

splunk[®]>

Outline

Module 1: Introducing Splunk

Module 2: Splunk Components

Module 3: Installing Splunk

Module 4: Getting Data In

Module 5: Basic Search

Module 6: Using Fields

Module 7: Best Practices

Module 8: Splunk's Search Language

Module 9: Transforming Commands

Module 10: Creating Reports and Dashboards

Module 11: Pivot and Datasets

Module 12: Creating and Using Lookups

Module 13: Creating Scheduled Reports and Alerts

Module 1

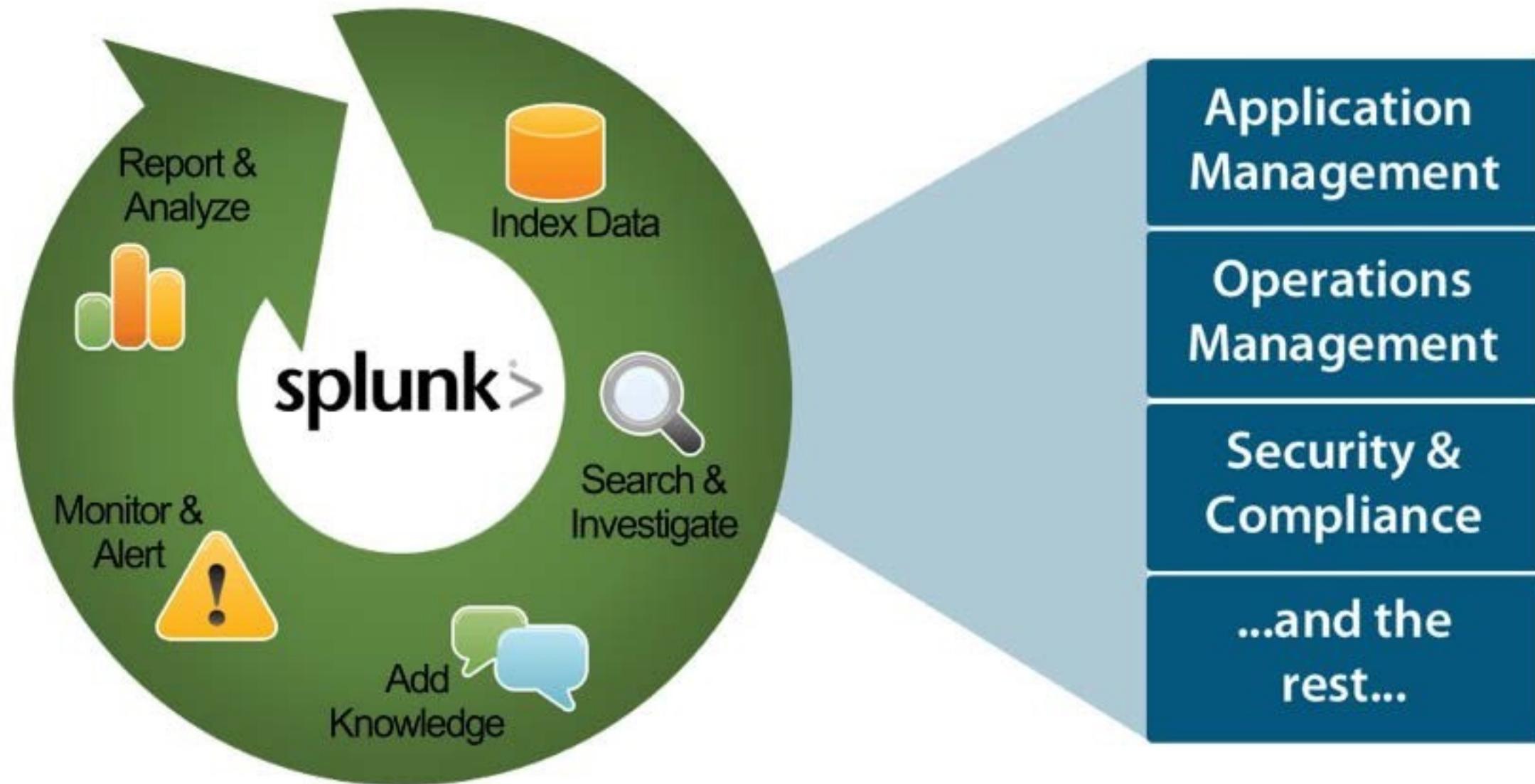
Introducing Splunk

Understanding Splunk



- What Is Splunk?
- What Data?
- How Does Splunk Work?
- How Is Splunk Deployed?
- What are Splunk Apps?
- What are Splunk Enhanced Solutions?

What Is Splunk?



Aggregate, analyze, and get answers from your machine data

What Data?

Index **ANY** data from **ANY** source



- Computers
- Network devices
- Virtual machines
- Internet devices
- Communication devices
- Sensors
- Databases

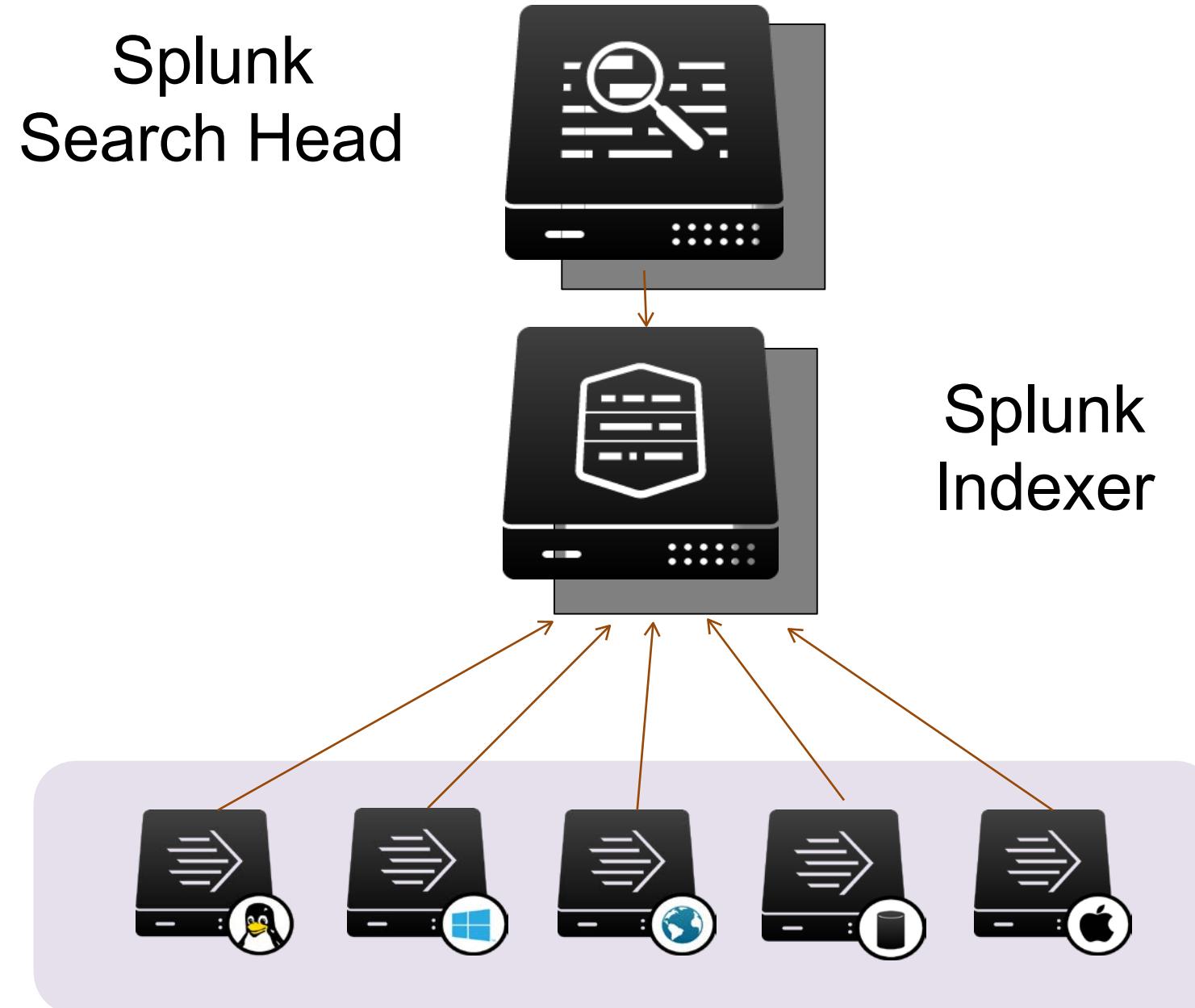
Note

For **lots** of ideas on data to collect in your environment, get the Splunk publication [The Essential Guide to Machine Data](#).



