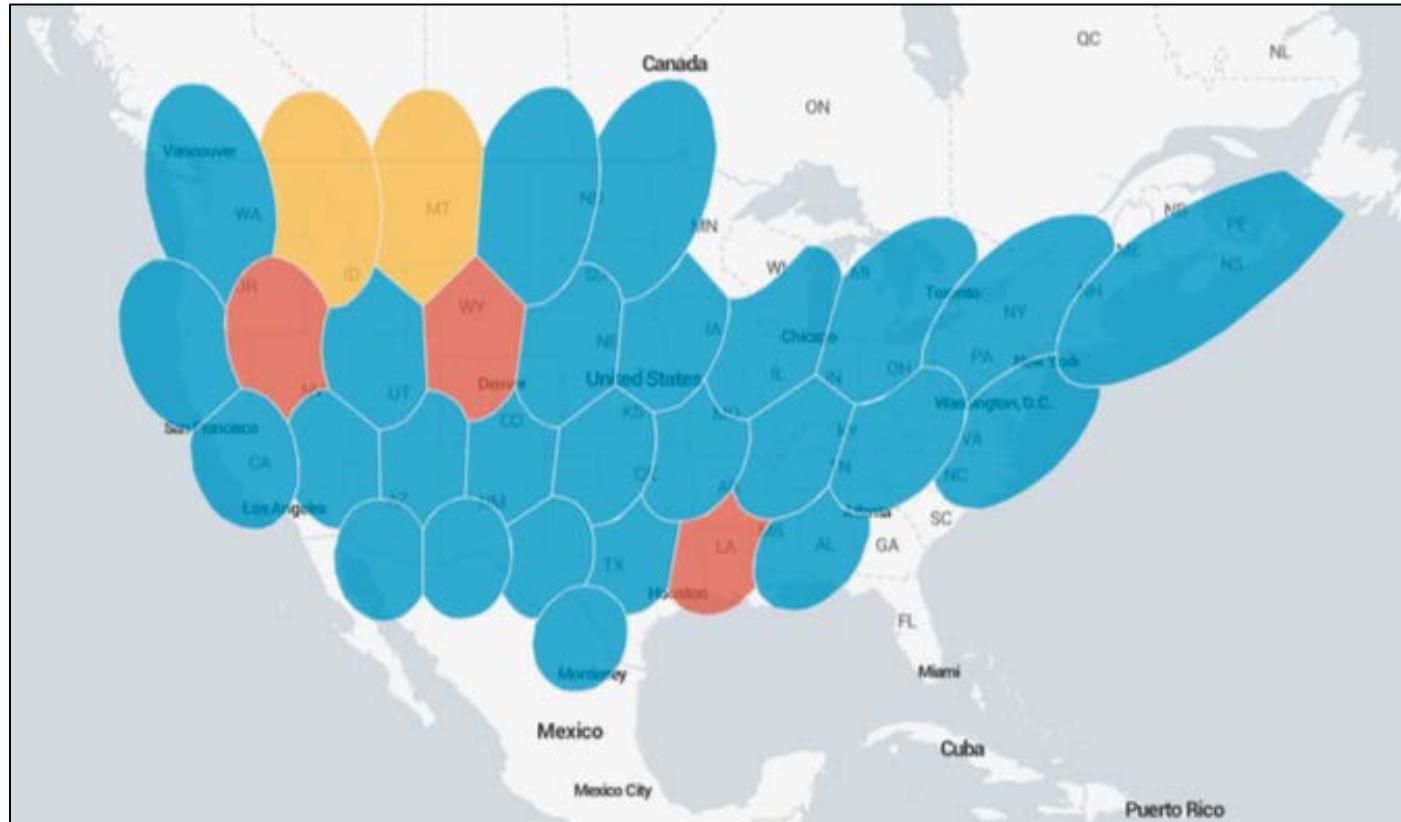
# Choropleth Terminology

- KML (Keyhole Markup Language): type of XML developed by Google and others
- KMZ: a zipped KML file
- Polygon: the specific KML tag that Splunk uses to define its choropleth map data

```
<?xml version="1.0" encoding="UTF-8"?>
<kml xmlns="http://www.opengis.net/kml/2.2">
<Document><name>My document</name>
<description>Content</description>
<Style id="Lump">
<LineStyle><color>CD0000FF</color><width>2</width>
<PolyStyle><color>9AFF0000</color></PolyStyle>
</Style>
<Style id="Path">
<LineStyle><color>FF0000FF</color><width>3</width>
</Style>
<Style id="markerstyle">
<IconStyle><Icon><href>
http://maps.google.com/intl/en_us/mapfiles/ms/
</href></Icon></IconStyle>
</Style>
<Placemark><name>C</name>
<description></description>
<styleUrl>#Lump</styleUrl>
<Polygon>
<tessellate>1</tessellate>
<altitudeMode>clampToGround</altitudeMode>
<outerBoundaryIs><LinearRing><coordinates>
-86.264648,28.091366,0.0 -86.704102,28.188244,
-87.561035,27.722436,0.0 -87.604980,27.137368,
-87.209473,26.293415,0.0 -86.726074,26.194877,
-86.088867,26.431228,0.0 -86.022949,26.588527,
-86.418457,26.549223,0.0 -86.682129,26.470573,
-87.209473,26.725987,0.0 -87.253418,27.117813,
-87.011719,27.839076,0.0 -86.748047,27.858504,
-86.352539,27.761330,0.0 -86.220703,27.702984,
-86.264648,28.091366,0.0 </coordinates></LinearRing>
</Polygon>
```

