



Splunk Fundamentals 1

Outline

Module 1-2: Introducing Splunk and Splunk's Components

Module 3: Installation

Module 4: Inputs

Module 5: Searching

Module 6: Using Fields in Searches

Module 7: Best Practices for Searching

Module 8: Splunk's Search Language

Module 9: Transforming Commands

Module 10: Creating Reports and Dashboards

Module 11: Using Pivot

Module 12: Creating and Using Lookups

Module 13: Creating Scheduled Reports and Alerts

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Modules 1-2: Introducing Splunk and Splunk's Components

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

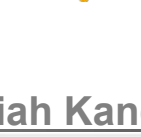
Module Objectives

- Understand the uses of Splunk
- Define Splunk apps
- Learn basic navigation in Splunk

Got Data?



- Computers
- Network devices
- Virtual machines
- Internet devices
- Communication devices
- Sensors
- Databases
- **Any source**



- Logs
- Configurations
- Messages
- Call detail records
- Clickstream
- Alerts
- Metrics
- Scripts
- Changes
- Tickets
- **Any data**

Users Searching



Splunk Search Head



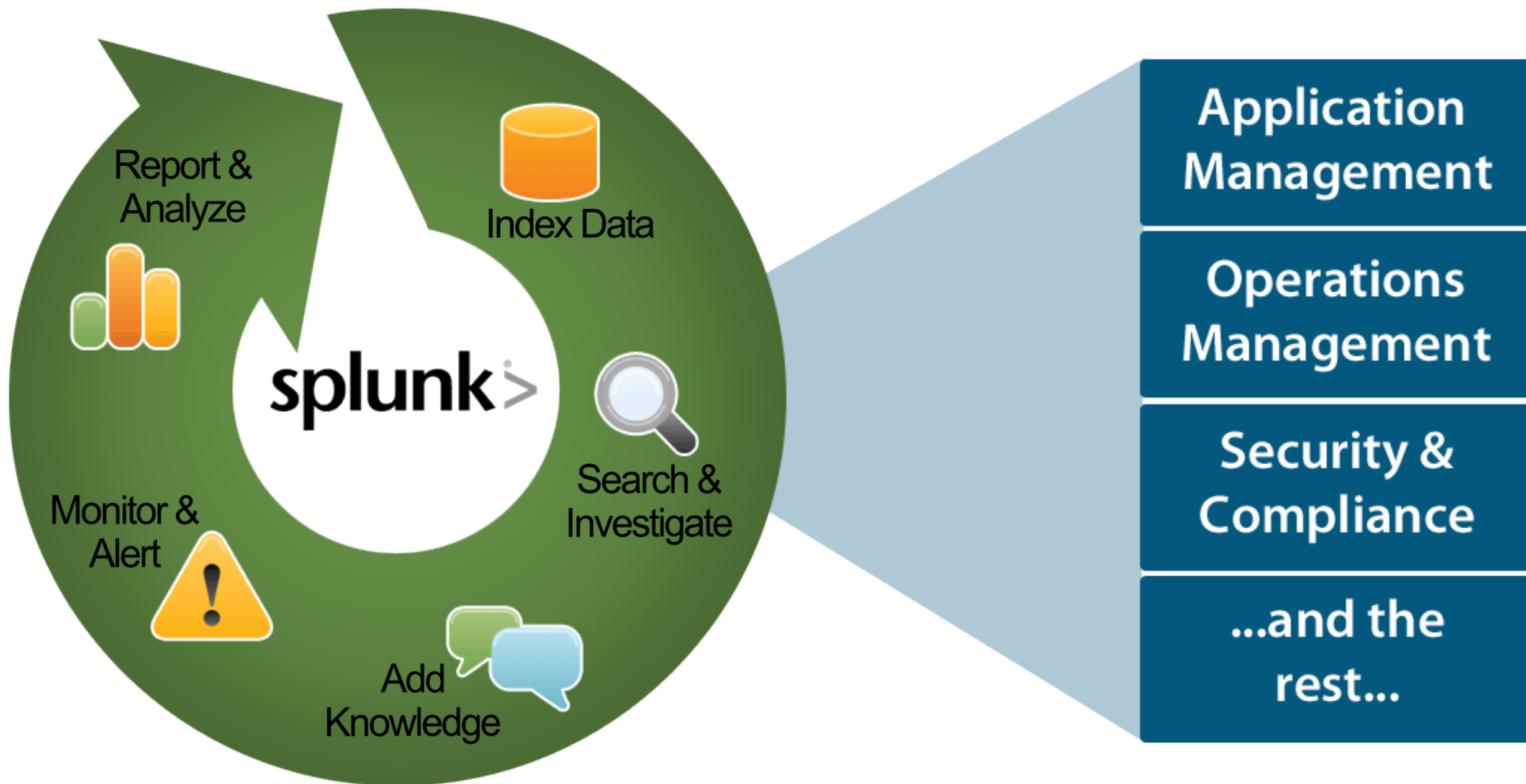
Splunk Indexer



Index any data from any source

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

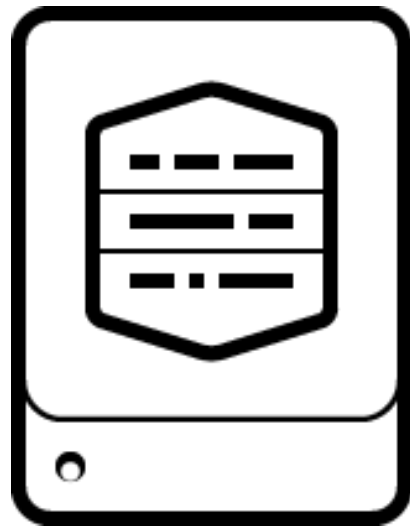
One Splunk. Many Uses.



Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Splunk Components

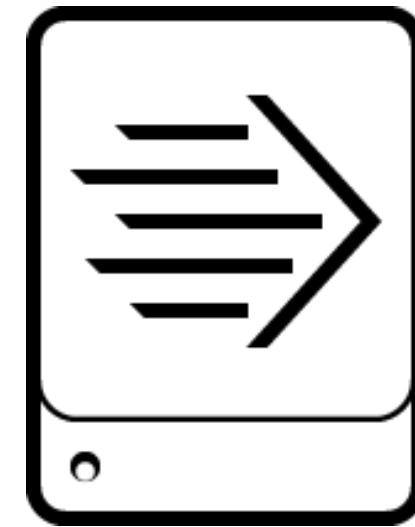
- Splunk is comprised of three main processing components:



Indexer



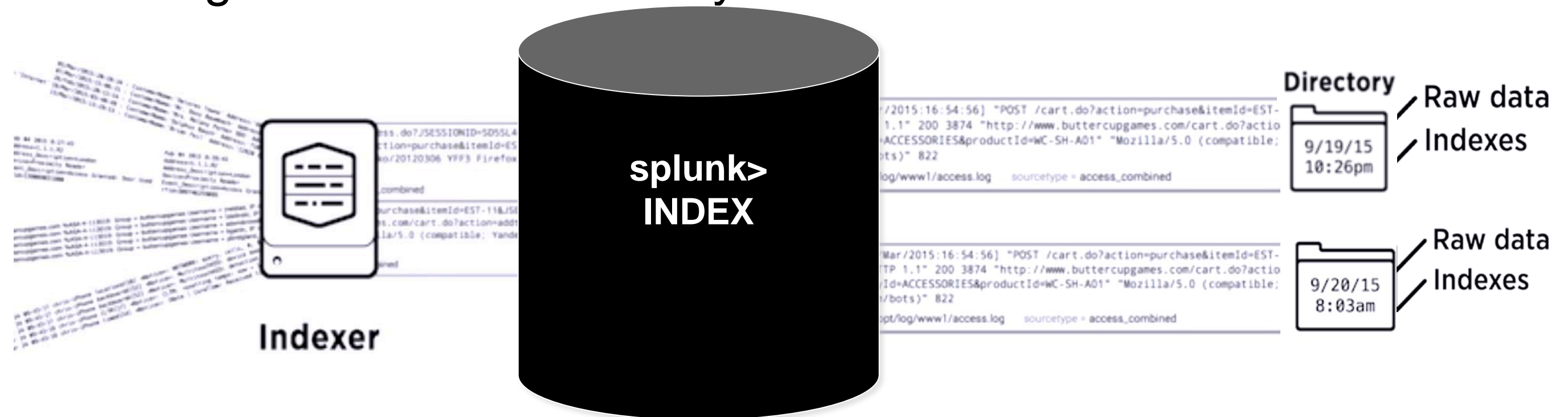
Search Head



Forwarder

Splunk Components - Indexer

- Processes machine data, storing the results in Indexes as events, enabling fast search and analysis

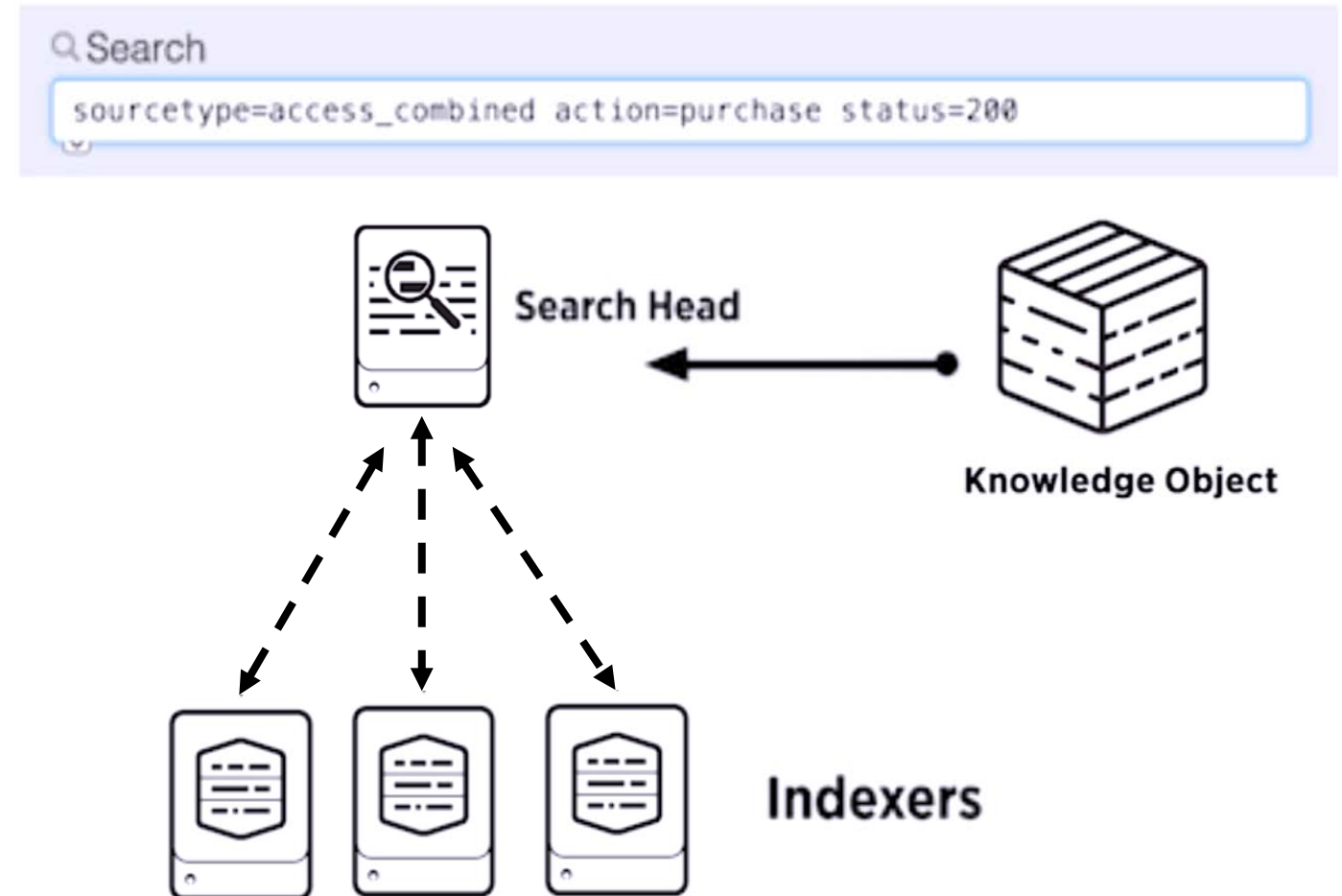


- As the Indexer indexes data, it creates a number of files organized in sets of directories by age
 - Contains raw data (compressed) and Indexes (points to the raw data)

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Splunk Components – Search Heads

- Allows users to use the Search language to search the indexed data
- Distributes user search requests to the Indexers
- Consolidates the results and extract field value pairs from the events to the user
- Knowledge Objects on the Search Heads can be created to extract additional fields and transform the data without changing the underlying Index data

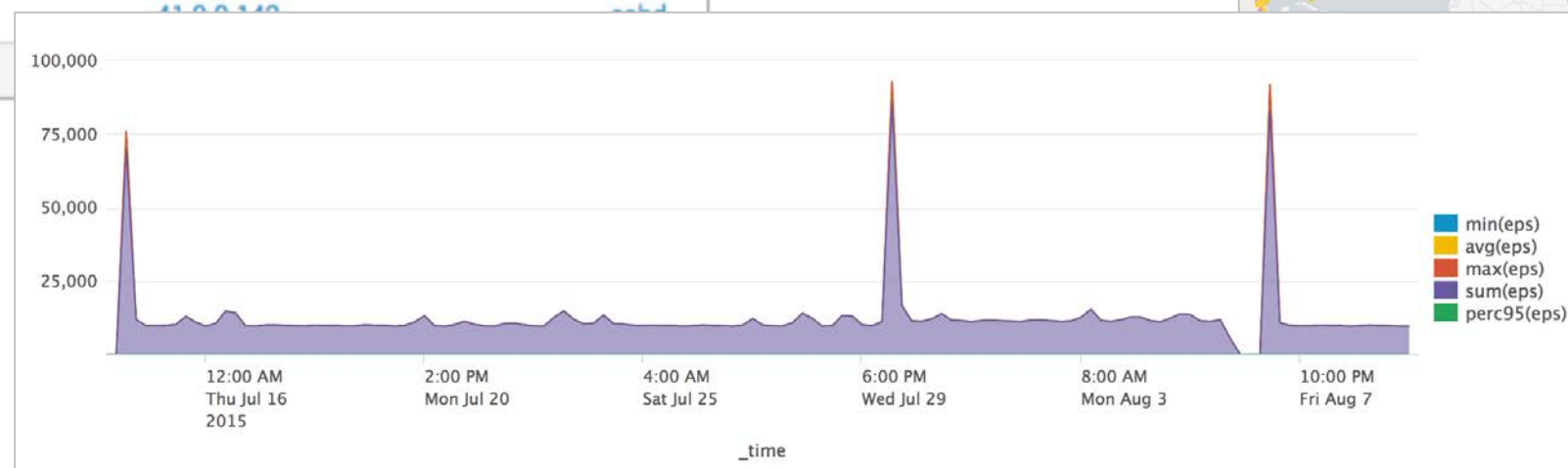
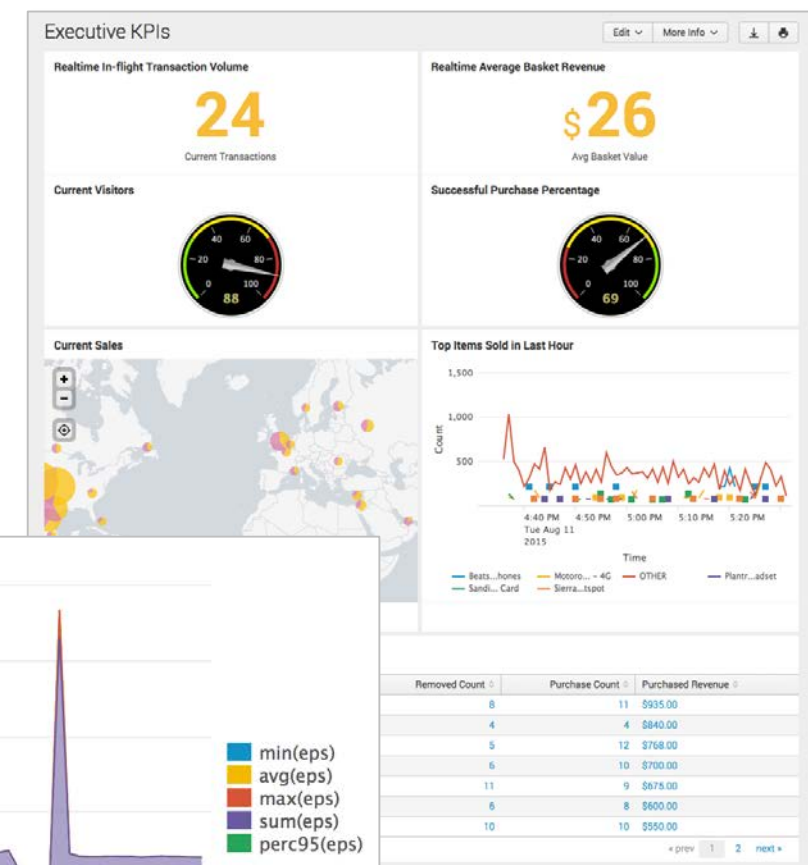


Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Splunk Components – Search Heads (cont.)

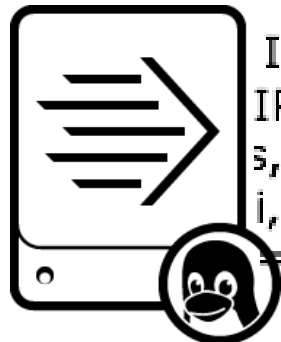
- Search Heads also provide tools to enhance the search experience such as reports, dashboards and visualizations

user	src_ip	app
charles	2.144.0.22	sshd
sales	2.144.0.22	sshd
karla	2.144.0.210	sshd
man	2.144.0.210	sshd
oracle	2.144.0.210	sshd
postfix	2.144.0.210	sshd
upload	2.144.0.210	sshd
glasshouse	5.11.128.21	sshd
oracle01	41.0.0.140	sshd
oracle1	41.0.0.140	sshd



Splunk Components – Forwarders

- Splunk Enterprise instances that consume and send data to the index
- Require minimal resources and have little impact on performance
- Typically reside on the machines where the data originates
- Primary way data is supplied for indexing



**Web Server
with Forwarder Instance
installed**

IP = 10.3.10.6, Session disconnected. Session type = TPsecOver
IP = 10.1.10.216, Session connected. Session type = SSL, Durat
s, IP = 10.1.10.133, Session connected. Session type = IKE, Dur
i, IP = 10.3.10.18, Session disconnected. Session type = IKE, D
= 10.1.10.211, Session connected. Session type = SSL, Duratio

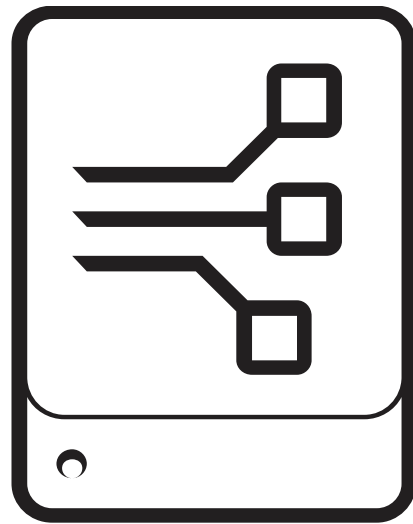


Indexer

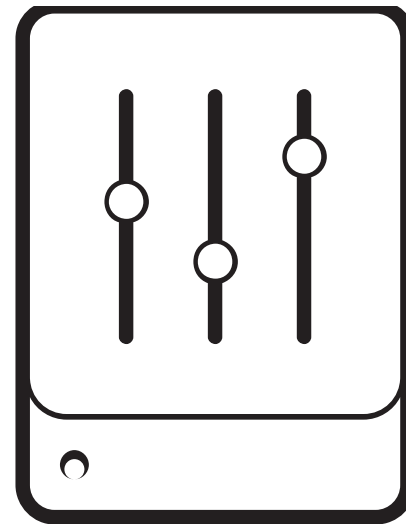
Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Additional Splunk Components

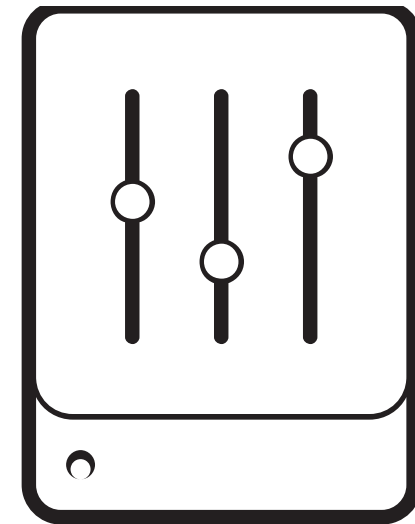
- In addition to the three main Splunk processing components, there are some less-common components including :



**Deployment
Server**



Cluster Master



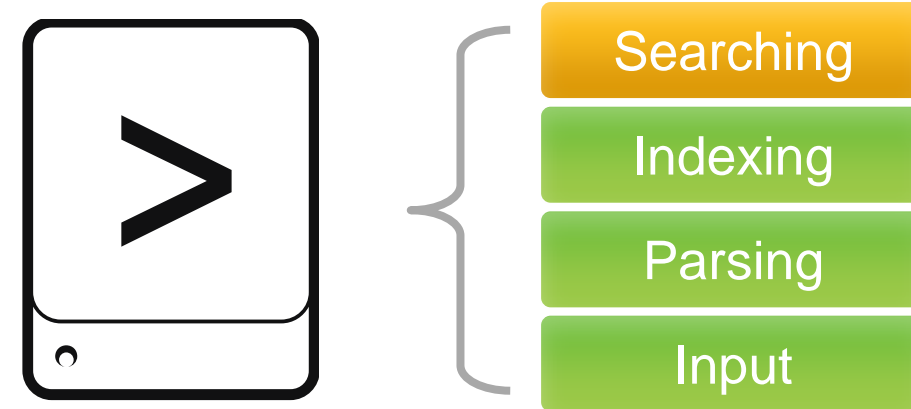
License Master

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Splunk Deployment – Standalone

- **Single Server**

- All functions in a single instance of Splunk
- For testing, proof of concept, personal use, and learning
- This is what you get when you download Splunk and install with default settings



- **Recommendation**

- Have at least one test/development setup at your site

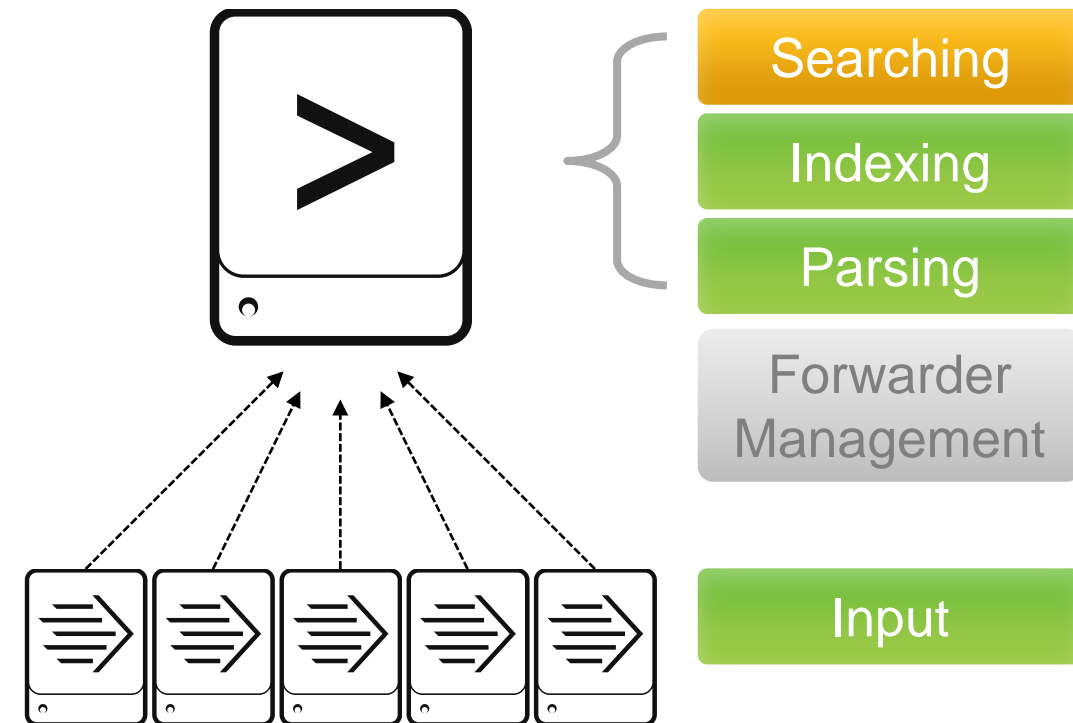
Splunk Deployment – Basic

- **Splunk server**

- Similar to server in standalone configuration
- Manage deployment of forwarder configurations

- **Forwarders**

- Forwarders collect data and send it to Splunk servers
- Install forwarders at data source (usually production servers)

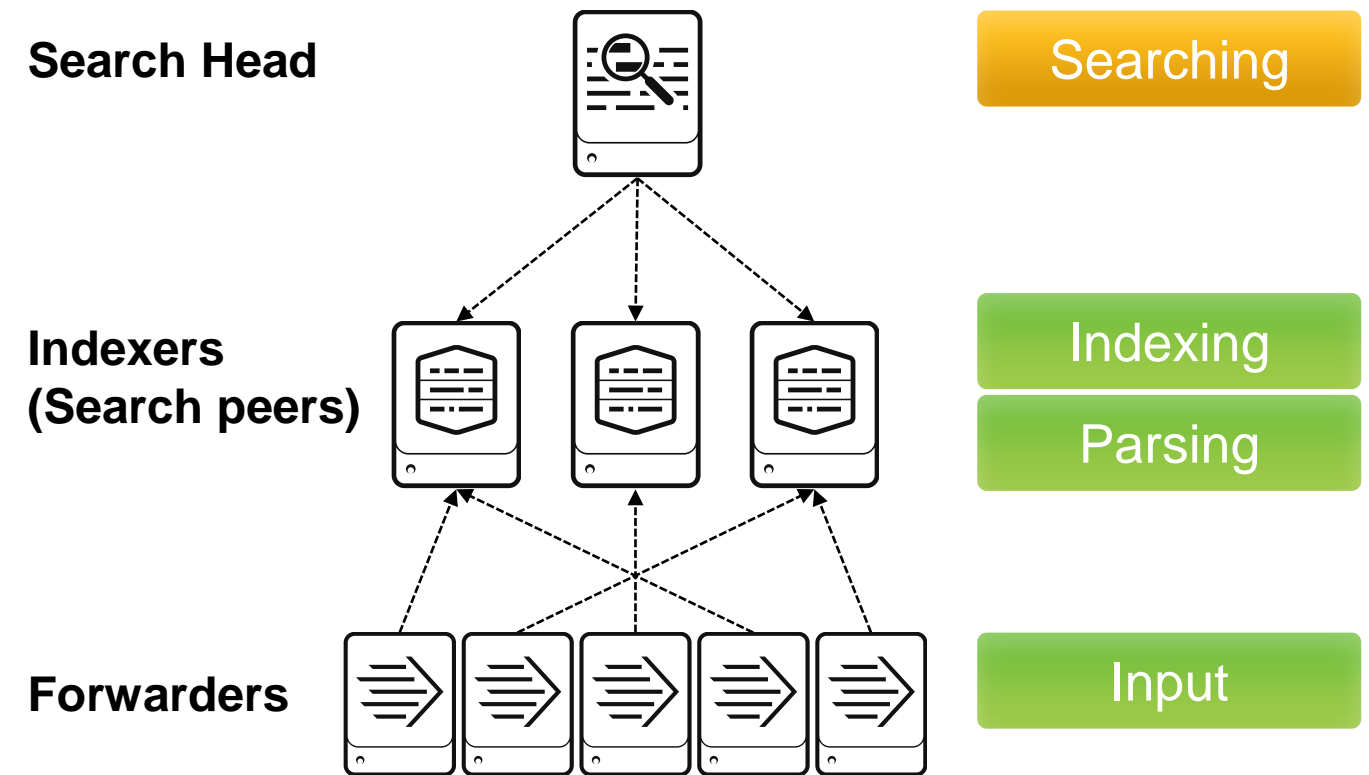


Basic Deployment for organizations:

- Indexing less than 20GB per day
- With under 20 users
- Small amount of forwarders

Splunk Deployment – Multi-Instance

- Increases indexing and searching capacity
- Search management and index functions are split across multiple machines

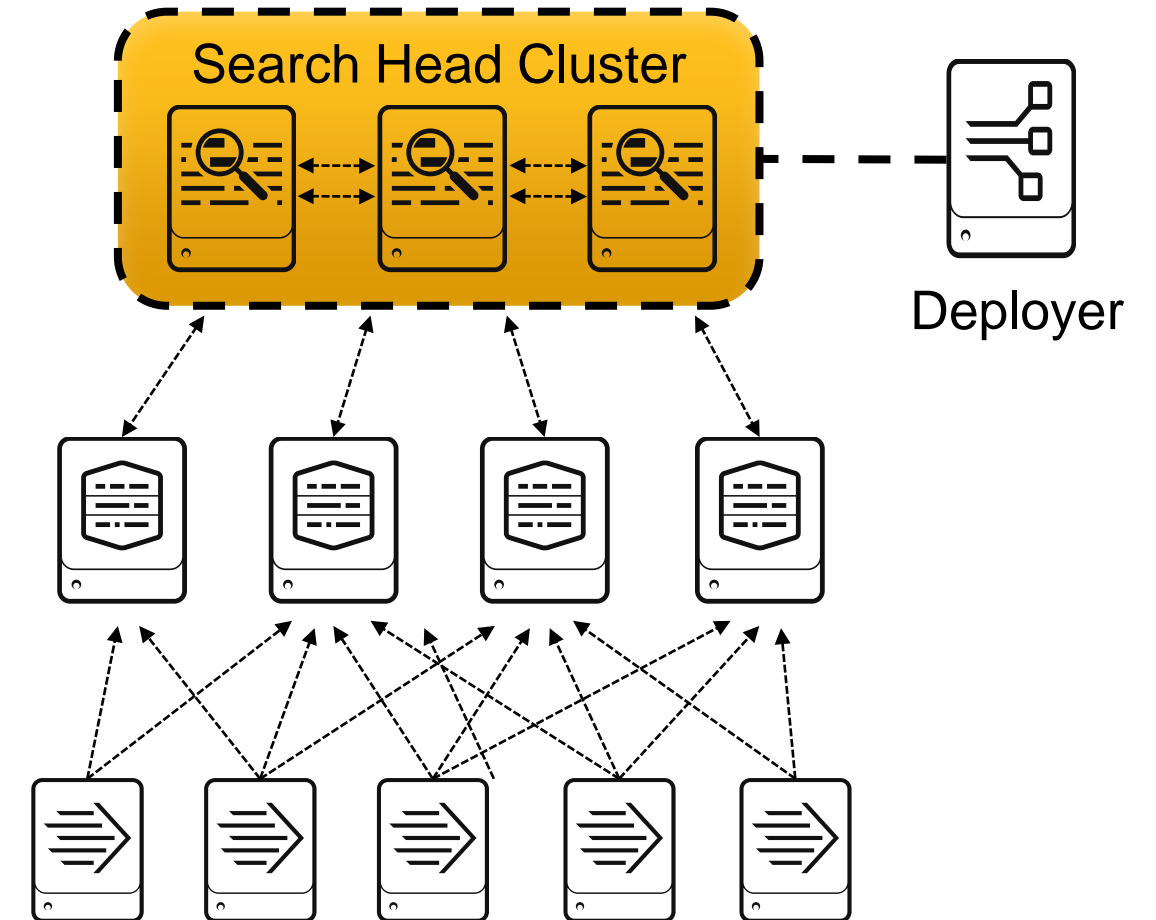


Deployment for organizations:

- Indexing up to 100 GB per day
- Supports 100 users
- Supports several hundred forwarders

Splunk Deployment – Increasing Capacity

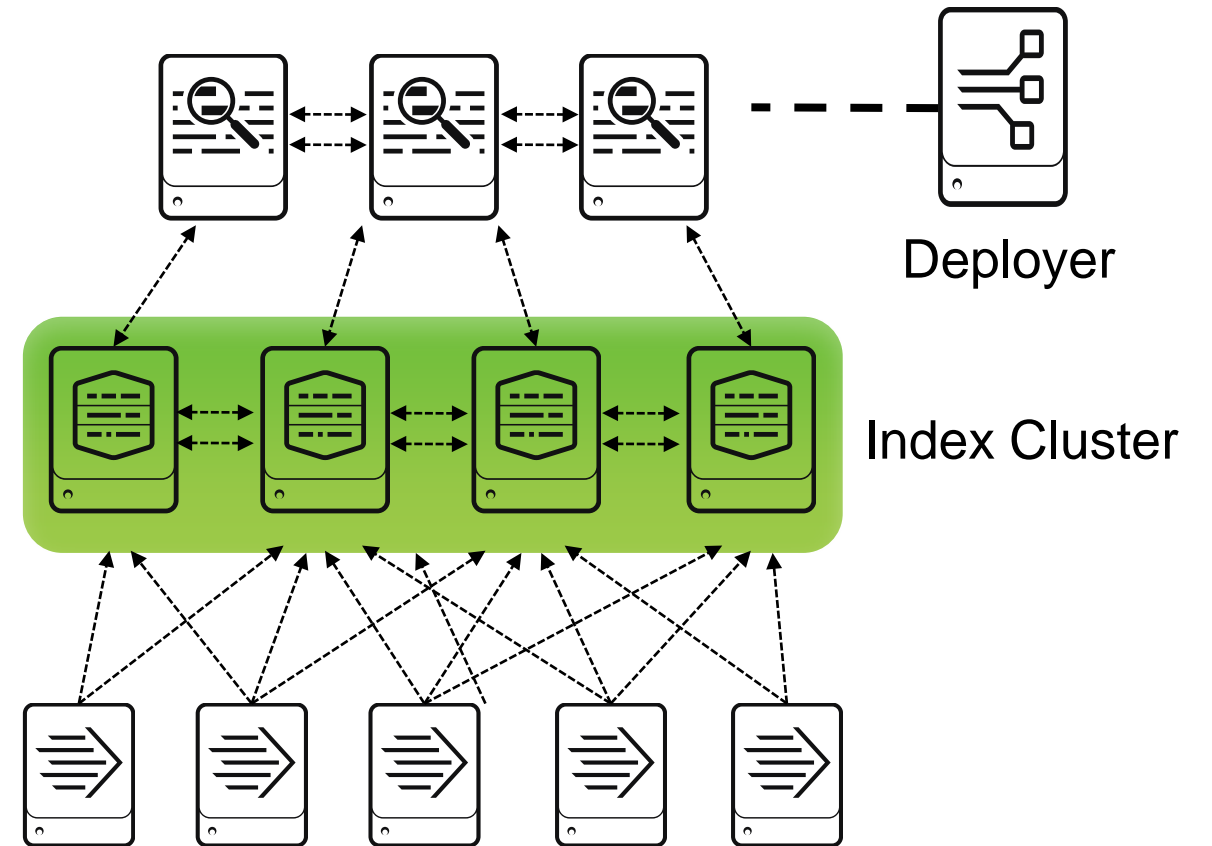
- Adding a Search Head Cluster:
 - services more users for increased search capacity
 - allows users and searches to share resources
 - Coordinate their activities to handle search requests and distribute the requests across the set of indexers
- Search Head Clusters require a minimum of three Search Heads
- A Deployer is used to manage and distribute apps to the members of the Search Head Cluster



Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Splunk Deployment – Index Cluster

- Traditional Index Clusters:
 - Configured to replicate data
 - Prevent data loss
 - Promote availability
 - Manage multiple indexers
- Non-replicating Index Clusters
 - Offer simplified management
 - Do not provide availability or data recovery



Module 3: Installation

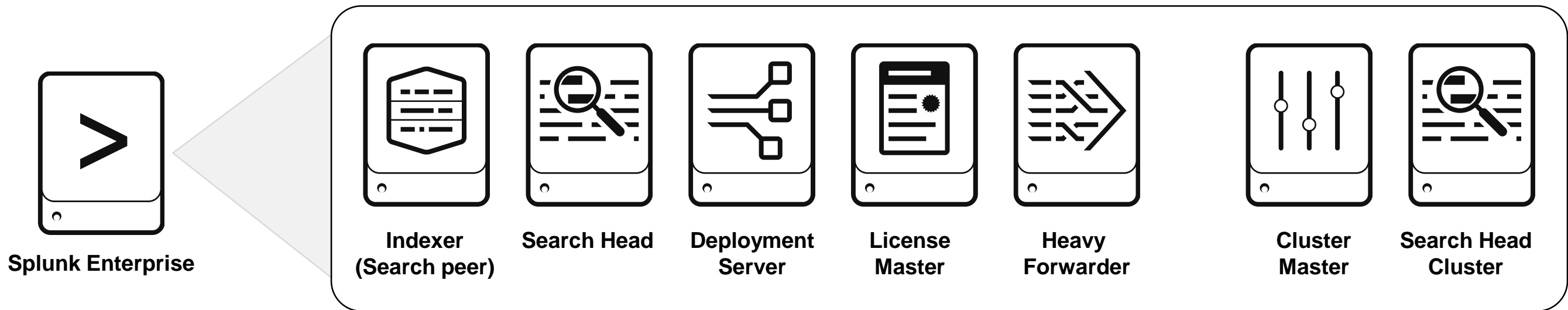
Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Module Objectives

- Describe Splunk installation
- Describe Splunk component installation
- Using Splunk Web Admin
- Identify common Splunk commands
- Identify Splunk directory structure

Splunk Enterprise Install Package

- There are multiple Splunk components installed from the Splunk Enterprise package:



Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Splunk Enterprise Installation Overview

- Verify required ports are open (splunkweb, splunkd, forwarder) and start-up account
- Download Splunk Enterprise from www.splunk.com/download
- Installation: (as account running Splunk)
 - ***NIX** – un-compress the **.tar.gz** file in the path you want Splunk to run from
 - **Windows** – execute the **.msi** installer and follow the wizard steps
- Complete installation instructions at:
docs.splunk.com/Documentation/Splunk/latest/Installation/Chooseyourplatform
- After installation:
 - Splunk starts automatically on Windows
 - Splunk must be manually started on *NIX until **boot-start** is enabled

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Splunk Component Installation Overview

- Installing Splunk Enterprise as an Indexer or Search Head is identical to installing a single deployment instance
- The difference happens at a configuration level
 - Installation as configuration is an iterative and ongoing event as you build and scale your deployment
 - Administrators need to be in control of the environment to fulfill emerging needs
 - Before installing Indexers or Search Heads, be sure to keep in mind the different hardware requirements

Common Splunk Commands

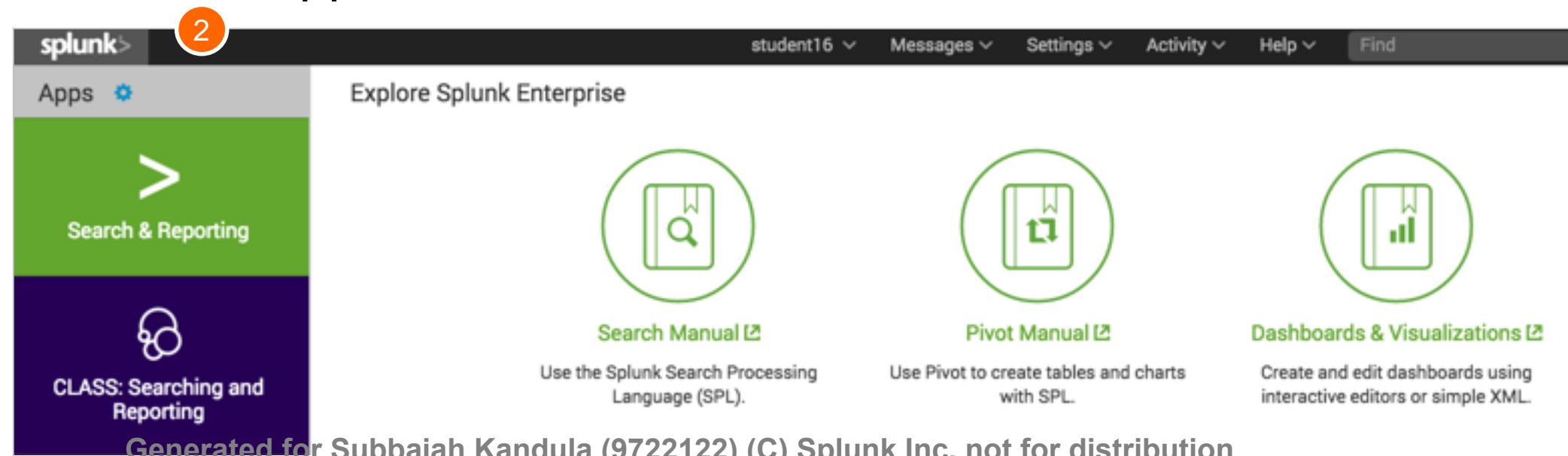
- `splunk` is the program in the `bin` directory to run the CLI