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

How Does Splunk Work?



How Is Splunk Deployed?

- Splunk Enterprise
 - Splunk components installed and administered on-premises



- Splunk Cloud
 - Splunk Enterprise as a scalable service
 - No infrastructure required



- Splunk Light
 - Solution for small IT environments



What are Splunk Apps?

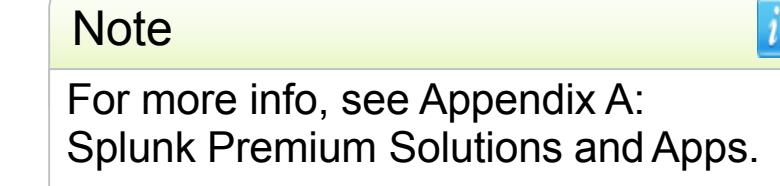
- Designed to address a wide variety of use cases and to extend the power of Splunk
- Collections of files containing data inputs, UI elements, and/or knowledge objects
- Allows multiple workspaces for different use cases/user roles to co-exist on a single Splunk instance
- 1000+ ready-made apps available on Splunkbase (splunkbase.com) or admins can build their own



What are Splunk Enhanced Solutions?

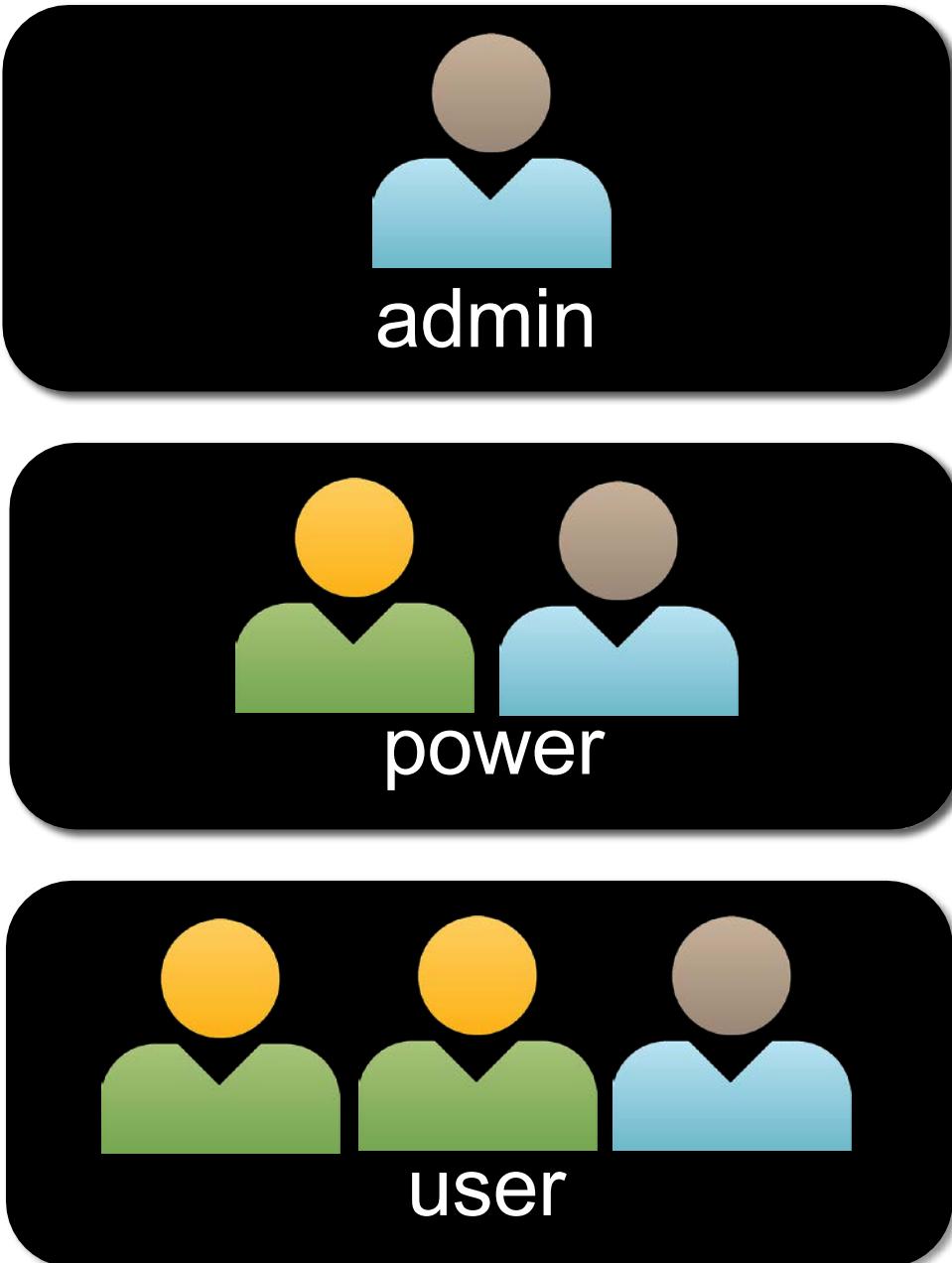
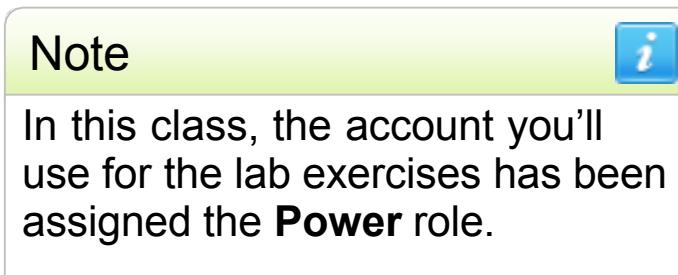
- **Splunk IT Service Intelligence (ITSI)**
 - Next generation monitoring and analytics solution for IT Ops
 - Uses machine learning and event analytics to simplify operations and prioritize problem resolution
- **Splunk Enterprise Security (ES)**
 - Comprehensive Security Information and Event Management (SIEM) solution
 - Quickly detect and respond to internal and external attacks
- **Splunk User Behavior Analytics (UBA)**

Finds known, unknown, and hidden threats by analyzing user behavior and flagging unusual activity



Users and Roles

- Splunk users are assigned roles, which determine their capabilities and data access
- Out of the box, there are 3 main roles:
 - Admin
 - Power
 - User
- Splunk admins can create additional roles



Logging In

- 1 Log into Splunk with a web browser
- 2 The main view of your default app appears