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) | © Splunk Inc. not for distribution

# How Choropleth Maps Work

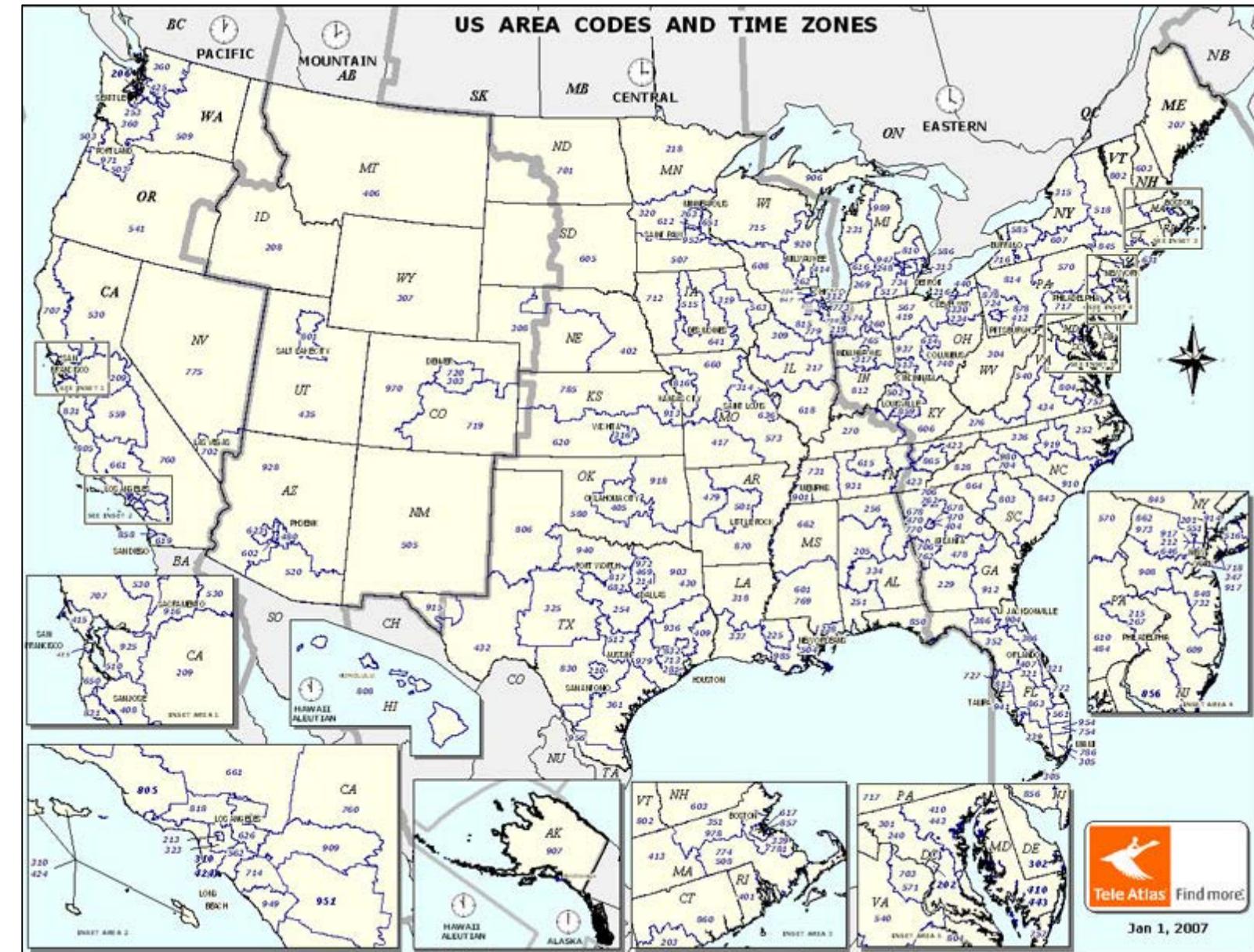


- Choropleth map data serves two purposes:
  1. Defines Polygons to produce the colored map
  2. Provides method to determine within which Polygon a given latitude/longitude is located
- Splunk can use a choropleth KML file as a lookup