Command	Operation
<code>splunk help</code>	Display a usage summary
<code>splunk [start stop restart]</code>	Manages the Splunk processes
<code>splunk start --accept-license</code>	Automatically accept the license without prompt
<code>splunk status</code>	Display the Splunk process status
<code>splunk show splunkd-port</code>	Show the port that the splunkd listens on
<code>splunk show web-port</code>	Show the port that Splunk Web listens on
<code>splunk show servername</code>	Show the servername of this instance
<code>splunk show default-hostname</code>	Show the default host name used for all data inputs
<code>splunk enable boot-start -user</code>	Initialize script to run Splunk Enterprise at system startup

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

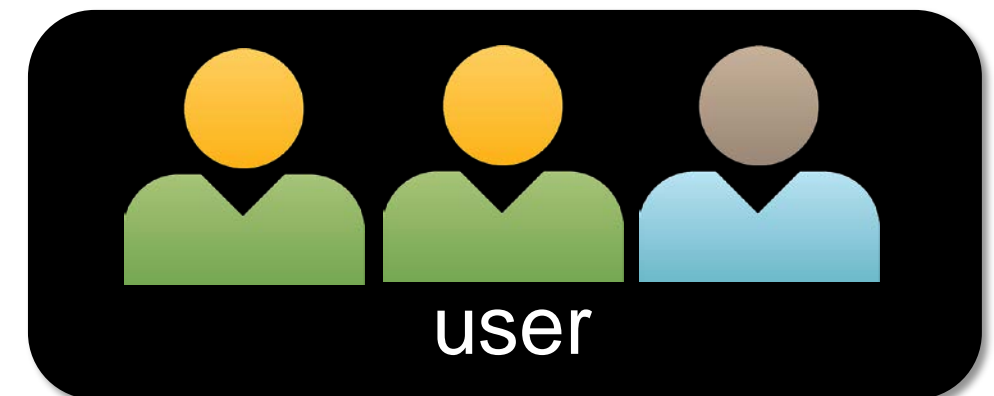
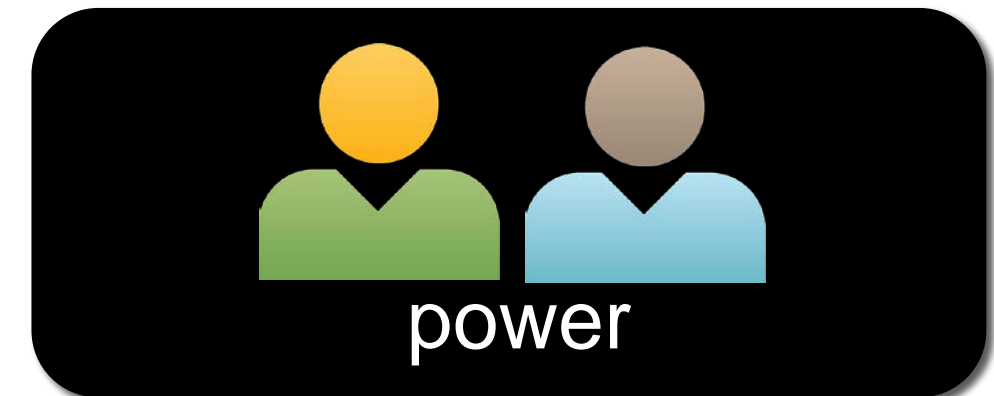
Logging In

- 1 Log in to Splunk with a web browser
- 2 Based on your default app, its main view appears
 - The Home view is shown here
 - You or your organization may change your default app



Users and Roles

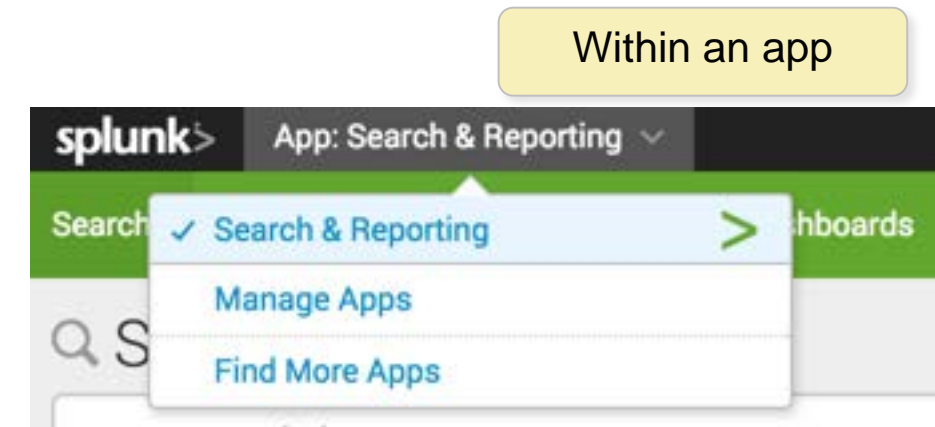
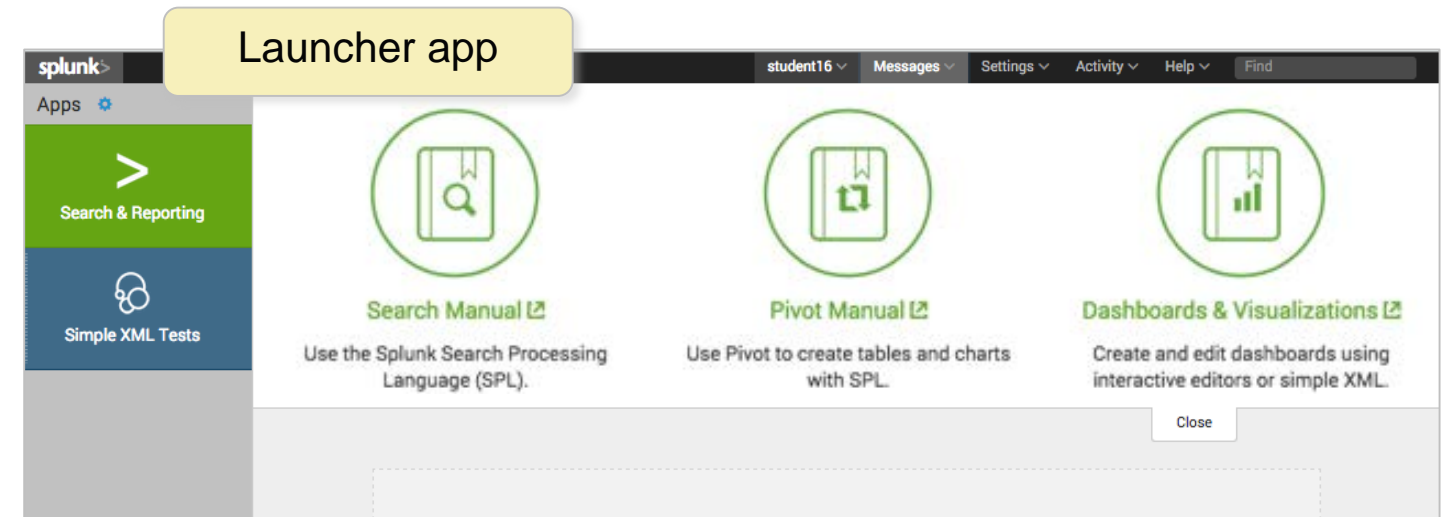
- Splunk users are assigned roles
 - Roles determine capabilities and data access
- Out of the box, there are 3 main roles:
 - Admin
 - Power
 - User
- Splunk administrators can create additional roles
- The account you use for the lab exercises has the **power** role



Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

What Are Apps?

- Apps allow different workspaces, tailored to a specific use case or user role, to exist on a single Splunk instance
- This class focuses on the Search & Reporting app (also called the Search app)
- Administrators can create or install additional apps to your Splunk instance from <http://splunkbase.splunk.com>



Note

Simply put, a Splunk app is a collection of files. Some apps are more robust and may contain data inputs, knowledge objects, and UI elements.

<http://docs.splunk.com/Documentation/Splunk/latest/Admin/Whatsanapp>

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Home App

Click the Splunk logo to return to the app that is set as your default app; the default is the Launcher app

Select app context

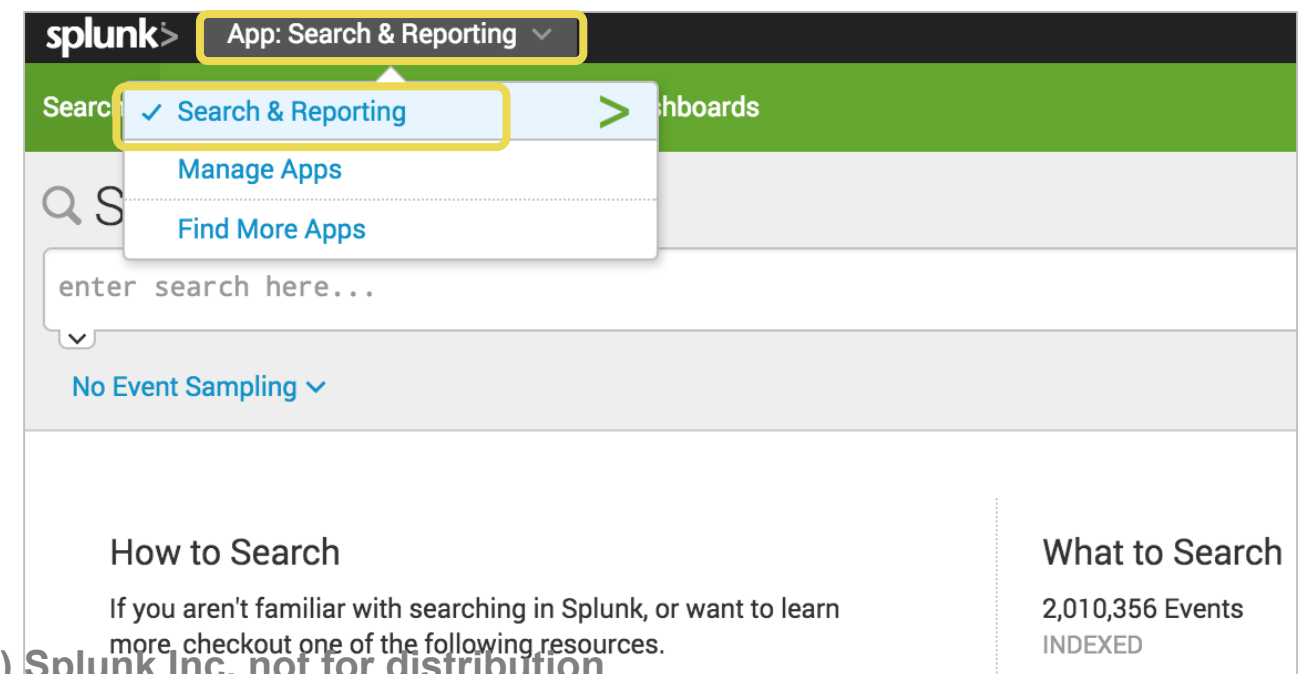
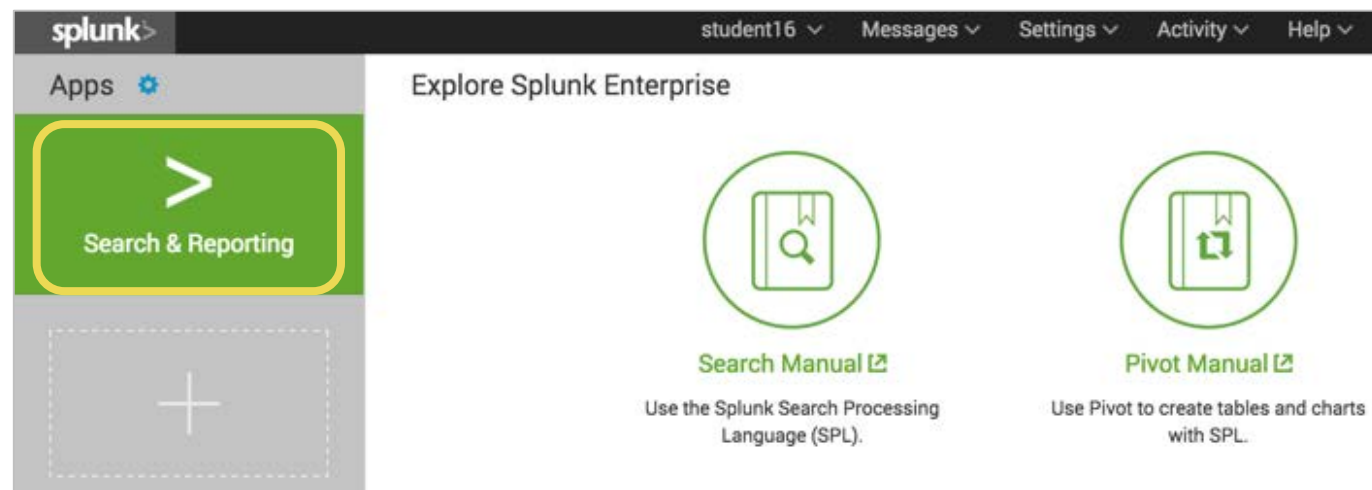
Links to several helpful resources

After you've built dashboards with your data, you can choose one to appear in your Launcher app

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Search & Reporting App Overview

- Provides a default interface for searching and analyzing data
- Enables you to create knowledge objects, reports, and dashboards
- Access by selecting the **Search & Reporting** button on the Home view or from an app view, select **Apps**, then select **Search & Reporting**



Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Module 4: Inputs

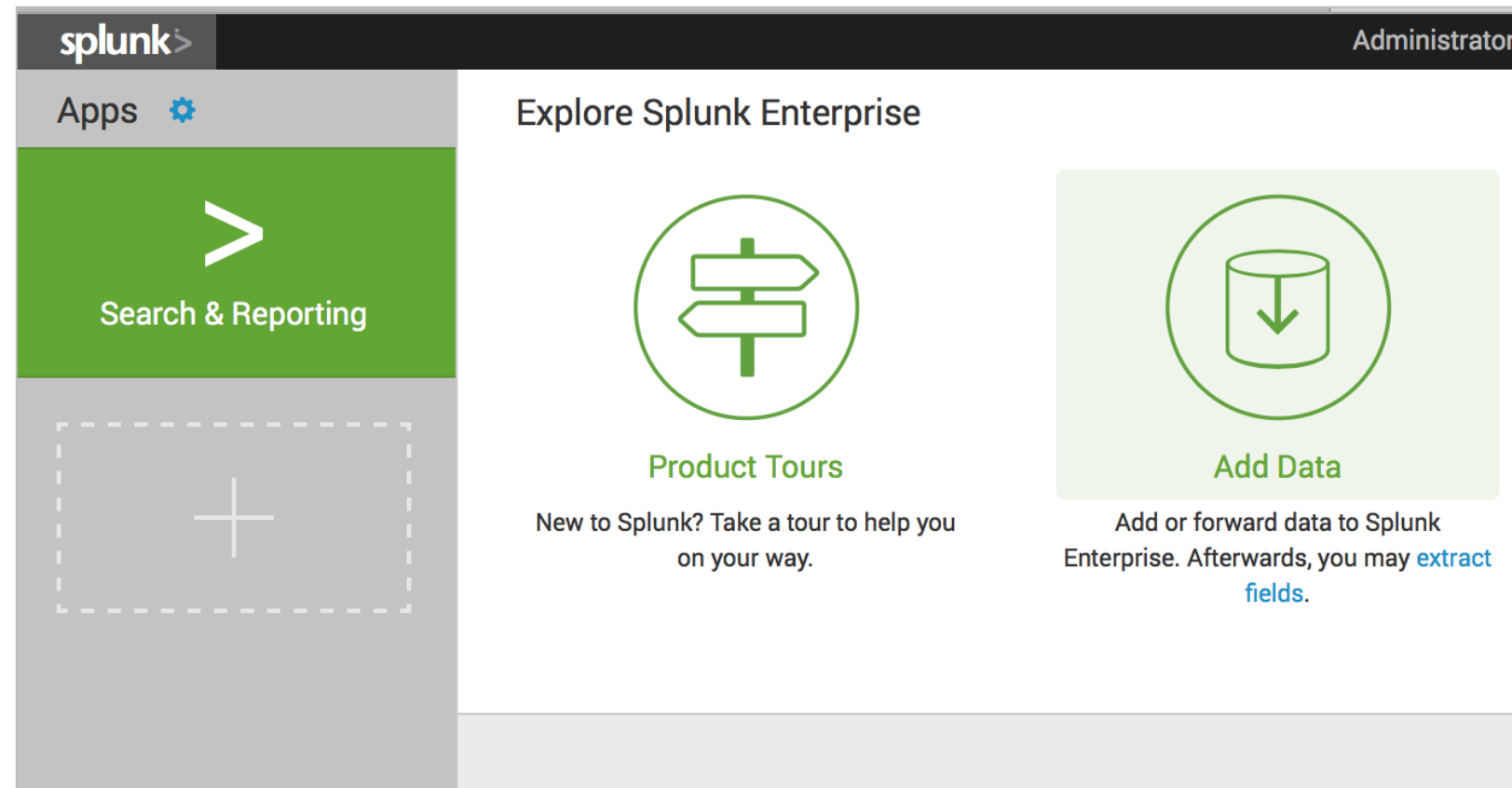
Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Module Objectives

- Identify the input types
- Uploading data using Splunk Web
- Using the Monitor option

Adding Data

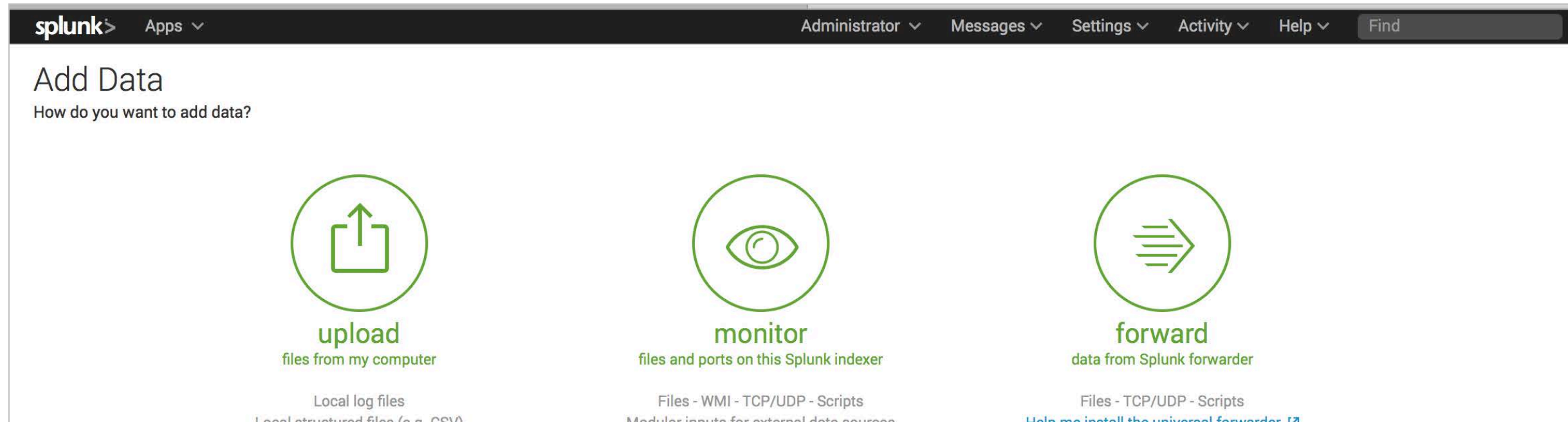
Administrators can access the Add Data menu by clicking the Add Data icon located on the Splunk Enterprise home app



Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Add Data Menu

Add Data menu provides three options depending on the source to be used



Upload Option

Upload option allows users to upload local files that only get indexed once. Useful for testing or data that is created once and never gets updated.

Monitor Option

Monitors files, directories, http events, network ports, or data gathering scripts located on Splunk Enterprise instances.

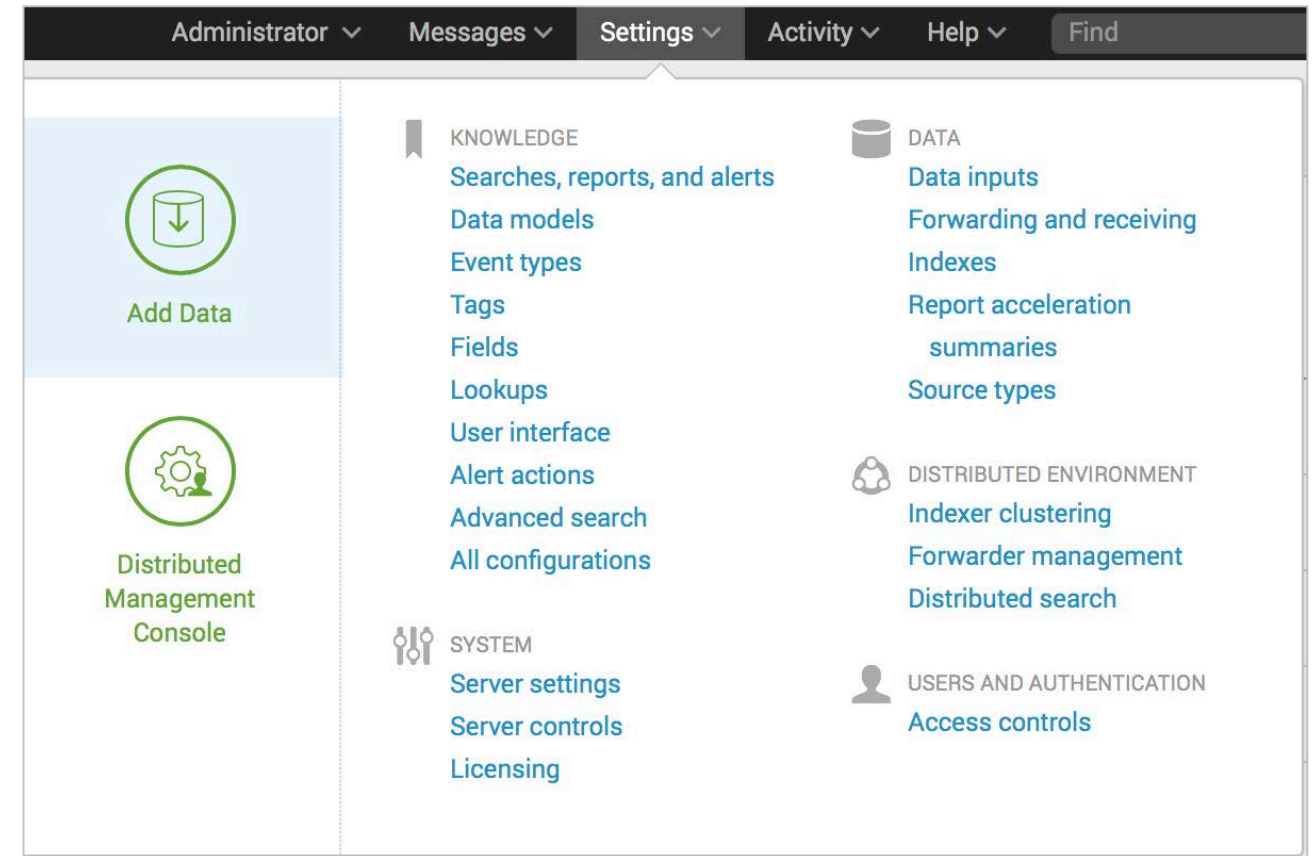
Forward Option

Main source of input in most production environments. Installed on remote machines where data is gathered on forwarded to an index over a receiving port.

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Additional Data Input Management Options

- Data can also be added and managed by:
 - **Settings > Data** Inputs below the **Data** header
 - Splunk CLI
 - Editing **.conf** files



Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Using the Upload Option

Ideal for testing and searching small datasets that are not updated

1 Click the **Upload** icon

2 Two options to upload a local dataset:

- Click the **Select File** and choose a local file, or
- Drag and drop the file

3 Click **Next**

upload
files from my computer

Local log files
Local structured files (e.g. CSV)
[Tutorial for adding data](#)

Select Source

Choose a file to upload to Splunk, either by browsing your computer or by dropping a file into the target box below. [Learn More](#)

Selected File: **CustomerSurvey.csv**

Select File

Drop your data file here

The maximum file upload size is 500 Mb

Done

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Set Sourcetype

The screenshot shows the 'Set Source Type' step in the Splunk 'Add Data' wizard. The progress bar indicates the current step is 'Set Source Type'. A yellow callout box points to the 'Next >' button, stating: 'If the data separation format is acceptable, click **Next**'. Another yellow callout box explains: 'Data recognized by Splunk will be assigned a pre-trained sourcetype (e.g. CSV file)'. A third yellow callout box points to the 'Source type: csv' dropdown menu, stating: 'Using the **Source type** drop down menu, you can change the data to a different predefined source type or create a new one.' The dropdown menu is open, showing options like 'Default Settings', 'Application', 'Database', 'Email', 'Miscellaneous', 'Network & Security', 'Operating System', 'Structured', 'Uncategorized', and 'Web'. Below the menu is a table of data with columns: _time, AccountId, age, bday, city, CONTENT_QUALITY, and CONTE.

Source: **CustomerSurvey.csv**

Source type: csv

Save As

	_time	AccountId	age	bday	city	CONTENT_QUALITY	CONTE
1	10/13/15	61181	40	1975-07-20 00:00:00	Norlane	5	5
			44	1971-08-11 00:00:00	Marmora	5	3
3	10/13/15 8:58:42.000 PM	22892	19	1996-07-13 00:00:00	Sycamore	4	4
4	10/13/15 8:47:36.000 PM	103339	43	1972-10-18 00:00:00	Cividate Camuno	1	5

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Adjusting Time Stamps and Event Breaks

Adjustments can be made to time stamps and event breaks by using the corresponding drop-down menus.

Note

The menus will change depending on the sourcetype selected.

splunk> Apps Administrator Messages

Add Data < Next >

Select Source **Set Source Type** Input Settings Review Done

Set Source Type

This page lets you see how Splunk sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: **CustomerSurvey.csv**

Source type: csv Save As

Table Format 20 Per Page

	_time	AccountId	age	bday	city	CO
1	10/13/15 10:14:00.000 PM	61181	40	1975-07-20 00:00:00	Norlane	5
2	10/13/15 9:29:28.000 PM	26554	44	1971-08-11 00:00:00	Marmora	5
3	10/13/15 8:58:42.000 PM	22892	19	1996-07-13 00:00:00	Sycamore	4
4	10/13/15 8:47:36.000 PM	103339	43	1972-10-18 00:00:00	Cividate Camuno	1

Timestamp Extraction: Auto Current time Advanced...

Delimited settings

Field delimiter: (comma) ,

Quote character: (double quote) "

File preamble:

A regular expression that instructs Splunk to ignore these preamble lines within the file.

Field names: Auto Line... Custom... Regex...

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

How Splunk Uses Sourcetypes with Data


- **sourcetype** is Splunk's way of categorizing the type of data
 - Splunk indexing processes frequently reference sourcetype
 - Many searches, reports, dashboards, apps, etc. also rely on sourcetype
 - When using predefined sourcetypes, Splunk knows where to break the event, the location of the timestamp, and automatically create field value pairs.

	_time	AccountId	age	bday	city	CONTENT_QUALITY	CONTENT_QUANTITY	country	DESIGN	email
1	10/13/15 9:29:28.000 PM	26554	44	1971-08-11 00:00:00	Marmora	5	3	US	4	uabbott@yahoo.com
2	10/13/15 8:09:05.000 PM	55084	43	1972-04-09 00:00:00	Tarko-Sale	3	3	RU	4	kernser@gmail.com

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

How Splunk Uses Sourcetypes with Data (cont.)

- When Splunk does not have a predefined way to break events, it looks for a time stamp to break the data
 - In the case of multiple time stamps, a regular expression can be used to extract the desired time
 - Regular expressions can be used with any expected patterns in the data to create a line break

	Time	Event
1 	6/3/16 12:38:47.000 PM	AccountId,"CONTENT_QUALITY","CONTENT_QUANTITY",DESIGN,JSESSIONID,NAVIGATION,SATISFACTION,"_raw","_time",age,bday,"change_type",city,country,"date_hour","date_mday","date_minute","date_month","date_second","date_wday","date_year","date_zone",email,eventtype,fname,gender,host,index,karma,lat,linecount,lname,lon,punct,region,registered,"site_release",source,sourcetype,"splunk_server","splunk_server_group",tag,"tag:eventtype",timeendpos,timestartpos,username timestamp = none
2	10/13/15 10:14:00.000 PM	61181,5,5,4,SD9SL6FF5ADFF2948092910,3,4,"[13/Oct/2015:22:14:00] AccountId=61181 JSESSIONID=SD9SL6FF5ADFF2948092910 site_release=v4 .1
3	10/13/15 5:14:00.000 PM	CONTENT_QUANTITY=5 CONTENT_QUALITY=5 NAVIGATION=3 DESIGN=4 SATISFACTION=4","2015-10-13T15:14:00.000-0700",40,"1975-07-20 00:00:00",,Norlane,AU,22,13,14,october,0,tuesday,2015,local,"jauer@kuvalis.org","nix-all-logs",Arno,M,"customer_survey",main,6807,"-38.1014",2,Mante,"144.3542","[//:::]_=_=.t=t=t=t=",Victoria,"2009-01-26 00:00:00","v4.1","/opt/log/customer_survey/bcg_survey.log","bcg_survey-3","ip-10-222-134-157",,,,21,1,mhammes

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Saving Sourcetypes

- You have the following options to save sourcetypes if any changes were made
 - Name
 - Description
 - Select a category to store in the predefined menu
 - Select which app context to save it to

Source type: SurveyData ▾ Save As

Save Source Type

Name SurveyData

Description Comma-separated value format. Set hi

Category Structured ▾

App Search & Reporting ▾

Cancel Save

Application

Custom

Database

Email

Miscellaneous

Network & Security

Operating System

✓ Structured

Web

Distributed Management Console

✓ Search & Reporting

system

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Input Settings

Add Data

Select Source Set Source Type **Input Settings** Review Done

< **Review** >

Input Settings

Optionally set additional input parameters for this data input as follows:

Host

When Splunk indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

The host name should reflect the machine the events are originating from.

Constant value Regular expression on path Segment in path

Host field value:

Index

Splunk stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index: [Create a new index](#)

- Default
- history
- main
- summary
- ✓ surveydata

Select the index to import the data. You can also create a new one if needed.

FAQ

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Review and Submit

Add Data

Select Source Set Source Type Input Settings **Review** Done

< Submit >

Review

Input Type	Uploaded File
File Name	CustomerSurvey.csv
Source Type	SurveyData
Host	splunkServer1
Index	surveydata

The Review page displays the settings for our input.

Add Data

Select Source Set Source Type Input Settings Review **Done**

< Next >

✓ File input has been created successfully.

Configure your inputs by going to Settings > [Data Inputs](#)

- Start Searching** Search your data now or see [examples and tutorials](#). ↗
- Extract Fields Create search-time field extractions. [Learn more about fields](#). ↗
- Add More Data Add more data inputs now or see [examples and tutorials](#). ↗
- Download Apps Apps help you do more with your data. [Learn more](#). ↗
- Build Dashboards Visualize your searches. [Learn more](#). ↗

After clicking **Submit**, Splunk indexes the data, and we can start searching

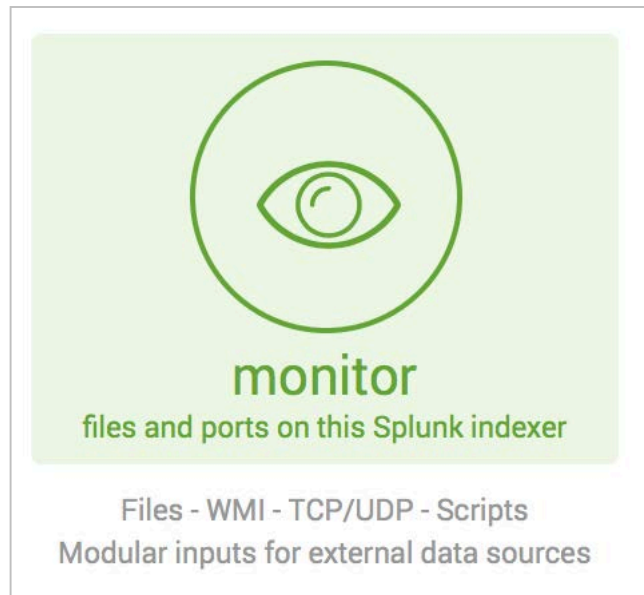
Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Using the Monitor Option

Monitors files, directories, http events, network ports, or data gathering scripts located on a Splunk indexer

1

Click the **Monitor** icon



splunk> Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾

Add Data Select Source Input Settings Review Done < Next >

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure Splunk to listen on a network port.

Scripts
Get data from from any API, service, or database with a script.

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

2
Options to monitor files, directories, http events, ports, or monitor sources with custom script you can write.

option

Monitoring Files or Directories

The screenshot shows the Splunk 'Add Data' configuration interface. The top navigation bar includes 'splunk', 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a search bar. The 'Add Data' progress bar is at the top, with 'Select Source' highlighted. The 'Files & Directories' section is selected, showing instructions and a 'File or Directory?' input field with a 'Browse' button. Below this are options for 'Continuously Monitor' (selected) and 'Index Once'. There are also fields for 'Whitelist?' and 'Blacklist?'. Three yellow callout boxes with arrows point to the 'Browse' button, the 'Continuously Monitor' button, and the 'Whitelist?' and 'Blacklist?' fields.

Annotations:

- Browse to select the file or directory.
- Select the option to continuously monitor or index the data once.
- When a directory is selected, there are options to whitelist or blacklist files in the directory.

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Monitoring Files or Directories (cont)

splunk > Apps ▾ Administrator ▾ Messages ▾

Add Data < Review >

Select Source Set Source Type **Input Settings** Review Done

Input Settings

Optionally set additional input parameters for this data input as follows:

App context
Application contexts are folders within a Splunk instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. Splunk loads all app contexts based on precedence rules. [Learn More](#)

Host
When Splunk indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input options. [Learn More](#)

Index
Splunk stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

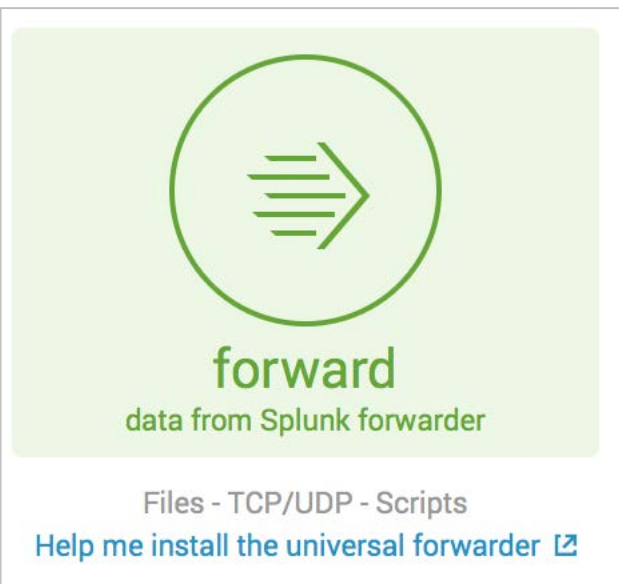
Annotations:

- Browse to select the file or directory. (points to App Context)
- Similar to the Upload option, you can set values for other metadata fields or keep the original settings. (points to Host field value and Index)

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Using the Forward Option

- Production environments use forwarders as the main source of data input
 - Installed on remote machines and forward data to an indexer over a receiving



A screenshot of the Splunk web interface. The top navigation bar shows "splunk" and "Apps". The main heading is "Add Data". A progress bar indicates the current step is "Select Forwarders", with other steps being "Select Source", "Input Settings", and "Re". A "Next >" button is visible. A "Note" box states: "Only forwarders setup to use the server will be displayed in this interface, regardless of sending data to the server." Below the note, the "Select Forwarders" section contains instructions: "Create or select a server class for data inputs. Use this page only in a single-instance Splunk instance." and "To enable forwarding of data from deployment clients to this instance, set the output configuration for the indexer to 'forward'." A red warning icon and message are highlighted with a green box: "There are currently no forwarders configured as deployment clients to this instance. Learn More" with a link icon.

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Module 5: Searching

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Module Objectives

- Run basic searches
- Use autocomplete to help build a search
- Set the time range of a search
- Identify the contents of search results
- Refine searches
- Use the timeline
- Control a search job
- Save search results

Search & Reporting App Overview (cont.)

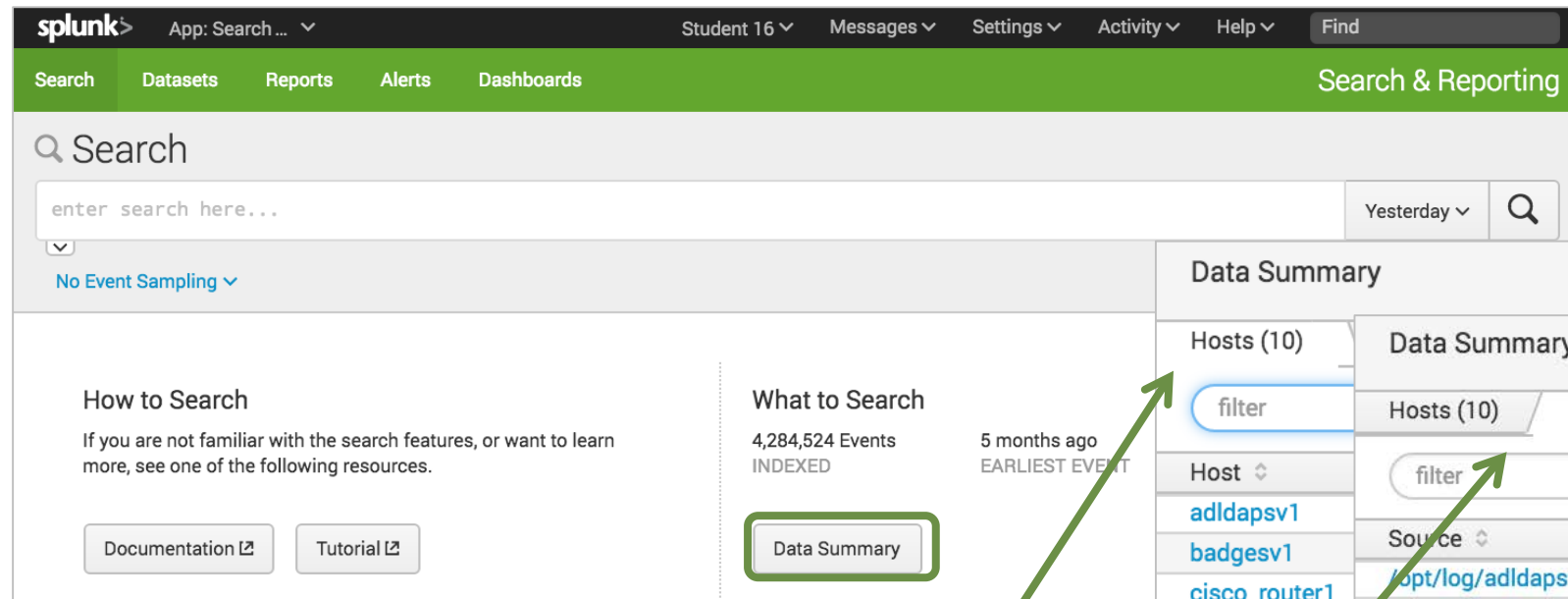
The screenshot shows the Splunk Search & Reporting app interface with several key components annotated:

- splunk bar**: The top navigation bar containing the Splunk logo, current app name, and user menu.
- app navigation bar**: The secondary navigation bar with tabs for Search, Datasets, Reports, Alerts, and Dashboards.
- current view**: The 'Search' tab in the navigation bar.
- search bar**: The main search input field with the placeholder text 'enter search here...'. A secondary search bar is also present on the right side.
- global stats**: A section displaying search statistics: '4,252,416 Events INDEXED', '5 months ago EARLIEST EVENT', and 'a minute ago LATEST EVENT'. A 'Data Summary' button is located below this section.
- time range picker**: A dropdown menu currently set to 'All time'.
- start search**: A search button icon.
- data sources**: A label pointing to the 'Data Summary' button.
- search history**: A link to view search history, with an 'Expand your search history' option below it.

Footer text: © 2005-2016 Splunk Inc. All rights reserved.