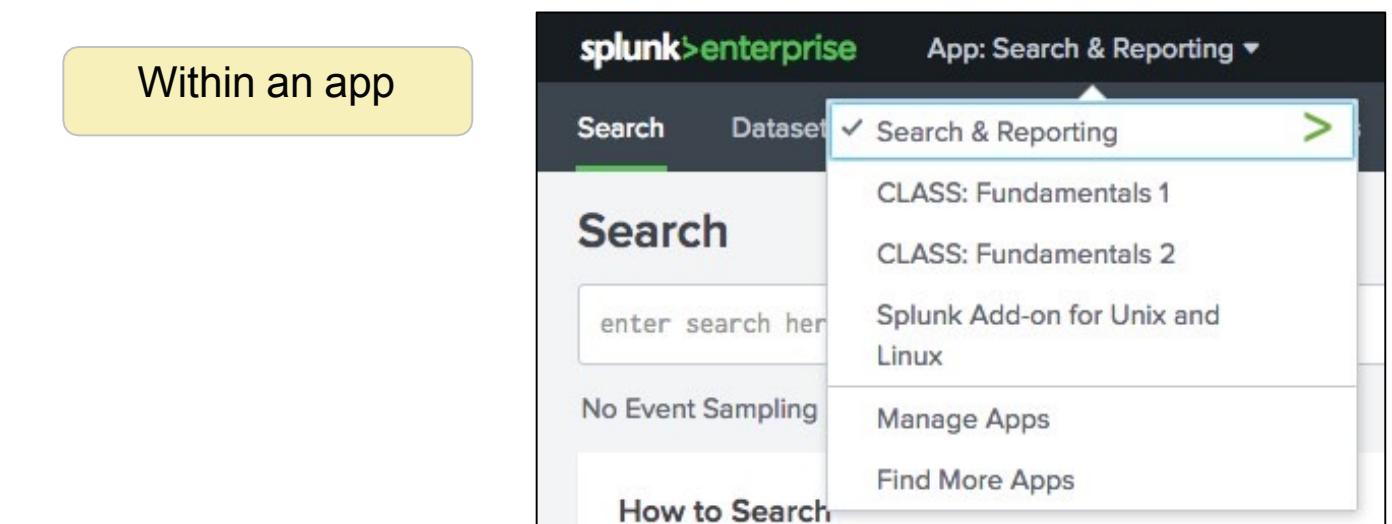
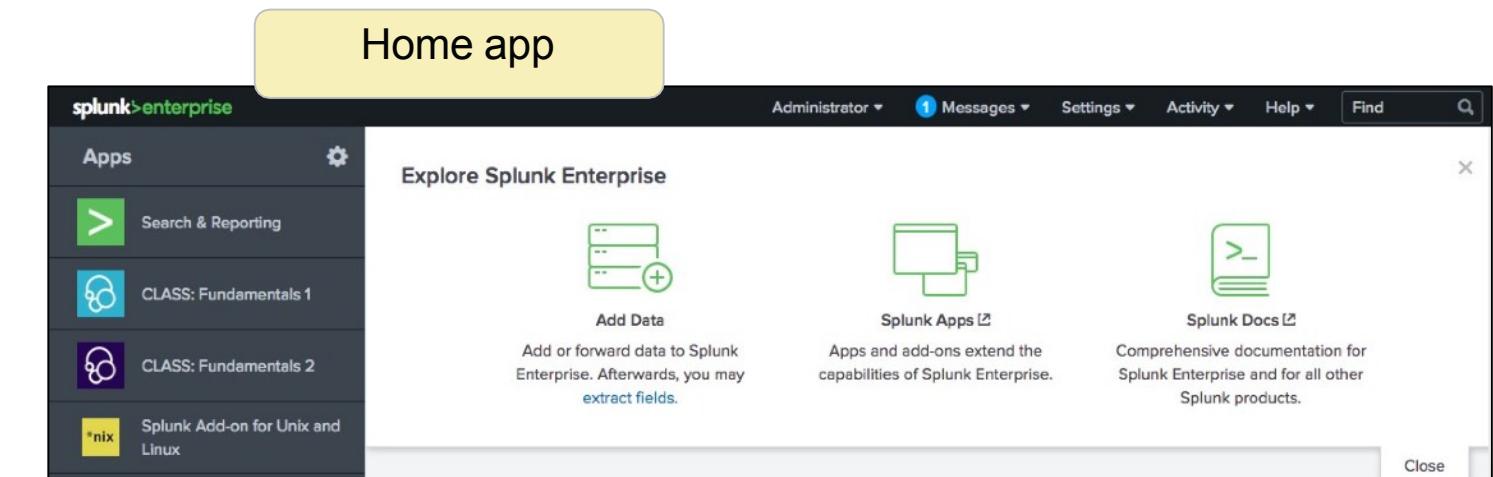
You or your organization may change your default app



A screenshot of the Splunk enterprise search & reporting dashboard. At the top, there is a navigation bar with links for 'Search', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The 'Search' link is highlighted with a red circle containing the number '2'. The main area shows a search bar with a placeholder 'enter search here...' and a time range selector set to 'Last 24 hours'. Below the search bar, there are sections for 'How to Search' and 'What to Search'. The 'How to Search' section contains a brief description and links to 'Documentation' and 'Tutorial'. The 'What to Search' section displays event statistics: '5,981,905 Events' (INDEXED), '7 months ago' (EARLIEST EVENT), 'Now' (LATEST EVENT), and a 'Data Summary' button.

Choosing Your App

- Apps allow different workspaces for specific use cases or user roles to co-exist on a single Splunk instance
- In this class, you'll explore:
 - The Home app
 - The Search & Reporting app (also called the Search app)



Note

For more info on apps, see. <http://docs.splunk.com/Documentation/Splunk/latest/Admin/Whatsanapp>

Home App

The screenshot shows the Splunk Enterprise Home App interface. On the left, a sidebar titled 'splunk>enterprise' lists several apps: 'Search & Reporting' (green icon), 'CLASS: Fundamentals 1' (blue icon), 'CLASS: Fundamentals 2' (purple icon), and 'Splunk Add-on for Unix and Linux' (yellow icon). A yellow callout box with a green arrow points to the Splunk logo at the top of the sidebar, containing the text: 'You can always click the Splunk logo to return to whatever app is set as your default app.' Below the sidebar is a 'Note' section with a blue 'i' icon, stating: 'If you or your organization doesn't choose a default app, then your default app is the Home app.'

The main content area is titled 'Explore Splunk Enterprise' and contains three sections:

- Search Manual**: Shows a magnifying glass icon and describes using SPL.
- Pivot Manual**: Shows a document icon and describes using Pivot.
- Dashboards & Visualizations**: Shows a dashboard icon and describes creating dashboards.