# Finding Other KML Choropleth Data Files

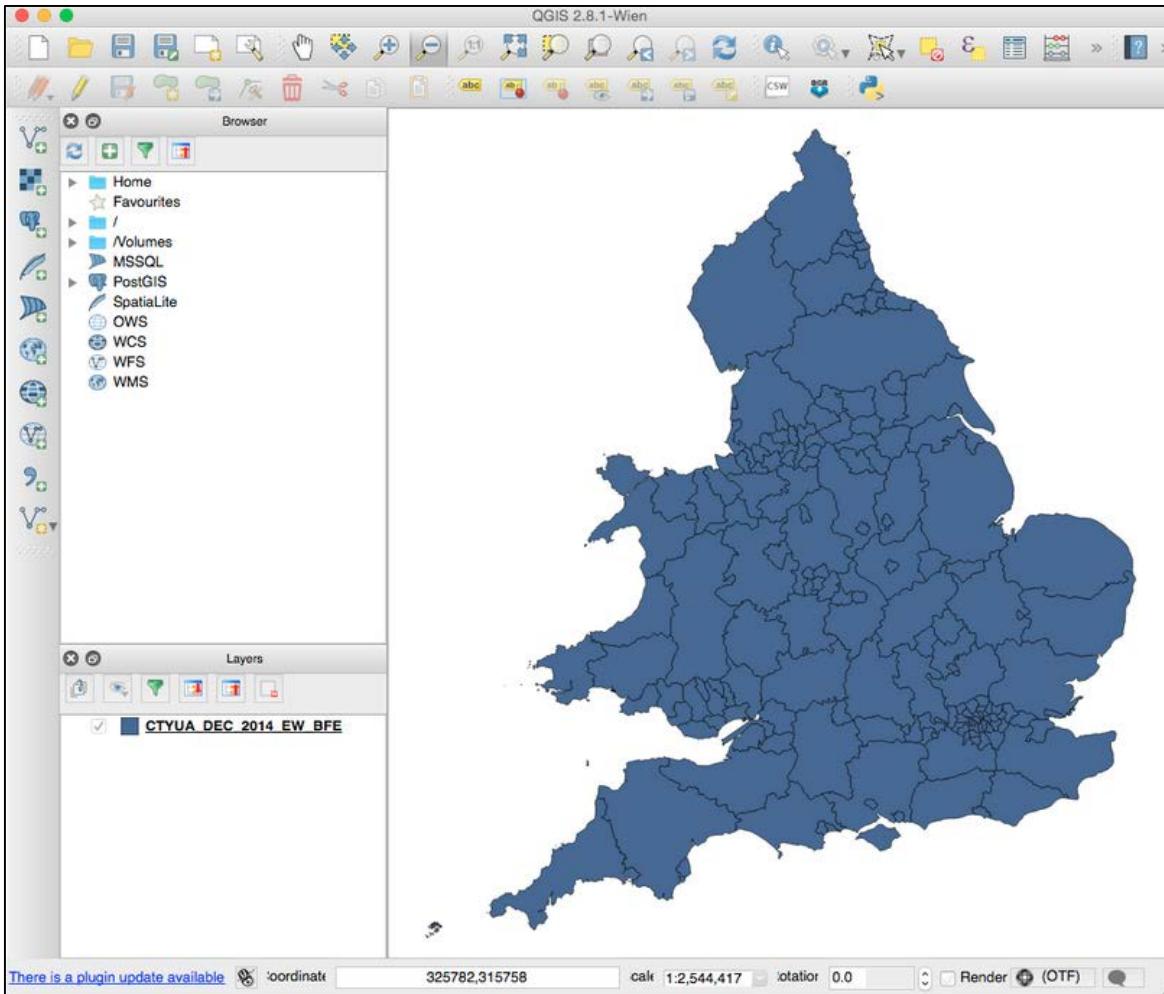
- Census bureau sites for US, UK, Australia
- Lots of other free KML/KMZ files available online
- For example, Google published a KMZ for phone area codes

<https://productforums.google.com/forum/#topic/gec-tools/6y6PrVFDPIY>



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Converting Other File Types to KML



- You can also convert choropleth files to KML from other formats, such as Shapefile
- Mapping systems have been around for over 20 years—some formats not so easy to work with