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Data Summary Tabs



Click **Data Summary** to see hosts, sources, or sourcetypes on separate tabs

- **Host** – Host name, IP address, or name of network host from which the events originated
- **Source** - Name of the file, stream, or other input
- **Sourcetype** - Specific data type or data format

Tables can be sorted or filtered

Sourcetype	Count	Last Update
access_combined	594,639	10/11/16 2:05:42.000 PM
cisco_esa	317,488	10/11/16 2:07:08.000 PM
cisco_firewall	4,430	10/11/16 12:23:43.000 PM
cisco_wsa_squid	142,222	10/11/16 2:06:34.000 PM
history_access	37,393	10/11/16 2:03:47.000 PM
linux_secure	927,883	10/11/16 2:07:28.000 PM
ps	1,000,828	10/11/16 2:07:24.000 PM
sales_entries	1,046,728	10/11/16 2:06:42.000 PM
vendor_sales	128,023	10/11/16 1:56:00.000 PM
win_audit	1	8/11/16 12:53:24.000 AM
winauthentication_security	53,050	10/11/16 2:03:47.000 PM

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Key Details

The screenshot shows the Splunk Search & Reporting interface. At the top, the navigation bar includes 'App: Search & Reporting', 'Student 16', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. Below this, the 'Search & Reporting' header contains 'Search', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The main search area shows a search query 'error OR fail*' and a 'search' button. Below the search bar, it indicates '6,382 events' and provides options for 'No Event Sampling', 'Job', and 'Smart Mode'. A timeline visualization shows a peak of '255 events at 10 PM on Monday, October 10, 2016'. Below the timeline, a table of search results is displayed with columns for 'i', 'Time', and 'Event'. The first row is highlighted with a green box and contains the following text: '10/10/16 11:59:54.000 PM Mon Oct 10 2016 23:59:54 www2 sshd[3286]: Failed password for nsharpe from 10.2.10.163 port 447 2 ssh2 host = www2 | source = /opt/log/www2/secure.log | sourcetype = linux_secure'. A 'field' label points to the 'www3' value in the 'host' field of the third row, and a 'field value' label points to the 'www3' value in the 'host' field of the fourth row. On the left side, the 'Selected Fields' list includes 'event', 'host', 'source', and 'sourcetype'. A 'Note' box on the right contains information about Splunk's online glossary and Splexicon.

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Why Learn to Search?

- Why is it important to be able to write searches?
 - You have questions about your data -- searches retrieve the events that can answer them
 - Every report and visualization is built based on an underlying search
 - Understanding, analyzing, and troubleshooting visualizations depends on your ability to understand the search string
 - Mastering the search language enables you to do as much as possible with your data to meet your specific needs

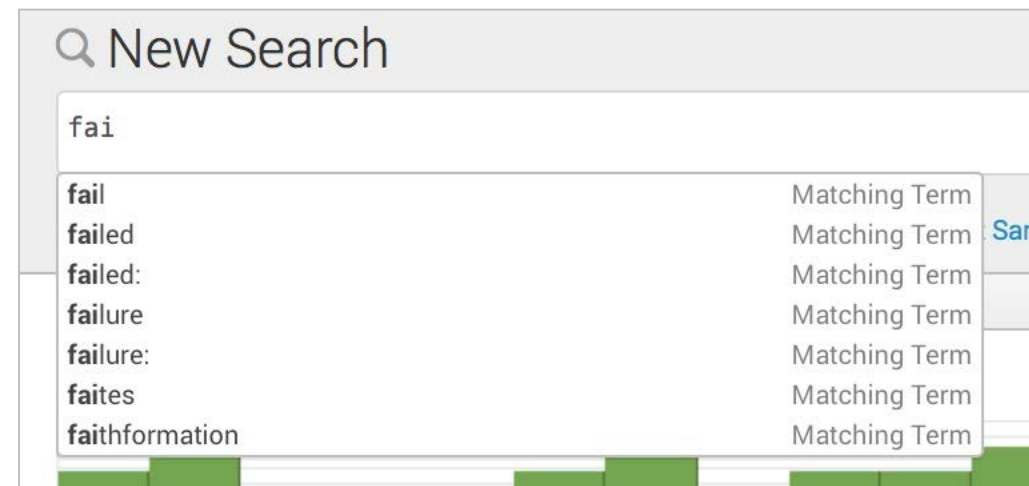
Search Guidelines

- * wildcard supported
- Search terms are case insensitive
- Booleans AND, OR, NOT
 - Must be uppercase
 - AND is implied between terms
 - Use () for complex searches
- Quotation marks for phrases

fail	Yesterday	Q
fail*	Yesterday	Q
fail* nfs	Yesterday	Q
error OR 404	Yesterday	Q
error OR failed AND 500 OR 503	Yesterday	Q
error OR (failed AND (500 OR 503))	Yesterday	Q
"login failure"	Yesterday	Q

Search Assistant

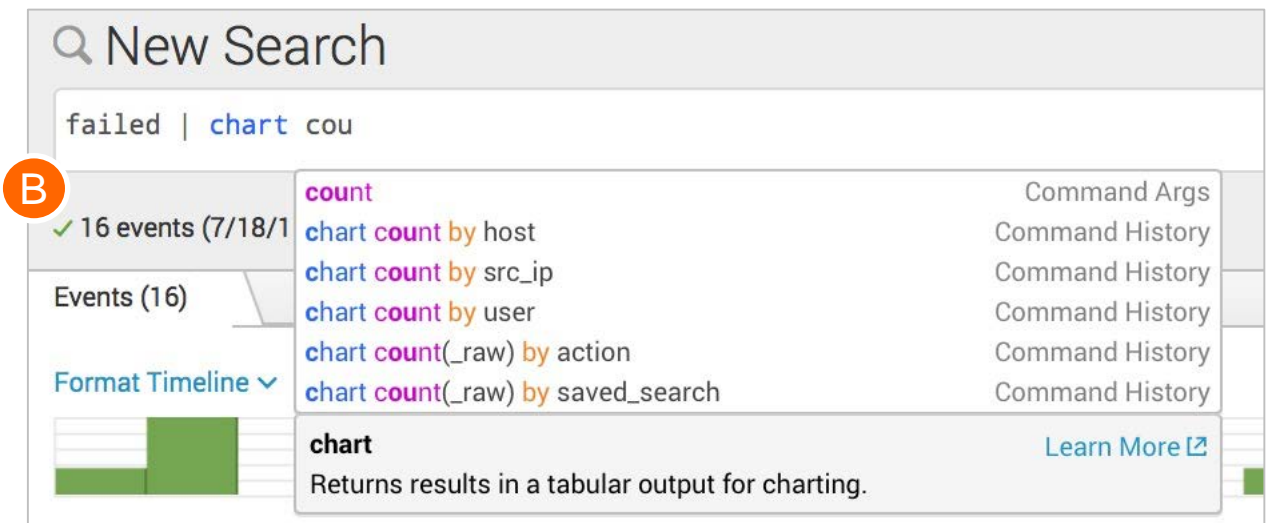
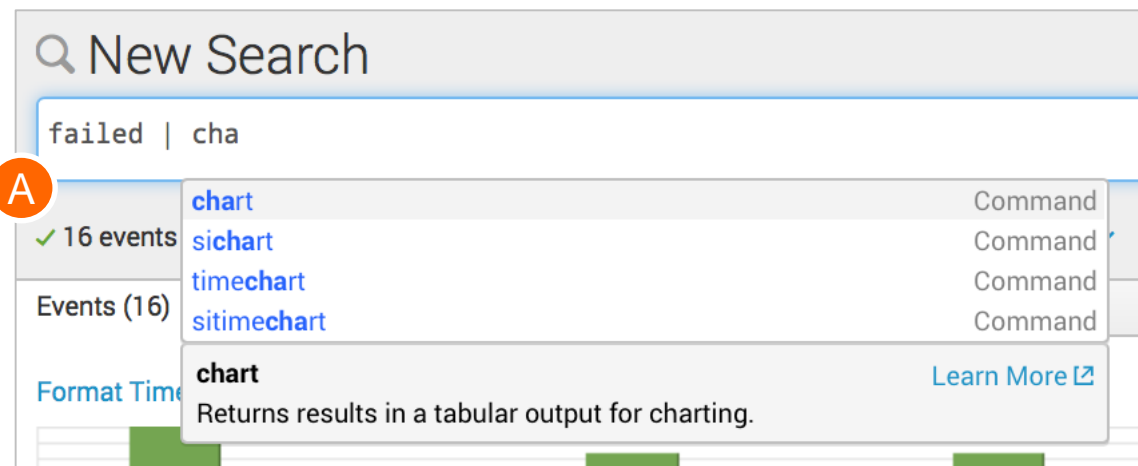
- Search Assistant provides selections for how to complete the search string
- Before the first pipe (|), it will look for matching terms
- You can continue typing OR select a term from the list
 - If you select a term from the list, it is added to the search



Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Search Assistant (cont.)

- After the first pipe, the Search Assistant will show a list of commands that can be entered into the search string
- A** • You can continue typing OR scroll through and select a command to add
- If you mouse over a command, more information about the command is shown
- As you continue to type, Search Assistant makes more suggestions **B**



Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Search Assistant (cont.)

- Search Assistant is enabled by default, in the user settings
- By default, **Compact** is selected
- If desired, to show more information, choose **Full**

Search

Use these properties for assistance with command syntax including examples, autocomplete syntax, or to turn off search assistant. Syntax highlighting displays search string components in different colors.

Search assistant

- Compact
- Full
- None

Syntax highlighting

- On
- Off

Cancel Save

Compact

Search

failed | chart cou

No Event Sampling

How to Search

If you are not familiar with search syntax, see one of our search syntax guides.

chart Command Args
Returns results in a tabular output for charting.
Example:
... | chart max(delay) over foo

Learn More

Full

Search

failed | chart cou

Command History

- ... | chart count by host
- ... | chart count by user
- ... | chart count by src_ip
- ... | chart count over vendor_action by src_ip
- ... | chart count(_raw) by action

Command Args

count

chart Help More Auto Open

Returns results in a tabular output for charting.

Examples

Return max(delay) for each value of foo.
... | chart max(delay) over foo

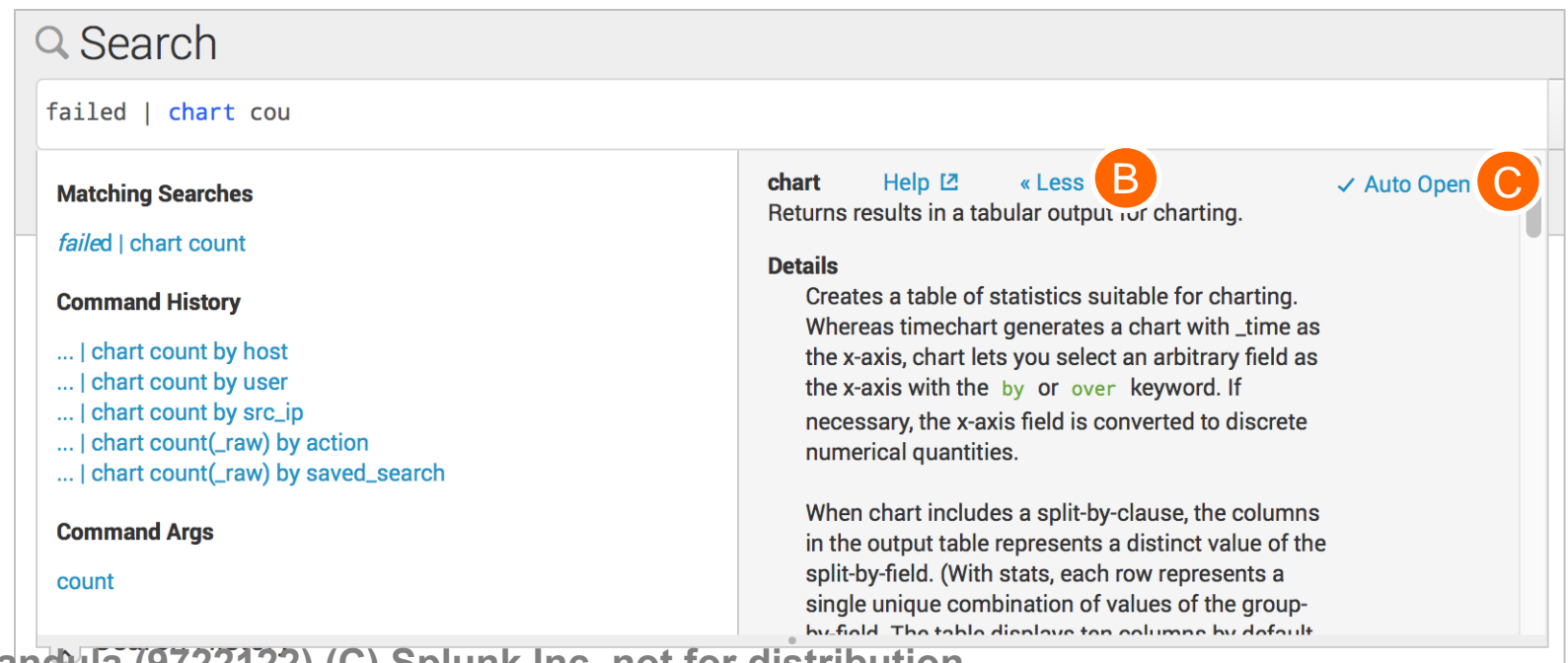
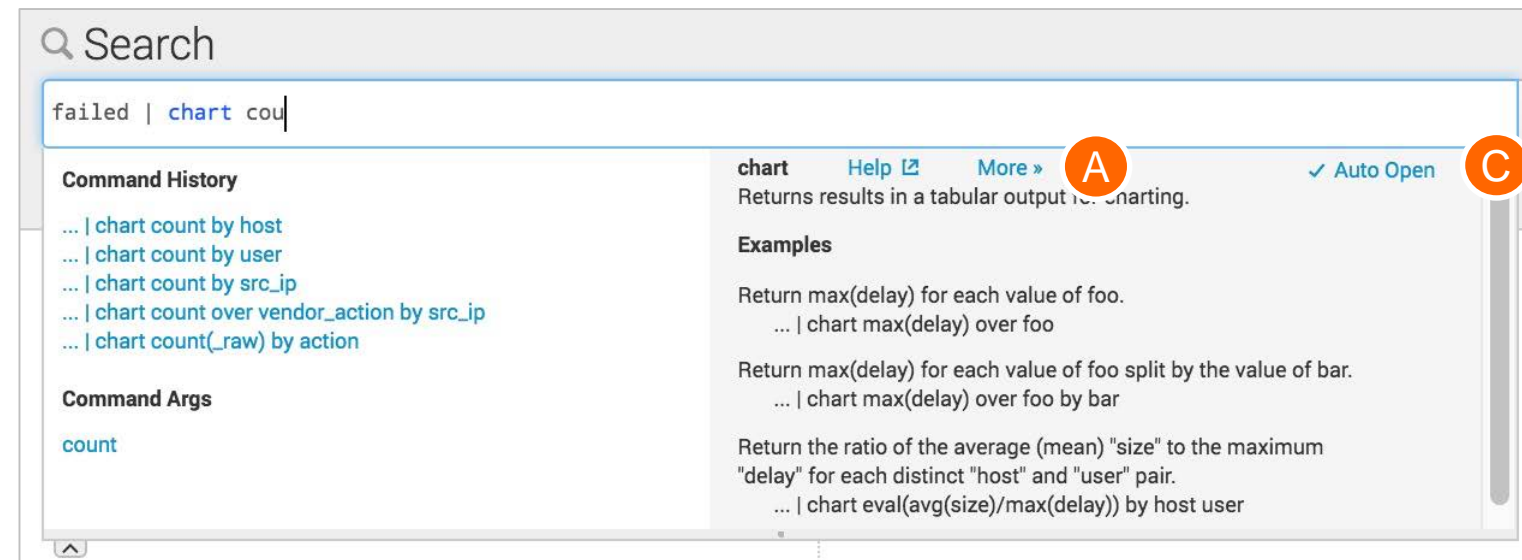
Return max(delay) for each value of foo split by the value of bar.
... | chart max(delay) over foo by bar

Return the ratio of the average (mean) "size" to the maximum "delay" for each distinct "host" and "user" pair.
... | chart eval(avg(size)/max(delay)) by host user

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Search Assistant - Full

- A** To show more information, click **More »**
- B** To show less information, click **« Less**
- C** To toggle Full mode off, de-select **Auto Open**



Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Search Results

- Matching results are returned immediately
- Displayed in reverse chronological order (newest first)
- Matching search terms are highlighted

The screenshot shows a Splunk search interface for the query "failed password". The search results are displayed in a table format, showing the time and event details for each match. The events are listed in reverse chronological order, with the most recent event at the top. The search results are displayed in a table format, showing the time and event details for each match. The events are listed in reverse chronological order, with the most recent event at the top. The search results are displayed in a table format, showing the time and event details for each match. The events are listed in reverse chronological order, with the most recent event at the top.

i	Time	Event
>	6/27/16 11:57:39.000 PM	Jun 19 23:57:39 bcg-payroll sshd[853]: Failed password for root from 3.0.0.44 port 51547 ssh2 host = www2 source = /opt/log/www2/auth.nix sourcetype = linux_secure
>	6/27/16 11:57:06.000 PM	Jun 19 23:57:06 bcg-payroll sshd[3329]: Failed password for root from 3.0.0.44 port 53736 ssh2 host = www1 source = /opt/log/www1/auth.nix sourcetype = linux_secure
>	6/27/16 11:51:40.000 PM	Jun 19 23:51:40 bcg-payroll sshd[1061]: Failed password for root from 3.0.0.44 port 56986 ssh2 host = www3 source = /opt/log/www3/auth.nix sourcetype = linux_secure

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Event Details

- Splunk parses data into individual events
- Each event has a:
 - timestamp
 - host
 - source
 - sourcetype

The screenshot shows a Splunk search interface for the query "failed password". It displays 436 events from June 27, 2016, to June 28, 2016. A timeline visualization shows the distribution of events over time. Below the timeline, a table lists individual events with their timestamps and details. Three events are highlighted with green boxes, showing their timestamps and the fields host, source, and sourcetype.

i	Time	Event
>	6/27/16 11:57:39.000 PM	Jun 19 23:57:39 bcg-payroll sshd[853]: Failed password for root from 3.0.0.44 port 51547 ssh2 host = www2 source = /opt/log/www2/auth.nix sourcetype = linux_secure
>	6/27/16 11:57:06.000 PM	Jun 19 23:57:06 bcg-payroll sshd[3329]: Failed password for root from 3.0.0.44 port 53736 ssh2 host = www1 source = /opt/log/www1/auth.nix sourcetype = linux_secure
>	6/27/16 11:51:40.000 PM	Jun 19 23:51:40 bcg-payroll sshd[1061]: Failed password for root from 3.0.0.44 port 56986 ssh2 host = www3 source = /opt/log/www3/auth.nix sourcetype = linux_secure

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Search Results Details

The screenshot shows the Splunk search results interface for the query "failed password". The search returned 436 events from 6/27/16 12:00:00.000 AM to 6/28/16 12:00:00.000 AM. The interface includes a search bar, a time range picker, a search mode dropdown (set to Smart Mode), and a navigation bar with tabs for Events (436), Patterns, Statistics, and Visualization. A timeline visualization is displayed above a table of search results. The table has columns for index (i), time, and event details. Annotations highlight various UI elements: "time range picker" points to the search bar area; "search results appear in the Events tab" points to the Events tab; "search mode" points to the Smart Mode dropdown; "paginator" points to the pagination controls; "Fields sidebar" points to the left sidebar; "timestamp" points to the time column; "selected fields" points to the event details; and "events" points to the event content.

time range picker

Save As v Close

"failed password"

search results appear in the Events tab

Yesterday v

436 events (6/27/16 12:00:00.000 AM to 6/28/16 12:00:00.000 AM) No Event Sampling v Job v || ■ → + ↓ Smart Mode v

Events (436) Patterns Statistics Visualization

search mode

Format Timeline v timeline 1 hour per column

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

< Hide Fields All Fields

Selected Fields

- a host 3
- a source 3
- a sourcetype 1

Interesting Fields

- a app 1
- # date_hour 24

i	Time	Event
>	6/27/16 11:57:39.000 PM	Jun 19 23:57:39 bcg-payroll sshd[853]: Failed password for root from 3.0.0.4 port 51547 ssh2 host = www2 source = /opt/log/www2/auth.nix sourcetype = linux_secure
>	6/27/16 11:57:06.000 PM	Jun 19 23:57:06 bcg-payroll sshd[3329]: Failed password for root from 3.0.0.4 port 51547 ssh2 host = www1 source = /opt/log/www1/auth.nix sourcetype = linux_secure
>	6/27/16 11:51:40.000 PM	Jun 19 23:51:40 bcg-payroll sshd[1061]: Failed password for root from 3.0.0.44 port 56986 ssh2 host = www3 source = /opt/log/www3/auth.nix sourcetype = linux_secure

Fields sidebar

timestamp

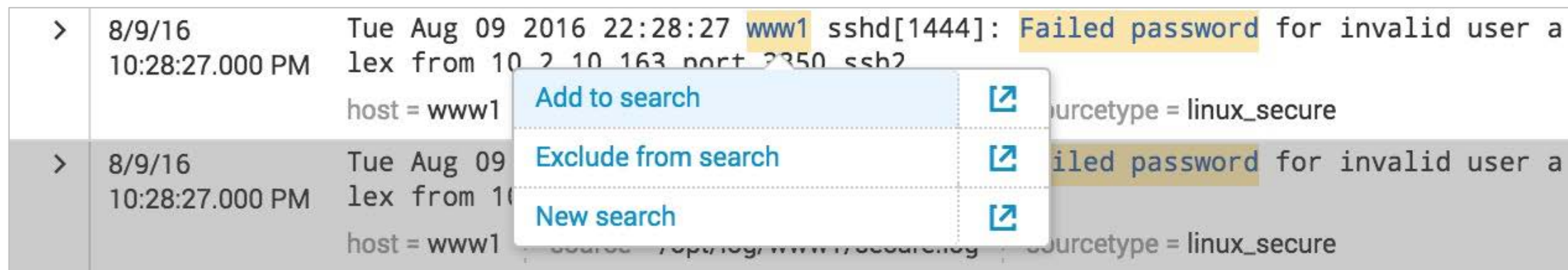
selected fields

events

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Using Search Results to Modify a Search

- When you mouse over search results, keywords are highlighted
- Click any item in your search results; a window appears allowing you to:
 - Add the item to the search
 - Exclude the item from the search
 - Open a new search including only that item



The screenshot shows a table of search results with a context menu open over a row. The table has columns for time, date, host, and message. The message column contains log entries with highlighted keywords. The context menu has three options: 'Add to search', 'Exclude from search', and 'New search', each with a corresponding icon.

>	8/9/16 10:28:27.000 PM	Tue Aug 09 2016 22:28:27	www1 sshd[1444]: Failed password for invalid user alex from 10.2.10.163 port 2350 ssh2	host = www1	sourcetype = linux_secure
>	8/9/16 10:28:27.000 PM	Tue Aug 09	Failed password for invalid user a	host = www1	source = /opt/log/www1/securelog sourcetype = linux_secure

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Changing Search Results View Options

You have several layout options for displaying your search results

New Search

"failed password" Last 7 days

9,208 events (1/13/16 9:00:00.000 PM to 1/20/16 9:10:35.000 PM) No Event Sampling

Events (9,208) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

List Format 20 Per Page

i	Time	Event
>	1/20/16 9:10:31.000 PM	Wed Jan 20 2016 21:10:31 www1 sshd[5283]: Failed password for invalid user desktop from 10.1.10.172 port 1256 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
>	1/20/16 9:10:21.000 PM	Wed Jan 20 2016 21:10:21 www1 sshd[5391]: Failed password for invalid user rdb from 10.1.10.172 port 2469 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
>	1/20/16 9:10:07.000 PM	Wed Jan 20 2016 21:10:07 www1 sshd[1777]: Failed password for invalid user sales from 10.1.10.172 port 2732 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
>	1/20/16 9:09:35.000 PM	Wed Jan 20 2016 21:09:35 www1 sshd[1771]: Failed password for myuan from 10.1.10.172 port 1854 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure

i	_time	host	source	sourcetype
>	1/20/16 9:10:31.000 PM	www1	/opt/log/www1/secure.log	linux_secure
>	1/20/16 9:10:21.000 PM	www1	/opt/log/www1/secure.log	linux_secure
>	1/20/16 9:10:07.000 PM	www1	/opt/log/www1/secure.log	linux_secure

Raw Format 20 Per Page

- Raw
- List
- Table

2016 21:10:31 www1 sshd[5283]: Failed password for invalid user desktop from 10.1.10.172 sh2

2016 21:10:21 www1 sshd[5391]: Failed password for invalid user rdb from 10.1.10.172 port 2469 ssh2

> Wed Jan 20 2016 21:10:07 www1 sshd[1777]: Failed password for invalid user sales from 10.1.10.172 port 2732 ssh2

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Selecting a Specific Time

Relative

Earliest: 7 Days Ago

Latest: now Beginning of today

No Snap-to Beginning of day

1/13/16 12:00:00.000 AM 1/20/16 9:30:33.000 PM

Apply

Real-time

Earliest: 7 Days Ago

Latest: now

1/13/16 9:30:33.000 PM

Apply

Date Range

Between 01/13/2016 and 01/20/2016

00:00:00 24:00:00

Apply

Date & Time Range

Between 01/17/2016 00:00:00.000 and 01/20/2016 21:28:09.000

HH:MM:SS.SSS HH:MM:SS.SSS

Apply

Advanced

Earliest: Latest:

1/1/70 12:00:00.000 AM 1/20/16 8:58:07.000 PM

Apply

[Documentation](#)

Last 7 days

Presets

Real-time	Relative	Other
30 second window	Today	Last 15 minutes
1 minute window	Week to date	Last 60 minutes
5 minute window	Business week to date	Last 4 hours
30 minute window	Month to date	Last 24 hours
1 hour window	Year to date	Last 7 days
All time (real-time)	Yesterday	Last 30 days
	Previous week	
	Previous business week	
	Previous month	
	Previous year	

preset time ranges

Relative

Real-time

Date Range

Date & Time Range

Advanced

custom time ranges

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Viewing the Timeline

- Timeline shows distribution of events specified in the time range
 - Mouse over for details, or single-click to filter results for that time period

When hovering over a column, the banner shows the number of events and the time range. This preview does not filter the events displayed in search results

Timeline legend shows the scale of the timeline

1 hour per column

265 events at 2 AM on Wednesday, February 3, 2016

#	Time	Event
>	2/3/16 9:53:59.000 PM	Wed Feb 03 2016 21:53:59 www1 sshd[4791]: Failed password for invalid user operator from 124.160.192.241 port 1253 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
>	2/3/16 9:53:53.000 PM	Wed Feb 03 2016 21:53:53 www1 sshd[4139]: Failed password for invalid user admin from 124.160.192.241 port 1255 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure

Generated for Subbiah Kandula (9722122) (10) Splunk Inc. for distribution

View a Subset of the Results with Timeline

- To select a narrower time range, click and drag across a series of bars
 - This action filters the current search results
 - Does not re-execute the search
 - This filters the events and displays them in reverse chronological order (most recent first)

The screenshot shows a Splunk search interface for the query "failed password". The search results are displayed in a timeline view, showing 43,789 events from 2/3/16 8:00:00.000 PM to 2/10/16 8:52:45.000 PM. The timeline view is currently set to "Format Timeline" and shows a selection of 8 hours starting from Feb 5, 2016 12:00 PM to Feb 5, 2016 8:00 PM. A yellow arrow points from this selection to a table view below, which displays the selected events in reverse chronological order. The table has columns for "Time" and "Event". The selected event is highlighted with a green box and shows the time "2/5/16 7:59:57.000 PM" and the event description "Fri Feb 05 2016 19:5 from 209.160.24.63 p host = www1 | source =".

i	Time	Event
>	2/5/16 7:59:57.000 PM	Fri Feb 05 2016 19:5 from 209.160.24.63 p host = www1 source =

Use Other Timeline Controls

- **Format Timeline**

- Hides or shows the timeline in different views

- **Zoom Out**

- Expands the time focus and re-executes the search

- **Zoom to Selection**

- Narrows the time range and re-executes the search

- **Deselect**

- If in a drilldown, returns to the original results set
- Otherwise, grayed out / unavailable

"failed password"

✓ 43,789 events (2/3/16 8:00:00.000 PM to 2/10/16 8:52:45.000 PM) No Event Sampling

Events (2,081) Patterns Statistics Visualization

Format Timeline – Zoom Out + Zoom to Selection × Deselect

Feb 5, 2016 12:00 PM Feb 5, 2016 8:00 PM

8 hours

List Format 20 Per Page

< Hide Fields All Fields

	i	Time	Event
>		2/5/16 7:59:57.000 PM	Fri Feb 05 2016 19:5 from 209.160.24.63 p

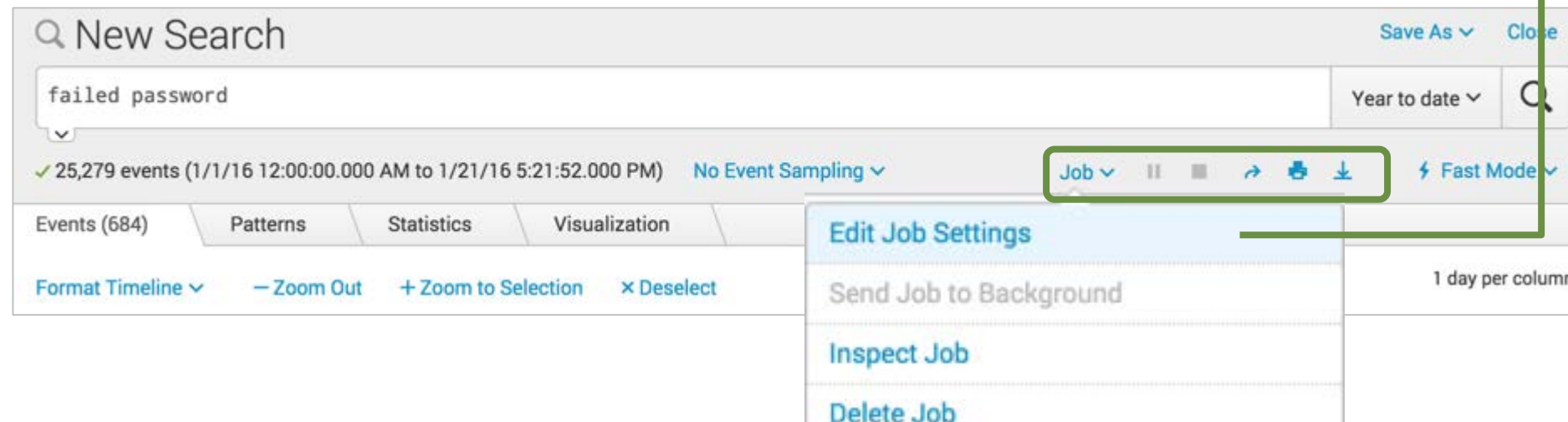
Selected Fields
a host 4

host = www1 | source =

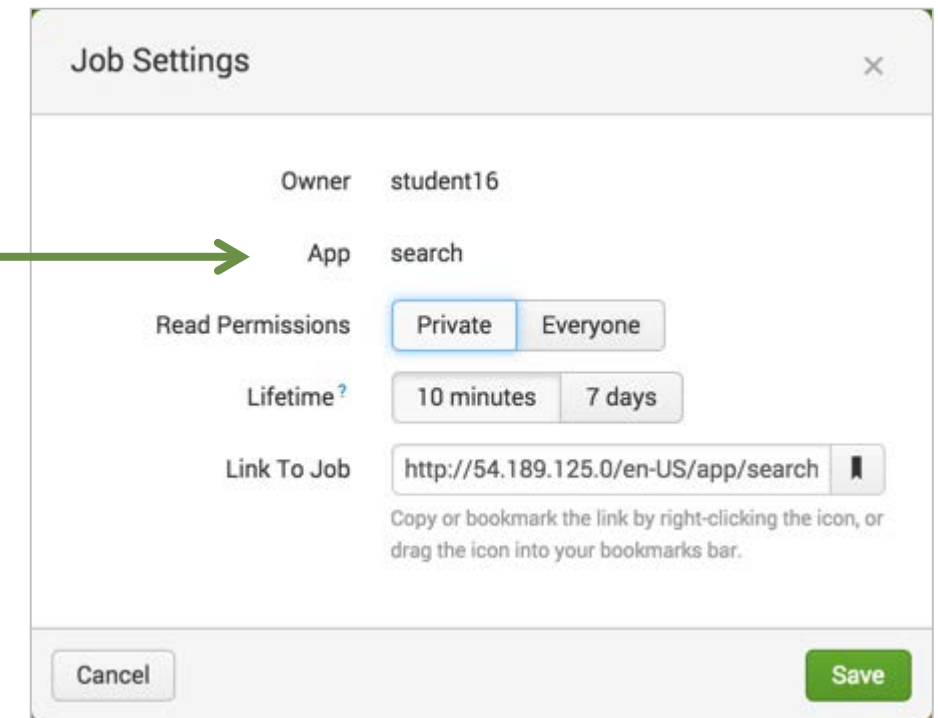
Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Control or Save Search Jobs

- Every search is also a **job**
- Use the Job bar to control search execution
 - ▢ **Pause** – toggles to resume the search
 - ▣ **Stop** – finalizes the search in progress
 - Jobs are available for 10 minutes (default)
 - Get a link to results from the **Job** menu



The screenshot shows the Splunk search interface. At the top, there is a search bar with the text "failed password" and a search button. Below the search bar, there is a status bar showing "25,279 events (1/1/16 12:00:00.000 AM to 1/21/16 5:21:52.000 PM)". The Job bar is highlighted with a green box and contains icons for Job, Pause, Stop, Share, and Download. A context menu is open over the Job bar, showing options: Edit Job Settings, Send Job to Background, Inspect Job, and Delete Job. The Job bar also includes a "Fast Mode" toggle and a "1 day per column" zoom setting.



The screenshot shows the "Job Settings" dialog box. It contains the following information:

- Owner: student16
- App: search
- Read Permissions: Private (selected) and Everyone
- Lifetime?: 10 minutes (selected) and 7 days
- Link To Job: <http://54.189.125.0/en-US/app/search>

At the bottom, there are "Cancel" and "Save" buttons. A green arrow points from the Job bar in the previous screenshot to the "App" field in this dialog.

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Set Permissions

- **Private** [default]
 - Only the creator can access
- **Everyone**
 - All app users can access search results
- **Lifetime**
 - Default is 10 minutes
 - Can be extended to 7 days
 - To keep your search results longer, schedule a report

The screenshot shows the 'Job Settings' dialog box in Splunk. It has a title bar with 'Job Settings' and a close button (X). The main content area contains the following settings:


- Owner:** becky
- App:** search
- Read Permissions:** Two buttons, 'Private' (selected with a blue border) and 'Everyone'.
- Lifetime ?:** Two buttons, '10 minutes' (selected) and '7 days'.
- Link To Job:** A text input field containing 'http://localhost:8008/en-US/app/sear' and a bookmark icon.

Below the 'Link To Job' field, there is a note: 'Copy or bookmark the link by right-clicking the icon, or drag the icon into your bookmarks bar.'

At the bottom of the dialog, there are two buttons: 'Cancel' on the left and 'Save' on the right.

Share Search Jobs


- Use the Share button next to the Job bar to quickly:
 - Apply read permissions to everyone
 - Extend the retention of the results to 7 days
 - Get a sharable link to the results
- Click the printer icon to print results or save them as PDF

Note 

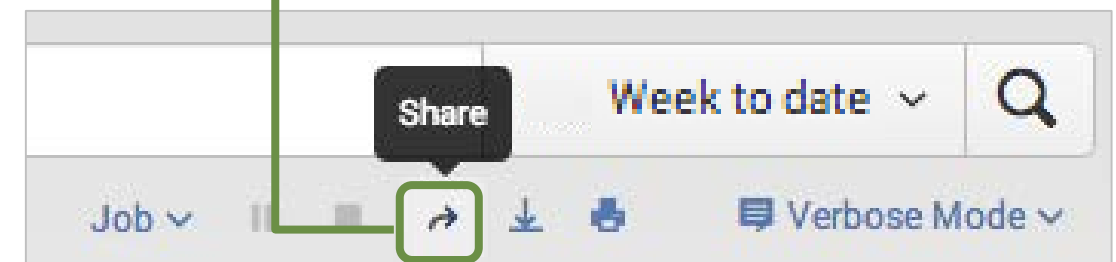
Saving and sharing the actual search strings for reuse (known as **Reports**) is discussed later in this course.

Share Job ✕

The job's lifetime has been extended to 7 days and read permissions have been set to Everyone. Manage the job via [Job Settings](#).

Link To Job 

Copy or bookmark the link by right-clicking the icon, or drag the icon into your bookmarks bar.

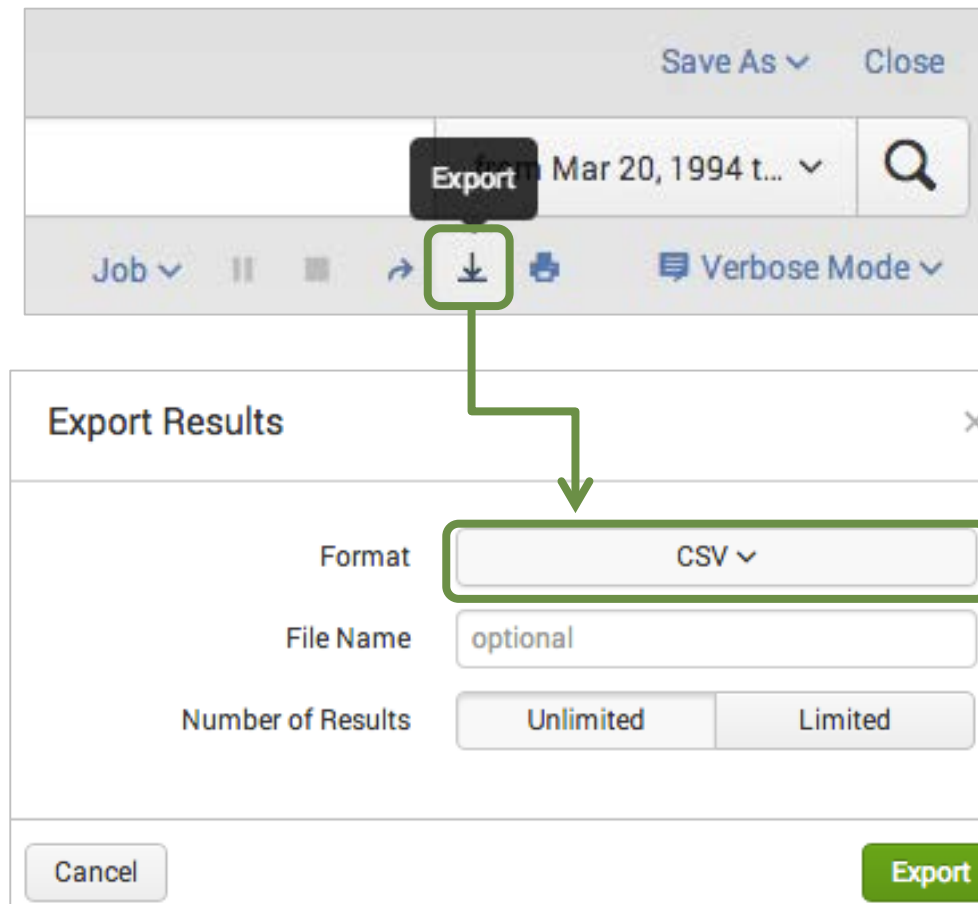


Job Week to date 🔍

🔗 📄 🖨️ Verbose Mode

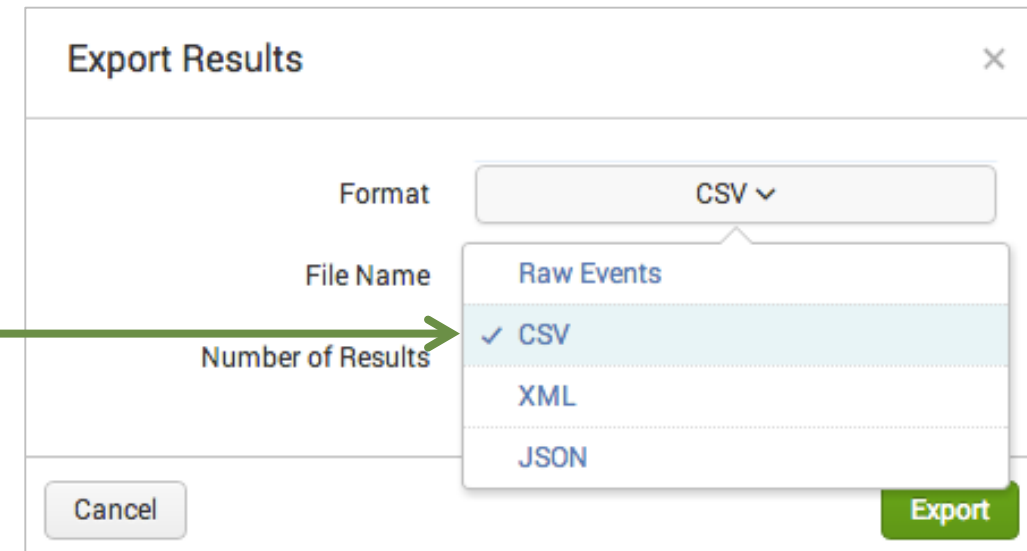
Export Search Results

For an external copy of the results, **export** search results to Raw Events (text file), CSV, XML, or JSON format



Note

Note that exporting the results of a large search is very memory-intensive!