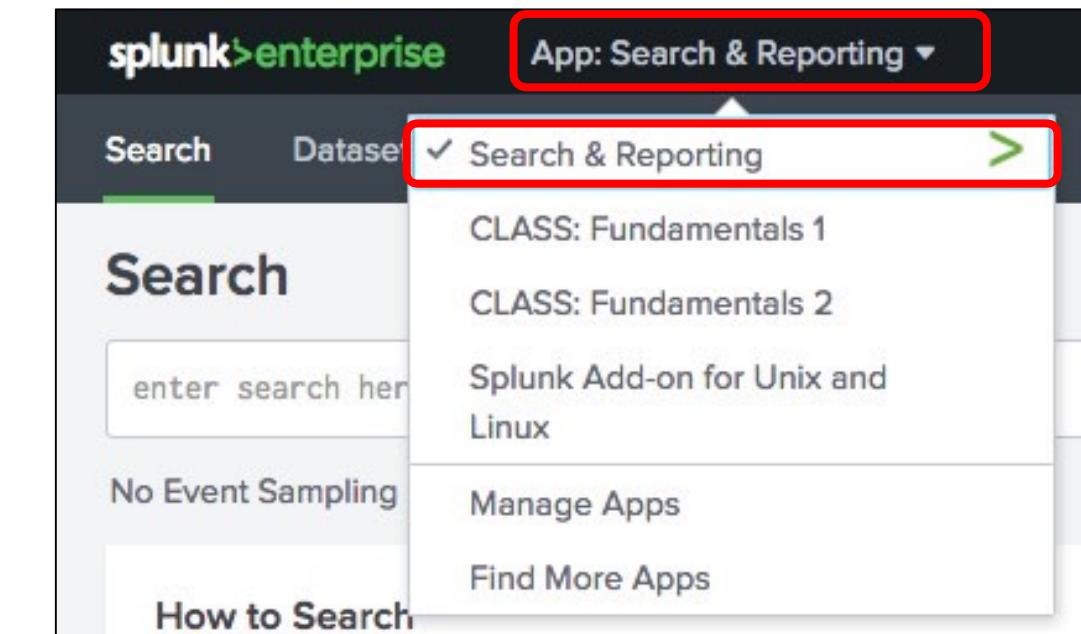
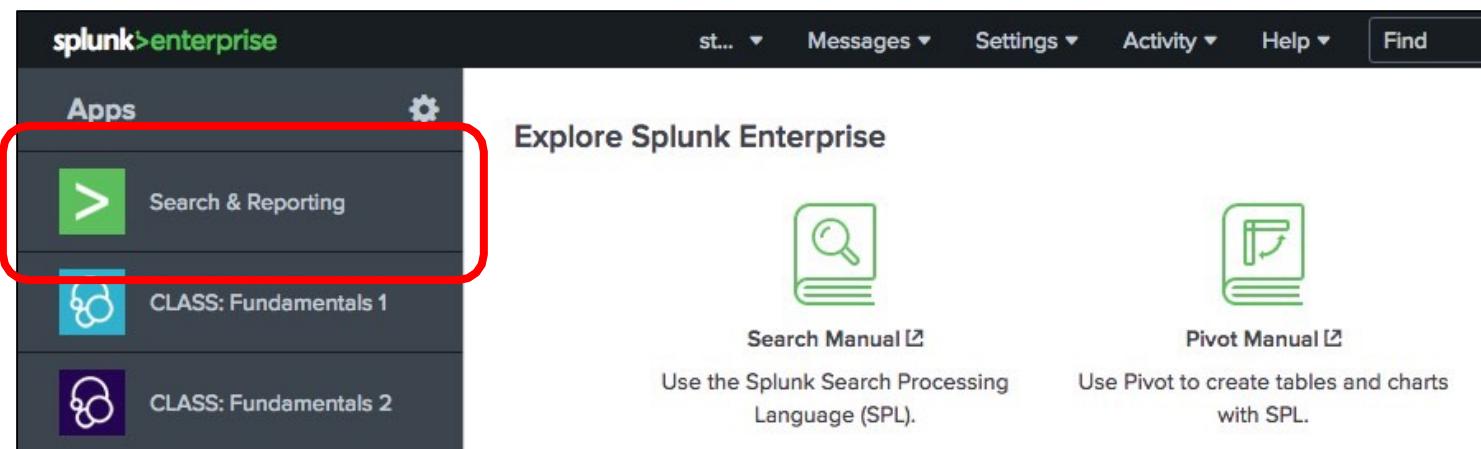
At the bottom, there's a section titled 'Choose a home dashboard' with a monitor icon.

A yellow callout box on the right side of the interface contains the text: 'Links to several helpful resources'.

A second yellow callout box at the bottom right contains the text: 'After you've built dashboards with your data, you can choose one to appear in your Home app'.

Search & Reporting App

- 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 app or from an app view, select **Apps > Search & Reporting**



Search & Reporting App (cont.)

The screenshot shows the Splunk Search & Reporting App interface. Key components highlighted include:

- splunk bar**: Located at the top left.
- current app**: Located at the top right.
- app navigation bar**: A dark bar with links: Search, Datasets, Reports, Alerts, Dashboards, and Search & Reporting.
- current view**: The "Search" link in the navigation bar is highlighted.
- search bar**: A search input field labeled "enter search here...".
- global stats**: Global statistics summary: 532,298 Events INDEXED, 3 months ago EARLIEST EVENT, Now LATEST EVENT.
- time range picker**: Time range selector showing "Last 24 hours".
- start search**: A green search button with a magnifying glass icon.
- data sources**: A button labeled "Data Summary".
- search history**: A link to "Search History".
- student1**: User profile link.
- Messages**, **Settings**, **Activity**: Navigation links.
- Help**: Navigation link.

Data Summary Tabs

The screenshot shows the Splunk Enterprise search interface. At the top, there's a navigation bar with 'splunk>enterprise' and various dropdown menus. Below it, a 'Search' tab is selected, followed by 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. A search bar contains 'enter search here...' with a 'Last 24 hours' dropdown. To the right, there's a yellow callout box with the text 'Click Data Summary to see hosts, sources, or sourcetypes on separate tabs'. On the left, a sidebar has 'How to Search' and 'What to Search' sections. The 'What to Search' section displays '532,486 Events' indexed '3 months ago', with 'EARLIEST EVENT' and 'LATEST' buttons. Below this, there are three tabs: 'Data Summary' (which is highlighted with a green box), 'Documentation', and 'Tutorial'. A green arrow points from the 'Data Summary' button in the sidebar to the first 'Data Summary' panel. The first panel has tabs for 'Hosts (10)' (selected), 'Sources', and 'Sourcetypes'. It lists hosts like 'adiddapsv1', 'badgesv1', etc. A second green arrow points from the 'Sources' tab to the second 'Data Summary' panel. The second panel also has tabs for 'Hosts (10)', 'Sources (15)', and 'Sourcetypes (10)'. It lists sources like '/opt/log/SIMlog', '/opt/log/adiddapsv1', etc. A third green arrow points from the 'Sourcetypes' tab to the third 'Data Summary' panel. The third panel has tabs for 'Hosts (10)', 'Sources (15)', and 'Sourcetypes (10)'. It lists sourcetypes like 'SimCubeBeta', 'access_combined', etc., with a table below showing details such as count and last update.

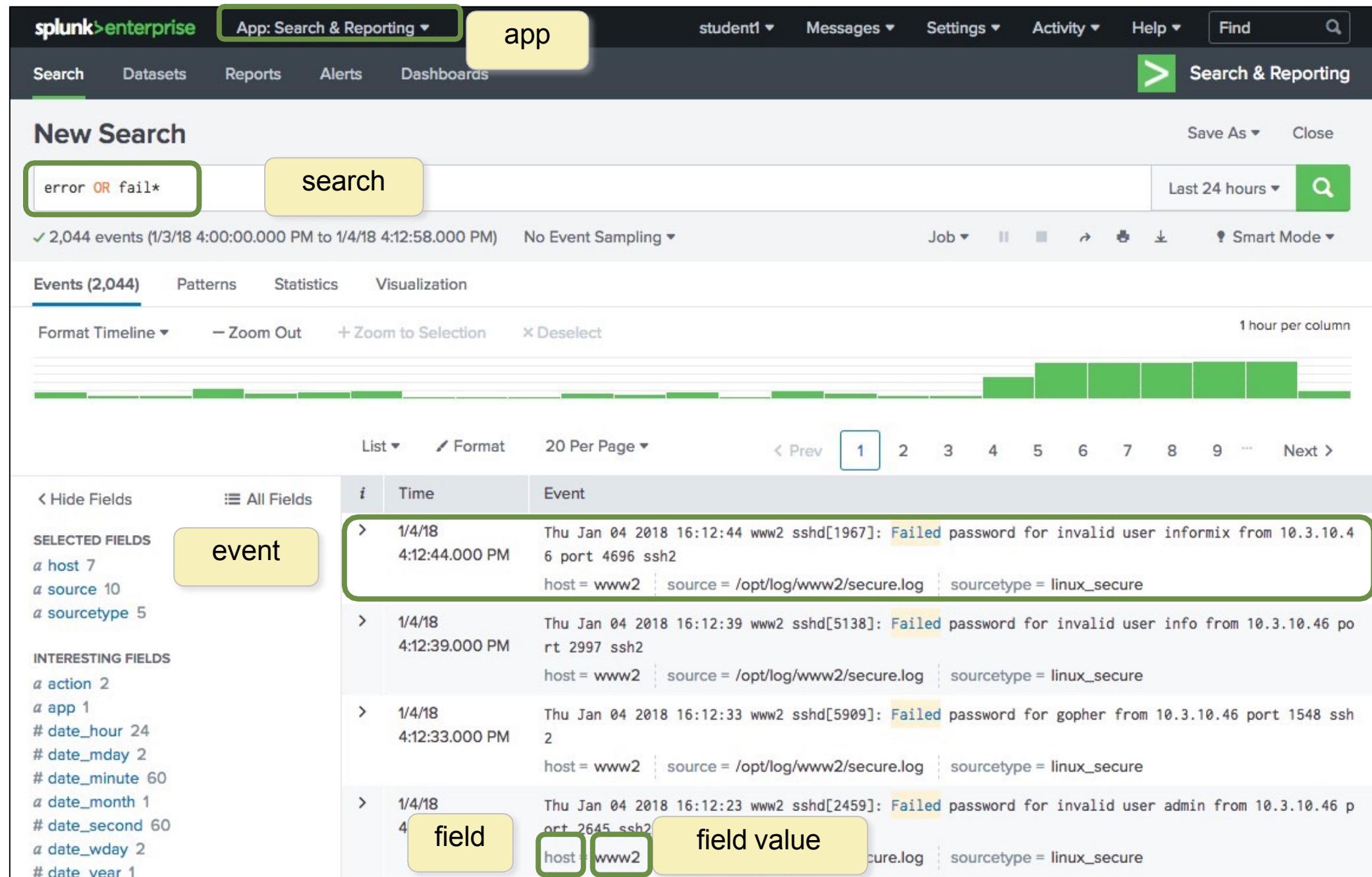
Click **Data Summary** to see hosts, sources, or sourcetypes on separate tabs