## Note

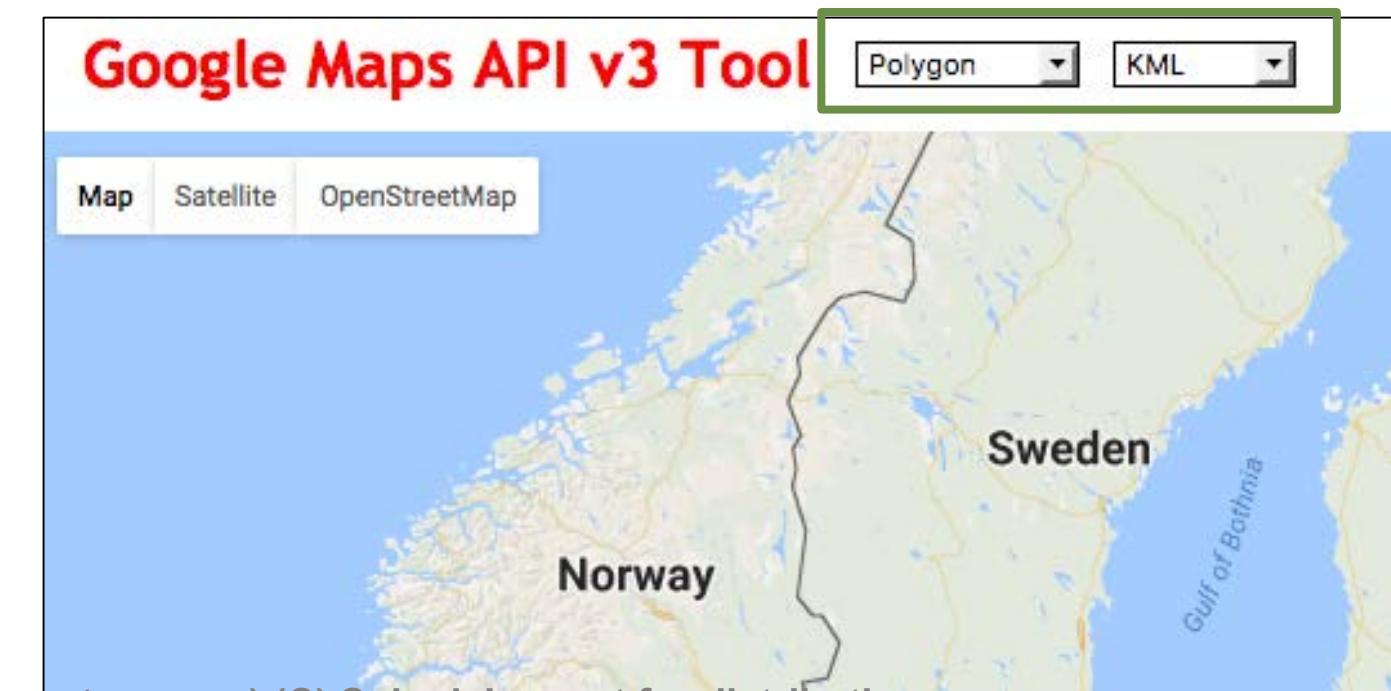


For complete details, see <http://blogs.splunk.com/2015/10/01/use-custom-polygons-in-your-choropleth-maps/>

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Build Your Own Choropleth Files using Online Tools

- Google Earth (<http://earth.google.com>)
- Sketchup (<http://www.sketchup.com>)
- Other online point-and-click tools (for example, <http://www.birdtheme.org/useful/v3tool.html>)
- Make sure:
  - Shapes being created are Polygon, not Polyline
  - Polygons are closed (start and end at the same coordinate)
  - No carriage returns in coordinates list (Splunk won't accept them)



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Using KML Files in Splunk

1. Upload the KML/KMZ file into Splunk as a lookup file
2. In the search, indicate an events data source that contains either featureID (location name) or latitude and longitude

If file contains only lat/long, you can use lookup to find location name (e.g.,  
|lookup my\_geo\_map latitude longitude )

3. Use transforming command to aggregate data by location name  
For example, stats count by featureId |
4. Optionally, select and configure a visualization
5. Create the choropleth map using the geom command

For example, geom my\_geo\_map

#### Note

For complete details, see

<https://docs.splunk.com/Documentation/SplunkCloud/latest/Viz/ChoroplethGenerate>