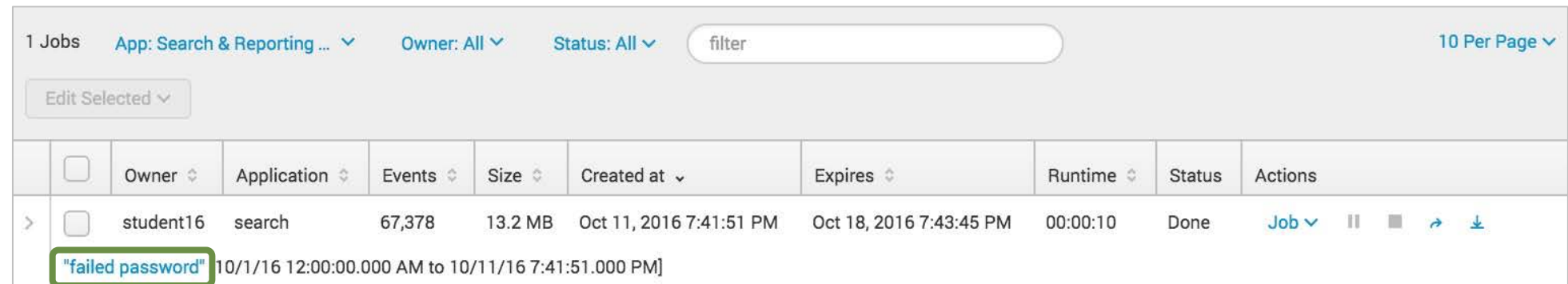
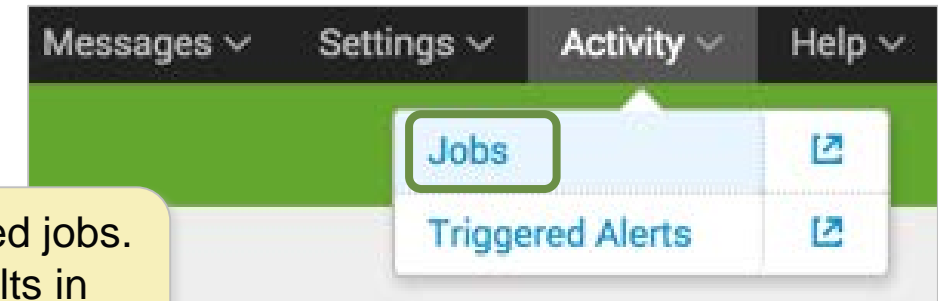


Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Review Your Job History

- Access saved search jobs from the **Activity** menu
- The Search Jobs view displays jobs that:
 - You have run in the last 10 minutes
 - You have extended for 7 days
- Click on a job link to view the results in the designated app view

Click **Activity > Jobs** to view your saved jobs. Click the job's name to examine results in Search view. (The job name is the search string.)



1 Jobs App: Search & Reporting ... Owner: All Status: All filter 10 Per Page

Edit Selected

	Owner	Application	Events	Size	Created at	Expires	Runtime	Status	Actions
>	student16	search	67,378	13.2 MB	Oct 11, 2016 7:41:51 PM	Oct 18, 2016 7:43:45 PM	00:00:10	Done	Job
		"failed password"	10/1/16 12:00:00.000 AM to 10/11/16 7:41:51.000 PM]						

Review Your Search History

1. Search History displays your most recent ad-hoc searches – 5 per page
2. You can set a time filter to further narrow your results
3. Click the > icon in the leftmost column to expand long queries to display the full text

The screenshot shows the Splunk Search & Reporting interface. At the top, there are navigation tabs: Search, Pivot, Reports, Alerts, and Dashboards. The main search bar contains the text "enter search here...". Below the search bar, there are options for "No Event Sampling" and "Smart Mode".

The "Search History" section is highlighted with a green box and a red circle labeled "1". It contains a link "> Expand your search history.". A dropdown menu is open, showing time filter options: "No Time Filter" (selected), "Today", "Last 7 Days", and "Last 30 Days". A red circle labeled "2" points to the "No Time Filter" option.

The search history table is shown below. A red circle labeled "3" points to the expand icon (>) in the first row. The table has columns for "Search", "Actions", and "Last Run".

Search	Actions	Last Run
(sourcetype=cisco_wsa_squid OR sourcetype=access_combined) status>399 timechart count by sourcetype eval cisco_wsa_squid=cisco_wsa_squid*3 where access_combined>cisco_wsa_squid	Add to Search	a few seconds ago
> (sourcetype=cisco_wsa_squid OR sourcetype=access_combined) status>399 timechart count by sourcetype eval...	Add to Search	Tue Apr 19 2016 15:50:07
> sourcetype=vendor_sales VendorID < 3000 chart count over VendorStateProvince geom geo_us_states featureID...	Add to Search	Tue Apr 19 2016 15:19:55
> sourcetype=vendor_sales VendorID < 3000 chart count over	Add to Search	Tue Apr 19 2016 15:19:43
> sourcetype=vendor_sales VendorID < 3000 chart count by VendorStateProvince geom geo_us_states featureIDFie...	Add to Search	Tue Apr 19 2016 15:19:23

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Module 6: Using Fields in Searches

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Module Objectives

- Understand fields
- Use fields in searches
- Use the fields sidebar
- Use search modes (fast, verbose, and smart)

What Are Fields?

- Fields are searchable key/value pairs in your event data
 - Examples: `host=www1 status=503`
- Fields can be searched with their names, like separating an http status code of 404 from Atlanta's area code (`area_code=404`)
- Between search terms, unless otherwise specified, AND is implied

The screenshot shows four search bars in a Splunk interface, each with a search button and a 'Yesterday' dropdown menu. The search queries are:

- `area_code=404`
- `action=purchase status=503`
- `source=/var/log/messages* NOT host=mail2`
- `sourcetype=access_combined`

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Field Discovery

- Splunk discovers all fields based on sourcetype and any key/value pairs found in the data
- Already stored with the event in the index (prior to search time) are:
 - Meta fields, such as **host**, **source**, and **sourcetype**
 - Meta fields, including internal fields like **_time**, **_raw**
 - Splunk may extract other fields from the raw event data that may not be directly related to your search
- **Field discovery** is directly related to each search's results
 - Some fields in the overall data may not appear within the results of a particular search

Note



While Splunk auto-extracts many fields, you can learn how to create your own in the *Splunk Fundamentals 2* course.

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Identify Data-Specific Fields

- Data-specific fields come from the specific characteristics of your data
 - Sometimes, this is indicated by obvious key = value pairs (**action = purchase**)
 - Sometimes, this comes from data within the event, defined by the sourcetype (**status = 200**)

i	Time	Event
>	12/3/15 7:12:32.000 PM	207.36.232.245 - - [03/Dec/2015:19:12:32] "POST /cart/success.do?JSESSIONID=SD1SL3FF8ADFF4966 HTTP 1.1" 200 1443 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-26" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.6) Gecko/20070725 Firefox/2.0.0.6" 963

Note



For more information, please see:

<http://docs.splunk.com/Documentation/Splunk/latest/Data/Listofpretrainedsourcetypes>

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Fields Sidebar

For the current search:

- **Selected Fields** – a set of configurable fields displayed for each event
- **Interesting Fields** – occur in at least 20% of resulting events
- **All Fields** link to view all fields (including non-interesting fields)

The screenshot shows a Splunk search interface for the query "failed password". It displays a timeline visualization and a list of events. The Fields Sidebar is visible on the left, showing Selected Fields (host, source, sourcetype) and Interesting Fields (app, date_hour, date_mday). Annotations explain the field value indicators: 'a' for alphanumeric, '#' for numeric, and the number next to the field name for the number of unique values.

Annotations:

- click to view all fields (points to the All Fields link)
- indicates the field's values are alphanumeric (points to 'a' next to host)
- indicates that the majority of the field values are numeric (points to '#' next to date_hour)
- indicates number of unique values for the field (points to '2' next to date_hour)

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Describe Selected Fields

- Selected fields and their values are listed under every event that includes those fields
- By default, the selected fields are:
 - host
 - source
 - sourcetype
- You can choose any field and make it a selected field

The screenshot shows a Splunk search interface. At the top, the search query is `action=purchase` with a time range of 6/27/16 12:00:00.000 AM to 6/28/16 12:00:00.000 AM. Below the search bar, there are tabs for Events (752), Patterns, Statistics, and Visualization. A timeline visualization shows a series of green bars representing events. Below the timeline, there are navigation options like 'List', 'Format', and '20 Per Page'. The main table displays search results with columns for 'i', 'Time', and 'Event'. A 'Selected Fields' box on the left lists `host` (3), `source` (3), and `sourcetype` (1). The event details show a log entry from `175.44.1.122` with a `POST` request to `/cart/error.do`. A box highlights the selected fields for this event: `host = www2`, `source = /opt/log/www2/access.log`, and `sourcetype = access_combined`.

Make an Interesting Field a Selected Field

- You can modify selected fields
 - 1 Click a field in the Fields sidebar
 - 2 Click **Yes** in the upper right of the field dialog
- Now that it is a selected field, it appears:
 - In the Selected Fields section of the Fields sidebar
 - Below each event where a value exists for that field

The screenshot shows the Splunk Fields sidebar on the left. The 'Interesting Fields' section has 'action' selected, indicated by a green box and a red circle with the number '1'. A dialog box is open for the 'action' field, showing '1 Value, 100% of events'. In the top right of the dialog, the 'Selected' radio button is selected, and the 'Yes' button is highlighted with a green box and a red circle with the number '2'. Below the dialog, there are reports for 'Top values', 'Events with this field', and 'Values'. The 'Values' report shows a single entry: 'purchase' with a count of 26,347 and 100%.

The screenshot shows the Splunk Events view. The 'Selected Fields' section in the sidebar has 'action' selected, indicated by a green box. The main view shows a list of events. The first event is selected, and its 'action' field value 'purchase' is highlighted with a green box. The event details show: 'action = purchase', 'host = www1', 'source = /opt/log/www1/access.log', and 'sourcetype = access_combined'.

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Make Any Field Selected

You can identify other fields as selected fields from All Fields (which shows all of the discovered fields)

The screenshot shows the 'Select Fields' dialog in Splunk. The dialog has a header with 'Select All Within Filter', 'Deselect All', 'Coverage: 1% or more', a search filter, and 'Extract New Fields'. Below is a table of fields:

<input checked="" type="checkbox"/>	Field	# of Values	Event Coverage	Type
<input checked="" type="checkbox"/>	action	1	100%	String
<input checked="" type="checkbox"/>	host	3	100%	String
<input checked="" type="checkbox"/>	source	3	100%	String
<input checked="" type="checkbox"/>	sourcetype	1	100%	String
<input type="checkbox"/>	JSESSIONID	>100	100%	String
<input type="checkbox"/>	bytes	>100	100%	Number
<input type="checkbox"/>	categoryid	8	51.99%	String

On the left, the 'All Fields' button is highlighted with a green box. Below it, the 'Selected Fields' list shows: action 1, host 3, source 3, and sourcetype 1. A sample event is shown at the bottom: action = purchase | host = v | sourcetype = access_combined

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

The Field Window

Select a field from the Fields sidebar, then:

Narrow the search to show only results that contain this field

action = * is added to the search criteria

Get statistical results

Click a value to add the field/value pair to your search – in this case, **action = addtocart** is added to the search criteria

Top 10 Values	Count	%
failure	40,815	53.846%
purchase	6,609	8.719%
addtocart	6,474	8.541%
view	6,305	8.318%
TCP_REFRESH_HIT	5,720	7.546%
success	4,605	6.075%
TCP_MISS	1,871	2.468%
TCP_DENIED	208	0.274%

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

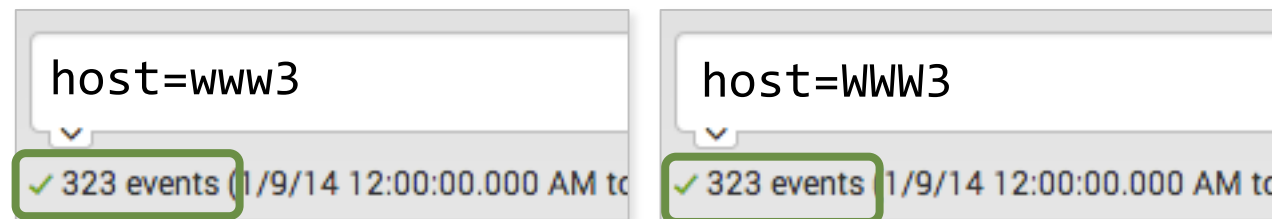
Using Fields in Searches

- Efficient way to pinpoint searches and refine results

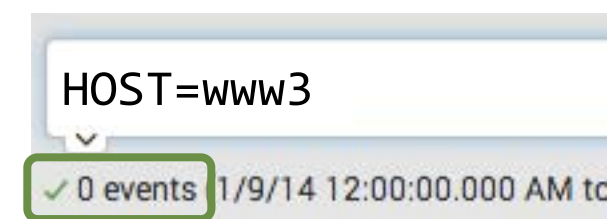


- Field names ARE case sensitive; field values are NOT

– Example:



These two searches return results



This one does not return results

Using Fields in Searches (cont.)

- For IP fields, Splunk is subnet/CIDR aware

```
clientip="141.146.8.0/24"
```

```
clientip="141.146.8.*"
```

- Use wildcards to match a range of field values
 - Example: **user=*** (to display all events that contain a value for user)

```
user=* sourcetype=access* (referer_domain=*.cn OR referer_domain=*.hk)
```

All time ▾



- Use relational operators

With numeric fields

```
src_port>1000 src_port<4000
```

With alphanumeric fields

```
host!=www3
```

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Example: != vs. NOT

- Note that the search on the left, which uses !=, returns 98 events from one sourcetype
- The search on the right, using NOT, returns 31,036 events from *ten* sourcetypes

New Search

sc_http_status!=200

✓ 98 events (4/20/16 12:00:00.000 AM to 4/21/16 12:00:00.000 AM)

Events (98) | Patterns | Statistics | Visualization

Format Timeline ▾ | - Zoom Out | + Zoom to Selection | × Deselect

List ▾ | Format ▾

< Hide Fields | All Fields

Selected Fields

- a host 1
- a source 1
- a sourcetype 1

i	Time	Event
>	4/20/16 11:36:37.627 PM	1 r c - h
>	4/20/16	1

New Search

NOT sc_http_status=200

✓ 31,036 events (4/20/16 12:00:00.000 AM to 4/21/16 12:00:00.000 AM)

Events (31,036) | Patterns | Statistics | Visualization

Format Timeline ▾ | - Zoom Out | + Zoom to Selection | × Deselect

List ▾ | Format ▾

< Hide Fields | All Fields

Selected Fields

- a host 10
- a source 15
- a sourcetype 10

i	Time	Event
>	4/20/16 11:59:59.000 PM	99.6 FF49 "Moz ome/ host
>	4/20/16	Apr

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Searching Against the Default Index

- In the Fields sidebar, note the **index** field
- An *index* is a location where Splunk stores – and searches for – event data
- The Splunk administrator configures the index locations that you can search, by default
- In the search shown here, data is returned from two indexes: web and sales

product_name="Dream Crusher"

✓ 201 events (7/26/16 12:00:00.000 AM to 7/27/16 12:00:00.000 AM) No Event Sampling Job

Events (201) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

< Hide Fields All Fields

Selected Fields

- a host 4
- a index 2
- a source 4
- a sourcetype 2

Interesting Fields

- a action 5
- # bytes 100+
- a categoryid 1

index

2 Values, 100% of events Selected Yes No

Reports

- Top values
- Events with this field
- Top values by time
- Rare values

Values	Count	%
web	187	93.035%
sales	14	6.965%

11:35:22.000 PM host = vendorUS1 index = sales source = /opt/log/vendorUS1/vendor_sales.log

Search Modes: Fast, Smart, Verbose

Search Mode →	Fast	Smart	Verbose
Emphasizes →	Speed	Balance of speed and completeness	Completeness (but slower)
When run with an event search, <ul style="list-style-type: none"> • Access to Events view? • Field discovery on? • Fields sidebar exists? • Statistics, Visualization tabs empty? 	<ul style="list-style-type: none"> • Yes • No • Yes • Yes 	<ul style="list-style-type: none"> • Yes • Yes • Yes • Yes 	<ul style="list-style-type: none"> • Yes • Yes • Yes • Yes
When run with a reporting/statistical search, <ul style="list-style-type: none"> • Access to Events view? • Field discovery on? • Fields sidebar exists? 	No	No	Yes
Default Search Mode?	No	Yes	No

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Module 7: Best Practices for Searching

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

General Search Practices

- Time is the most efficient filter
- For best performance, specify index values at the beginning of the search string
- Be specific
 - Searching for "access denied" is always better than searching for "denied"
 - To make searches more efficient, include as many terms as possible
 - If you want to find events with "error" and "sshd" and 90% of the events include "error", but only 5% "sshd", include both values in the search
- Inclusion is generally better than exclusion
 - Searching for "access denied" is faster than NOT "access granted"

Note



Note that search terms are *case-insensitive* and search fields are *case-sensitive*.

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

General Search Practices (cont.)

- Filter as early as possible
 - For example, remove duplicate events, then sort
- For fastest performance, try to avoid using wildcards at the beginning of a string
- Inconsistent performance can result from using wildcards in the middle of a string, especially if the string contains punctuation or quotes

Time Range Abbreviations

- Time ranges specified in the **Advanced** tab of the time range picker

- Time unit abbreviations include:

s = seconds m = minutes h = hours d = days w = week mon = months y = year

- @ symbol "snaps" to the time unit you specify
 - Snapping rounds *down* to the nearest specified unit
 - Example: Current time when the search starts is 09:37:12
-30m@h looks back to 09:00:00

Time Range: earliest and latest

- You can also specify a time range in the search bar
- To specify a beginning and an ending for a time range, use **earliest** and **latest**
- Examples:

earliest=-h

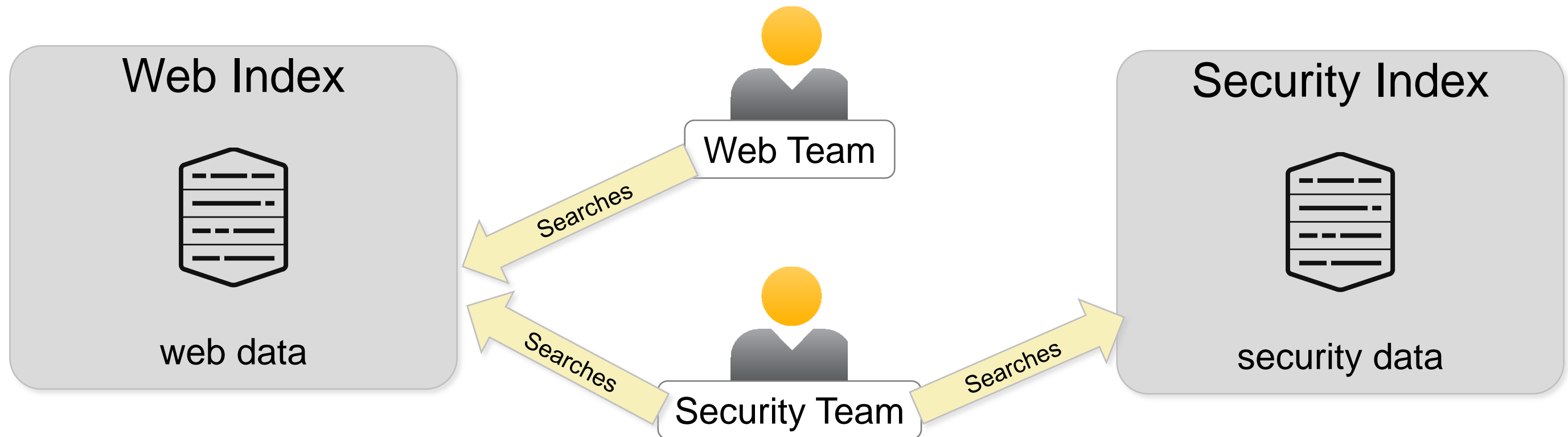
looks back one hour

earliest=-2d@d latest=@d

looks back from two days ago,
up to the beginning of today

Indexes

- An *index* is a location where Splunk stores and searches for event data

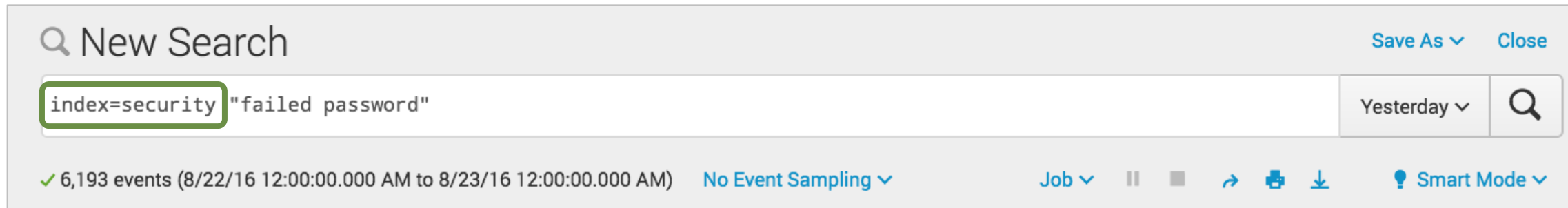


- Administrators segregate data into separate indexes to limit access by Splunk role

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

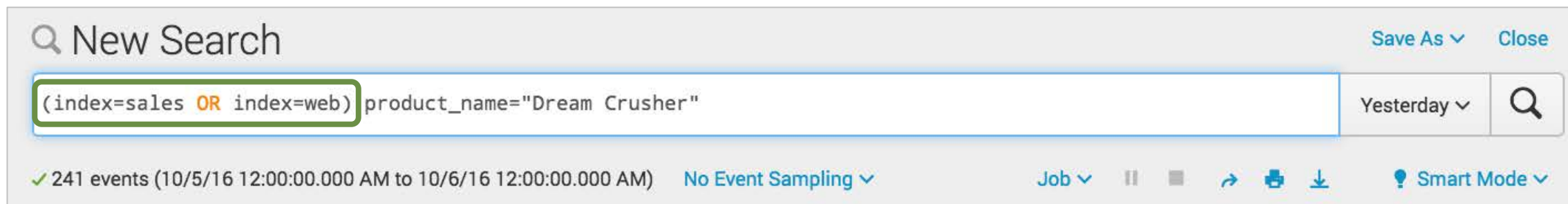
Working with Indexes

- This search returns event data from the security index



The screenshot shows the Splunk search interface. The search bar contains the query `index=security "failed password"`. The search results show 6,193 events from 8/22/16 12:00:00.000 AM to 8/23/16 12:00:00.000 AM. The interface includes a search bar, a search button, and a status bar with various controls like 'Save As', 'Close', 'Yesterday', 'Job', 'No Event Sampling', and 'Smart Mode'.

- It is possible to specify multiple index values



The screenshot shows the Splunk search interface. The search bar contains the query `(index=sales OR index=web) product_name="Dream Crusher"`. The search results show 241 events from 10/5/16 12:00:00.000 AM to 10/6/16 12:00:00.000 AM. The interface includes a search bar, a search button, and a status bar with various controls like 'Save As', 'Close', 'Yesterday', 'Job', 'No Event Sampling', and 'Smart Mode'.

Working with Indexes (cont.)

It is possible to use wildcards – *, %, _, etc. – in index values



The screenshot shows the Splunk search interface. At the top, there is a search bar with the text "index=* \"failed password\"". To the right of the search bar are buttons for "Save As" and "Close". Below the search bar, there is a dropdown menu for "Yesterday" and a search icon. Below the search bar, there is a status bar showing "15,972 events (8/8/16 12:00:00.000 AM to 8/9/16 12:00:00.000 AM)" and "No Event Sampling". To the right of the status bar are buttons for "Job", "Pause", "Stop", "Refresh", "Print", "Download", and "Smart Mode".

Note 1

Although `index=*` is a valid search, better performance is always obtained by specifying one or more specific index values.

Note 2

For best performance, specify the index values at the beginning of the search string.

Module 8: Splunk's Search Language

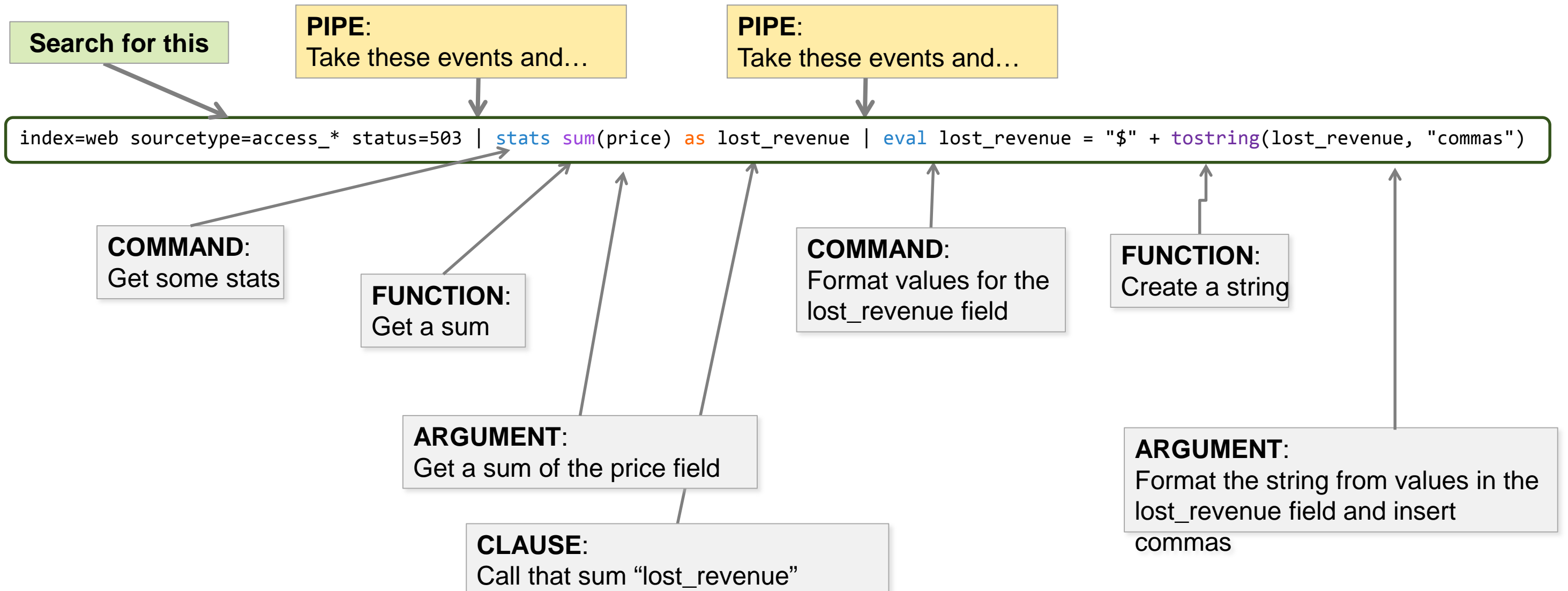
Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Module Objectives

- Understand the search pipeline
- Understand search syntax concepts
- Use the table, fields and sort commands

Search Pipeline Example

This diagram represents a search, broken into its syntax components:



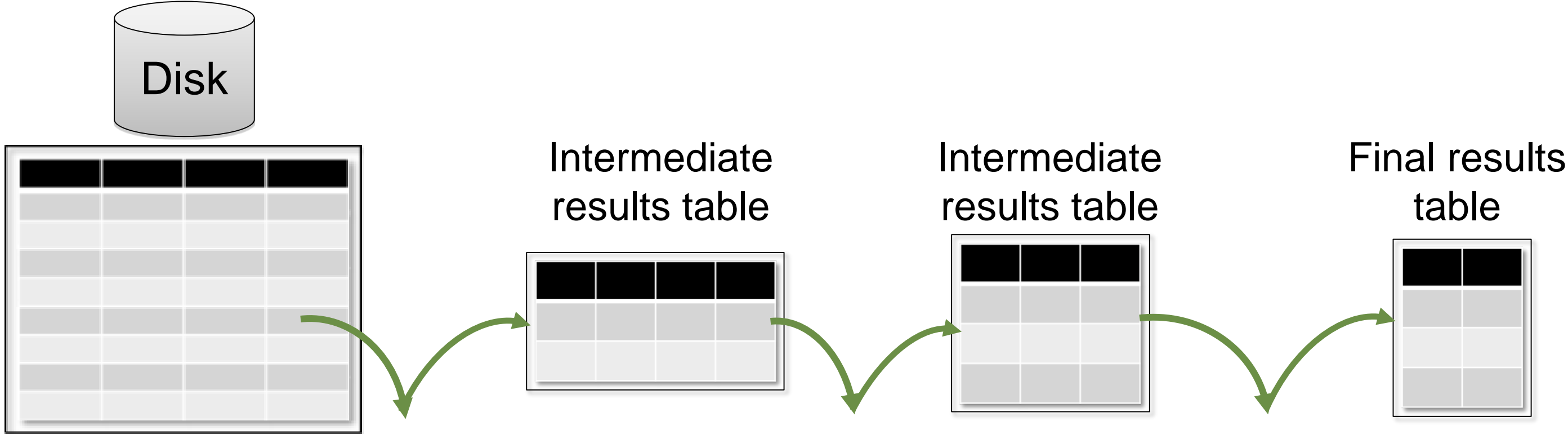
Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Search Language Syntax Concepts

Searches are made up of 5 basic components

- **Search terms** – what are you looking for?
 - Keywords, phrases, Booleans, etc.
- **Commands** – what do you want to do with the results?
 - Create a chart, compute statistics, evaluate and format, etc.
- **Functions** – how do you want to chart, compute, or evaluate the results?
 - Get a sum, get an average, transform the values, etc.
- **Arguments** – are there variables you want to apply to this function?
 - Calculate average value for a specific field, convert milliseconds to seconds, etc.
- **Clauses** – how do you want to group or rename the fields in the results?
 - Give a field another name or group values by or over

The Search Pipeline



```
index=security sourcetype=linux_secure fail | top user | fields - percent
```

Fetch events from disk that match

Summarize into table of top 10 users

Remove column showing percentage

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Making the Pipeline More Readable

- Clicking **Ctrl** - \ (Windows) or **⌘** - \ (MacOS) in the search box puts each pipe in the pipeline on a separate line
- For example, this:

```
Q New Search
index=web sourcetype=access_* status=503 | stats sum(price) as lost_revenue | eval lost_revenue = "$" + tostring(lost_revenue, "commas")
```

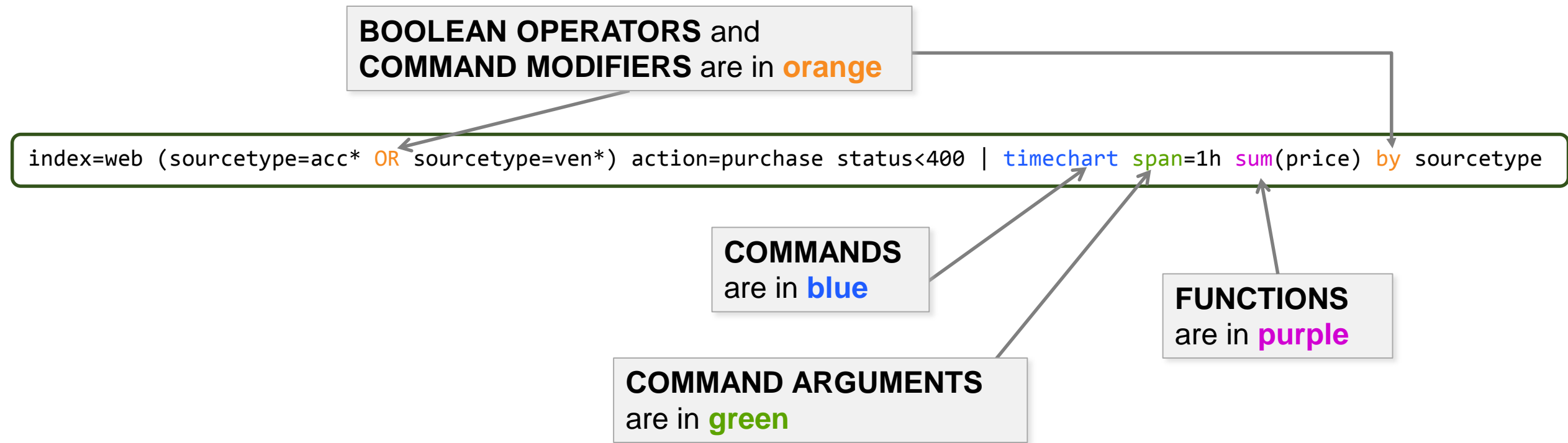
- Is transformed to this:

```
Q New Search
index=web sourcetype=access_* status=503
| stats sum(price) as lost_revenue
| eval lost_revenue = "$" + tostring(lost_revenue, "commas")
```

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Syntax Coloring

- As you type, some parts of the search string are automatically colored
- The color is based on the search syntax
 - The rest of the search string remains black



Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Search Assistant

- The Search Assistant provides an autocomplete feature
- It provides convenient reminders about commands available at any given point in the search string
 - If desired, click a reminder to have its contents inserted into the search

The screenshot illustrates the Search Assistant interface. On the left, a search bar contains the text 'index=security failed | chart co'. Below the search bar, a dropdown menu is open, displaying a list of suggestions for the 'chart' command. The suggestions include 'count', 'chart count by host', 'chart count by src_ip', 'chart count by user', 'chart count(_raw) by action', and 'chart count(_raw) by saved_search'. The 'chart count by user' option is highlighted with a yellow arrow. Below the suggestions, there is a section titled 'How to Search' with a brief explanation of the 'chart' command and an example: '... | chart max(delay) over foo'. A yellow arrow points from the highlighted suggestion to the right, where a second search bar shows the updated search string: 'index=security failed | chart count by user'. The interface also includes a 'No Event Sampling' dropdown and a 'Data Summary' button.

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Search Assistant and Parentheses

- The Search Assistant provides help to match parentheses as you type
- When an end parenthesis is typed, the corresponding beginning parenthesis is automatically highlighted
 - If a beginning parenthesis cannot be found, *nothing* is highlighted



(index=

Beginning parenthesis found!



Beginning parenthesis NOT found!

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Creating a Table

- `table` command returns a table formed by only fields in the argument list
- Columns are displayed in the order given in the command
 - Column headers are field names
 - Each row is an event
 - Rows are field values

Scenario

Display the `clientip`, `action`, `productId`, and `status` of customer interactions in the online store for the last 4 hours.

```
index=web sourcetype=access_combined  
| table clientip, action, productId, status
```

clientip	action	productId	status
223.205.219.67			200
69.80.0.18	view	WC-SH-A02	200
69.80.0.18		SF-BVS-01	408
91.205.189.15	view	FS-SG-G03	200
91.205.189.15	view	CU-PG-G06	200
91.205.189.15	view	WC-SH-A02	200
91.205.189.15	remove	WC-SH-A01	200
91.205.189.15			200

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Renaming Fields

- To change the name of a field, use the `rename` command
- Useful for giving fields more meaningful names
- When including spaces or special characters in field names, use double straight quotes:

- A** `rename productId as ProductID`
- B** `rename action as "Customer Action"`
- C** `rename status as "HTTP Status"`

Scenario

Display the `clientip`, `action`, `productId`, and `status` of customer interactions in the online store for the last 4 hours.

```
index=web sourcetype=access_combined
| table clientip, action, productId, status
| rename productId as ProductID, A
| action as "Customer Action", B
| status as "HTTP Status" C
```

clientip	Customer Action	ProductID	HTTP Status
141.146.8.66		MB-AG-T01	200
141.146.8.66		WC-SH-A01	200
195.80.144.22		DC-SG-G02	200
141.146.8.66		WC-SH-A02	200
195.80.144.22		SC-MG-G10	200
141.146.8.66		PZ-SG-G05	200
195.80.144.22	purchase		200
195.80.144.22	purchase	SC-MG-G10	200

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

fields Command

- Field extraction is one of the most costly parts of a search
- `fields` command allows you to include or exclude specified fields in your search or report
- To include, use `fields +(default)`
 - Occurs before field extraction
 - Improves performance
- To exclude, use `fields -`
 - Occurs after field extraction
 - No performance benefit
 - Exclude fields used in search to make the table/display easier to read

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

fields Command – Examples

Improves performance – only the fields you specify are extracted

Returned **6,567** results by scanning **6,567** events in **1.425** seconds:

Scenario ?

Display network failures during the previous week.

< Hide Fields	☰ All Fields	i	Time	Event
Selected Fields		>	1/23/16 11:59:40.000 PM	Jan 18 11:28:43 bcg-payroll sshd[21263]: Failed password for root from 175.4 5.176.223 port 33307 ssh2 host = www1 source = /opt/log/www1/auth.nix sourcetype = linux_secure
a host 3		>	1/23/16 11:59:39.000 PM	Jan 17 23:59:39 bcg-fileserver sshd[9954]: Failed password for invalid user brook from 41.32.0.85 port 47187 ssh2 host = www3 source = /opt/log/www3/auth.nix sourcetype = linux_secure
a source 3		>	1/23/16 11:59:37.000 PM	Jan 17 23:59:37 HOST0170 sshd[25089]: [ID 800047 auth.info] Failed publickey for naughtyuser from 23.16.0.232 port 50244 ssh2 host = www3 source = /opt/log/www3/auth.nix sourcetype = linux_secure
a sourcetype 1				
Interesting Fields				
a action 1				
a app 2				

Scenario ?

Display network failures during the previous week. Retrieve only user, app, and src_ip.

Returned **6,567** results by scanning **6,567** events in **0.753** seconds:

```
index=security
sourcetype=linux_secure
(fail* OR invalid)
| fields user, app, src_ip
```

A

< Hide Fields	☰ All Fields	i	Time	Event
Interesting Fields		>	1/23/16 11:59:40.000 PM	Jan 18 11:28:43 bcg-payroll sshd[21263]: Failed password for root from 175.4 5.176.223 port 33307 ssh2
a app 2		>	1/23/16 11:59:39.000 PM	Jan 17 23:59:39 bcg-fileserver sshd[9954]: Failed password for invalid user brook from 41.32.0.85 port 47187 ssh2
a src_ip 23		>	1/23/16 11:59:37.000 PM	Jan 17 23:59:37 HOST0170 sshd[25089]: [ID 800047 auth.info] Failed publickey for naughtyuser from 23.16.0.232 port 50244 ssh2
a user 100+		>	1/23/16 11:59:10.000 PM	Jan 18 23:59:10 bcg-payroll sshd[8372]: Failed password for root from 3.0.0.44 port 37138 ssh2
☕ Extract New Fields				

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

dedup Command

Use dedup to remove duplicates from your results

```
index=sales sourcetype=vendor_sales | table VendorCountry, VendorStateProvince, VendorCity, Vendor
```

VendorCountry	VendorStateProvince	VendorCity	Vendor
United States	Texas	Waco	Wow Games
United States	Utah	Cedar City	Woody's Games
United States	Virginia	Staunton	Woody's Games
United States	Utah	Cedar City	Woody's Games
United States	Utah	Cedar City	Woody's Games
Australia	Western Australia	Perth	Wonderland Hobbies
Australia	Western Australia	Perth	Wonderland Hobbies

```
...| dedup Vendor | table ...
```

VendorCountry	VendorStateProvince	VendorCity	Vendor
United States	Texas	Waco	Wow Games
United States	Utah	Cedar City	Woody's Games
Australia	Western Australia	Perth	Wonderland Hobbies

```
...| dedup VendorCity, Vendor | table ...
```

VendorCountry	VendorStateProvince	VendorCity	Vendor
United States	Texas	Waco	Wow Games
United States	Utah	Cedar City	Woody's Games
United States	Virginia	Staunton	Woody's Games
Australia	Western Australia	Perth	Wonderland Hobbies

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

sort Command

- Use `sort` to order your results in `+` ascending (default) or `-` descending
- To limit the returned results, use the `limit` option

```
... | sort limit=20 -categoryId, product_name
```

```
... | sort 20 count
```

sort

Sorts search results by the specified fields.

Example:

```
... | sort ip, -url
```

[Learn More](#)

sort Command (cont.)