- Host – Unique identifier of where the events originated (host name, IP address, etc.)
- Source - Name of the file, stream, or other input
- Sourcetype - Specific data type or data format

Sourcetype	Count	Last Update
SimCubeBeta	377	1/4/18 3:51:45.000 PM
access_combined	154,373	1/4/18 3:52:18.000 PM
cisco_esa	3,200	1/4/18 3:52:15.000 PM
cisco_firewall	538	1/4/18 10:23:47.000 AM
cisco_wsa_squid	3,749	1/4/18 3:50:37.000 PM
history_access	7,662	1/4/18 10:23:46.000 AM
linux_secure	16,950	1/4/18 3:52:12.000 PM
sales_entries	215,869	1/4/18 3:51:56.000 PM
vendor_sales	120,459	1/4/18 3:49:32.000 PM
winauthentication_security	9,372	1/4/18 10:23:46.000 AM

Tables can be sorted or filtered

Events Tab



The screenshot shows the Splunk Enterprise interface with the 'Search & Reporting' app selected. A search bar at the top contains the query 'error OR fail*'. The results summary indicates 2,044 events from 1/3/18 to 1/4/18. The 'Events (2,044)' tab is selected. The event table displays several log entries, with the first one highlighted. The highlighted row shows a timestamp of 1/4/18 4:12:44.000 PM, an event of 'Failed password for invalid user informix from 10.3.10.4 port 4696 ssh2', and fields host=www2, source=/opt/log/www2/secure.log, and sourcetype=linux_secure.

	i	Time	Event
>	1/4/18 4:12:44.000 PM	Thu Jan 04 2018 16:12:44 www2 sshd[1967]: Failed password for invalid user informix from 10.3.10.4 6 port 4696 ssh2 host = www2 source = /opt/log/www2/secure.log sourcetype = linux_secure	
>	1/4/18 4:12:39.000 PM	Thu Jan 04 2018 16:12:39 www2 sshd[5138]: Failed password for invalid user info from 10.3.10.46 po rt 2997 ssh2 host = www2 source = /opt/log/www2/secure.log sourcetype = linux_secure	
>	1/4/18 4:12:33.000 PM	Thu Jan 04 2018 16:12:33 www2 sshd[5909]: Failed password for gopher from 10.3.10.46 port 1548 ssh 2 host = www2 source = /opt/log/www2/secure.log sourcetype = linux_secure	
>	1/4/18 4:12:23.000 PM	Thu Jan 04 2018 16:12:23 www2 sshd[2459]: Failed password for invalid user admin from 10.3.10.46 p ort 2645 ssh2 host = www2 source = /opt/log/www2/secure.log sourcetype = linux_secure	

Course Scenario

- Use cases in this course are based on Buttercup Games, a fictitious gaming company
- Multinational company with its HQ in San Francisco and offices in Boston and London
- Sells products through its worldwide chain of 3rd party stores and through its online store



Your Role at Buttercup Games

- You're a Splunk power user
- You're responsible for providing info to users throughout the company
- You gather data/statistics and create reports on:
 - IT operations: information from mail and internal network data
 - Security operations: information from internal network and badge reader data
 - Business analytics: information from web access logs and vendor data

Callouts

Scenarios

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

Scenario

For failed logins into the network during the last 60 minutes, display the IP and user name.

Notes & Tips

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

Note

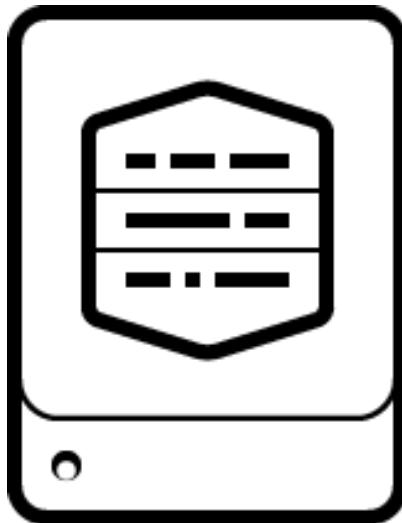
Learn more about Splunk from Splunk's online glossary, the Splexicon at <http://docs.splunk.com/Splexicon>

Module 2:

Splunk Components

Splunk Components

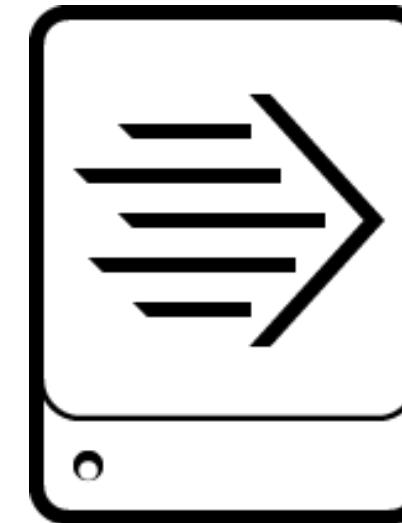
Splunk is comprised of three main processing components:



Indexer



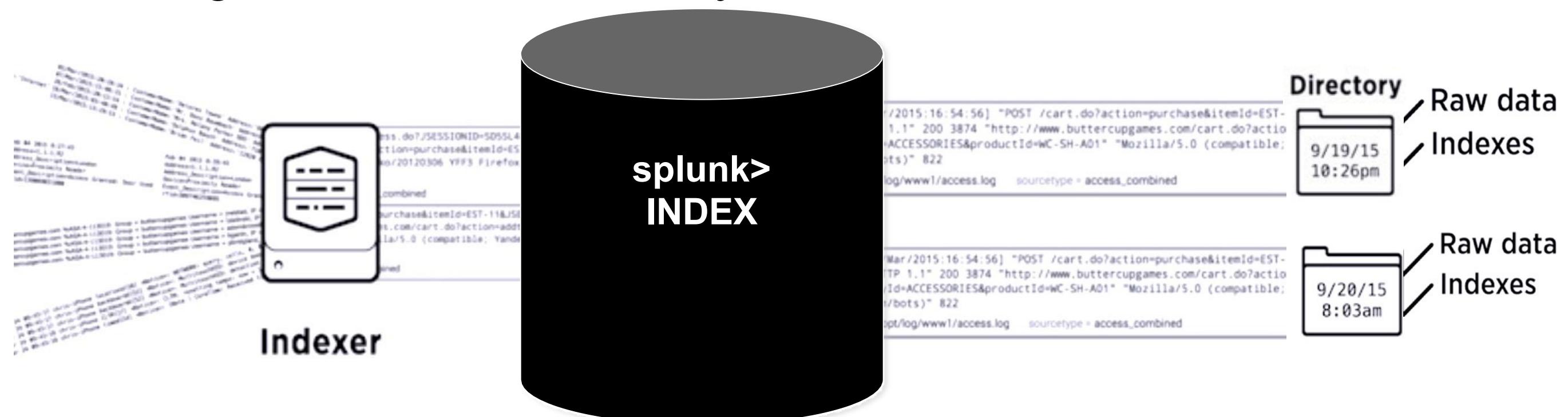
Search Head



Forwarder

Splunk Components - Indexer

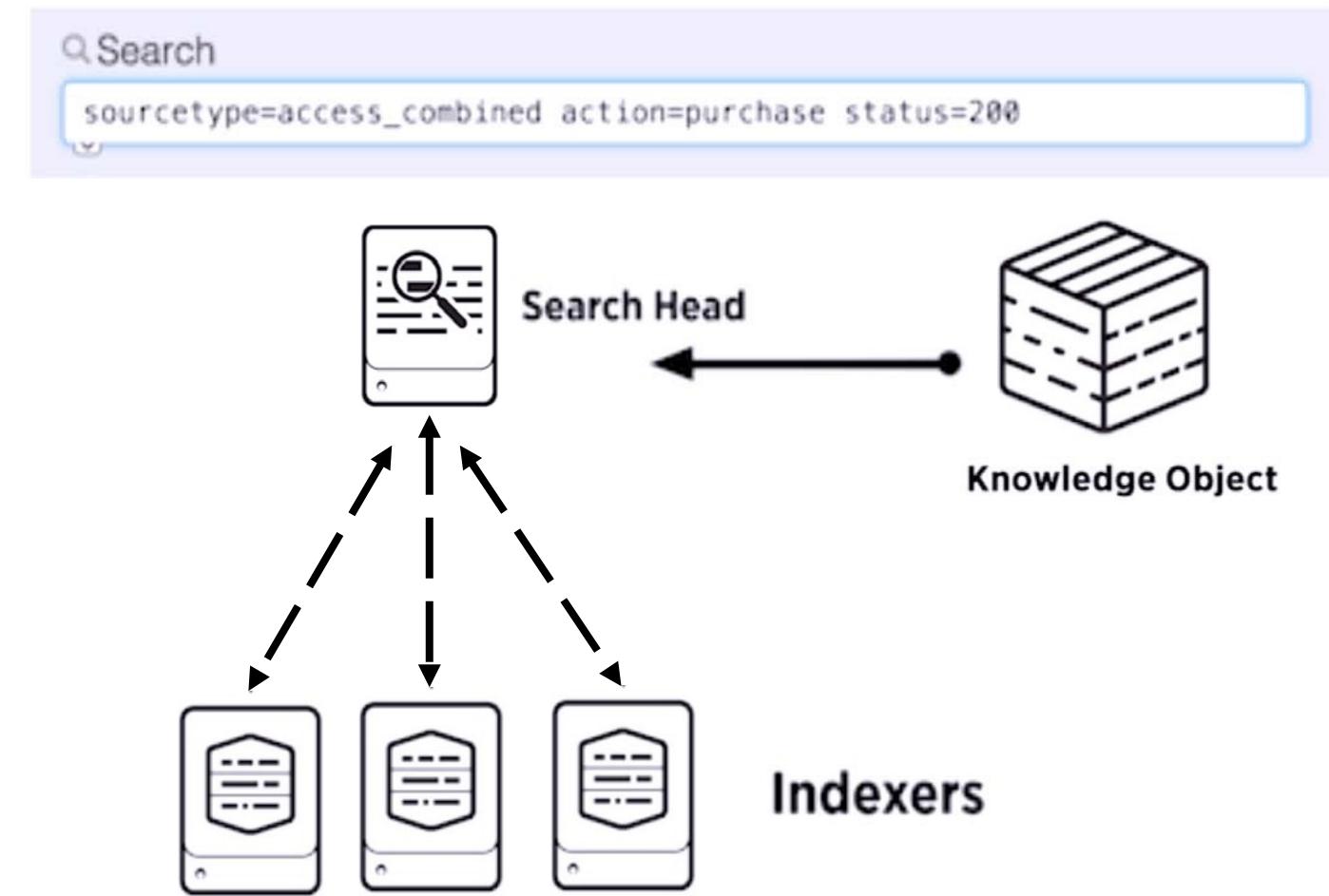
- Processes machine data, storing the results in indexes as events, enabling fast search and analysis



- 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)

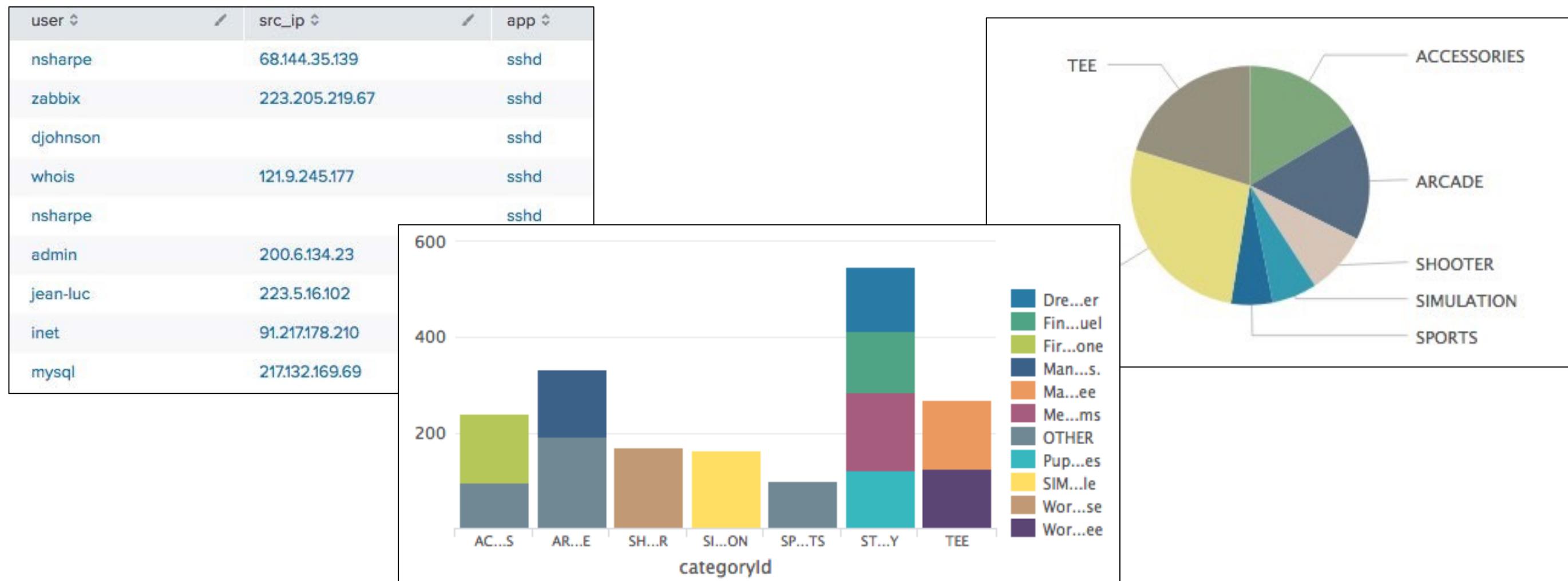
Splunk Components – Search Heads

- Allows users to use the Search language to search the indexed data
- Distributes user search requests to the Indexers
- Consolidates the results and extracts 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



Splunk Components – Search Heads (cont.)