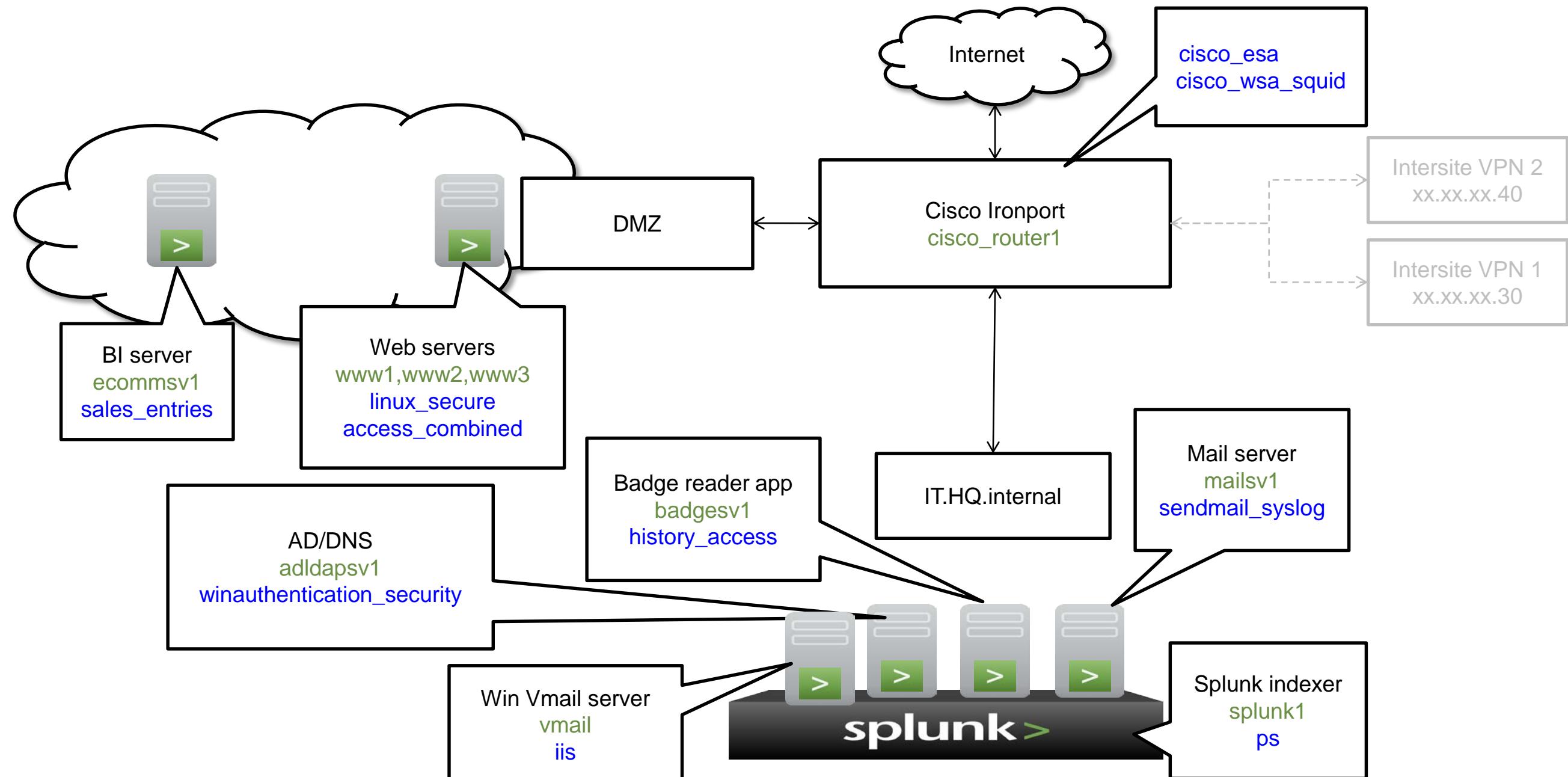
Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution



# Appendix E: Buttercup Games

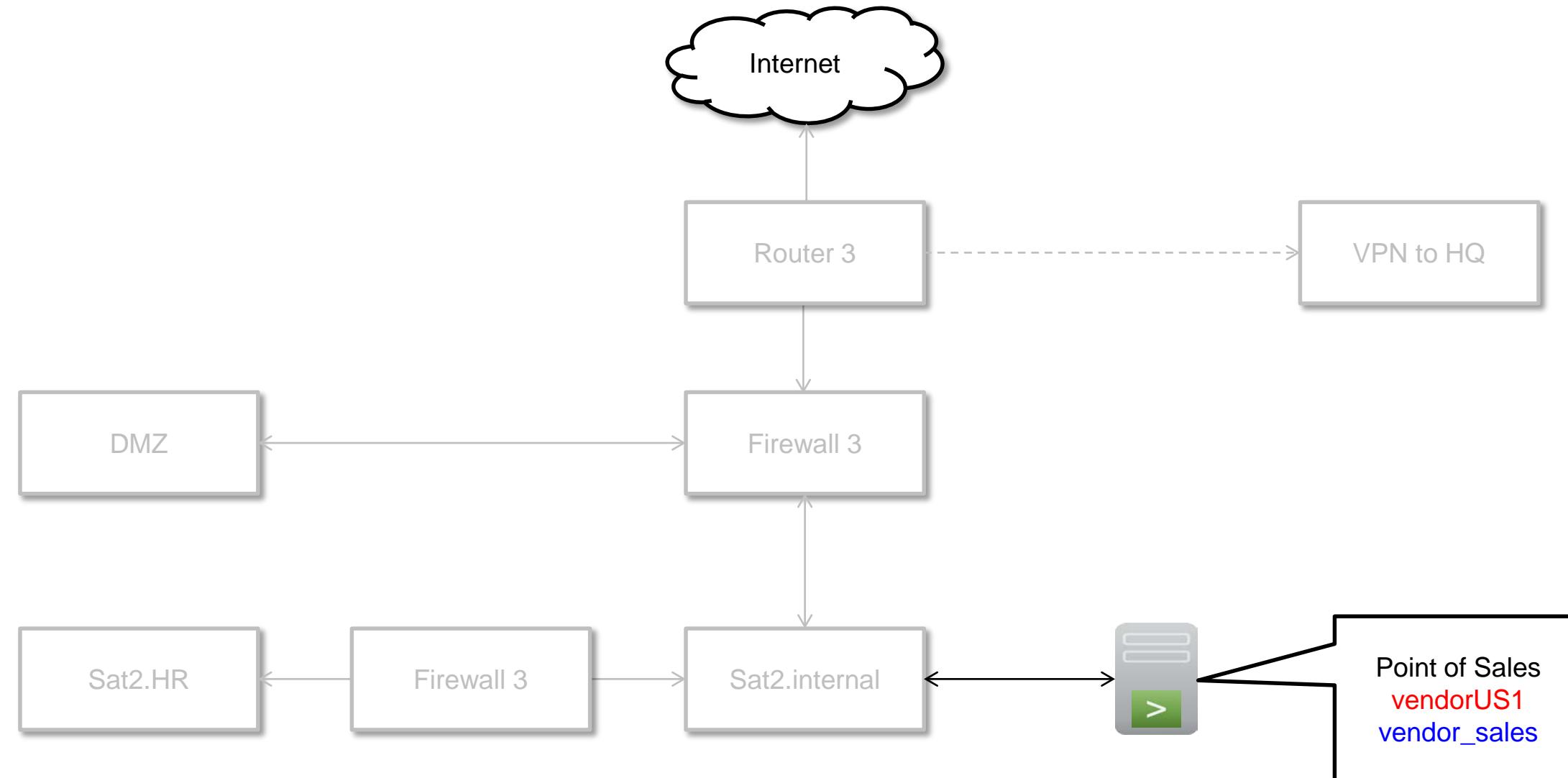
Generated for Subbaiah Kandula ([s.venkata.kandula@accenture.com](mailto:s.venkata.kandula@accenture.com)) (C) Splunk Inc, not for distribution

# San Francisco – Headquarters



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Boston – Satellite Office 2



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Buttercup Games Environment

Data	host	sourcetype
AD/DNS data	adldapsv1	WinEventLog:Security
Badge reader data	badgesv1	history_access
BI server data	ecommsv1	sales_entries
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

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Buttercup Games – HQ Employees

emp_no	birth_date	first_name	last_name	gender	hire_date	location
1	1963-12-25	Suzanne	Flaemmchen	F	2008-05-03	San Francisco
2	1960-04-20	Huang	Sham	M	2008-05-03	San Francisco
3	1950-06-09	Stefano	Pahkthecah	M	2008-05-03	San Francisco
4	1962-01-01	Shawn	Scallion	M	2008-05-03	San Francisco
5	1992-02-29	Shane	Youngin	M	2008-05-03	San Francisco
11	1969-08-19	Placido	Toscani	M	2009-06-09	San Francisco
12	1988-12-06	Meng	Yuan	F	2009-06-09	San Francisco
13	1963-09-29	Amanda	Curry	F	2009-06-09	San Francisco
14	1978-10-31	Bao	Lu	M	2009-06-09	San Francisco
			:			
			:			
68	1978-09-19	Pat	Leuchs	NR	2011-02-04	San Francisco
70	1964-05-19	Patricia	dAbbeville	F	2009-03-14	San Francisco
72	1978-07-10	Saran	Wrappe	F	2011-04-16	San Francisco
73	1988-12-01	Thomasina	Cugina	F	2012-05-19	San Francisco
75	1963-06-28	Frazer	Ullian	M	2013-12-13	San Francisco
76	1964-05-19	Mitsuko	Oh	F	2008-07-04	San Francisco
77	1962-04-01	Yurij	Schonegge	M	2010-01-11	San Francisco
81	1970-01-01	Buttercup	Pony	P	2008-05-03	San Francisco