`sort -/+<fieldname>` sign followed by fieldname sorts results in the sign's order

`sort -/+ <fieldname>` sign followed by space and then fieldname applies sort order to all following fields without a different explicit sort order

```
index=sales sourcetype=vendor_sales
| dedup Vendor
| sort - VendorCountry, +VendorStateProvince, VendorCity, Vendor
| table VendorCountry, VendorStateProvince, VendorCity, Vendor
```

VendorCountry	VendorStateProvince	VendorCity	Vendor
United States	Arizona	Yuma	Yumster Games
United States	Arizona	Tucson	Boothill Games
United States	Arizona	Phoenix	Rising Games
United States	Arizona	Phoenix	Phoenix Games
United States	Arizona	Flagstaff	Flaggin Games

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Module 9: Transforming Commands

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Module Objectives

Identify and use the following commands and their functions:

- top
- rare
- Stats
- dedup

Getting Top Values

- The top command finds the most common values of a given field in the result set
 - By default, returns top 10 results

src_ip	count	percent
10.3.10.46	53	19.629630
10.2.10.163	50	18.518519
10.1.10.172	43	15.925926
87.194.216.51	23	8.518519
217.132.169.69	19	7.037037
188.143.232.202	11	4.074074
69.80.0.18	10	3.703704
216.221.226.11	9	3.333333
142.233.200.21	8	2.962963
84.34.159.23	7	2.592593

Scenario

During the last 60 minutes, which IP addresses generated the most attacks?

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

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

top Command

- By default, output displays in table format
- Automatically returns **count** and **percent** columns
- Common constraints:
`limit` `countfield` `showperc`

Note



Refer to docs.splunk.com for the other available options.

top

Displays the most common values of a field.

Example:

```
... | top limit=20 url
```

[Learn More](#)

top Command – Single Field Example

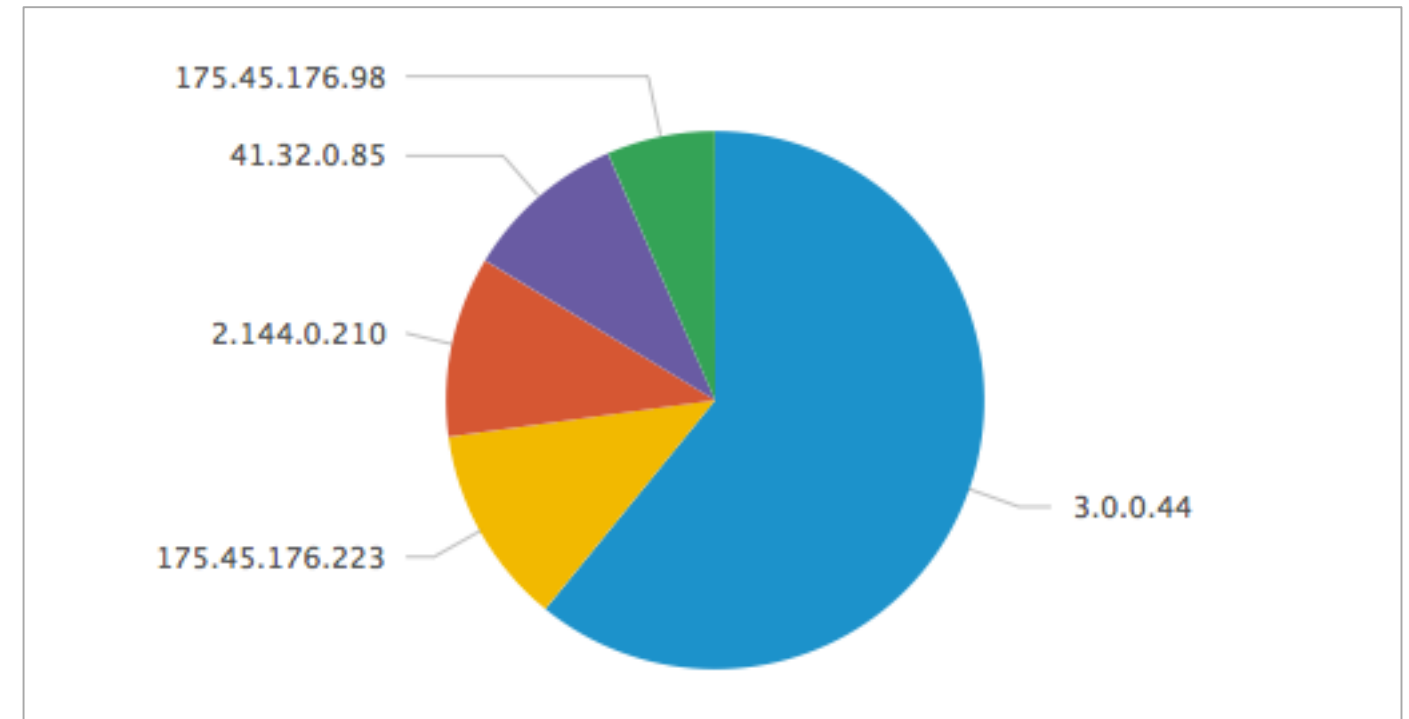
- `limit=#` returns this number of results
- By default, 10 results are displayed
- `limit=0` returns unlimited results

```
sourcetype=linux_secure index=security  
(fail* OR invalid)  
| top limit=5 src_ip
```

Scenario ?

During the last hour, display the top 5 IPs that generated the most attacks.

src_ip	count	percent
10.2.10.163	73	27.037037
10.1.10.172	42	15.555556
10.3.10.46	41	15.185185
87.194.216.51	19	7.037037
12.130.60.4	17	6.296296



Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

top – Multiple Field Example

- If the showperc is not included – or it is included and set to t – a **percent** column is displayed
- If showperc=f, then a percent column is NOT displayed

Scenario



Display the top 3 common values for users and web categories browsed during the last 24 hours.

```
index=network sourcetype=cisco_wsa_squid  
| top user A x_webcat_code_full limit=3 B
```

user	x_webcat_code_full	count	percent
apucci@buttercupgames.com	Games	79	6.152648
arangel@buttercupgames.com A	Society and Culture	61	4.750779
rerde@buttercupgames.com	Arts and Entertainment B	54	4.205607

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

top – Single Field with by Clause Example

Scenario

Display the top 3 common web categories browsed by each user during the last 24 hours.

```
index=network sourcetype=cisco_wsa_squid  
| top x_webcat_code_full B by user A limit=3
```

user	x_webcat_code_full	count	percent
acurry@buttercupgames.com A	Uncategorized URLs	10	71.428571
acurry@buttercupgames.com	Sports and Recreation B	1	7.142857
acurry@buttercupgames.com	Society and Culture	1	7.142857
adombrowski@buttercupgames.com	Computers and Internet	2	33.333333
adombrowski@buttercupgames.com	Spiritual Healing	1	16.666667
adombrowski@buttercupgames.com	Shopping	1	16.666667

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

top – Specifying Options

- By default, the value of the `countfield` is `count`
- `countfield=string` provides the name of a new field to write the count value

Scenario

Display the top 3 user/web categories browsed combinations during the last 24 hours. Rename the count field and show count, but not the percentage.

```
index=network sourcetype=cisco_wsa_squid  
| top user x_webcat_code_full limit=3  
countfield="Total Viewed" showperc=f
```

user	x_webcat_code_full	Total Viewed
apucci@buttercupgames.com	Games	79
arangel@buttercupgames.com	Society and Culture	61
rerde@buttercupgames.com	Arts and Entertainment	54

Note

A Boolean can be t/f, true/false, as well as 1/0.

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

rare Command

- The rare command returns the least common field values of a given field in the results
- Options are identical to the top command

Scenario

Which product is the least sold by Buttercup Games vendors over the last 60 minutes?

```
index=sales sourcetype=vendor_sales  
| rare product_name showperc=f limit=1
```

Events	Patterns	Statistics (1)	Visualization
20 Per Page	Format	Preview	
product_name			count
Fire Resistance Suit of Provolone			1

stats Command

- stats enables you to calculate statistics on data that matches your search criteria
- Common functions include:
 - count – returns the number of events that match the search criteria
 - distinct_count, dc – returns a count of unique values for a given field
 - sum – returns a sum of numeric values
 - avg – returns an average of numeric values
 - list – lists all values of a given field
 - values – lists unique values of a given field

Note



To view all of the functions for stats, please see:

<http://docs.splunk.com/Documentation/Splunk/Latest/SearchReference/CommonStatsFunctions>

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

stats Command – count

- count returns the number of matching events based on the current search criteria
- Use the as clause to rename the count field

Scenario

Count the invalid or failed login attempts during the last 60 minutes.

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

Events	Patterns	Statistics (1)	Visualization
10 Per Page ▾	Format ▾	Preview ▾	
count ↕			
63			

```
index=security sourcetype=linux_secure  
(invalid OR failed)  
| stats count as "Potential Issues"
```

Events	Patterns	Statistics (1)	Visualization
10 Per Page ▾	Format ▾	Preview ▾	
Potential Issues ↕			
63			


Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution











stats Command – count(*field*)

Adding a *field* as an argument to the count function returns the number of events where a value is present for the specified field

Scenario

Count the number of events during the last 15 minutes that contain a vendor action field. Also count the total events.

```
index=security sourcetype=linux_secure  
| stats count(vendor_action) as ActionEvents,  
count as TotalEvents 
```

Events (69)	Patterns	Statistics (1)	Visualization
20 Per Page 	 Format 	Preview 	
 ActionEvents  		 TotalEvents  	
61		69	

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

stats Command – by *fields*

Scenario

Count the number of events by user, app, and vendor action during the last 15 minutes.

- `by` clause returns a count for each value of a named field or set of fields
- Can use any number of fields in the `by field` list

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

user	app	vendor_action	count
abc	sshd	Failed	1
admin	sshd	Failed	4
administrator	sshd	Failed	1
alex	sshd	Failed	1
apache	sshd	Failed	1
backup	sshd	Failed	1
ben	sshd	Failed	1
bin	sshd	Failed	2
britany	sshd	Failed	1
daemon	sshd	Failed	1

stats Command – `distinct_count(field)`

- `distinct_count()` or `dc()` provides a count of how many unique values there are for a given field in the result set
- This example counts how many unique values for `s_hostname`

Scenario

How many unique websites have our employees visited in the last 4 hours?

```
index=network sourcetype=cisco_wsa_squid  
| stats dc(s_hostname) as "Websites visited:"
```

Events	Patterns	Statistics (1)	Visualization
20 Per Page ▾ Format ▾ Preview ▾			
Websites visited: ⌵			
25			

stats Command – *sum(field)*

Scenario

How much bandwidth did employees spend at each website during the past week?

For fields with a numeric value, you can sum the actual values of that field

```
index=network sourcetype=cisco_wsa_squid
```

```
| stats sum(sc_bytes) as Bandwidth by s_hostname  
| sort -Bandwidth
```

Events	Patterns	Statistics (54)	Visualization
20 Per Page <input type="checkbox"/> Format <input type="checkbox"/> Preview <input type="checkbox"/>			
s_hostname		A	Bandwidth
www.gctsindia.in			4866091
www.heals.co.uk			1233522
www.animationmagazine.net			1203433
www.kare11.com			1202753
www.finedinings.com			747407

stats Command – *sum(field)* – (cont.)

Scenario



Report the number of retail units sold and sales revenue for each product during the previous week.

```
index=sales sourcetype=vendor_sales
| stats A count(price) as "Units Sold"
| B sum(price) as "Total Sales" by product_name C
| sort -"Total Sales" D
```


- A** A single stats command
- B** can have multiple functions
- C** The by clause is applied to both functions
- D** sort Total Sales in descending order

product_name	Units Sold	Total Sales
Dream Crusher	A 73	B 2919.27
Manganiello Bros.	53	2119.47
World of Cheese	66	1649.34
C SIM Cubicle	81	1619.19
Orvil the Wolverine	35	1399.65
Final Sequel	49	1224.51
Mediocre Kingdoms	42	1049.58
Curling 2014	48	959.52
Benign Space Debris	25	624.75
Manganiello Bros. Tee	62	619.38

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution



stats Command – avg(*field*)

- The avg function provides the average numeric value for the given numeric field
- An event is not considered in the calculation if it:
 - Does not have the field
 - Has an invalid value for the field

Scenario 

What is the average bandwidth used for each website usage type?

```
index=network sourcetype=cisco_wsa_squid  
| stats avg(sc_bytes) as "Average Bytes" A  
by usage B
```

usage 	Average Bytes 
Borderline	13553.723173
Business	11277.155763
B Personal	A 14874.552763
Unknown	10724.935021
Violation	8982.340426

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

stats Command – list(*field*)

- list function lists all field values for a given field
- This example lists the websites visited by each employee
 - Security logs generate an event for each network request
 - This causes the same hostname to appear multiple times
 - To return a list of “unique” field values, use the values function

Scenario

Which websites has each employee accessed during the last 60 minutes?

```
index=network sourcetype=cisco_wsa_squid  
| stats list(s_hostname) as "Websites visited:"  
by cs_username
```

cs_username	Websites visited:
basselin@buttercupgames.com	-
blu@buttercupgames.com	www.lowermybills.com
cquinn@buttercupgames.com	static.pochta.ru
dhale@buttercupgames.com	-
dpiazza@buttercupgames.com	www.ayles.com www.ayles.com www.ayles.com www.ayles.com www.ayles.com www.ayles.com

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

stats Command – values(*field*)

Scenario



Display by IP address the names of users who have failed access attempts in the last 60 minutes.

```
index=security sourcetype=linux_secure fail*  
| stats values(user) as "User Names",  
count(user) as Attempts by src_ip
```

values function lists unique values for the specified field

src_ip	User Names	Attempts
1.0.32.67	root	2
10.232.44.142	twilliam	1
10.232.44.71	jsimon1	1
175.45.176.223	gbottazzi oracle root scanner user	37
175.45.176.98	abc andrew cvs enquiries logs michael test test3	8

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Module 10: Creating Reports and Dashboards

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Module Objectives

- Save a search as a report
- Edit a report
- Create reports that display statistics (tables) or visualizations (charts)
- Create a dashboard
- Add a report to a dashboard
- Add a pivot to a dashboard
- Edit a dashboard

Reports

- Reports are saved searches
- Reports can show events, statistics (tables), or visualizations (charts)
- Running a report returns fresh results each time you run it
- Statistics and visualizations allow you to drill down by default to see the underlying events
- Reports can be shared and added to dashboards
- There are two ways to create a report: pivot or search

Smart Naming

- Before you begin using Splunk on the job, define a naming convention so you can always find your reports and tell them apart
- For example, you can create something simple like this:
 - <group>_<object>_<description>
 - **group**: the name of the group or department using the knowledge object such as sales, IT, finance, etc.
 - **object**: report, dashboard, macro, etc.
 - **description**: WeeklySales, FailedLogins, etc.
 - Using this example, a quarterly sales report can be identified as:
 - Sales_Report_QuarterlySalesRevenue

Note



If you set up naming conventions early in your implementation, you can avoid some of the more challenging object naming issues. The example is a suggestion. The details are found in the Splunk product documentation:

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

Create a Report from Search

- 1 Run a search
- 2 Select **Save As**
- 3 Select **Report**

The screenshot shows the Splunk Search interface. At the top, the search bar contains the query: `sourcetype=access_combined action=purchase status!=200`. Below the search bar, it indicates 1,133 events. A 'Save As' dropdown menu is open, showing options: Report, Dashboard Panel, Alert, and Event Type. The 'Report' option is highlighted. Below the search bar, there are tabs for Events (1,133), Patterns, Statistics, and Visualization. A timeline visualization is shown with green bars. Below the timeline, there are navigation options like 'List', 'Format', and '20 Per Page'. At the bottom, a table of search results is displayed.

Hide Fields	All Fields	<i>i</i>	Time	Event
		>	2/10/16 9:19:56.000 PM	176.212.0.44 - - [10/Feb/2016:21:19:56] "POST /cart.do?action=purchase&itemId=EST-6&JSESSIONID=SD3SL4FF1ADFF4963 HTTP 1.1" 503 978 "http://www.buttercup games.com/cart.do?action=addtocart&itemId=EST-6&categoryId=STRATEGY&productId=PZ-SG-G05" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 677 action = purchase host = www1 source = /opt/log/www1/access.log sourcetype = access_combined status = 503

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Create a Report from Search (cont.)

- A** Give the report a meaningful title (required)
- B** Specify a description (optional)
- C** Select whether to include or not to include a time range picker
 - The report will be saved with the time range that was selected when it was created
 - Adding a time range picker allows you to adjust the time range of the report when you run it

Save As Report

A Title support_report_failpurchases30day

B Description optional

Content Events

C Time Range Picker Yes No

Cancel Save

Create a Report from Search (cont.)

You can change Additional Settings, as well as use the dialog buttons:

- Click **Continue Editing** to make changes to your report
- Click **Add to Dashboard** to add your report to a dashboard
- Click **View** to display your report or run it again

Save As Report

Title: support_report_failpurchases30day

Description: optional

Content: Events

Time Range Picker: Yes No

Cancel Save

Your Report Has Been Created

You may now view your report, add it to a dashboard, change additional settings, or continue editing it.

Additional Settings:

- Permissions
- Schedule
- Acceleration
- Embed

Continue Editing Add to Dashboard View

Additional Settings

Dialog buttons

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Running Reports

- Click **Reports**, then click the report title to run it
 - The report runs using the time range that was specified when it was saved
- Use the time range picker to change the time range of the report (if available)

Search Pivot Reports Alerts Dashboards

Reports

Reports are based on single searches and can include visualizations. Open the report in Pivot or Search to refine the parameters or filters.

6 Reports

All Yours This

i	Title ^
>	Errors in the last 24 hours
>	Errors in the last hour
>	License Usage Data Cube
>	Orphaned scheduled searches
>	support_report_failpurchases30day

support_report_failpurchases30day

Last 30 days

2,866 events (5/22/16 12:00:00.000 AM to 6/21/16 2:42:37.000 AM)

20 per page

i	Time	Event
>	6/21/16 1:27:56.000 AM	217.23.14.61 - - [21/Jun/2016:01:27:56] "POST /cart.do?action=purchase&itemId=EST-26&JSESSIONID=SD8SL2FF3ADFF4965 HTTP 1.1" 503 3803 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-26&categoryId=ARCADE&productId=MB-AG-G07" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 949 host = www1 source = /opt/log/www1/access.log sourcetype = access_combined
>	6/21/16 1:13:00.000 AM	128.241.220.82 - - [21/Jun/2016:01:13:00] "POST /cart.do?action=purchase&itemId=EST-12&JSESSIONID=SD10SL3FF2ADFF4958 HTTP 1.1" 503 2917 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-12&categoryId=STRATEGY&productId=DC-SG-G02" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)" 871 host = www2 source = /opt/log/www2/access.log sourcetype = access_combined

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Editing Reports

- To edit a report's underlying search, select **Edit > Open in Search**
 - You can then edit and re-save, not save, or save-as a new report
- You can also edit the description, permissions, schedule, and acceleration
- Additionally, you can clone or delete the report

The screenshot displays the Splunk interface for editing a report titled "support_report_failpurchases...". The search bar contains the query: `sourcetype=access_combined action=purchase status!=200`. The report shows 2,866 events from 5/22/16 12:00:00.000 AM to 6/21/16 2:42:37.000 AM. The interface includes a table of events, a timeline visualization, and a menu with options: Open in Search, Edit Description, Edit Permissions, Edit Schedule, Edit Acceleration, Clone, Embed, and Delete. The "Open in Search" option is highlighted.

i	Time	Event
>	6/21/16 1:27:56.000 AM	217.23.14.6 4965 HTTP 1 DE&productI Chrome/19.0 host = www1

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

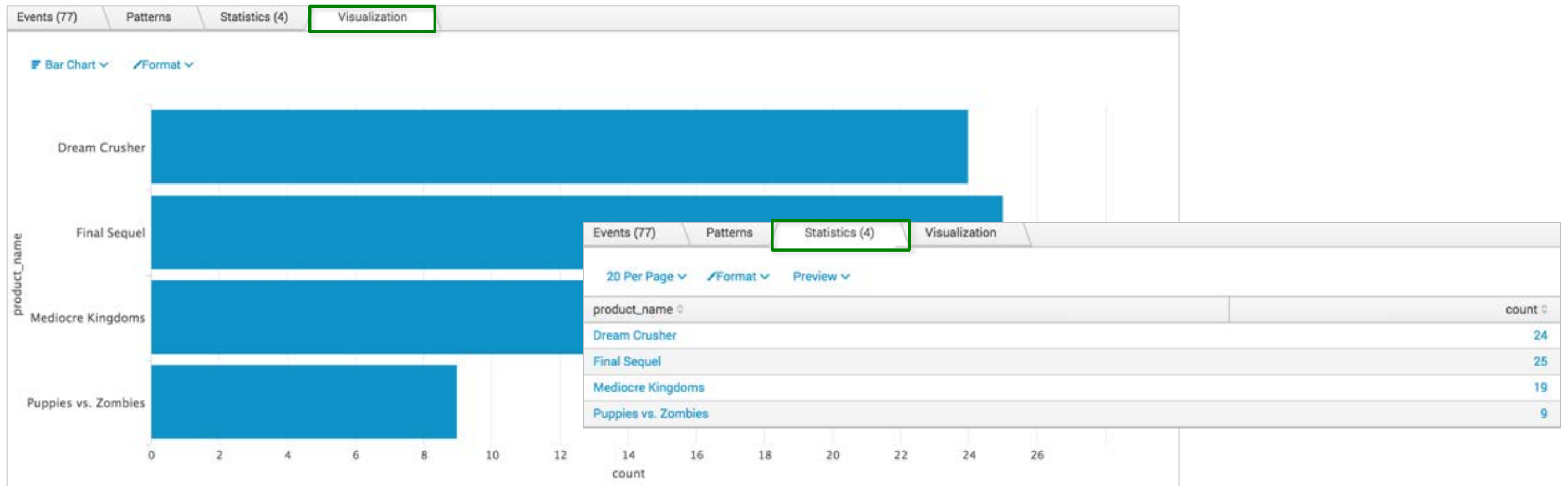
Creating Tables and Visualizations

Three main methods to create tables and visualizations in Splunk are:

- Select a field from the fields sidebar and choose a report to run
- Use the Pivot interface
 - Start with a dataset
 - or*
 - Start with Instant Pivot
- Use the Splunk search language transforming commands in the Search bar
 - Transforming commands are discussed in the *Searching & Reporting with Splunk* course

Tables and Visualizations

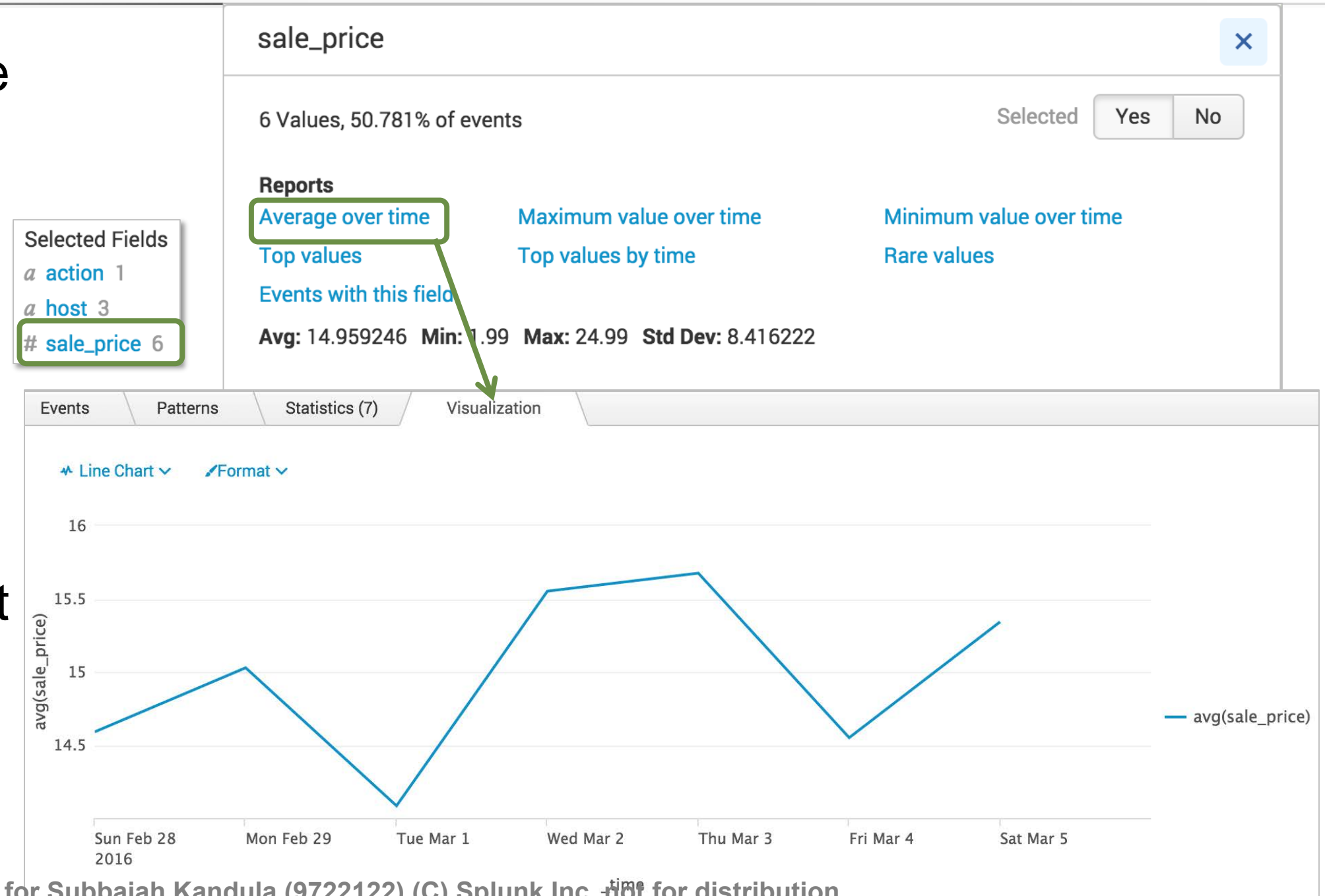
- Statistical reports leverage Splunk's built-in visualizations or table format
- These views give you insights into your organization's data



Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Create Reports From the Field Window

- Numeric fields: choose from six report types with mathematical functions, such as average, maximum value, and minimum value
- This example generates a report that shows the average over time
 - This is known as a **timechart**



Create a Top Values Report

- For alphanumeric character fields, there are only 3 available reports
- In this example, we want a report that shows the top **categories** purchased
 - Basic search: `sourcetype=access_combined status=200 action=purchase`
 - Click the **categoryId** field
 - Click **Top values**

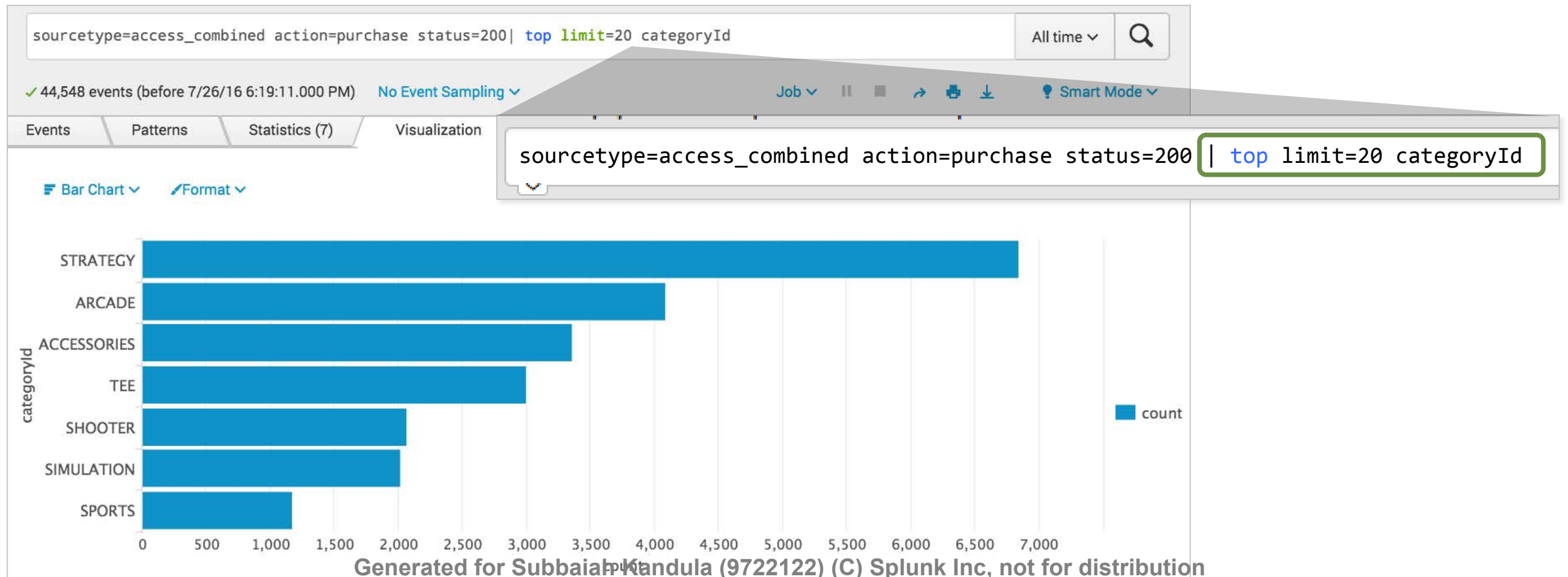
The screenshot shows the Splunk interface for a search. On the left, the 'Selected Fields' list includes 'categoryId' (7 values). A green box highlights 'categoryId' in the list, and a green arrow points from it to the 'Top values' report in the main panel. The report shows 7 values, representing 50.653% of events. The data is as follows:

Values	Count	%
STRATEGY	574	29.588%
ARCADE	395	20.361%
ACCESSORIES	269	13.866%
TEE	261	13.454%
SHOOTER	192	9.897%
SIMULATION	165	8.505%
SPORTS	84	4.33%

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

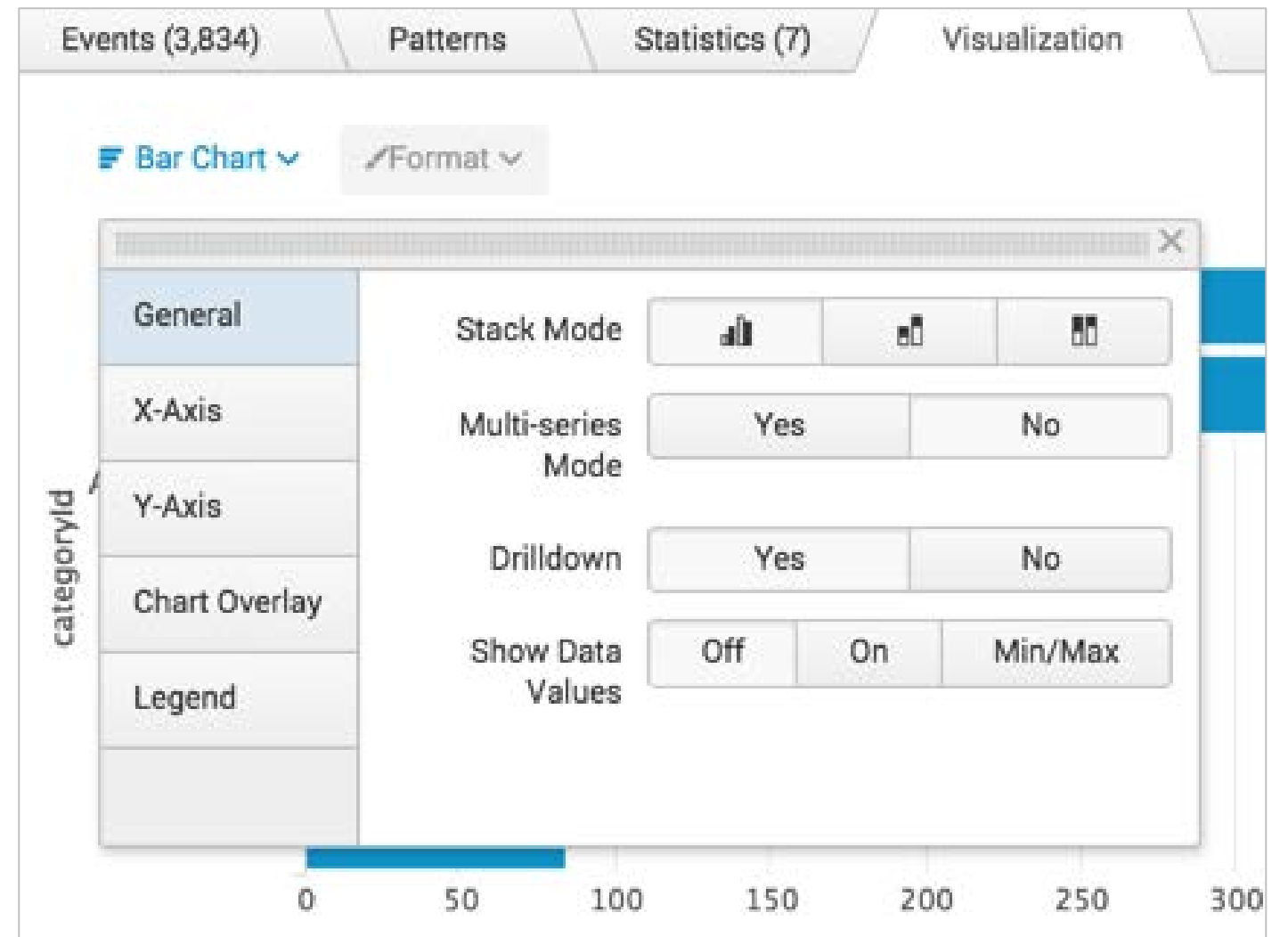
Create a Top Values Report (cont.)

- A | (pipe symbol) and the top command are added to the search string
- A bar chart is returned on the Visualizations tab, displaying the top categories purchased



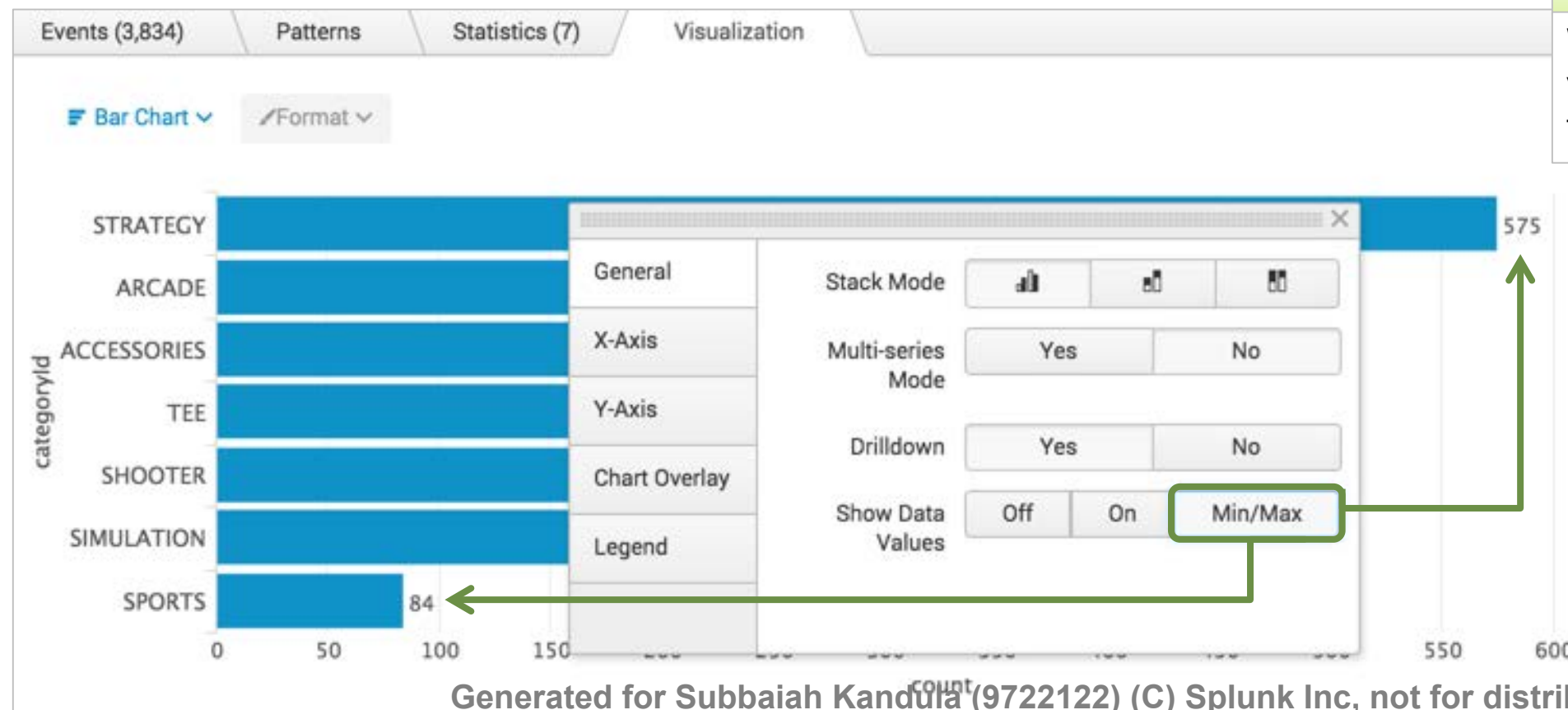
Change the Format

- The **Format** menu allows you to change formatting options
- For example, for bar and column charts:
 - The **General** tab allows you to change Stack, Multi-series, and Drilldown modes
 - The **X-Axis** and **Y-Axis** tabs allow you to change the axis labels and orientation
 - The **Legend** tab allows you to position the visualization legend as desired



Change the Format (cont.)

- **Show Data Values** determines whether to show data values in the visualization
 - If **Min/Max** is selected, data is only shown on the bars containing the minimum and maximum values



Note

When you make a change to the visualization settings – such as Min/Max – the visualization updates immediately.

Note

Learn more about modes and axes in the *Splunk Fundamentals 2* course. These modes require more sophisticated searches.

View as a Table

Switch to the **Statistics** tab to view the results as a table

categoryId	count	percent
STRATEGY	315	23.899848
NULL	246	18.664643
ARCADE	194	14.719272
ACCESSORIES	155	11.760243
TEE	150	11.380880
SIMULATION	103	7.814871
SHOOTER	99	7.511381
SPORTS	56	4.248862

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Statistics Overlay Format

- **Heat map** highlights outstanding values

20 Per Page Format Preview

	count	percent
	6857	30.347422
	4092	18.110201
	3366	14.897101
	3004	13.294977
	2071	9.165745
	2026	8.966586
	1179	5.217969

General: Wrap Results (Yes/No), Row Numbers (Yes/No), Drilldown (Row/Cell/None), Data Overlay: Heat map

Summary: Table column color overrides heat map and high/low value data overlay.

- **High and low values** highlights max and min of non zero values

20 Per Page Format Preview

	count	percent
	6857	30.347422
	4092	18.110201
	3366	14.897101
	3004	13.294977
	2071	9.165745
	2026	8.966586
	1179	5.217969

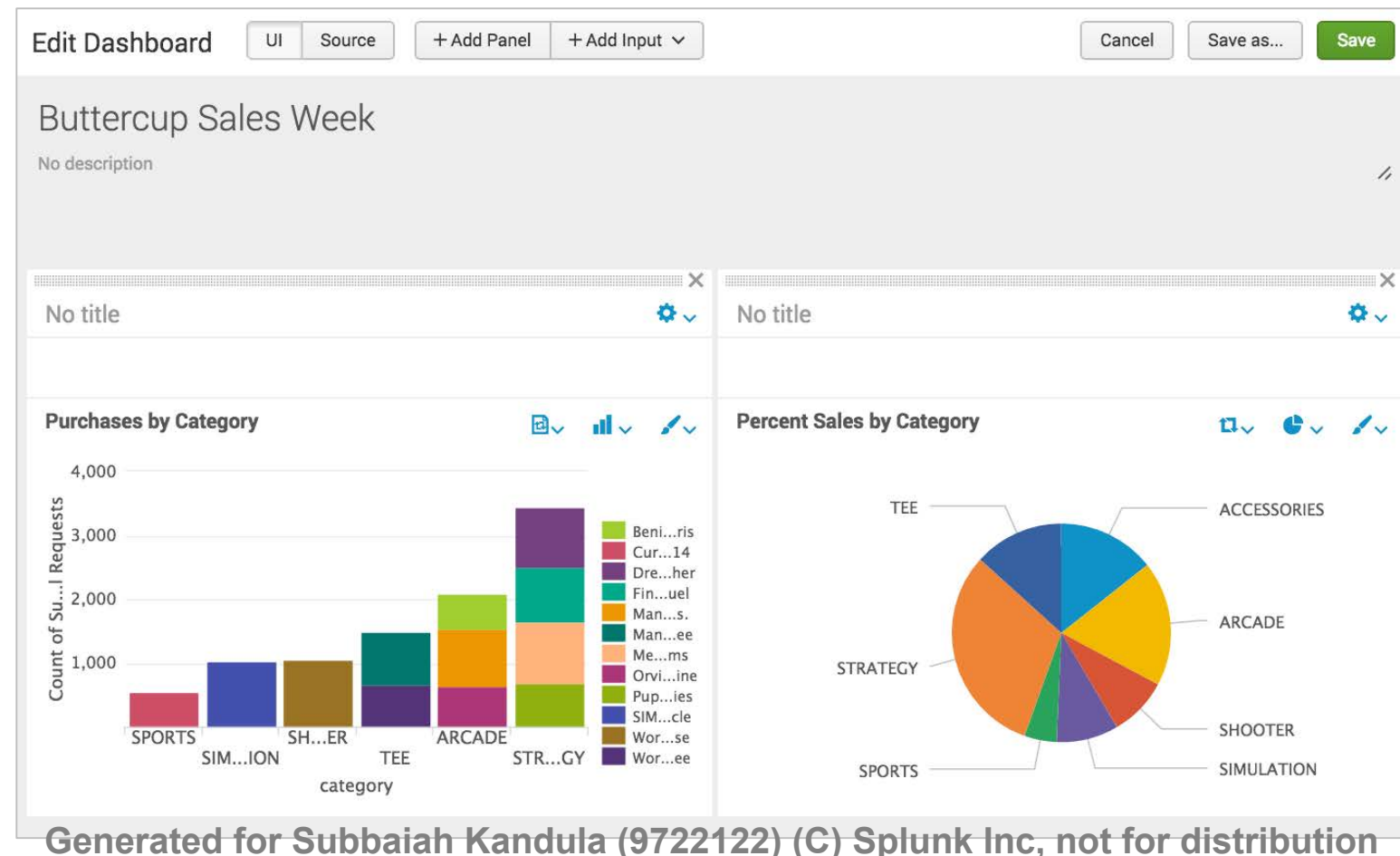
General: Wrap Results (Yes/No), Row Numbers (Yes/No), Drilldown (Row/Cell/None), Data Overlay: High and low values

Summary: Table column color overrides heat map and high/low value data overlay.

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

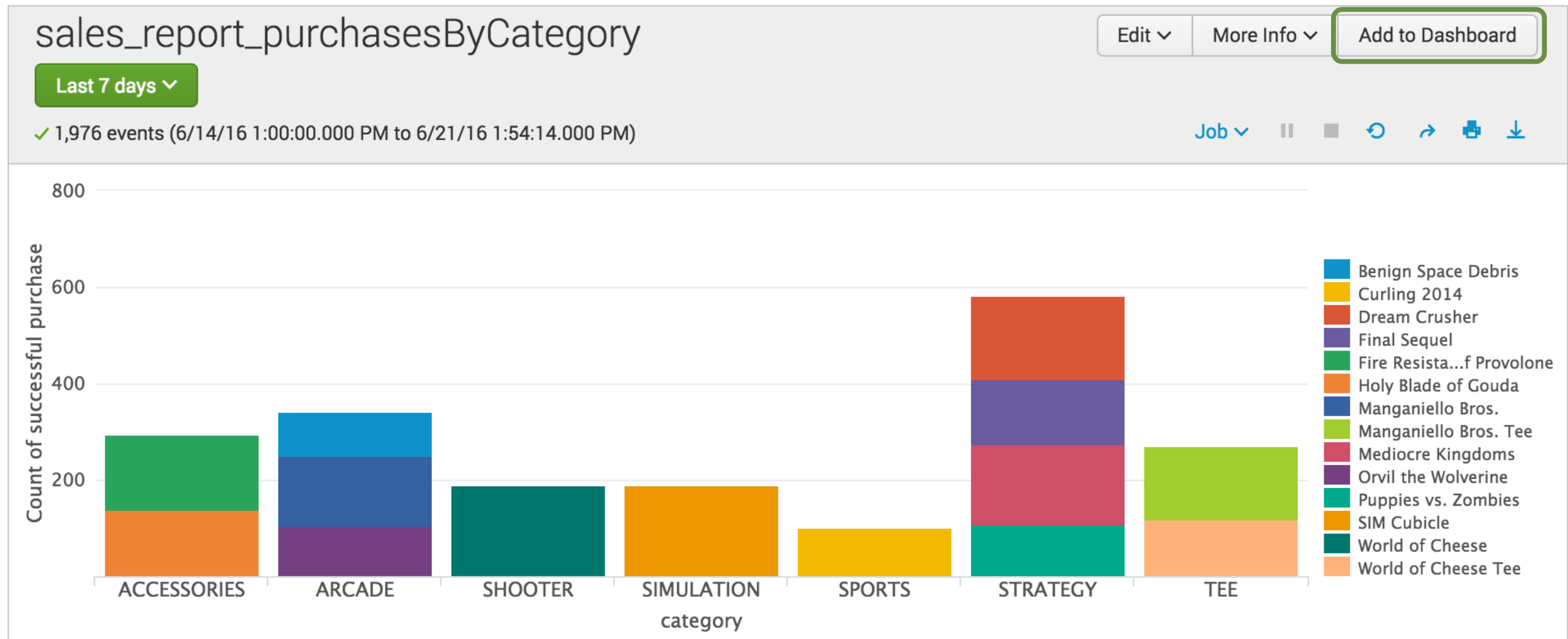
What Is a Dashboard?

- A dashboard consists of one or more panels displaying data visually in a useful way – such as events, tables, or charts
- A report or a pivot can be used to create a panel on a dashboard



Adding a Report to a Dashboard

In the report, click **Add to Dashboard** to begin



Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Adding a Report to a Dashboard (cont.)

- A** Name the dashboard and optionally provide a description
- B** Change the permissions (use Private until tested)
- C** Enter a meaningful title for the panel
- D** For **Panel Powered By**, click **Report**
- E** For the **Panel Content**, select **Statistics** to display as a table, or the *visualization type* (in this case, a **Column Chart**)

Note

The Dashboard ID is automatically populated with a unique value used by Splunk and should not be changed.

Save As Dashboard Panel

Dashboard:

Dashboard Title: **A**

Dashboard ID?: Can only contain letters, numbers and underscores.

Dashboard Description:

Dashboard Permissions: **B**

Panel Title: **C**

Panel Powered By: **D**

Panel Content: **E**

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

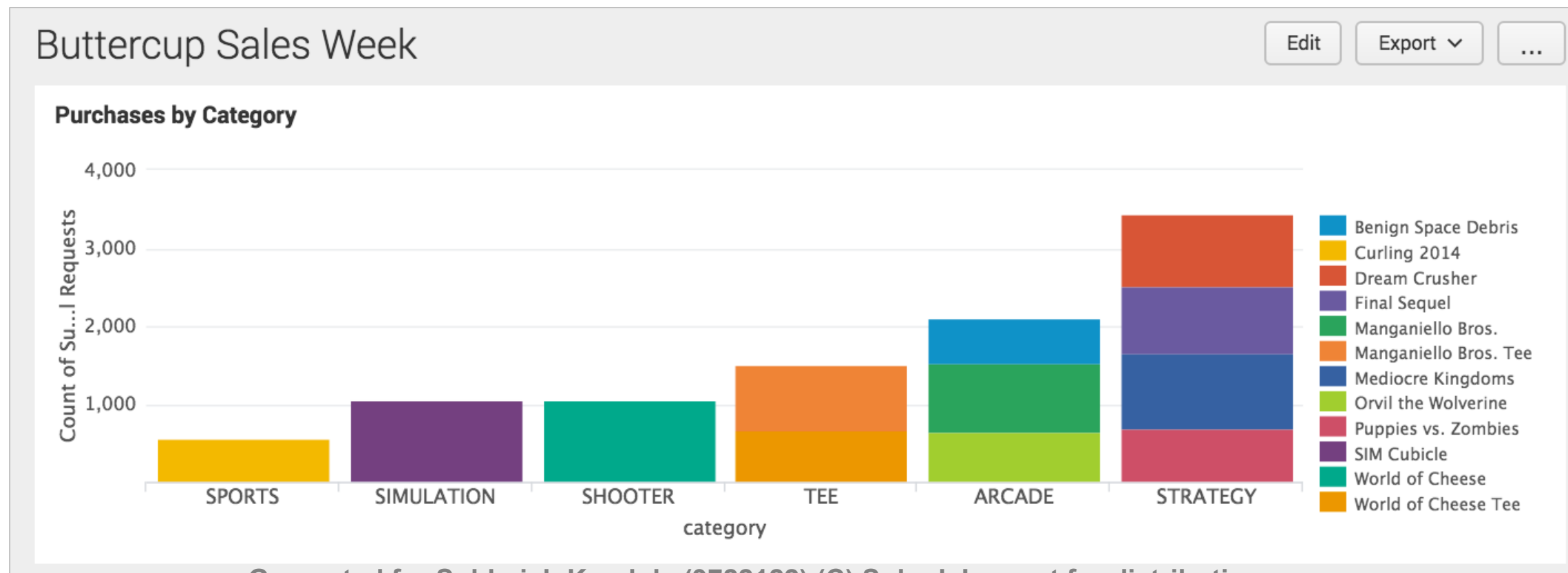
Adding a Report to a Dashboard (cont.)

After it is saved, you can view the dashboard immediately, or select the dashboard from the **Dashboards** view

Your Dashboard Panel Has Been Created ×

The panel has been created and added to buttercup_sales_week. You may now view the dashboard.

[View Dashboard](#)



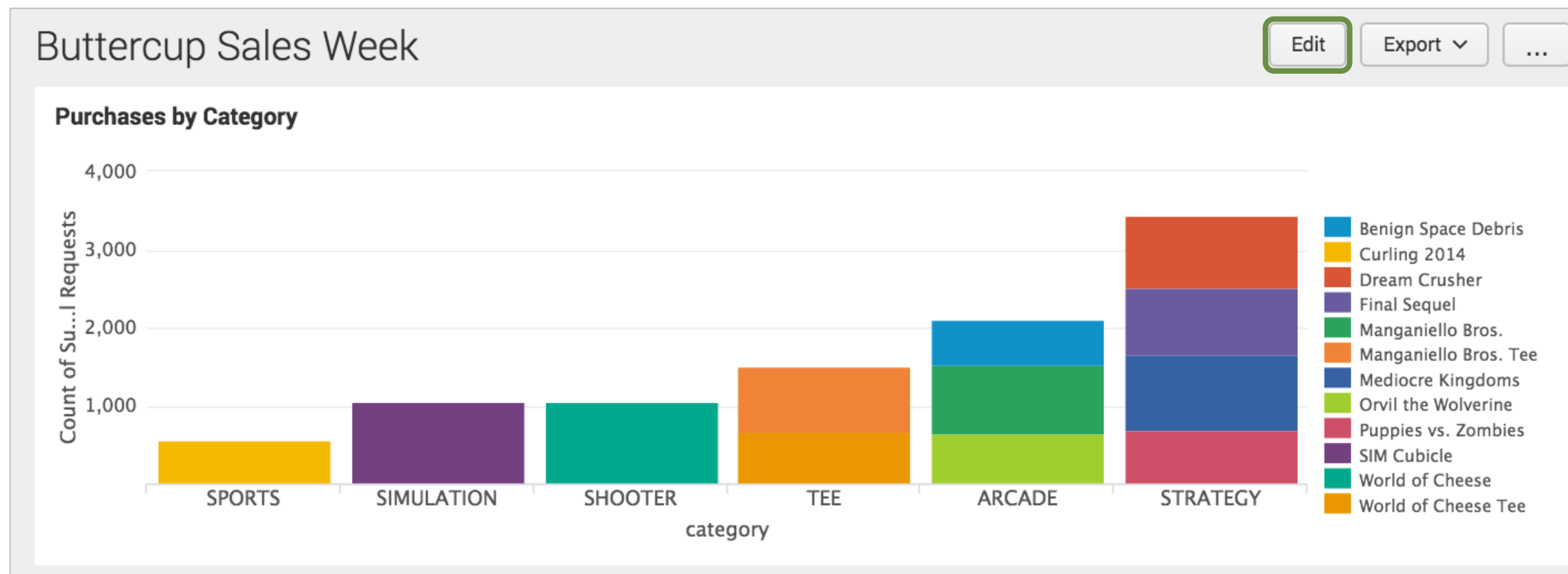
Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Why Create Panels from Reports?

- It is efficient to create most dashboard panels based on reports because
 - A single report can be used across different dashboards
 - This links the report definition to the dashboard
- Any change to the underlying report will affect every dashboard panel that utilizes that report

Editing Panels

- After saving the panel, a window appears from which you can view the updated dashboard
- Click **Edit** to customize the dashboard



Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Editing Panel Layout

Click on the dotted bar on a panel to drag the panel to a new location

The screenshot shows the Splunk dashboard editor interface. At the top, there is a navigation bar with the following elements: 'Edit Dashboard', 'UI', 'Source', '+ Add Panel', '+ Add Input', 'Cancel', 'Save as...', and 'Save'. Below this, the dashboard title is 'Buttercup Sales Week' with a subtitle 'No description'. Two panels are visible, each with a dotted bar at the top highlighted by a green box, indicating they can be dragged. The left panel is titled 'Purchases by Category' and displays a stacked bar chart showing the count of sub-requests for various categories. The right panel is titled 'Percent Sales by Category' and displays a pie chart showing the percentage of sales for various categories. Both panels have a 'No title' label and a settings icon. The footer of the dashboard editor reads: 'Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution'.

Category	Count of Sub-requests
SPORTS	~500
SIMULATION	~1000
SHOOTER	~1000
TEE	~1500
ARCADE	~2000
STRATEGY	~3500

Category	Percentage
TEE	~15%
ACCESSORIES	~15%
ARCADE	~15%
SHOOTER	~15%
SIMULATION	~15%
SPORTS	~15%

Drill Down from Visualization to Search

Click an object in a chart or table to see its underlying events in Search view

The screenshot shows the Splunk interface for a search. The search bar contains `sourcetype=access_combined` and `categoryId=STRATEGY`. The search results show 2,973 events from 8/14/16 to 8/21/16. A visualization shows a bar chart of events over time, with a tooltip indicating 25 events at 7 PM on Saturday, August 20, 2016. A pie chart shows the distribution of events by category, with STRATEGY being the largest category at 27.915%. A table below the pie chart shows the underlying search results for the selected event, including fields like `host`, `source`, `action`, `bytes`, and `categoryid`.

Search: `sourcetype=access_combined` `categoryId=STRATEGY`

2,973 events (8/14/16 12:00:00.000 AM to 8/21/16 12:00:00.000 AM) No Event Sampling

Events (2,973) | Patterns | Statistics | Visualization

Format Timeline | Zoom Out | Zoom to Selection | Deselect | 1 hour per column

25 events at 7 PM on Saturday, August 20, 2016

categoryid: STRATEGY
count: 2,973
count%: 27.915%

i	Time
>	8/20/16 11:49:29.000
>	8/20/16 11:49:25.000

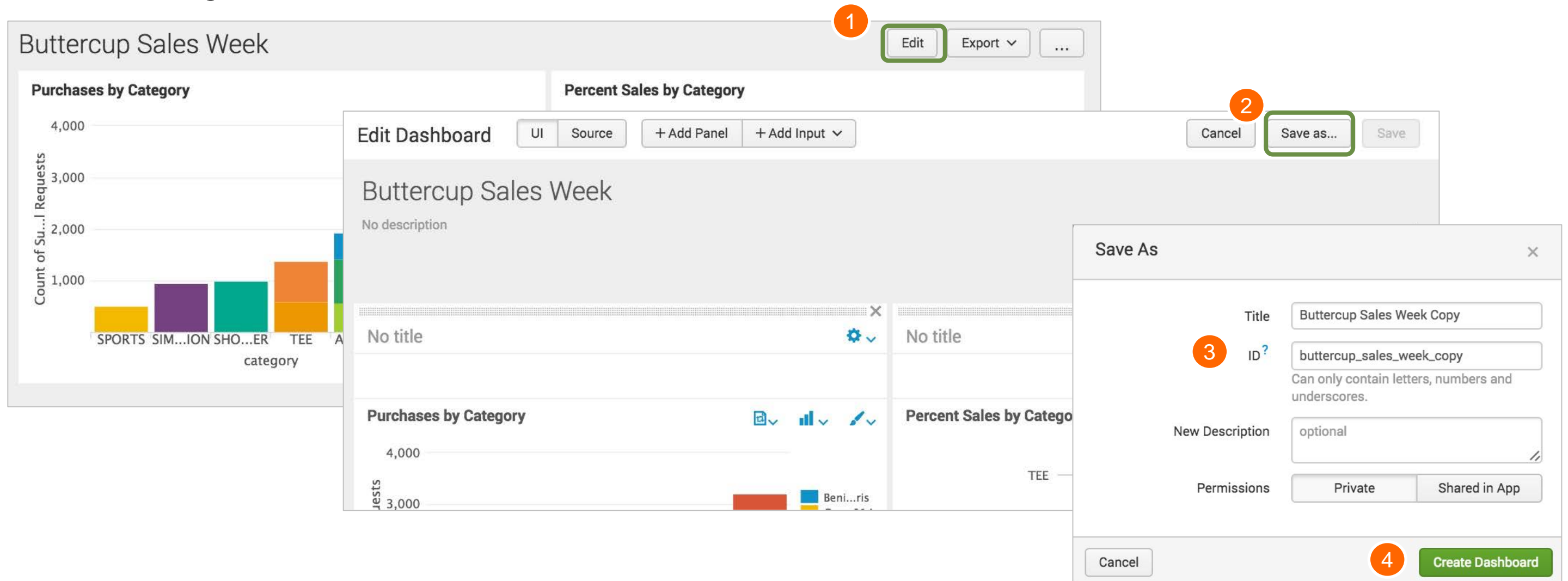
Selected Fields: `host` 3, `source` 3, `sourcetype` 1

Interesting Fields: `action` 5, `bytes` 100+, `categoryid` 1

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Clone a Dashboard

- To clone a dashboard, click **Edit** – and then **Save as...**
 - Change the **Title** as desired, and then click **Create Dashboard**



The screenshot illustrates the process of cloning a dashboard in Splunk. It shows a dashboard titled "Buttercup Sales Week" with two panels: "Purchases by Category" and "Percent Sales by Category". The "Purchases by Category" panel is a bar chart showing the count of successful requests for different categories: SPORTS, SIMULATION, SHOES, and TEE. The "Percent Sales by Category" panel is a bar chart showing the percentage of sales for different categories: TEE, Beni...ris, and others.

The "Edit Dashboard" modal is open, showing the dashboard's title "Buttercup Sales Week" and a "No description". The "Save as..." button is highlighted with a green box and a red circle labeled "2".

The "Save As" modal is open, showing the following fields:

- Title: Buttercup Sales Week Copy
- ID: buttercup_sales_week_copy (Note: Can only contain letters, numbers and underscores.)
- New Description: optional
- Permissions: Private (selected), Shared in App

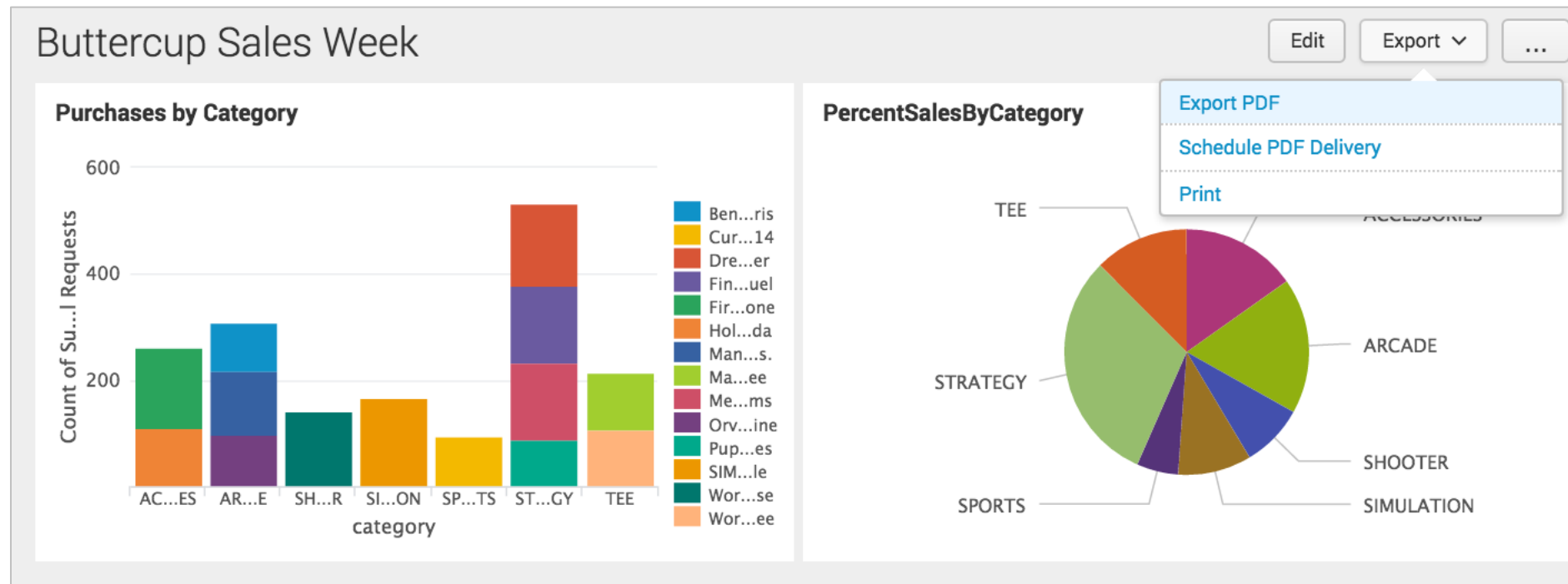
The "Create Dashboard" button is highlighted with a green box and a red circle labeled "4".

Numbered callouts: 1 points to the "Edit" button on the dashboard; 2 points to the "Save as..." button in the "Edit Dashboard" modal; 3 points to the "ID" field in the "Save As" modal; 4 points to the "Create Dashboard" button in the "Save As" modal.

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Export a Dashboard (cont.)

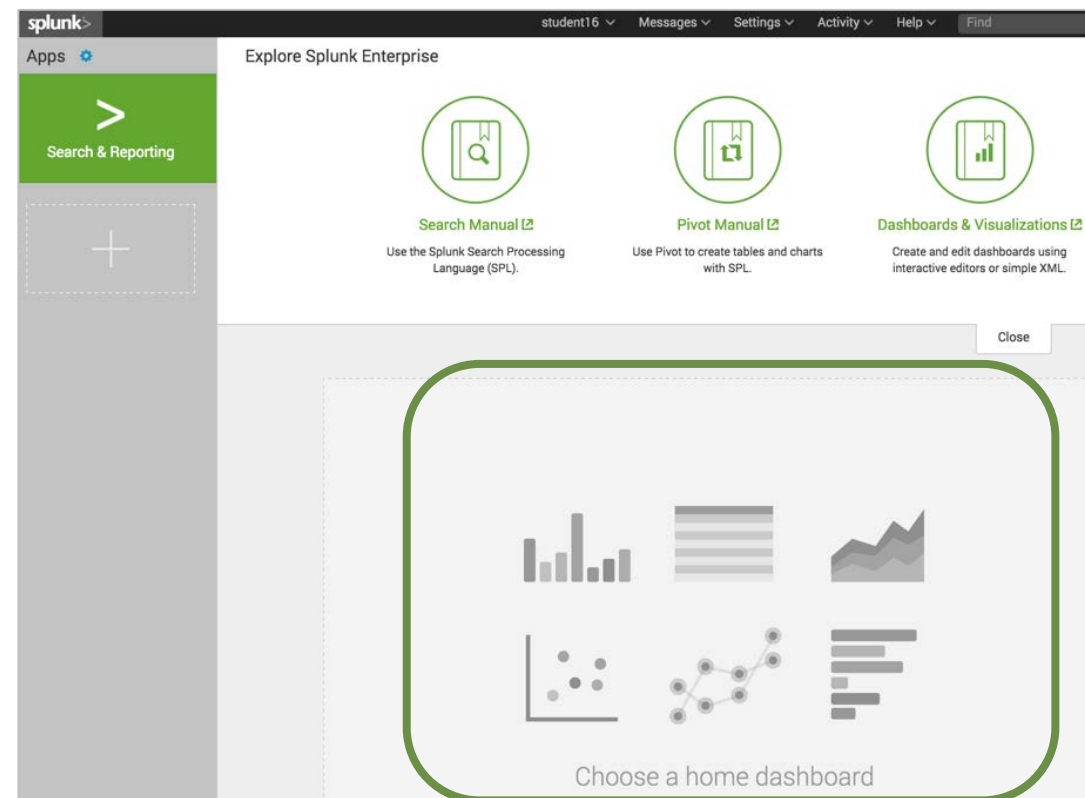
- Without the add-on, dashboards can be exported as PDF
 - They can also be printed



Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Make a Default Dashboard

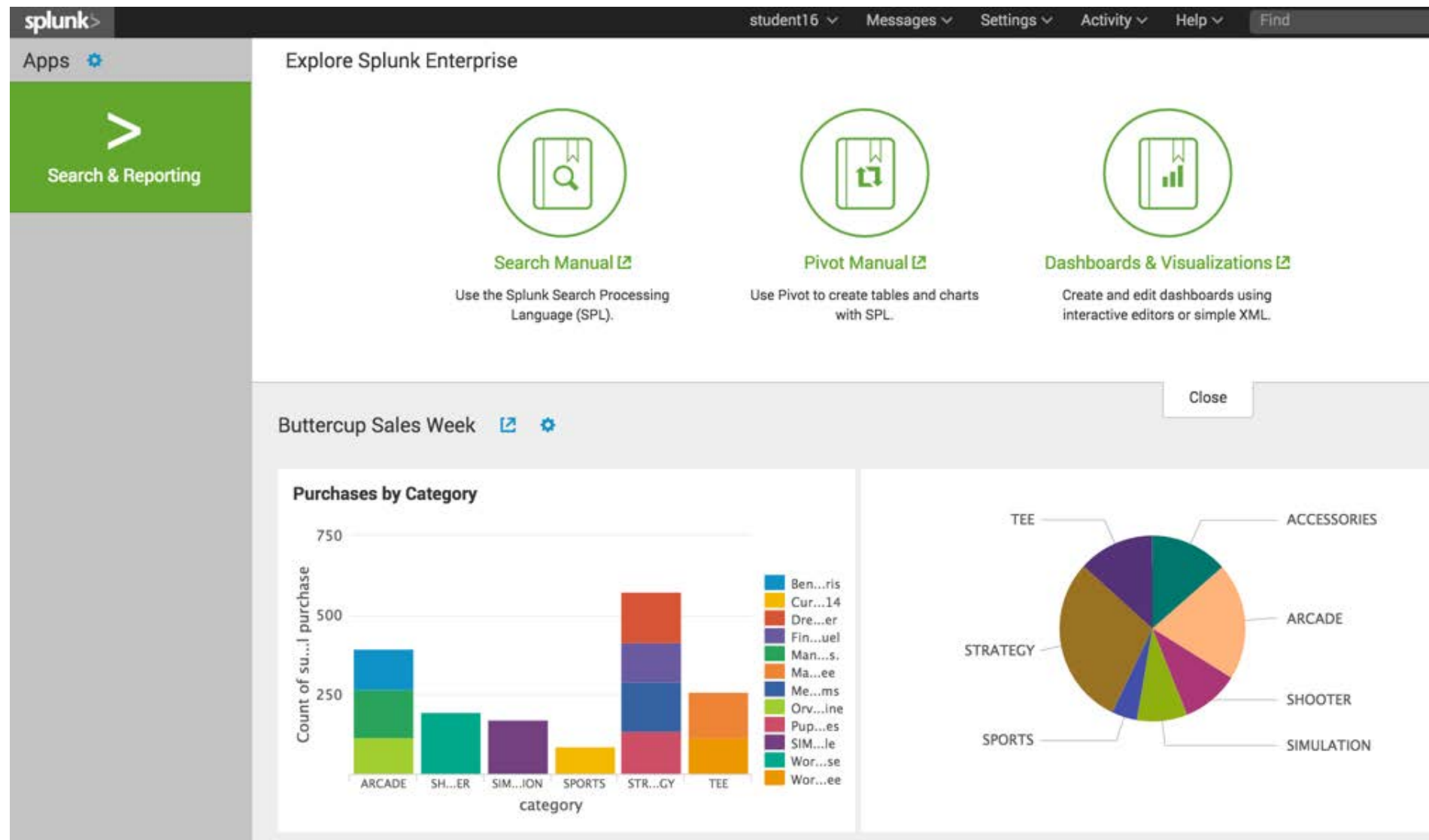
- Set a dashboard to appear by default in the bottom panel of your home view
- From Home, click **Choose a home dashboard**



Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

View Your Default Dashboard

After you've set a dashboard as default, your home view may look like this:



Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Module 11: Using Pivot

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Objectives

- Describe pivot
- Understand the relationship between the data model and the pivot
- Select a data model object
- Create a pivot report
- Use instant pivot to create a report

Completed Pivot

Pivot is a quick way to design visualizations of data. Let's see how.

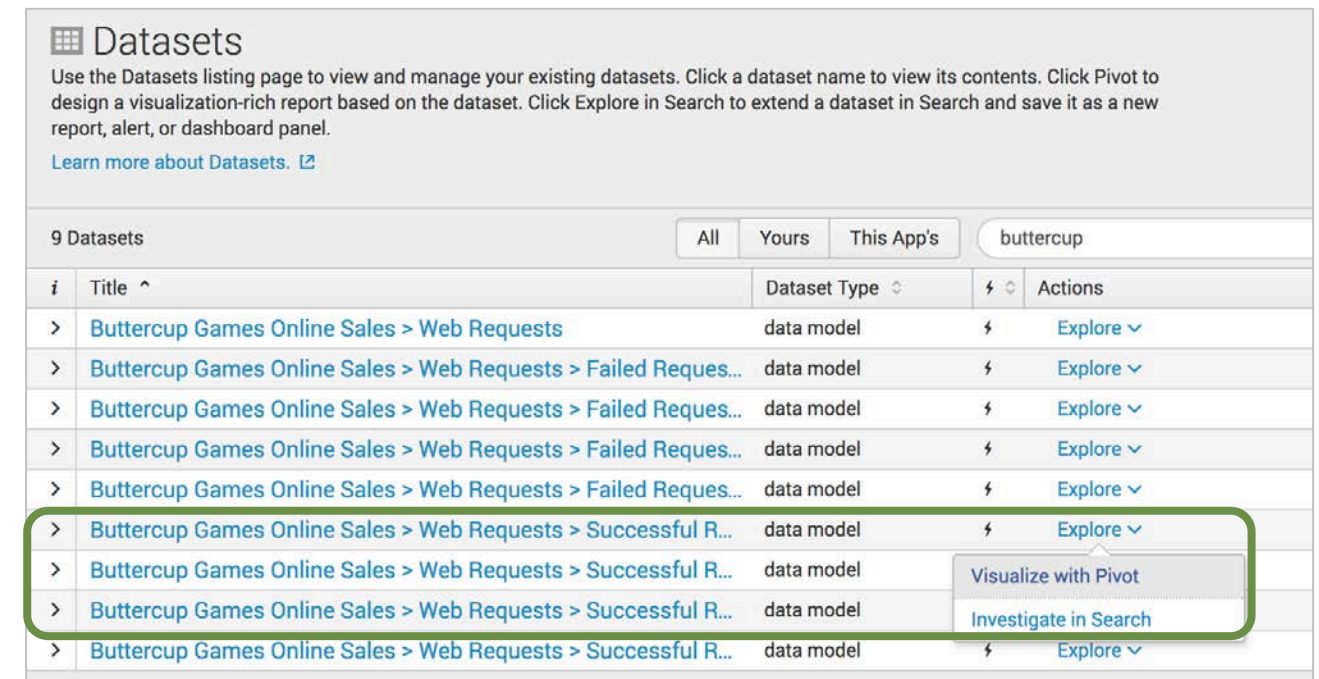
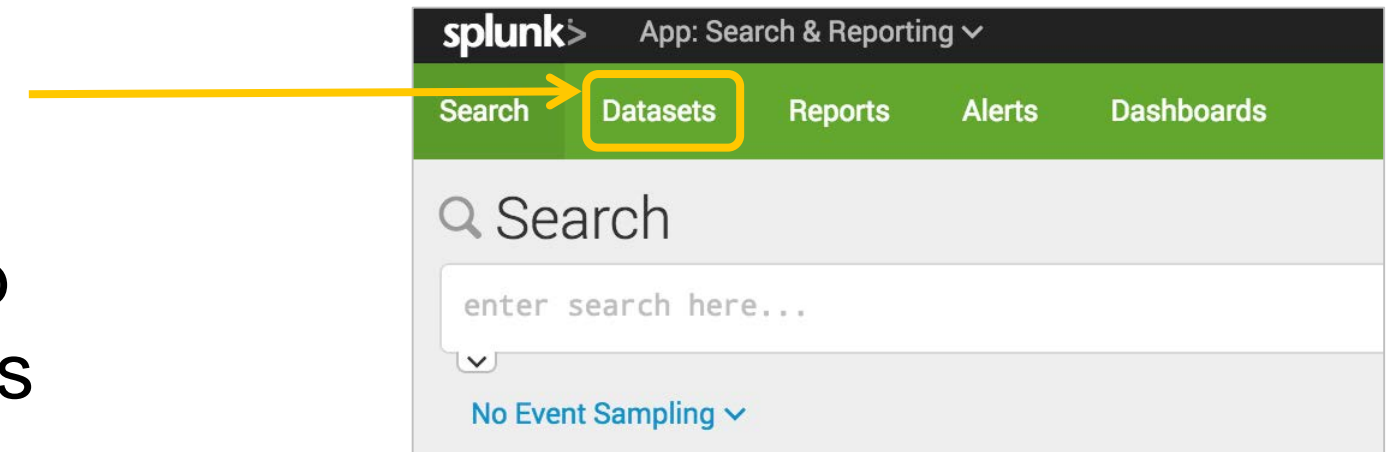
The screenshot displays the 'New Pivot' configuration window in Splunk. On the left, a table lists event categories with their counts. The 'category' field is selected for visualization. The right pane shows a pie chart with six segments labeled: TEE, ARCADE, SHOOTER, SIMULATION, SPORTS, and STRATEGY. The configuration panel includes settings for Time Range, Filter, Color, Field, Label, Sort, Limit, Size, and Minimum Size.

category	Benign Space Debris	Curling 2014	Drum Crush
ARCADE	128	0	
SHOOTER	0	0	
SIMULATION	0	0	
SPORTS	0	85	
STRATEGY	0	0	
TEE	0	0	
ALL	128	85	

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Selecting a Dataset

1. From the Search & Reporting app, select the **Datasets** tab
 - This displays a list of available lookup table files ("lookups") and data models
 - Each lookup and data model represent a specific category of data
 - ▶ Prebuilt lookups and data models make it easier to interact with your data
2. Click **Explore > Visualize with Pivot**



Datasets

Use the Datasets listing page to view and manage your existing datasets. Click a dataset name to view its contents. Click Pivot to design a visualization-rich report based on the dataset. Click Explore in Search to extend a dataset in Search and save it as a new report, alert, or dashboard panel.

[Learn more about Datasets.](#)

9 Datasets All Yours This App's

i	Title ^	Dataset Type	⚡	Actions
>	Buttercup Games Online Sales > Web Requests	data model	⚡	Explore
>	Buttercup Games Online Sales > Web Requests > Failed Reques...	data model	⚡	Explore
>	Buttercup Games Online Sales > Web Requests > Failed Reques...	data model	⚡	Explore
>	Buttercup Games Online Sales > Web Requests > Failed Reques...	data model	⚡	Explore
>	Buttercup Games Online Sales > Web Requests > Failed Reques...	data model	⚡	Explore
>	Buttercup Games Online Sales > Web Requests > Successful R...	data model	⚡	Explore
>	Buttercup Games Online Sales > Web Requests > Successful R...	data model	⚡	Visualize with Pivot
>	Buttercup Games Online Sales > Web Requests > Successful R...	data model	⚡	Investigate in Search
>	Buttercup Games Online Sales > Web Requests > Successful R...	data model	⚡	Explore

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Open in Pivot

- The Pivot automatically populates with a count of events for the selected object
- In this example, it shows all successful purchase requests for all time

The screenshot displays the Splunk Pivot interface. At the top, it says "New Pivot" and shows "208,243 events (before 7/25/16 8:40:39.000 PM)". The interface includes a sidebar with various visualization icons. The main area is divided into sections: "Filters" (set to "All time"), "Split Rows" (empty), "Split Columns" (empty), and "Column Values" (set to "Count of Successful Requests"). The pivot table below shows a single row with the value "208243". A green box highlights the "Count of Successful Requests" field in the Column Values section and the resulting value in the table. Another green box highlights the "Count of Successful Requests" field in the Filters section. The bottom of the interface shows a footer: "Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution".

Open in Pivot

- The Pivot automatically populates with a count of events for the selected object
- In this example, it shows all successful purchase requests for all time

The screenshot displays the Splunk Pivot interface. At the top, it says "New Pivot" and shows "208,243 events (before 7/25/16 8:40:39.000 PM)". The interface includes a sidebar with various visualization icons. The main area is divided into sections: "Filters" with "All time", "Split Rows" with a plus sign, "Split Columns" with a plus sign, and "Column Values" with "Count of Successful Requests". The pivot table below shows a single row with the value "208243".

Count of Successful Requests
208243

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution


Select a Time Range

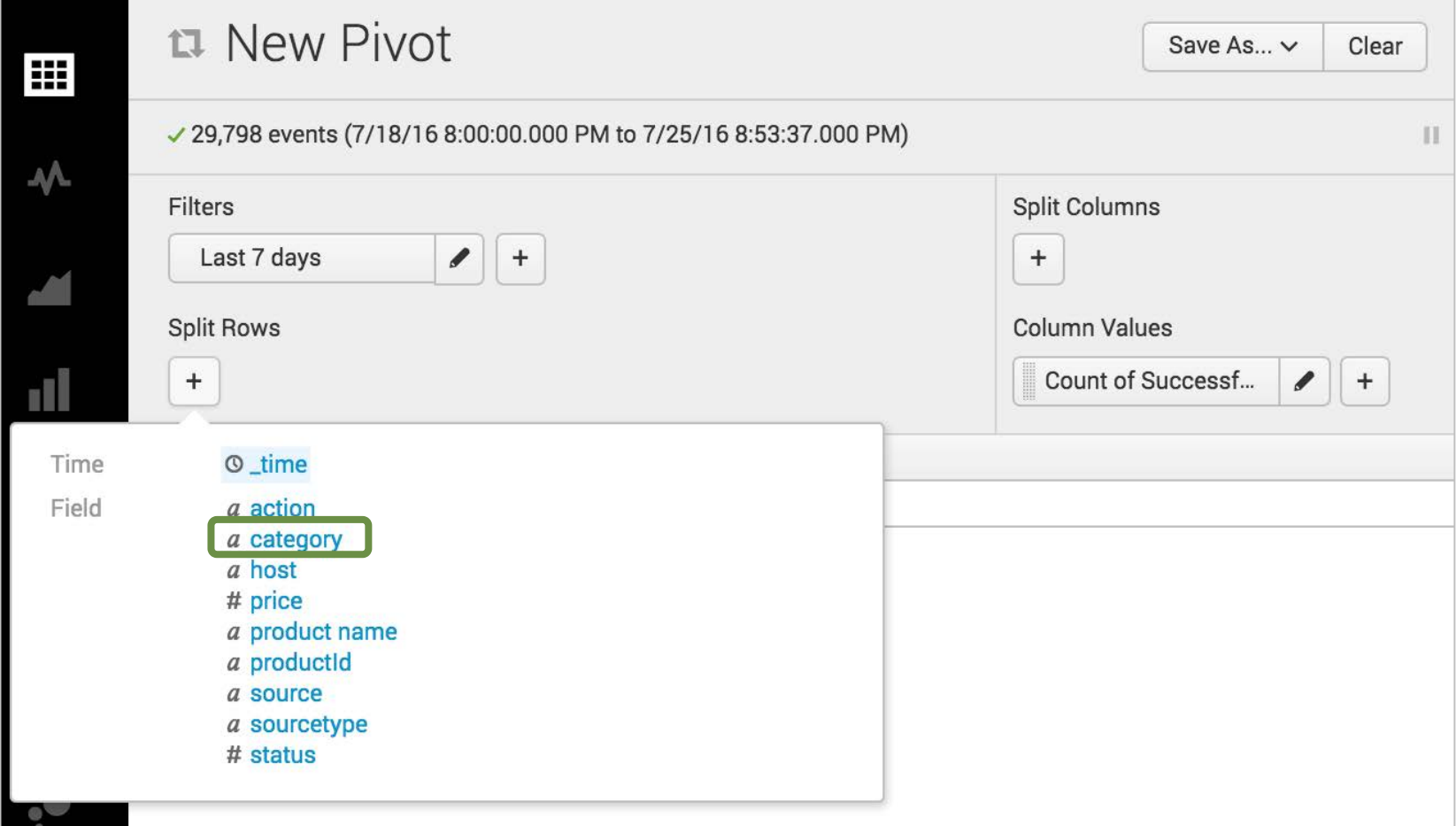
- The default is **All time**
- Click the pencil icon to select the desired time range
- The pivot runs immediately upon selecting the new time range

The screenshot shows the 'New Pivot' interface in Splunk. At the top, it says 'New Pivot' with a refresh icon and buttons for 'Save As...' and 'Clear'. Below that, it displays '208,243 events (before 7/25/16 8:40:39.000 PM)'. The 'Filters' section shows 'All time' with a pencil icon and a plus sign. A dropdown menu is open, showing 'Presets' with three columns: 'Real-time', 'Relative', and 'Other'. The 'Last 7 days' option is highlighted with a green box. Below the presets, there are expandable sections for 'Relative', 'Real-time', 'Date Range', 'Date & Time Range', and 'Advanced'.