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Buttercup Games – Satellite Employees

emp_no	birth_date	first_name	last_name	gender	hire_date	location
7	1963-06-07	Daniil	Piazza	M	2009-06-09	Boston
8	1961-05-02	Enrique	Dutra	M	2009-06-09	Boston
9	1974-06-19	Louis	Sagers	M	2009-06-09	Boston
23	1978-02-19	Saniya	Kalloffi	M	2009-09-15	Boston
			:			
69	1962-09-18	Kish	Perna	F	2008-10-21	Boston
79	1973-10-18	Debatosh	Khasidashvili	M	2009-01-30	Boston
emp_no	birth_date	first_name	last_name	gender	hire_date	location
10	1986-02-12	Cosima	Quinn	F	2009-06-09	London
32	1977-05-23	Tzvetan	Zielinski	F	2010-02-10	London
34	1986-02-12	Berni	Genin	M	2010-03-11	London
35	1966-11-14	Cedric	Munson	M	2010-03-18	London
37	1983-09-02	Gianpaolo	Facello	M	2010-06-26	London
			:			
71	1977-01-27	Gioia	Bottazzi	F	2013-05-12	London
74	1963-06-07	Moses	Adeyemi	M	2013-05-11	London
78	1984-05-27	Santino	Sbarro	M	2009-11-06	London
80	1975-07-22	Giancarlo	Rao	M	2008-10-21	London

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Buttercup Games – Employee Information

emp no	RFID	IP	user	host	email	splunk role
1	417852300683	10.1.10.201	sflaemmchen	BG01-sflaemmchen	sflaemmchen@buttercupgames.com	user
2	542830538161	10.1.10.231	hsham	BG01-hsham	hsham@buttercupgames.com	user
3	520156890727	10.1.10.230	spahkthecah	BG01-spahkthecah	spahkthecah@buttercupgames.com	user
4	564931543224	10.1.10.216	sscallion	BG01-sscallion	sscallion@buttercupgames.com	user
5	534931200268	10.1.10.241	syoungin	BG01-syoungin	syoungin@buttercupgames.com	power
6	768166372290	10.1.10.290	lhaddadi	BG01-lhaddadi	lhaddadi@buttercupgames.com	power
7	659636929855	10.2.10.38	dpiazza	BG02-dpiazza	dpiazza@buttercupgames.com	user
8	559129672655	10.2.10.77	edutra	BG02-edutra	edutra@buttercupgames.com	power
9	960318676000	10.2.10.45	lsagers	BG02-lsagers	lsagers@buttercupgames.com	power
10	513908343176	10.3.10.28	cquinn	BG03-cquinn	cquinn@buttercupgames.com	admin
11	125179529264	10.1.10.234	ptoscani	BG01-ptoscani	ptoscani@buttercupgames.com	power
12	382839148784	10.1.10.238	myuan	BG01-myuan	myuan@buttercupgames.com	power
13	713929421175	10.1.10.246	acurry	BG01-acurry	acurry@buttercupgames.com	power
14	900191452102	10.1.10.252	blu	BG01-blu	blu@buttercupgames.com	user
				:		
				:		
81	999999999999	10.1.10.1	bpony	BG01-bpony	bpony@buttercupgames.com	user