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Split Rows

- Click  under **Split Rows** for a list of available attributes to populate the rows
- In this example, the rows are split by the **category** attribute, which will list
 - Each game category on a separate row
 - A count of successful requests for each game category



The screenshot shows the 'New Pivot' configuration window in Splunk. The main area displays '29,798 events (7/18/16 8:00:00.000 PM to 7/25/16 8:53:37.000 PM)'. The 'Filters' section is set to 'Last 7 days'. The 'Split Rows' section has a dropdown menu open, listing various fields: `_time`, `action`, `category` (highlighted with a green border), `host`, `price`, `product name`, `productId`, `source`, `sourcetype`, and `status`. The 'Split Columns' section is empty, and the 'Column Values' section is set to 'Count of Successf...'. The interface includes 'Save As...' and 'Clear' buttons at the top right.

Split Rows (cont.)

- Once selected, you can:
 - Modify the label
 - Change the sort order
 - ▶ **Default** – sorts by the field value in ascending order
 - ▶ **Ascending** - sorts by the count in ascending order
 - ▶ **Descending** – sorts by the count in descending order
 - Define maximum # of rows to display
- Click **Add to Table** to view the results

New Pivot

✓ 29,798 events (7/18/16 8:00:00.000 PM to 7/25/16 8:53:37.000 PM)

Filters

Last 7 days

Split Rows

category

Label optional

All Rows

Sort Descending

(By Count of Successful Requests) ?

Max Rows 100

Add To Table

Results

New Pivot

Save As... Clear Successful Requests

28,021 events (7/19/16 2:00:00.000 PM to 7/26/16 2:58:00.000 PM)

Filters: Last 7 days

Split Rows: category

Split Columns: +

Column Values: Count of Successf...

category	Count of Successful Requests
SPORTS	569
SIMULATION	1053
SHOOTER	1065
TEE	1538
ACCESSORIES	1687
ARCADE	2132
STRATEGY	3482

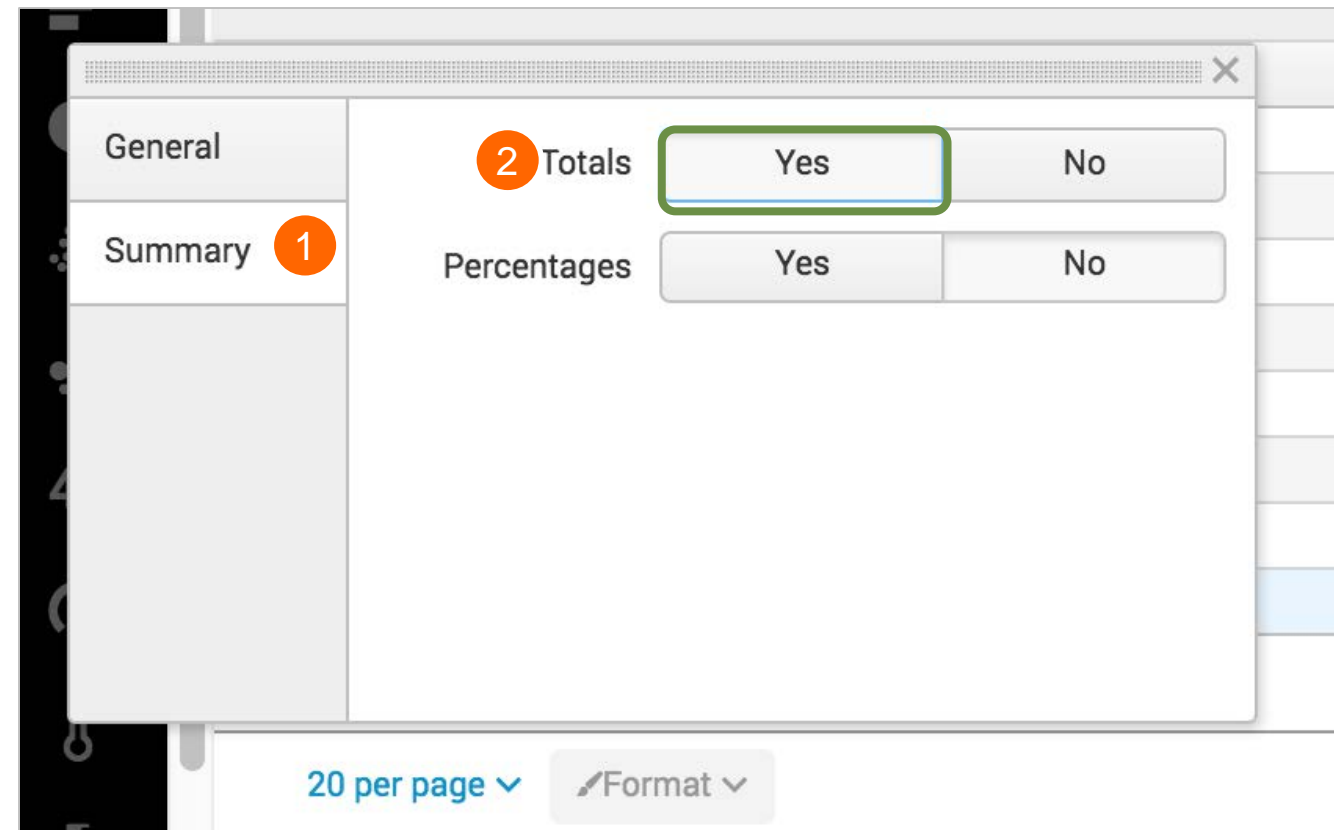
20 per page Format

To format the results, click here

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Formatting the Results

For example, to add totals on the **Summary** tab, click **Yes** next to **Totals**



Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Updated Results (with Total)

New Pivot

Save As... Clear Successful Requests

✓ 27,890 events (7/19/16 3:00:00.000 PM to 7/26/16 3:10:36.000 PM)

Filters: Last 7 days

Split Rows: category

Split Columns: +


Column Values: Count of Successf... +

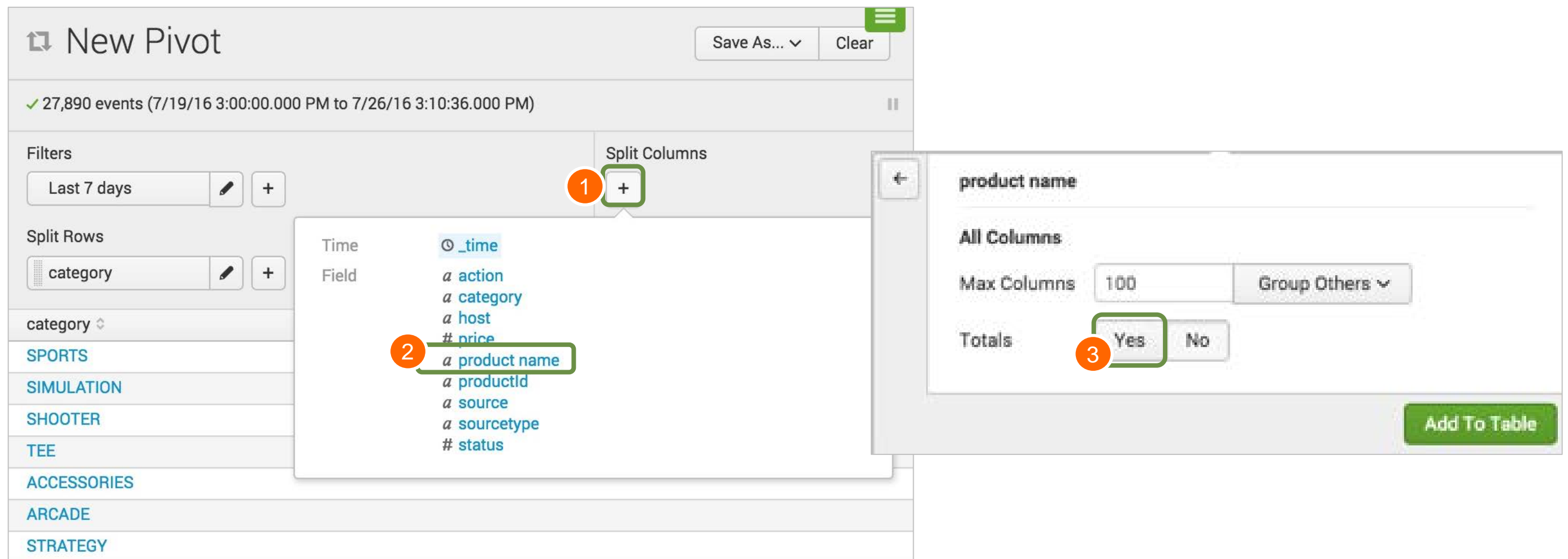
category	Count of Successful Requests
SPORTS	568
SIMULATION	1049
SHOOTER	1059
TEE	1530
ACCESSORIES	1679
ARCADE	2126
STRATEGY	3469
	11480

20 per page Format

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Split Columns

- Click  under **Split Columns** and select the desired split
- Specify the maximum number of columns and whether you want Totals





New Pivot



Save As... ▾ Clear

✓ 27,890 events (7/19/16 3:00:00.000 PM to 7/26/16 3:10:36.000 PM) ||

Filters

Last 7 days  

Split Rows

category  

category ▾

SPORTS

SIMULATION

SHOOTER


TEE


ACCESSORIES

ARCADE

STRATEGY

Split Columns

1 

Time  `_time`

Field

`a action`

`a category`

`a host`

`# price`

2 `a product name`

`a productId`

`a source`

`a sourcetype`

`# status`

product name

All Columns

Max Columns

Totals Yes No

3

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Results

New Pivot Save As... ▾ Clear Successful Requests ▾

✓ 27,880 events (7/19/16 4:00:00.000 PM to 7/26/16 4:52:58.000 PM)

Filters: Last 7 days ✎ +

Split Rows: category ✎ +

Split Columns: product name ✎ +

Column Values: Count of Successf... ✎ +

The ALL column shows row totals by category

category	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	World of Cheese	World of Cheese Tee	ALL
SPORTS	0	568	0	0	0	0	0	0	0	0	0	0	0	0	568
SIMULATION	0	0	0	0	0	0	0	0	0	0	0	1055	0	0	1055
SHOOTER	0	0	0	0	0	0	0	0	0	0	0	0	1069	0	1069
TEE	0	0	0	0	0	0	0	855	0	0	0	0	0	667	1522
ACCESSORIES	0	0	0	0	863	814	0	0	0	0	0	0	0	0	1677
ARCADE	572	0	0	0	0	0	907	0	0	647	0	0	0	0	2126
STRATEGY	0	0	947	853	0	0	0	0	986	0	675	0	0	0	3461
	572	568	947	853	863	814	907	855	986	647	675	1055	1069	667	11478

The bottom (bolded) row shows column totals by product name

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Add Additional Filters

- You can refine a pivot by filtering on key/value pairs
 - Think of ‘split by’ as rows and columns as the fields to display
 - Think of filters as a field=value inclusion, exclusion or specific condition to apply to the search (=, <, >, !=, *)
- In the example, the pivot is filtered to exclude events from the ACCESSORIES category

The screenshot shows the 'New Pivot' configuration window in Splunk. At the top, it displays '1,893 events (1/15/16 11:00:00.000 PM to 1/22/16 11:03:42.000 PM)'. Below this, the 'Filters' section shows 'Last 7 days' with a plus sign icon (1). A dropdown menu (2) is open, listing attributes: action, category, host, price, product name, productId, source, sourcetype, and status. The 'category' attribute is selected. A filter configuration dialog is shown, where the 'Filter Type' is set to 'Match'. The 'Match' field is set to 'is not' (3), the value is 'ACCESSORIES' (5), and a dropdown arrow (4) is visible. An 'Add To Table' button (6) is at the bottom right.

Filtered Pivot

- The ACCESSORIES category is filtered out
- All the other categories remain

New Pivot Save As... ▾ Clear Successful Requests ▾

✓ 26,005 events (7/19/16 5:00:00.000 PM to 7/26/16 5:03:19.000 PM)

Filters: Last 7 days | category is not AC... | +

Split Rows: category | +

Split Columns: product name | +

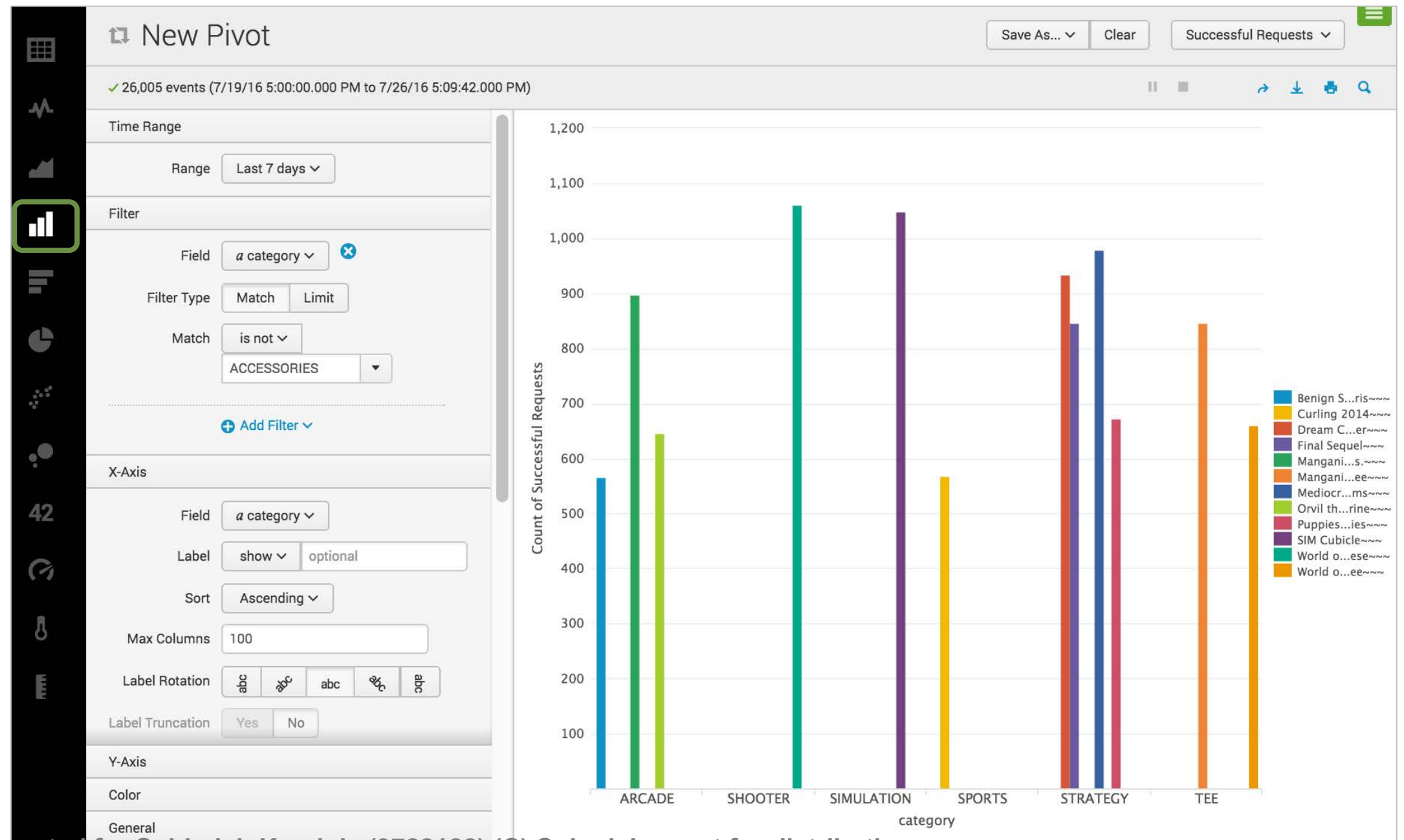
Column Values: Count of Successf... | +

category	Benign Space Debris	Curling 2014	Dream Crusher	Final Sequel	Manganiello Bros.	Manganiello Bros. Tee	Mediocre Kingdoms	Orvil the Wolverine	Puppies vs. Zombies	SIM Cubicle	World of Cheese	World of Cheese Tee	ALL
SPORTS	0	568	0	0	0	0	0	0	0	0	0	0	568
SIMULATION	0	0	0	0	0	0	0	0	0	1048	0	0	1048
SHOOTER	0	0	0	0	0	0	0	0	0	0	1061	0	1061
TEE	0	0	0	0	0	847	0	0	0	0	0	660	1507
ARCADE	567	0	0	0	898	0	0	647	0	0	0	0	2112
STRATEGY	0	0	935	846	0	0	980	0	673	0	0	0	3434
	567	568	935	846	898	847	980	647	673	1048	1061	660	9730

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution


Select a Visualization Format

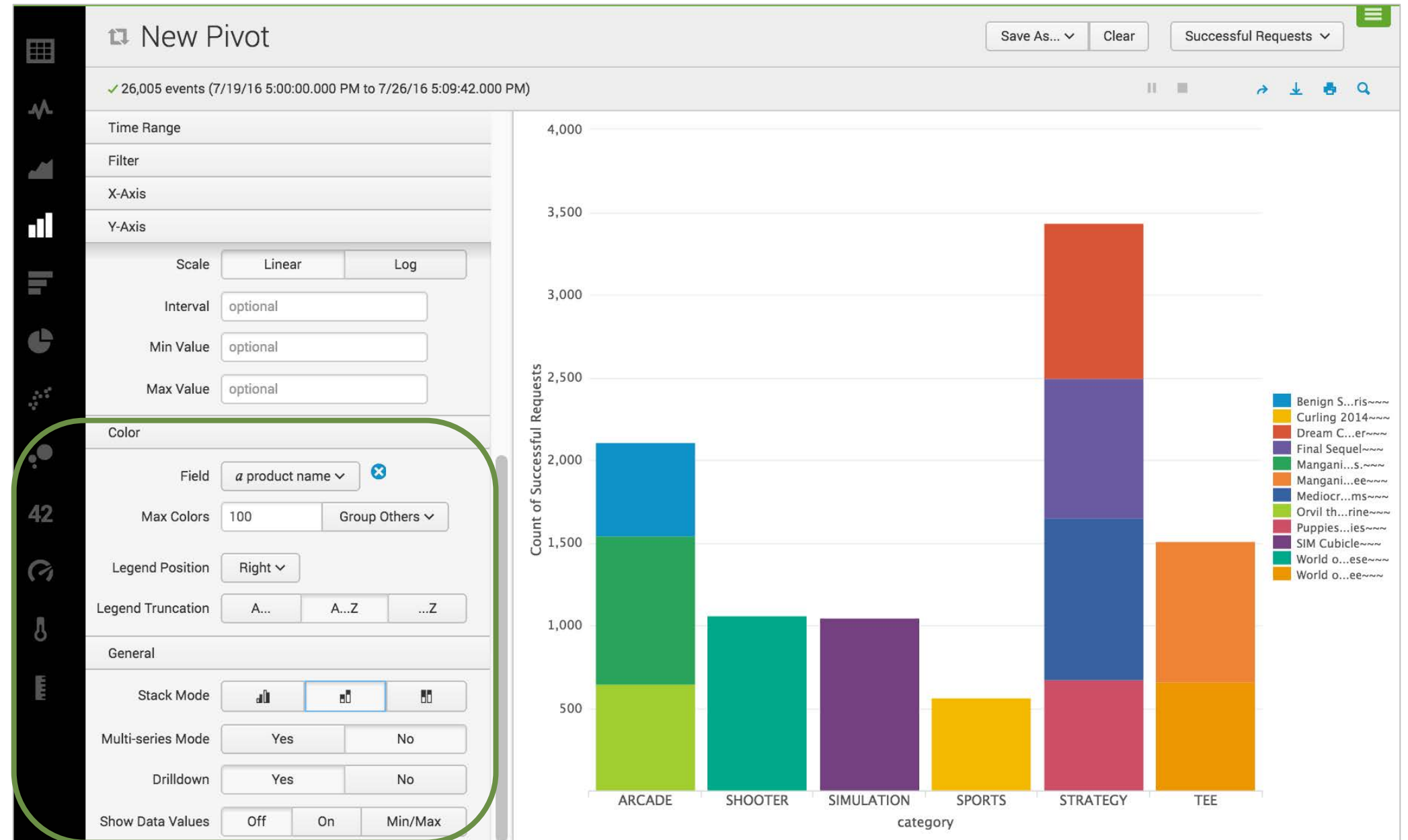
You can display your pivot as a table or a visualization, such as a column chart



Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Modify Visualization Settings

- When a visualization control is selected, panels appear that let you configure its settings
- In this example:
 - The results for each category are broken down by **product_name**
 - The stack mode is set to stacked 



Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Saving a Pivot

- Pivots can be saved as reports
 - You can choose to include a Time Range Picker in the report to allow people who run it to change the time range (default is Yes)
 - You will learn more about reports later in this course

The screenshot shows the Splunk 'New Pivot' interface. On the left, there are configuration options for the pivot, including 'Time Range', 'Filter', 'X-Axis', 'Y-Axis', 'Scale' (Linear/Log), 'Interval', 'Min Value', 'Max Value', 'Color', 'Field' (set to 'product name'), 'Max Colors' (100), and 'Legend Position' (Right). The main area displays a bar chart titled 'Count of Successful Requests' by 'category'. The categories are ARCADE, SHOOTER, SIMULATION, SPORTS, STRATEGY, and TEE. The Y-axis ranges from 0 to 4,000. A legend on the right lists various product names. A 'Save As...' button is highlighted with a red circle '1', and a dropdown menu is open with 'Report' selected, highlighted with a red circle '2'. To the right, a 'Save As Report' dialog box is open, showing the title 'sales_report_purchasesByCategory', a description field with 'optional' entered, and a 'Time Range Picker' set to 'Yes'. The 'Save' button is highlighted with a red circle '4'. A red circle '3' is also present near the description field.

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Saving a Pivot (cont.)

When you click **View**, the report is displayed with a Time Range Picker

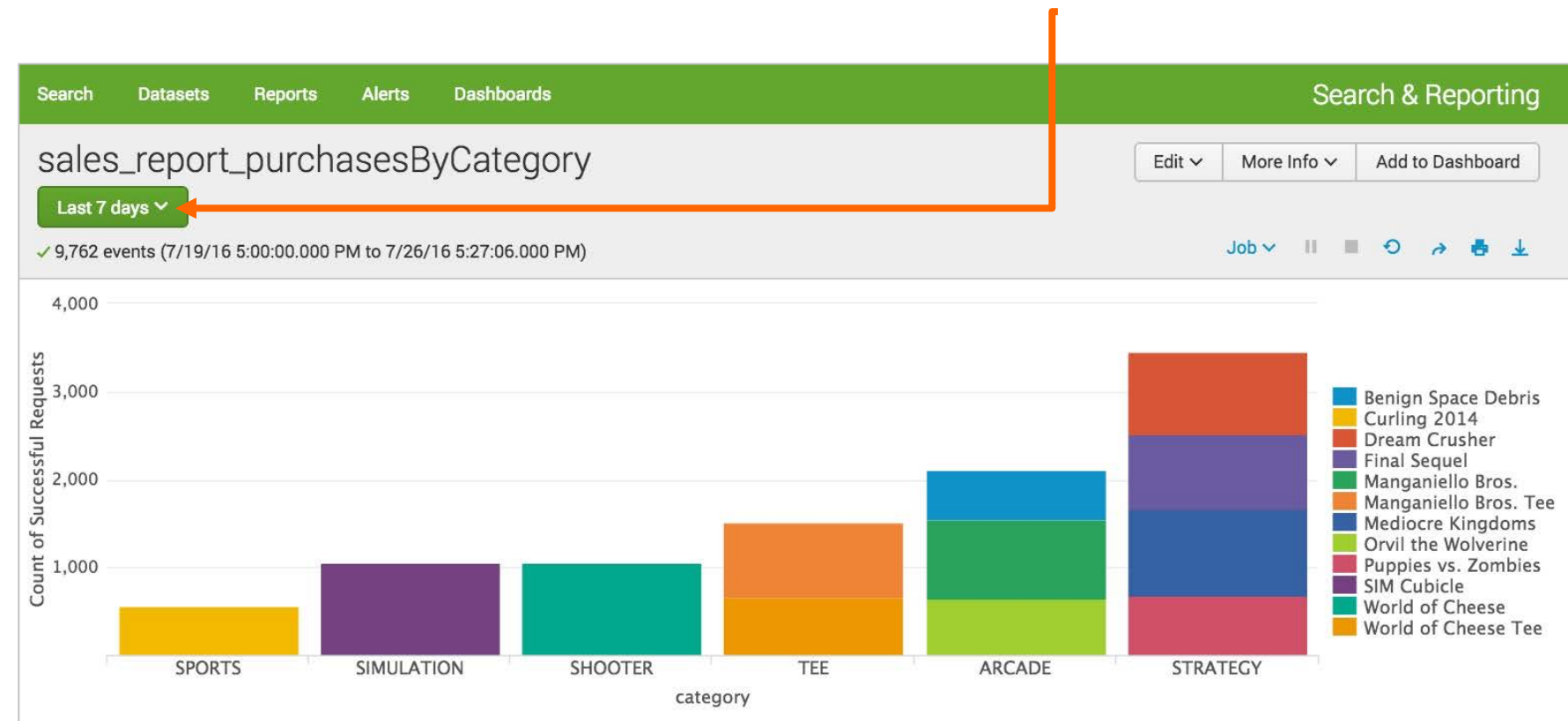
Your Report Has Been Created ✕

You may now view your report, add it to a dashboard, change additional settings, or continue editing it.

Additional Settings:

- [Permissions](#)
- [Schedule](#)
- [Embed](#)

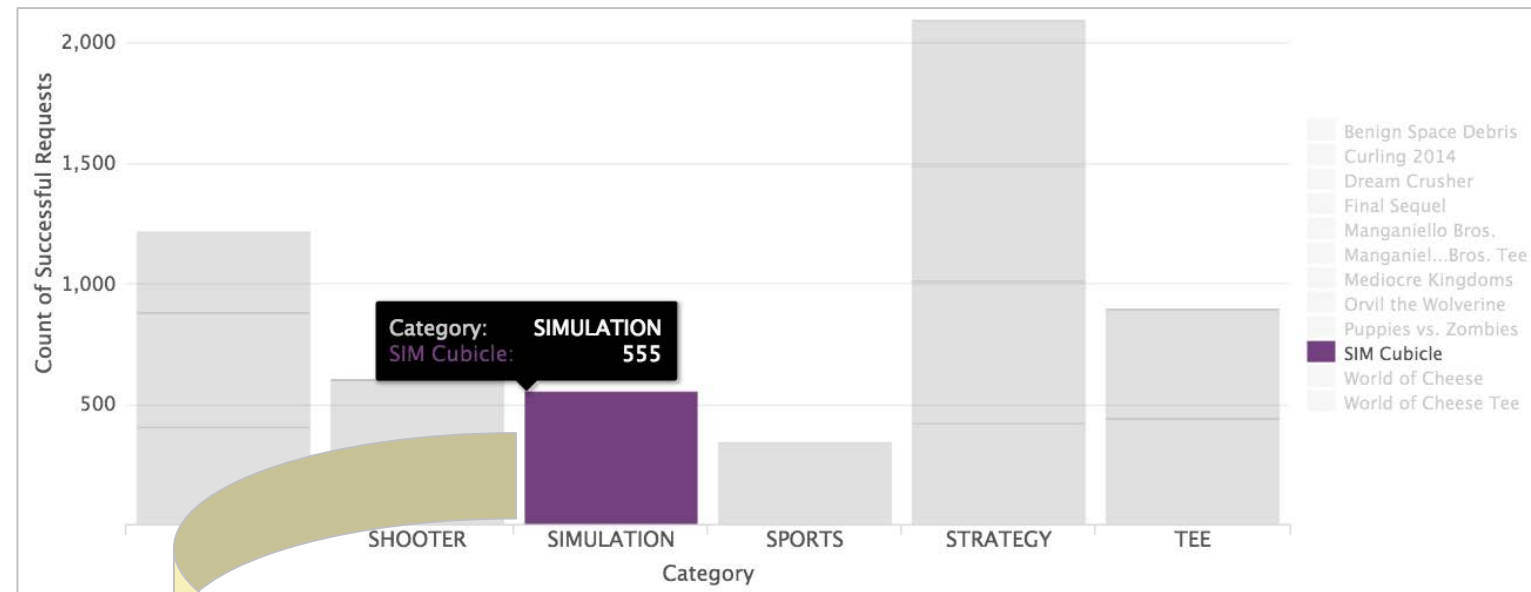
[Continue Editing](#) [Add to Dashboard](#) [View](#)



Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Mouse Actions

- Mouse over an object to reveal its details
- If drilldown is enabled (default), it is possible to click on the object to expose the underlying search



New Search

```
(index=* OR index=*) (sourcetype=access_* productId="*") (categoryId!=ACCESSORIES) | search (status=200) | eval is_successful_purchase=if(searchmatch("action=purchase"),1,0), is_not_successful_purchase=1-is_successful_purchase, is_successful_add_to_cart=if(searchmatch("action=addtocart"),1,0), is_not_successful_add_to_cart=1-is_successful_add_to_cart, is_successful_remove=if(searchmatch("action=remove"),1,0), is_not_successful_remove=1-is_successful_remove | rename action AS http_request.action categoryId AS http_request.categoryId price AS http_request.price product_name AS http_request.product_name productId AS http_request.productId status AS http_request.status is_successful_purchase AS http_request.successful_request.is_successful_purchase is_not_successful_purchase AS http_request.successful_request.is_not_successful_purchase is_successful_add_to_cart AS http_request.successful_request.is_successful_add_to_cart is_not_successful_add_to_cart AS http_request.successful_request.is_not_successful_add_to_cart is_successful_remove AS http_request.successful_request.is_successful_remove is_not_successful_remove AS http_request.successful_request.is_not_successful_remove | search "http_request.categoryId=SIMULATION" "http_request.product_name="SIM Cubicle"
```

555 events (8/18/16 8:00:00.000 PM to 8/25/16 8:28:09.000 PM) No Event Sampling

Events (555) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

2 events at 4 AM on Thursday, August 25, 2016

Time	Event
8/25/16 8:15:18.000 PM	89.11.192.18 - - [25/Aug/2016:20:15:18] "GET /category.screen?categoryId=SIMULATION&JSESSIONID=SD1SL5FF4ADFF4955 HTTP/1.1" 200 3809 "http://www.buttercupgames.com/product.screen?productId=SC-MG-G10" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)" 126

Note

The search generated by drilldown may be more detailed than your original search. However, it produces the same results.

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Instant Pivot Overview

- Instant pivot allows you to utilize the pivot tool without a preexisting data model
 - Instant pivot creates an underlying data model utilizing the search criteria entered during the initial search
- How to create an Instant Pivot
 1. Execute a search (search criteria only, no search commands)
 2. Click the **Statistics** or **Visualization** tab
 3. Click the **Pivot** icon
 4. Select the fields to be included in the data model object
 5. Create the pivot (table or chart)

Open Instant Pivot

The screenshot shows the Splunk Search & Reporting interface. At the top, the search bar contains the query `action=purchase` (marked with a red circle 1). Below the search bar, the results show 615 events. The 'Statistics' tab is selected (marked with a red circle 2), and a message states: "Your search isn't generating any statistic or visualization results. Here are some possible ways to get results." A 'Pivot' icon (marked with a red circle 3) is highlighted, and a dialog box titled 'Fields' is open. The dialog asks "Which fields would you like to use as a Data Model?" and has three options: "All Fields (46)" (marked with a red circle 4), "Selected Fields (4)", and "Fields with at least 9 % coverage (43)". The "All Fields (46)" option is selected. The dialog also has 'Cancel' and 'OK' buttons.

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Saving a Pivot as a Report

Save As Report

Title: sales_report_purchases

Description: optional

Time Range Picker: Yes No

You **2**st save the original search as a data model. This will power the report.

Model Title: purchase data model

Model ID?: purchase_data_model
Can only contain letters, numbers and underscores.

Cancel **3** Save

Note

It is is not recommended to manually change the Model ID.

New Pivot

Save As... Clear Edit Dataset

Report **1**

Dashboard Panel

Filters: Yesterday

Split Rows: +

Split Columns: host

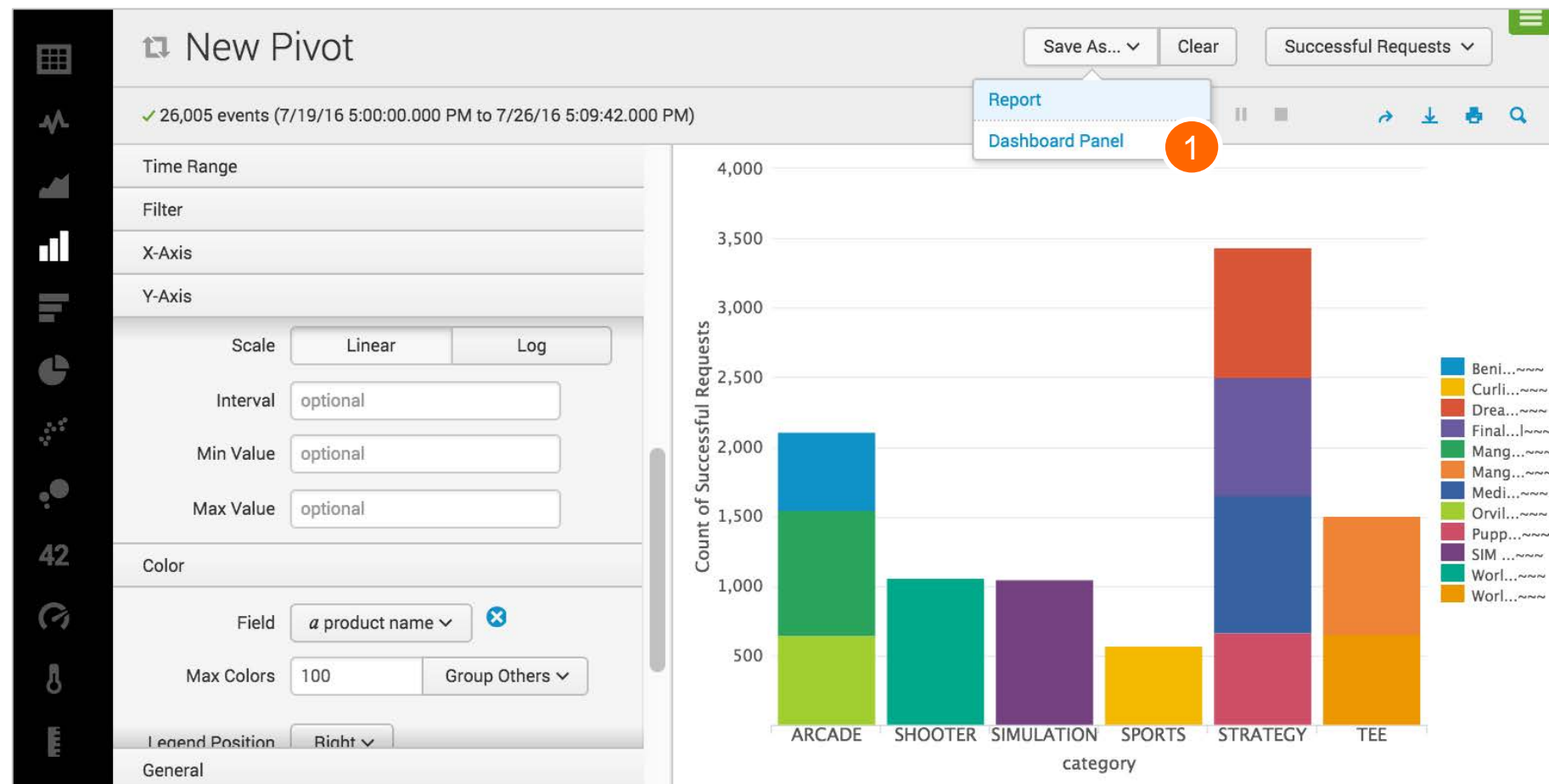
Column Values: Count of 1469554...

- When saving as a report, the **Model Title** is required
 - This is used to create a data model, which is required by the pivot report
- The **Model ID** is automatically generated based on the **Model Title**

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Add a Pivot to a Dashboard

Similarly, you can save any pivot to a new or existing dashboard



The screenshot shows the 'Save As Dashboard Panel' dialog box. It has a close button (X) in the top right. The 'Dashboard' section has 'New' and 'Existing' buttons, and a dropdown menu showing 'Buttercup Sales Week'. The 'Panel Title' section has an 'optional' text input field. The 'Panel Powered By' section has 'Inline Search' and 'Report' buttons. The 'Panel Content' section has 'Statistics' and 'Pie Chart' buttons. At the bottom, there are 'Cancel' and 'Save' buttons, with the 'Save' button circled in red with the number 3.

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Module 12: Creating and Using Lookups

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Module Objectives

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

Describing Lookups

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

1/25/16 Jan 25 2016 17:46:5
11:42:07.000 AM Address=1.1.1.R2
Address_Description=San Francisco
Device=Proximity Reader
Event_Description=Access Granted: Door Used
rfid=564931543224
Collapse

Event Actions ▾

Type	Field	Value
Selected	host	badgesv1
	source	/opt/log/badgesv1
	sourcetype	history_access
Event	Address	1.1.1.R2
	Address_Description	San Francisco
	Device	Proximity
	Event_Description	Access
	eventtype	nix-all-logs
	index	main
	linecount	6
	rfid	564931543224
	splunk_server	ip-10-222-134-157
	timestamp	none
Time	_time	2016-01-25T11:42:07.000-08:00
Default	punct	

Raw event data

1/25/16 Jan 25 2016 17:46:5
11:42:07.000 AM Address=1.1.1.R2
Address_Description=San Francisco
Device=Proximity Reader
Event_Description=Access Granted: Door Used
rfid=564931543224
Collapse

Event Actions ▾

Type	Field	Value
Selected	host	badgesv1
	source	/opt/log/badgesv1/history_access.log
	sourcetype	history_access
Event	Address	1.1.1.R2
	Address_Description	San Francisco
	Department	Products
	Device	Proximity
	Email	sscallion@buttercupgames.com
	Event_Description	Access
	First_Name	Shawn
	Last_Name	Scallion
	Username	sscallion
	eventtype	nix-all-logs
	index	main
	linecount	6
	rfid	564931543224
	splunk_server	ip-10-222-134-157
	timestamp	none
Time	_time	2016-01-25T11:42:07.000-08:00
Default	punct	

Data added from a lookup

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Describing Lookups (cont.)

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

Defining a File-based Lookup

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

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

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Lookup File – Example

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

```
GNU nano 2.3.1 File: products.csv
productId,product_name,categoryId,price,sale_price,Code
DB-SG-G01,Mediocre Kingdoms,STRATEGY,24.99,19.99,A
DC-SG-G02,Dream Crusher,STRATEGY,39.99,24.99,B
FS-SG-G03,Final Sequel,STRATEGY,24.99,16.99,C
WC-SH-G04,World of Cheese,SHOOTER,24.99,19.99,D
WC-SH-T02,World of Cheese Tee,TEE,9.99,6.99,E
PZ-SG-G05,Puppies vs. Zombies,STRATEGY,4.99,1.99,F
CU-PG-G06,Curling 2014,SPORTS,19.99,16.99,G
MB-AG-G07,Manganiello Bros.,ARCADE,39.99,24.99,H
MB-AG-T01,Manganiello Bros. Tee,TEE,9.99,6.99,I
FI-AG-G08,Orvil the Wolverine,ARCADE,39.99,24.99,J
BS-AG-G09,Benign Space Debris,ARCADE,24.99,19.99,K
SC-MG-G10,SIM Cubicle,SIMULATION,19.99,16.99,L
WC-SH-A01,Holy Blade of Gouda,ACCESSORIES,5.99,2.99,M
WC-SH-A02,Fire Resistance Suit of Provolone,ACCESSORIES,3.99,1.99,N
```

Creating a Lookup Table

Settings > Lookups > Lookup table files

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

Add new
Lookups > Lookup table files > Add new

Destination app *
search

Upload a lookup file
Browse... products.csv

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

Destination filename *
products.csv

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

Cancel Save

inputlookup Command

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

Note



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

The screenshot shows a Splunk search interface for a new search named 'inputlookup products.csv'. The search was performed on 7/12/16 from 10:00:00 AM to 7/13/16 at 10:38:52 AM, resulting in 14 records. The interface includes tabs for Events, Patterns, Statistics (14), and Visualization. Below the tabs are options for '100 Per Page', 'Format', and 'Preview'. The main content is a table with the following columns: Code, categoryId, price, productId, product_name, and sale_price. The table contains 14 rows of data, each representing a different product category and its associated items.

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

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Creating a Lookup Definition

Settings > Lookups > Lookup definitions

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

The screenshot shows the 'Add new' dialog in Splunk. The breadcrumb trail is 'Lookups > Lookup definitions > Add new'. The dialog contains the following fields and options:

- Destination app:** A dropdown menu with 'search' selected. A red circle with the number '2' is next to it.
- Name *:** A text input field containing 'product_lookup'. A red circle with the number '3' is next to it.
- Type:** A dropdown menu with 'File-based' selected. A red circle with the number '4' is next to it.
- Lookup file *:** A dropdown menu with 'products.csv' selected. A red circle with the number '5' is next to it.
- Below the 'Lookup file *' field, there is a link: 'Create and manage lookup table files.'
- There are two checkboxes: 'Configure time-based lookup' and 'Advanced options', both of which are unchecked.
- At the bottom, there is a 'Cancel' button on the left and a green 'Save' button on the right. A red circle with the number '6' is next to the 'Save' button.

Applying Advanced Options

Under Advanced Options, you can specify:

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

Configure time-based lookup

Advanced options

Minimum matches

1

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

Maximum matches

Enter a number from 1-1000 to specify the maximum number of matches for each

Default matches

other

If fewer than the minimum number of matches are present for any given input, wr

Cancel

Lookup Command

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

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

Examples

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

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

Using the Lookup Command

Search interface showing a query: `index=web sourcetype=access* action=purchase | lookup product_lookup productID OUTPUT price product_name | stats sum(price) as sales by product_name`. The results table displays product names and their corresponding sales values for the last 24 hours.

Scenario: Calculate the sales for each product in the last 24 hours.

product_name	sales
Benign Space Debris	374.85
Curling 2014	599.70
Dream Crusher	799.80
Final Sequel	674.73
Fire Resistance Suit of Provolone	111.72
Holy Blade of Gouda	77.87
Manganiello Bros.	759.81
Manganiello Bros. Tee	209.79
Mediocre Kingdoms	699.72
Orvil the Wolverine	559.86
Puppies vs. Zombies	79.84
SIM Cubicle	359.82
World of Cheese	499.80
World of Cheese Tee	159.84

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Creating an Automatic Lookup

Settings > Lookups > Automatic lookups > New

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

Add new
Lookups » Automatic lookups » Add new

Destination app *
1 search

Name *
2 product_auto_lookup

Lookup table *
3 product_lookup

Apply to *
4 sourcetype

named *
access_combine

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Creating an Automatic Lookup (cont.)

5. Define the Lookup input fields

- Field(s) that exist in your events that you are relating to the lookup table
 - A. Column name in CSV
 - B. Field name in Splunk, if different from column name

6. Define the Lookup output fields

- Field(s) from your lookup table that are added to the events
 - C. Field name in lookup table
 - D. Name you want displayed in Splunk; otherwise it inherits the column name

7. Save

Lookup input fields

A productid B Delete

column name in lookup field name in Splunk

file

Lookup output fields

C categoryid D Delete

price = Delete

product_name = Delete

sale_price = Delete

Add another field

Overwrite field values

Cancel Save

Using the Automatic Lookup

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

The screenshot shows a Splunk search interface. The search bar contains the query: `index=web sourcetype=access* action=purchase productId=* | stats sum(price) as sales by productId product_name`. The fields `sum(price)` and `product_name` are highlighted with green boxes. Below the search bar, there are two tables. The top table shows event logs with columns `i`, `Time`, and `Event`. The bottom table is a summary table with columns `productId`, `product_name`, and `sales`. Green arrows point from the highlighted fields in the search bar to the corresponding columns in the summary table.

productId	product_name	sales
BS-AG-G09	Benign Space Debris	499.80
CU-PG-G06	Curling 2014	259.87
DB-SG-G01	Mediocre Kingdoms	824.67
DC-SG-G02	Dream Crusher	799.80
FI-AG-G08	Orvil the Wolverine	519.87

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Time-based Lookups

- If a field in the lookup table represents a timestamp, you can create a time-based lookup
- In this example, the search retrieved events for February and March and calculated the sales based on the correct unit price for those dates.

products.csv

PRODUCTTIME	productId	product_name	categoryId	price	sale_price
1/1/10	DB-SG-G01	Mediocre Kingdoms	STRATEGY	24.99	19.99
1/1/10	DC-SG-G02	Dream Crusher	STRATEGY	39.99	24.99
1/1/10	FS-SG-G03	Final Sequel	STRATEGY	24.99	16.99
1/1/10	WC-SH-G04	World of Cheese	SHOOTER	24.99	19.99
1/1/10	WC-SH-T02	World of Cheese Tee	TEE	9.99	6.99
1/1/10	PZ-SG-G05	Puppies vs. Zombies	STRATEGY	4.99	1.99
1/1/10	CU-PG-G06	Curling 2014	SPORTS	19.99	16.99
1/1/10	MB-AG-G07	Manganiello Bros.	ARCADE	39.99	24.99
1/1/10	MB-AG-T01	Manganiello Bros. Tee	TEE	9.99	6.99
1/1/10	FI-AG-G08	Orvil the Wolverine	ARCADE	39.99	24.99
1/1/10	BS-AG-G09	Benign Space Debris	ARCADE	24.99	19.99
3/1/16	DB-SG-G01	Mediocre Kingdoms	STRATEGY	26.55	21.55
3/1/16	DC-SG-G02	Dream Crusher	STRATEGY	41.55	36.55
3/1/16	FS-SG-G03	Final Sequel	STRATEGY	26.55	21.55
3/1/16	WC-SH-G04	World of Cheese	SHOOTER	26.55	21.55
3/1/16	WC-SH-T02	World of Cheese Tee	TEE	11.55	8.55
3/1/16	PZ-SG-G05	Puppies vs. Zombies	STRATEGY	5.55	2.55
3/1/16	CU-PG-G06	Curling 2014	SPORTS	21.55	18.55
3/1/16	MB-AG-G07	Manganiello Bros.	ARCADE	41.55	26.55
3/1/16	MB-AG-T01	Manganiello Bros. Tee	TEE	11.55	8.55
3/1/16	FI-AG-G08	Orvil the Wolverine	ARCADE	41.55	26.55
3/1/16	BS-AG-G09	Benign Space Debris	ARCADE	26.55	21.55

product_name	Month	price	count	sales	SubTotal Sales
Benign Space Debris	Feb	24.99	402	10,045.98	
Benign Space Debris	Mar	26.55	548	14,549.40	
Benign Space Debris Subtotal					24,595.38
Curling 2014	Feb	19.99	420	8,395.80	
Curling 2014	Mar	21.55	575	12,391.25	
Curling 2014 Subtotal					20,787.05
Dream Crusher	Feb	39.99	691	27,633.09	
Dream Crusher	Mar	41.55	852	35,400.60	
Dream Crusher Subtotal					63,033.69
Final Sequel	Feb	24.99	513	12,819.87	
Final Sequel	Mar	26.55	766	20,337.30	
Final Sequel Subtotal					33,157.17

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Configuring Time-based Lookups

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

Note



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

Configure time-based lookup

Name of time field *

1 PRODUCTTIME

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

Time format

2 %m-%d-%Y

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

Minimum offset

3

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

Maximum offset


4

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

Advanced options

Using the Lookup as a Dataset

- A lookup is categorized as a dataset
 - Manage
 - Pivot
 - View the lookup in a search (`inputlookup`)

 **Datasets**

Use the Datasets listing page to view and manage your existing datasets. Click a dataset name to view its contents. Click Pivot to design a visualization-rich report based on the dataset. Click Explore in Search to extend a dataset in Search and save it as a new report, alert, or dashboard panel.

[Learn more about Datasets.](#)

29 Datasets

All Yours **This App's** Filter by title, description, fields

<i>i</i>	Title ^	Type	Actions	Owner	App	Sharing
>	geo_attr_countries	lookup definition	Manage ▾ Pivot Explore in Search	nobody	search	Global
>	geo_attr_countries.csv	lookup table file	Manage ▾ Pivot Explore in Search	nobody	search	Global
>	geo_attr_us_states	lookup definition	Manage ▾ Pivot Explore in Search	nobody	search	Global
>	geo_attr_us_states.csv	lookup table file	Manage ▾ Pivot Explore in Search	nobody	search	Global

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Additional Lookup Options

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

- Populate a lookup table with search results
 - `outputlookup` is discussed in more detail in the *Advanced Searching & Reporting* class
- Define a field lookup based on an external command; Python- and binary-based scripts
 - For more information, see the *Knowledge Manager Manual*
docs.splunk.com/Documentation/Splunk/latest/Knowledge/Addfieldsfromexternaldatasources
- Use the Splunk DB Connect app to create lookups with data from external SQL databases

Additional Lookup Options (cont.)

- Use Geospatial lookups to create queries that can be used to generate choropleth map visualizations

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

- Populate events with fields from an App Key Value Store (KV Store) collection

- KV Store lookups can only be invoked through REST endpoints or by using search commands such as lookup, inputlookup, and outputlookup; therefore, cannot be set up as automatic

- For more information, see the *Knowledge Manager Manual*

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

Module 13: Creating Scheduled Reports and Alerts

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Module Objectives

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

Using Scheduled Reports

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

Creating a Scheduled Report

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

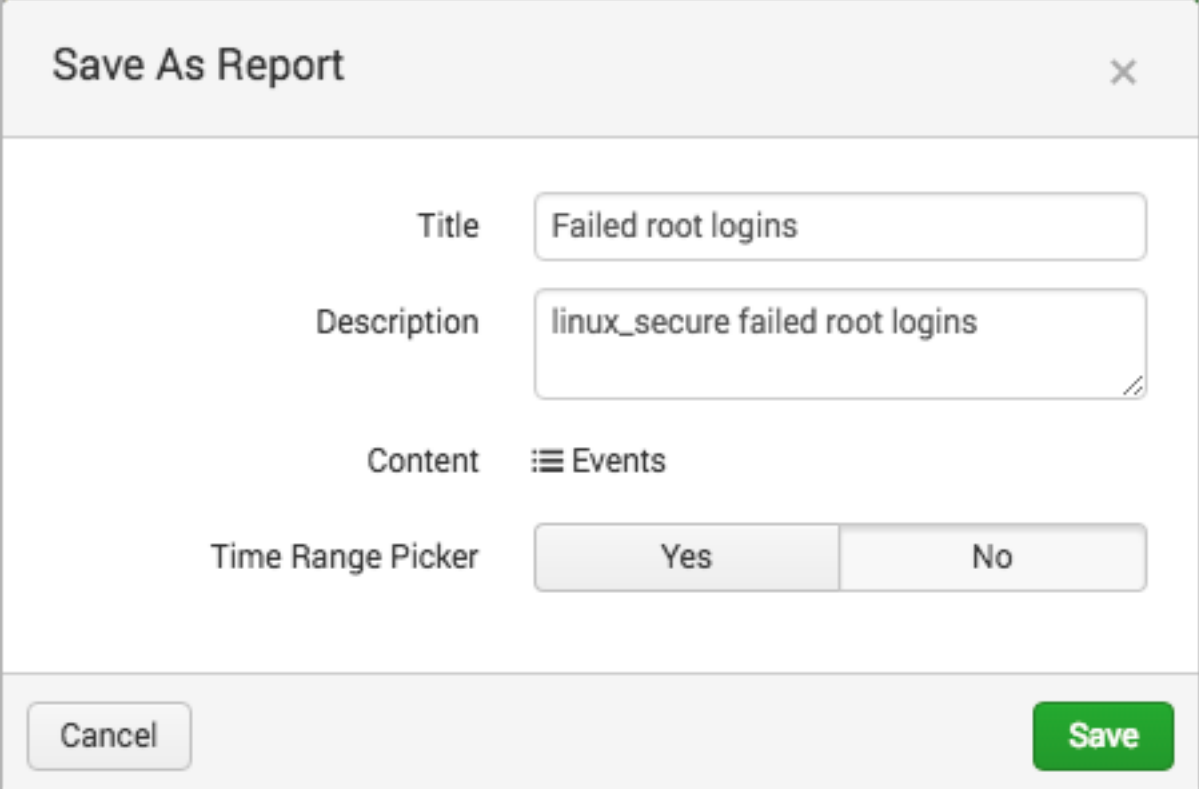
The screenshot shows the Splunk search interface. At the top, the search bar contains the query: `index=web OR index=security fail* root`. Below the search bar, it indicates 210 events were found for the time range 8/17/16 10:00:00.000 AM to 8/18/16 10:11:05.000 AM. A 'Save As' dropdown menu is open, with 'Report' selected. Below the search results, there is a visualization showing a timeline of events. The table below the visualization shows two failed login events for root.

i	Time	Event
>	8/18/16 9:45:08.000 AM	Thu Aug 18 2016 16:45:08 www2 sshd[4167]: Failed password for root from 91.214.92.22 port 4499 ssh2 eventtype = error error eventtype = failed_login eventtype = failed_privileged_logins eventtype = sshd_authentication authentication remote eventtype = nix-all-logs eventtype = nix_errors error host = www2 port = 4499 source = /opt/log/www2/secure.log sourcetype = linux_secure tag = authentication tag = error tag = privileged tag = remote
>	8/18/16 9:42:43.000 AM	Thu Aug 18 2016 16:42:43 www1 sshd[3438]: Failed password for root from 91.208.184.24 port 2820 ssh2 eventtype = error error eventtype = failed_login eventtype = failed_privileged_logins eventtype = sshd_authentication authentication remote eventtype = nix-all-logs eventtype = nix_errors error host = www1 port = 2820 source = /opt/log/www1/secure.log sourcetype = linux_secure tag = authentication tag = error tag = privileged tag = remote

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Creating a Scheduled Report (cont.)

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



Save As Report

Title: Failed root logins

Description: linux_secure failed root logins

Content: Events

Time Range Picker: Yes No

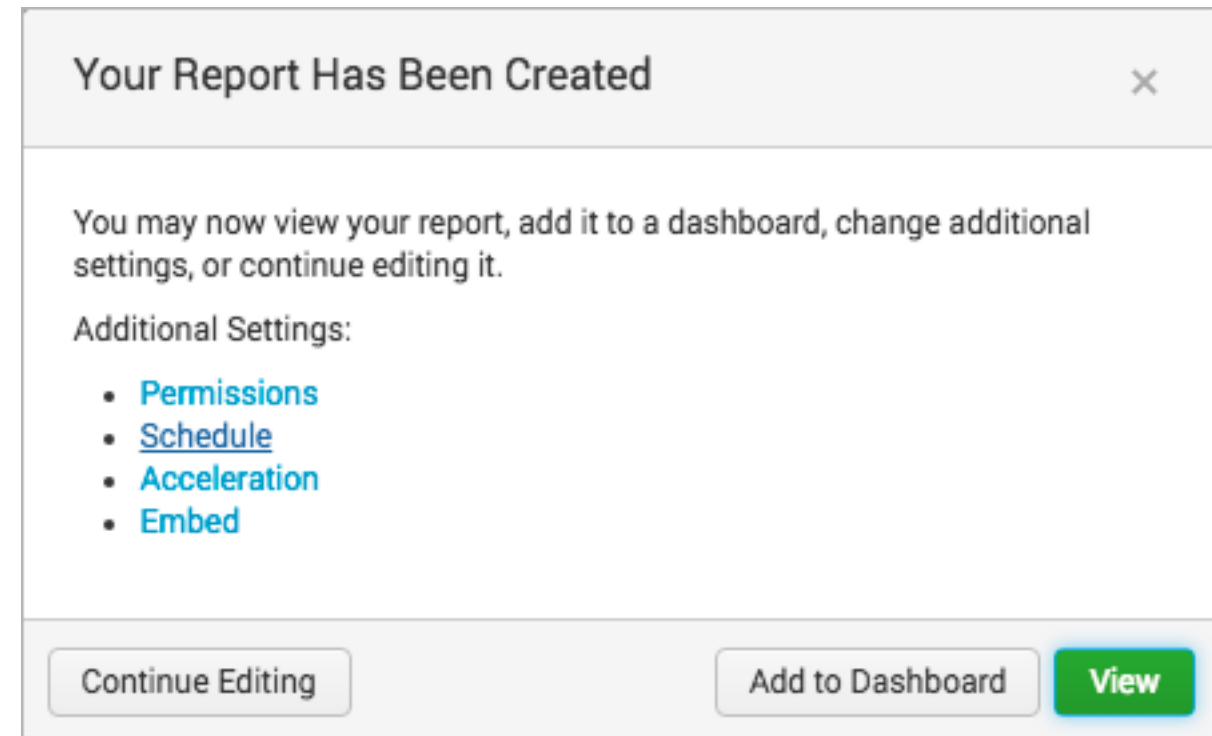
Cancel Save

Note

When you schedule a report, the Time Range Picker will not be available.

Creating a Scheduled Report (cont.)

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



Your Report Has Been Created ×

You may now view your report, add it to a dashboard, change additional settings, or continue editing it.

Additional Settings:

- [Permissions](#)
- [Schedule](#)
- [Acceleration](#)
- [Embed](#)

[Continue Editing](#) [Add to Dashboard](#) [View](#)

Creating a Scheduled Report – Define Schedule

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

The screenshot shows the 'Edit Schedule' dialog box for a report named 'Failed root logins'. The 'Schedule Report' checkbox is checked. The 'Schedule' dropdown is set to 'Run every week'. The 'On' dropdown is set to 'Monday' and the 'at' dropdown is set to '0:00'. The 'Time Range' dropdown is set to 'Last 7 days' and the 'Schedule Window?' dropdown is set to '5 minutes'. There are 'Cancel' and 'Next' buttons at the bottom.

Creating a Scheduled Report – Select Time Range

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

The screenshot shows the 'Edit Schedule' dialog box for a report titled 'Failed root logins'. The 'Schedule Report' checkbox is checked. The schedule is set to 'Run every week' on 'Monday' at '0:00'. The 'Time Range' is currently set to 'Last 7 days'. A green box highlights the 'Time Range' dropdown, and a green arrow points to the 'Select Time Range' dialog box. The 'Select Time Range' dialog shows a list of presets under the 'Relative' section, including 'Last 15 minutes', 'Last 60 minutes', 'Last 4 hours', 'Last 24 hours', 'Last 7 days', and 'Last 30 days'. There is also an 'Other' section with 'All time'. The 'Back' button is visible at the bottom of the dialog.

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Creating a Scheduled Report – Schedule Window

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

The screenshot shows the 'Edit Schedule' dialog box for a report named 'Failed root logins'. The 'Schedule Report' checkbox is checked. The 'Schedule' is set to 'Run every week', 'On' is 'Monday' at '0:00', and 'Time Range' is 'Last 7 days'. The 'Schedule Window' dropdown is highlighted with a green border and shows a list of options: Auto, No window, 5 minutes (selected), 15 minutes, 30 minutes, 1 hour, 2 hours, 4 hours, 8 hours, and Custom. A 'Cancel' button is visible on the left.

Creating a Scheduled Report – Enable Actions

- **Enable Actions**

- **Send Email:** When a report runs, an email is sent to the specified recipient(s)
- **Run a script:** A script is launched when a report runs

Learn More '. At the bottom of the dialog, there are two buttons: 'Back' on the left and 'Save' on the right."/>

Edit Schedule

Enable Actions

Send Email

Run a Script

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

Back Save

Creating a Scheduled Report – Send Email

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

Edit Schedule [X]

Enable Actions

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

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

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

Subject

Message

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

Type

Run a Script

[Back](#) [Save](#)

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Creating a Scheduled Report – Run a Script

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

Note



The proper permissions for your Splunk server are required to upload your script to this Splunk directory.

Edit Schedule

Enable Actions

Send Email

To

Email Priority

Subject

Message

Include Link to Report Link to Results
 Search String Inline
 Attach CSV Attach PDF

Type

Run a Script

Filename

Located in `$SPLUNK_HOME/bin/scripts` or `$SPLUNK_HOME/etc/search/bin/scripts`

Managing Reports – Edit Permissions

Display For determines who sees the scheduled report

Reports

Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Pivot or Search to refine the parameters or further explore the data.

3 Reports

All Yours This App's filter

i	Title ^	Actions	Owner	App	Sharing	Embedding
>	Failed logins	Open in Search Edit	cfarrell	search	Private	Disabled
>	Failed root logins	Open in Search Edit	cfarrell	search	Private	Disabled
>	Weekly T-shirt Sales	Open i Edit Description Edit Permissions Edit Schedule Edit Acceleration Clone Embed Delete	cfarrell	search	Private	Disabled

Edit Permissions

Report Failed root logins

Owner cfarrell

App search

Display For Owner App All apps

Run As Owner Learn More

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

Cancel Save

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Managing Reports – Edit Permissions (cont.)

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

The screenshot shows the 'Reports' section in Splunk. It contains a table with 3 reports. The 'Failed root logins' report is selected, and its 'Edit' dropdown menu is open, with 'Edit Permissions' highlighted. A green box highlights the 'Edit Permissions' option, and a green arrow points from it to the 'Edit Permissions' dialog box on the right.

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

The 'Edit Permissions' dialog box shows the report name 'Failed root logins', owner 'cfarrell', and app 'search'. The 'Display For' section has 'Owner' and 'App' buttons. The 'Run As' dropdown is set to 'Owner'. Below, there is a table for permissions for various roles.

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

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Managing Reports – Embed

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

The screenshot shows the Splunk Reports interface. A table lists reports with columns for Title, Actions, Owner, App, Sharing, and Embedding. The 'Failed logins' report is selected, and the 'Embed' option in the 'Actions' menu is highlighted. A dialog box titled 'Enable Report Embedding' is open, asking for confirmation to enable embedding. A green arrow points from the 'Embed' button to the dialog, and another green arrow points from the 'Enable Embedding' button in the dialog to the 'Embed' dialog box on the right. The 'Embed' dialog box contains a warning message, a text area with the embed code, and buttons for 'Disable Embedding' and 'Done'.

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

Enable Report Embedding

Are you sure you want to enable embedding for this report? An embedded report can be viewed by anyone with access to the web page(s) in which it is inserted.

Cancel Enable Embedding

Embed

Embedded Report will not have data until the scheduled search runs.

Copy and paste this code into your HTML-based web page.

```
<iframe height="636" width="480" frameborder="0" src="http://54.184.179.177/en-US/embed?s=%2FservicesNS%2Fcfarrell%2Fsearch%2Fsaved%2Fsearches%2FFailed%2520root%2520logins&oid=ysj0DUUnWD_ynve3Ll9lCr!%5EowLIA%5ERHU4z3rxrNeQE74cqmn3ofHb0Y5izPEtrZBDt%5EMGpq6KXrEZQu%5EqK2BHx5qsKWJeEsp"
```

Disable embedding if you no longer want to share this report outside of Splunk.

Disable Embedding Done

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Alerting Overview

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

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Creating an Alert

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

The screenshot shows the Splunk search interface. The search bar contains the query: `index=web sourcetype=access_combined status=50*`. Below the search bar, it indicates 159 events were found. A dropdown menu is open, showing options: Report, Dashboard Panel, Alert (highlighted with a green box), and Event Type. To the right, the 'Save As Alert' dialog box is open, with a green box highlighting the 'Settings' section. The 'Settings' section includes: Title: 'Web server errors', Description: 'Alerts when http status 50* events are returned', Permissions: 'Private' and 'Shared in App', Alert type: 'Scheduled' and 'Real-time', Trigger Conditions: 'Per-Result', Throttle: unchecked, and Trigger Actions: '+ Add Actions'. The dialog has 'Cancel' and 'Save' buttons at the bottom.

Setting Alert Permissions

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

The screenshot shows the 'Save As Alert' dialog box with the following settings:

- Title:** Web server errors
- Description:** Alerts when http status 50* events are returned
- Permissions:** Private and Shared in App (highlighted with a green box)
- Alert type:** Scheduled and Real-time
- Trigger Conditions:** Trigger alert when: Per-Result
- Throttle?** (checkbox is unchecked)
- Trigger Actions:** + Add Actions

Buttons at the bottom: Cancel (left), Save (right, green).

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Choosing Real Time or Scheduled Alert Type

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

- **Scheduled** alerts

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

- **Real-time** alerts

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

The screenshot shows the 'Save As Alert' dialog box. It has a title bar with 'Save As Alert' and a close button. The main content area is divided into sections: 'Settings', 'Trigger Conditions', and 'Trigger Actions'. Under 'Settings', there are fields for 'Title' (Web server errors) and 'Description' (Alerts when http status 50* events are returned). There are two buttons for 'Permissions': 'Private' and 'Shared in App'. The 'Alert type' section has two buttons: 'Scheduled' and 'Real-time', with 'Scheduled' selected and highlighted by a green box. Under 'Trigger Conditions', there is a dropdown for 'Trigger alert when' set to 'Per-Result' and a checkbox for 'Throttle?' which is unchecked. Under 'Trigger Actions', there is a button '+ Add Actions'. At the bottom, there are 'Cancel' and 'Save' buttons.

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Setting the Alert Type – Scheduled

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

Save As Alert

Settings

Title: Web server errors

Description: Alerts when http status 50* events are returned

Permissions: Private | Shared in App

Alert type: Scheduled | Real-time

Run on Cron Schedule ▾

Earliest: - | 9 | 0 | 9 | *

Latest: | 9 | 0 | 9 | *

Cron Expression: *

- Run every hour e.g. -1h@h (1 hour ago, to the hour). [Learn More](#)
- Run every day e.g. -1h@h (1 hour ago, to the hour). [Learn More](#)
- Run every week e.g. -1h@h (1 hour ago, to the hour). [Learn More](#)
- Run every month e.g. -1h@h (1 hour ago, to the hour). [Learn More](#)
- ✓ Run on Cron Schedule e.g. 00 18 *** (every day at 6PM). [Learn More](#)

Setting Trigger Conditions – Scheduled

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

Save As Alert

Settings

Title: Web server errors

Description: Alerts when http status 50* events are returned

Permissions: Private Shared in App

Alert type: Scheduled Real-time

Run on Cron Schedule

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

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

Cron Expression: */5 * * * * e.g. 00 18 * * * (ev

Trigger Conditions

Trigger alert when: Number of Results

is greater than 2

Trigger: Once For each result

Throttle?

Trigger Actions

Cancel

Scenario

In this example, a scheduled search will run every 5 minutes.

Setting Trigger Conditions – Real-time

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

The screenshot shows the 'Save As Alert' dialog box in Splunk. The 'Alert type' is set to 'Real-time'. The 'Trigger Conditions' dropdown menu is open, showing the following options:

- Per-Result**
Triggers whenever search returns a result.
- Number of Results**
Triggers based on a number of search results during a rolling-window of time.
- Number of Hosts**
Triggers based on a number of hosts during a rolling-window of time.
- Number of Sources**
Triggers based on a number of sources during a rolling-window of time.
- Custom**
Triggers based on a custom condition during a rolling-window time.

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Setting Trigger Conditions – Real-time (cont.)

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

Save As Alert

Settings

Title: Web server errors

Description: Alerts when http status 50* events are returned

Permissions: Private Shared in App

Alert type: Scheduled Real-time

Trigger Conditions

Trigger alert when: Number of Results

is greater than: 2

in: 1 minute(s)

Trigger: Once For each result

Throttle?

Trigger Actions

+ Add Actions

Cancel Save

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Alert Actions – Trigger Conditions: Once

- **Once** executes actions *one time* for all matching events within the scheduled time and conditions
 - Example: If your alert is scheduled to run every 5 minutes, and 40 results are returned, the alert only triggers and executes actions one time
- Select the **Throttling** option to suppress the actions for results within a specified time range

The screenshot shows the 'Save As Alert' configuration window. The 'Description' field contains 'Alerts when http status 50* events are returned'. The 'Permissions' are set to 'Private'. The 'Alert type' is 'Scheduled'. The 'Run on Cron Schedule' dropdown is open. The 'Earliest' field is set to '-5m@m' and the 'Latest' field is '@m'. The 'Cron Expression' is '*/* * * * *'. The 'Trigger Conditions' section shows 'Trigger alert when' set to 'Number of Results' with a dropdown menu. The 'Trigger' dropdown is set to 'Once'. The 'Throttle' section is highlighted with a green box, showing 'Throttle?' checked and 'Suppress triggering for' set to '10 minute(s)'. The 'Trigger Actions' section has a '+ Add Actions' button. A 'Cancel' button is at the bottom left.

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Alert Actions – Trigger Conditions: For Each Result

- **For each result** – executes the alert actions once *for each result* that matches the conditions
- Select the **Throttling** option to suppress the actions for results that have the same field value, within a specified time range
 - Certain situations can cause a flood of alerts, when really you only want one
- In this example, the search runs every 5 minutes:
 - 70 events are returned in a 5 minute window
 - 50 events with status=**500** and 20 include status=**503**
 - 2 actions will trigger, once for each status

The screenshot shows the 'Save As Alert' configuration interface. The form includes the following fields and options:

- Description:** Alerts when http status 50* events are returned
- Permissions:** Private (selected) / Shared in App
- Alert type:** Scheduled (selected) / Real-time
- Run on Cron Schedule:** Run on Cron Schedule (dropdown)
- Earliest:** -5m@m (with example: e.g. -1h@h (1 hour))
- Latest:** @m (with example: e.g. -1h@h (1 hour))
- Cron Expression:** */5 **** (with example: e.g. 00 18 *** (every 5 minutes))
- Trigger Conditions:** Trigger alert when: Number of Results (dropdown) is greater than (dropdown) 2
- Trigger:** Once / For each result (selected and highlighted with a green box)
- Throttle? (checked):** Suppress results containing field value: status (highlighted with a green box)
- Suppress triggering for:** 10 minute(s) (dropdown) (highlighted with a green box)

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Add Trigger Actions

Add Actions

- **Add to Triggered Alerts** – adds the alert to the *Activity > Triggered alerts*
- **Log Event** – creates a log event to index and search
- **Run a script** – runs a script that can perform some other action
- **Send Email** – sends an email with results to recipients that you define
- **Webhook** – calls a rest endpoint using http post request

Save As Alert

Permissions: Private | Shared in App

Alert type: Scheduled | Real-time

Run on Cron Schedule ▾

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

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

Cron Expression: */5 **** | e.g. 00 18 *** (ev

Trigger Conditions

Trigger alert when: Number of Results ▾

is greater than ▾ | 2

Trigger: Once

Throttle?

Suppress results containing field value: status

Suppress triggering for: 10

Trigger Actions

+ Add Actions ▾

- Add to Triggered Alerts**
Add this alert to Triggered Alerts list
- Log Event**
Send log event to Splunk receiver endpoint
- Run a script**
Invoke a custom script
- Send email**
Send an email notification to specified recipients
- Webhook**
Generic HTTP POST to a specified URL

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Alert Actions – Triggered Alerts

Choose an appropriate severity for the alert

Save As Alert

Trigger Conditions

Trigger alert when is greater than in minute(s) Trigger

Throttle?

Suppress results containing field value

Suppress triggering for

Trigger Actions

+ Add Actions

When triggered Severity

- Info
- Low
- ✓ Medium
- High
- Critical

App Search & Reporting (search) Owner Administrator (a) Severity All Alert All

Showing 1-5 of 5 results

Time	Fired alerts	App	Type	Severity	Mode	Actions
<input type="checkbox"/> 2016-04-25 10:59:02 PDT	Login attempts	search	Real-time	Medium	Per Result	View results Edit search Delete
<input type="checkbox"/> 2016-04-25 10:57:48 PDT	Login attempts	search	Real-time	Medium	Per Result	View results Edit search Delete
<input type="checkbox"/> 2016-04-25 10:55:27 PDT	Login attempts	search	Real-time	Medium	Per Result	View results Edit search Delete
<input type="checkbox"/> 2016-04-25 10:55:01 PDT	Web server errors	search	Scheduled	Medium	Per Result	View results Edit search Delete
<input type="checkbox"/> 2016-04-25 10:50:01 PDT	Web server errors	search	Scheduled	Medium	Per Result	View results Edit search Delete

Select All | None Selected alerts Delete

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Alert Actions – Log Event

If you have *administrator privileges*, you can use a log event action

- **Event** – Enter the information that will be written to the event log
- **Source** – The name of the source (alert name is used by default)
- **Sourcetype** – The name of the sourcetype used in the alert
- **Host** – The IP address of the host of the alert
- **Index** – The target index for the log event (default value is main)

The screenshot shows the configuration for a 'Log Event' action. The 'When triggered' dropdown is set to 'Log Event'. The 'Event' field contains the text: '\$trigger_date\$ \$trigger_timeHMS\$ 50* web server errors sourcetype=\$result.sourcetype\$'. Below this is a link to 'Learn More'. The 'Source' field is 'alert:\$name\$'. The 'Sourcetype' field is 'access_combined'. The 'Host' field is empty. The 'Index' field is 'main'. At the bottom are 'Cancel' and 'Save' buttons.

Note

For a complete list of available tokens, go to: <http://docs.splunk.com/Documentation/Splunk/latest/Alert/EmailNotificationTokens>

Alert Actions – Log Event (cont.)

The image shows the configuration for a 'Log Event' action in Splunk. The configuration includes the following fields:

- Event:** \$trigger_date\$ \$trigger_timeHMS\$ 50* web server errors sourcetype=\$result.sourcetype\$
- Source:** alert:\$name\$
- Sourcetype:** access_combined
- Host:** (empty)
- Index:** main

The search results show a list of events with the following fields highlighted:

i	Time	Event
>	8/18/16 10:51:55.000 PM	2016-08-18 22:51:55 50* web server errors sourcetype=access_combined host = 127.0.0.1 source = alert:LogEvent sourcetype = access_combined
>	8/18/16 10:51:53.000 PM	2016-08-18 22:51:53 50* web server errors sourcetype=access_combined host = 127.0.0.1 source = alert:LogEvent sourcetype = access_combined
>	8/18/16 10:51:50.000 PM	2016-08-18 22:51:50 50* web server errors sourcetype=access_combined host = 127.0.0.1 source = alert:LogEvent sourcetype = access_combined

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Alert Actions – Send Email

Customize the content of email alerts

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

The screenshot shows the 'Save As Alert' configuration window for a 'Send email' action. The window is titled 'Save As Alert' and has a close button in the top right corner. Below the title bar, there is a '+ Add Actions' button. The main configuration area is divided into several sections:

- When triggered:** A dropdown menu is set to 'Send email' with a 'Remove' button to its right.
- To:** A text input field for email addresses. To the right, there is a note: 'Comma separated list of email addresses. Show CC and BCC'.
- Priority:** A dropdown menu currently set to 'Normal'.
- Subject:** A text input field containing 'Splunk Alert: \$name\$'.
- Message:** A text area containing 'The alert condition for '\$name\$' was triggered.' To the right, there is a note: 'The email subject and message can include tokens that insert text based on the results of the search. Learn More'.
- Include:** A section with two columns of checkboxes:
 - Column 1: Link to Alert, Search String, Trigger Condition, Trigger Time.
 - Column 2: Link to Results, Inline Table (with a dropdown arrow), Attach CSV, Attach PDF.
- Type:** Two buttons: 'HTML & Plain Text' (selected) and 'Plain Text'.

At the bottom of the window, there are 'Cancel' and 'Save' buttons.

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Alert Actions – Run a Script

- When an alert is triggered, you can launch a script

- Enter the name of the script
- All alert scripts need to reside in either of the following locations:

`$SPLUNK_HOME/bin/scripts`

`$SPLUNK_HOME/etc/apps/
<Appname>/bin/scripts`

Note ⓘ

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

The screenshot shows the configuration for an alert action. Under "Trigger Conditions", the alert is set to trigger when the "Number of Results" is "is greater than" 2, and it triggers "Once" (with "For each result" also visible). Under "Throttle", the "Throttle" checkbox is checked, and "Suppress results containing field value" is set to "status". The "Suppress triggering for" is set to "10" "minute(s)". Under "Trigger Actions", there is a "+ Add Actions" button. A single action is listed: "When triggered" (with a dropdown arrow), "Run a script" (with a code icon), and "Filename" set to "alertscript.py". A "Remove" button is to the right of the action. A note at the bottom right of the action box says "Located in \$SPLUNK_HOME/bin/scripts".

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Custom Alert Action - Example

- A custom alert action can be created or an admin can install and configure app from Splunkbase
- In this example, the HipChat Room Notification Alert app is used

Trigger Actions

+ Add Actions ▾

- Add to Triggered Alerts
Add this alert to Triggered Alerts list
- HipChat**
Send HipChat room notifications
- Run a script
Invoke a custom script
- Send email
Send an email notification to specified recipients
- Webhook
Generic HTTP POST to a specified URL

Trigger Actions

+ Add Actions ▾

When triggered

- HipChat
 - Room: Splunk_Alerts
 - Message: "\$result.user\$" has logged in unsuccessfully to linux_secure
 - Notification Style: Message
 - Card Attributes:
 - Message Format: Plain Text HTML
 - Message Color: Red
 - Notify users in the room
 - Auth Token: Xv9M0f92uF7Tw5fB6SBViiqlwA5i0mrl

HipChat

Search history

Splunk_Alerts
Failed login alerts

Splunk_S1	"myuan" has logged in unsuccessfully to linux_secure	3:30 PM
Splunk_S1	"myuan" has logged in unsuccessfully to linux_secure	3:32 PM
Splunk_S1	"djohnson" has logged in unsuccessfully to linux_secure	3:33 PM
Splunk_S1	"ftp" has logged in unsuccessfully to linux_secure	3:34 PM
Splunk_S1	"jira" has logged in unsuccessfully to linux_secure	3:35 PM
Splunk_S1	"djohnson" has logged in unsuccessfully to linux_secure	3:36 PM

Note



For more information about Custom Alerts, see docs.splunk.com/Documentation/Splunk/latest/AdvancedDev/ModAlertsIntro

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Viewing Triggered Alerts

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

The screenshot shows the Splunk web interface. At the top, the navigation bar includes 'splunk', 'Apps', and user options like 'c Farrell', 'Messages', 'Settings', 'Activity', and 'Help'. A search bar is on the right. Below the navigation, there are filters for 'App' (Search & Reporting), 'Owner' (c Farrell), 'Severity' (All), and 'Alert' (All). A dropdown menu is open over the 'Activity' link, showing 'Jobs' and 'Triggered Alerts' (which is highlighted with a green box). Below the filters, there are navigation links '«prev' and 'next»' and a search button. The main content area shows a table of triggered alerts with the following data:

	Time	Fired alerts	App	Type	Severity	Mode	Actions
<input type="checkbox"/>	2016-08-18 16:42:32 PDT	Failed login attempts	search	Real-time	High	Digest	View results Edit search Delete
<input type="checkbox"/>	2016-08-18 16:37:58 PDT	Failed login attempts	search	Real-time	High	Per Result	View results Edit search Delete
<input type="checkbox"/>	2016-08-18 16:20:37 PDT	Web server errors	search	Real-time	Medium	Per Result	View results Edit search Delete

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Editing Alerts

1. From the search bar, click **Alerts**
2. Select the alert and click **Edit**

The screenshot shows the Splunk Alerts page. The navigation bar at the top includes 'Search', 'Pivot', 'Reports', 'Alerts', and 'Dashboards'. The main content area is titled 'Alerts' and contains a table of alerts. The table has columns for 'Title', 'Actions', 'Owner', 'App', and 'Sharing'. Two alerts are listed: 'Failed login attempts by user admin' and 'Web server errors'. The 'Web server errors' alert is selected, and its 'Edit' dropdown menu is open, showing options like 'Edit Description', 'Edit Permissions', 'Edit Alert Type and Trigger Condition', 'Edit Actions', 'Disable', 'Clone', and 'Delete'. A green arrow points from the 'Alerts' tab in the navigation bar to the 'Edit' dropdown menu.

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

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Editing Alert Permissions

- Edit permissions
 - **Owner** – only you can access, edit, and view triggered alerts
 - **App** – users of the app can access, edit, and view triggered alerts

Alert has been saved

You can view your alert, change additional settings, or continue editing it.

Additional Settings:

- **Permissions**
- Alert type & triggers
- Actions

Continue Editing

View Alert

Edit Permissions

Alert: Web server errors

Owner: cfarrell

App: search

Display For: Owner App All apps

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

Cancel Save

Generated for Subbaiah Kandula (9722122) (C) Splunk Inc, not for distribution

Support Programs

- **Community**

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

- **Global Support**

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

- **Phone:** (855) SPLUNK-S or (855) 775-8657
- **Web:** http://www.splunk.com/index.php/submit_issue

- **Enterprise Support**

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