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

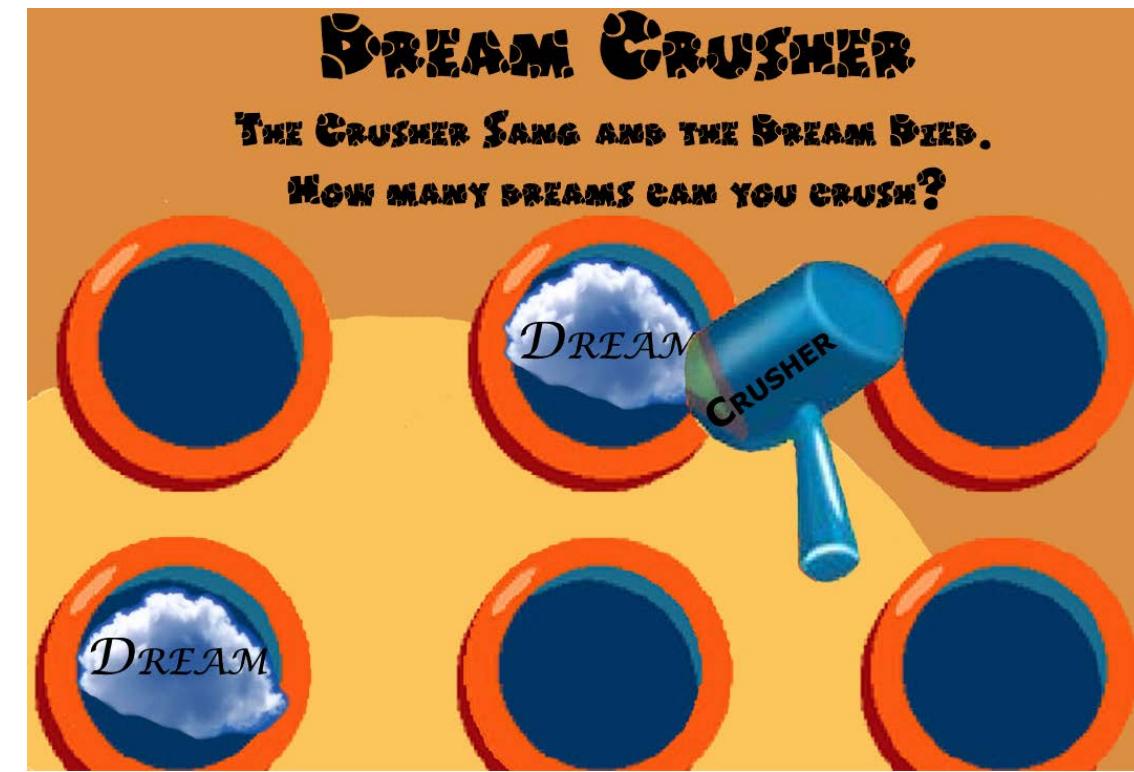
# Vendor Sales – Sample

<u>Vendor</u>	<u>VendorCity</u>	<u>VendorCountry</u>	<u>VendorID</u>	<u>VendorLatitude</u>	<u>VendorLongitude</u>	<u>VendorStateProvince</u>
Frozen Fun General Store	Amundsen-Scott Station	Antarctica	9999	90.0000	139.2667	Antarctica
Jeremy's House of Hobbies	Fort-Lamy	Chad	9116	12.134846	15.055742	Chari-Baguirmi
Pan-African RC and Toys	Ouagadougou	Burkina Faso	9115	12.364637	-1.533864	Nord Region
Passe-Temps	Yamoussoukro	Cote d'Ivoire	9114	6.816667	-5.283333	Lacs
Kahled's Amusements	Tripoli	Libya	9113	5.560735	-0.193087	Tripoli
Mburo Games	Kampala	Uganda	9112	0.313611	32.581111	Kampala
Pan-African RC and Toys	Yaounde	Cameroon	9111	3.866667	11.516667	Centre Region
Comics and Games	Dar es Salaam	Tanzania	9110	-6.822921	39.269661	Dar es Salaam
Pan-African RC and Toys	Mombasa	Kenya	9109	-4.043477	39.668207	Mombasa
Pan-African RC and Toys	Accra	Ghana	9108	5.555717	-0.196306	Greater Accra
Seminna-Werq Games Warehouse	Addis Ababa	Ethiopia	9107	9.022736	38.746799	Oromia
RTL Boutique de Train Miniature	Tunis	Tunisia	9106	36.81881	10.16596	Tunis
Rick's Toy Shop and Cafe	Casablanca	Morocco	9105	33.533333	-7.583333	Grand Casablanca
Laval's Joke and Toy Store	Oran	Algeria	9104	35.696944	-0.633056	Oran
Sweepstake Games	Lagos	Nigeria	9103	6.441158	3.417977	Lagos
Lightening Games of Johannesburg	Johannesburg	South Africa	9102	-26.204103	28.047305	Gauteng
Natal Games of Pietermaritzburg	Pietermaritzburg	South Africa	9101	-29.600607	30.379412	KwaZulu-Natal
Peers Games of Cape Town	Cape Town	South Africa	9100	-33.924868	18.424055	Western Cape
Kiwi Game Warehouse	Auckland	New Zealand	7045	-36.84846	174.763332	Auckland
Kiwi Game Warehouse	Christchurch	New Zealand	7044	-43.529854	172.637888	Canterbury

Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution

# Buttercup Games – Products

productId	product_name	categoryId
WC-SH-T02	World of Cheese Tee	TEE
WC-SH-G04	World of Cheese	SHOOTER
WC-SH-A02	Fire Resistance Suit of Provolone	ACCESSORIES
WC-SH-A01	Holy Blade of Gouda	ACCESSORIES
SC-MG-G10	SIM Cubicle	SIMULATION
PZ-SG-G05	Puppies vs. Zombies	STRATEGY
MB-AG-T01	Manganiello Bros. Tee	TEE
MB-AG-G07	Manganiello Bros.	ARCADE
FS-SG-G03	Final Sequel	STRATEGY
FI-AG-G08	Orvil the Wolverine	ARCADE
DC-SG-G02	Dream Crusher	STRATEGY
DB-SG-G01	Mediocre Kingdoms	STRATEGY
CU-PG-G06	Curling 2014	SPORTS
BS-AG-G09	Benign Space Debris	ARCADE



Generated for Subbaiah Kandula (s.venkata.kandula@accenture.com) (C) Splunk Inc, not for distribution