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



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

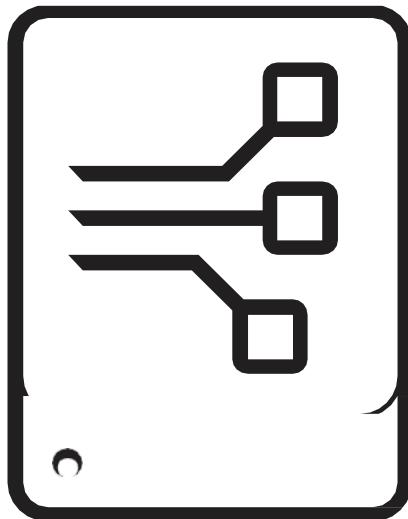
IP = 10.3.10.6, Session disconnected. Session type = TPsecOve
IP = 10.1.10.216, Session connected. Session type = SSL, Dura
s, IP = 10.1.10.133, Session connected. Session type = IKE, Dur
i, IP = 10.3.10.18, Session disconnected. Session type = IKE, D
= 10.1.10.211, Session connected. Session type = SSL, Duration



Indexer

Additional Splunk Components

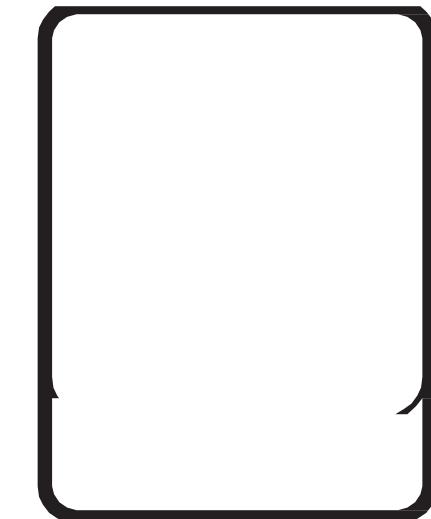
In addition to the three main Splunk processing components, there are some less-common components including :



**Deployment
Server**



Cluster Master

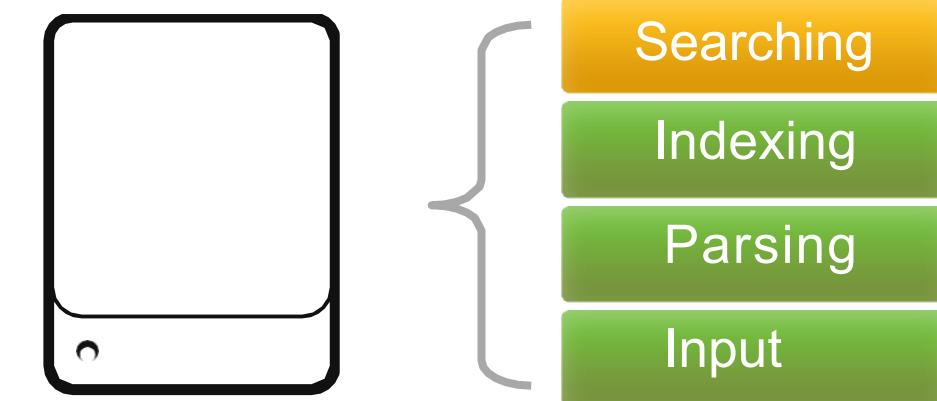


License Master

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

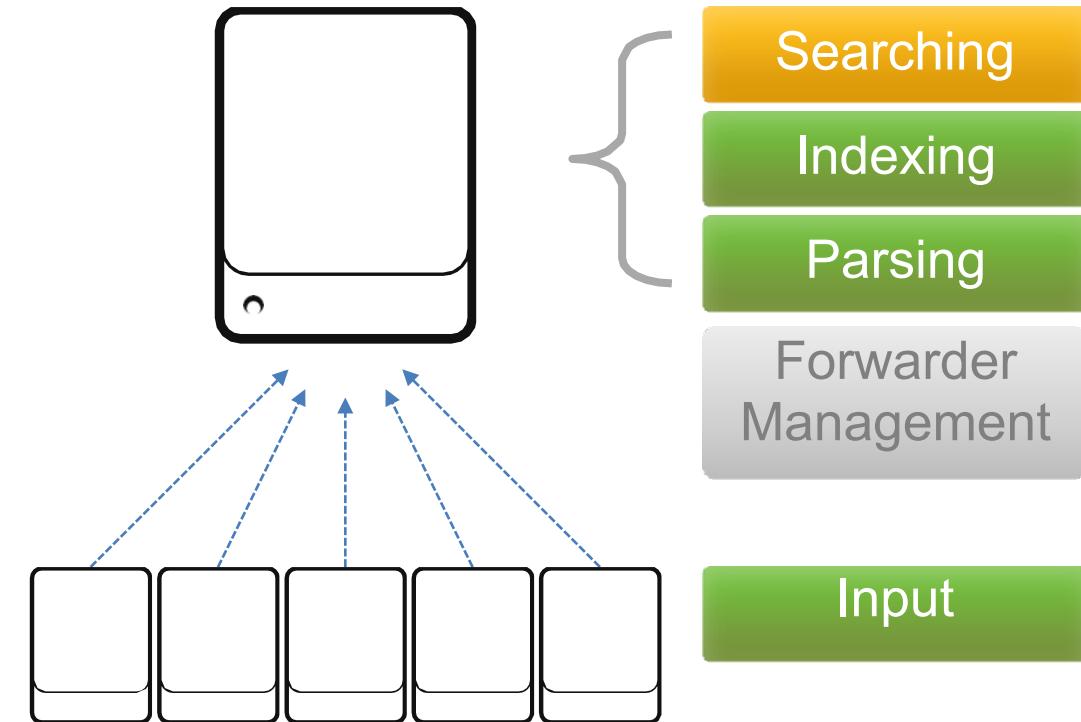


- Recommendation

- 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)

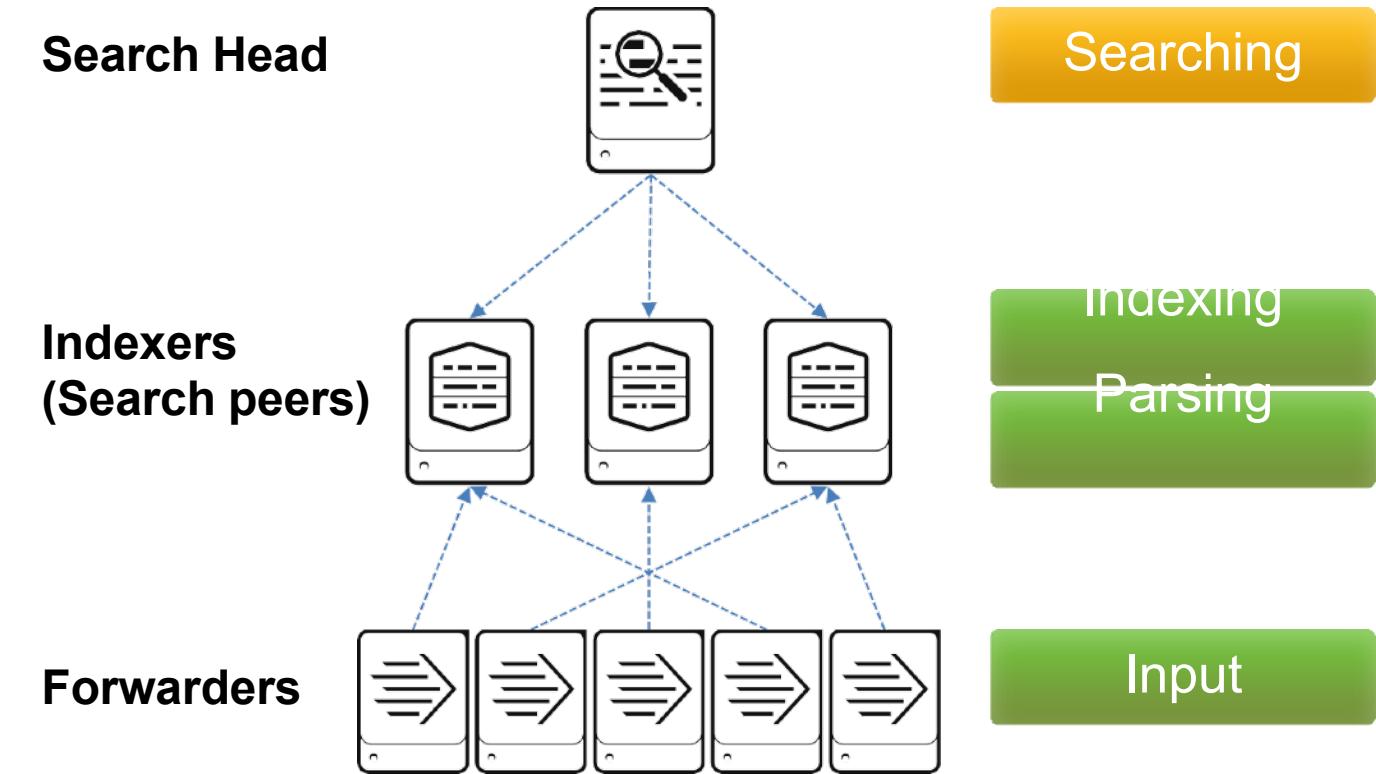


Basic Deployment for organizations:

- 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

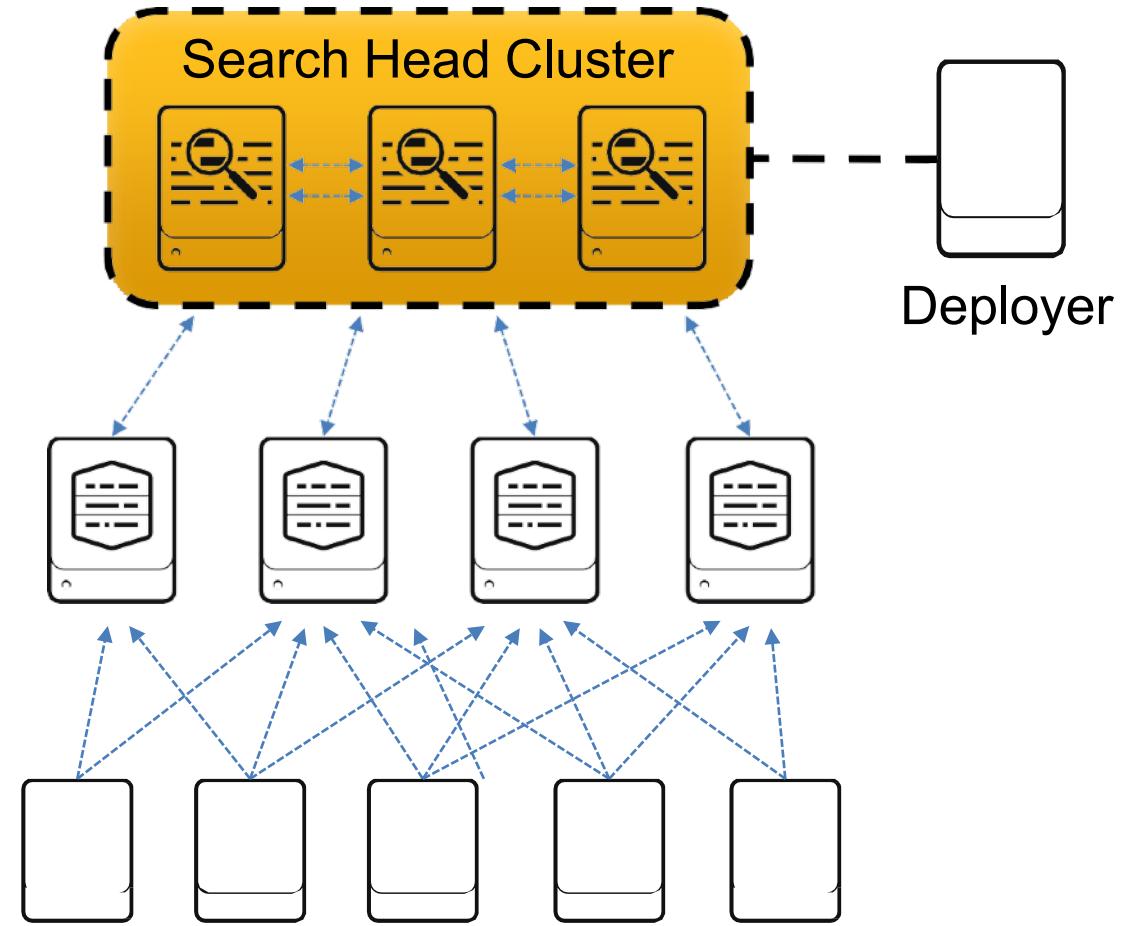


Deployment for organizations:

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

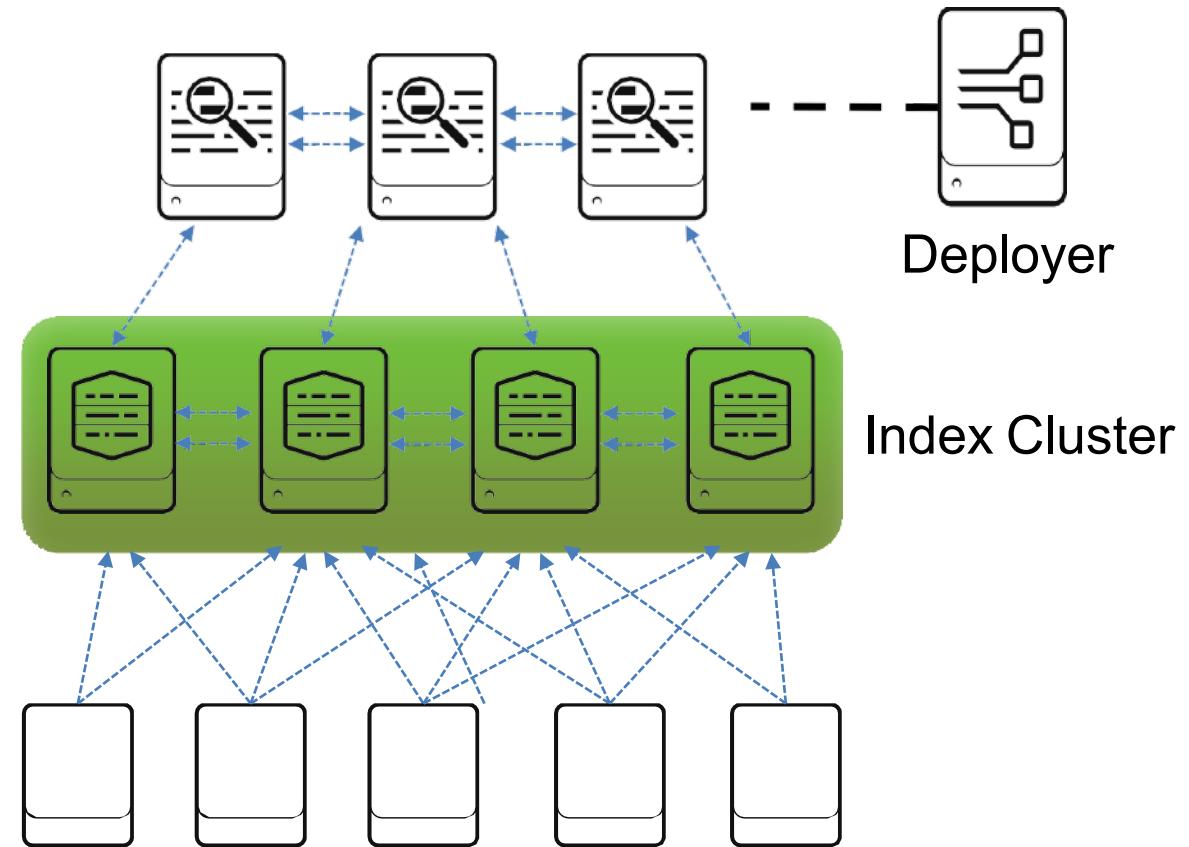
Splunk Deployment – Increasing Capacity

- Adding a Search Head Cluster:
 - Services more users for increased search capacity
 - Allows users and searches to share resources
 - Coordinate 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



Splunk Deployment – Index Cluster

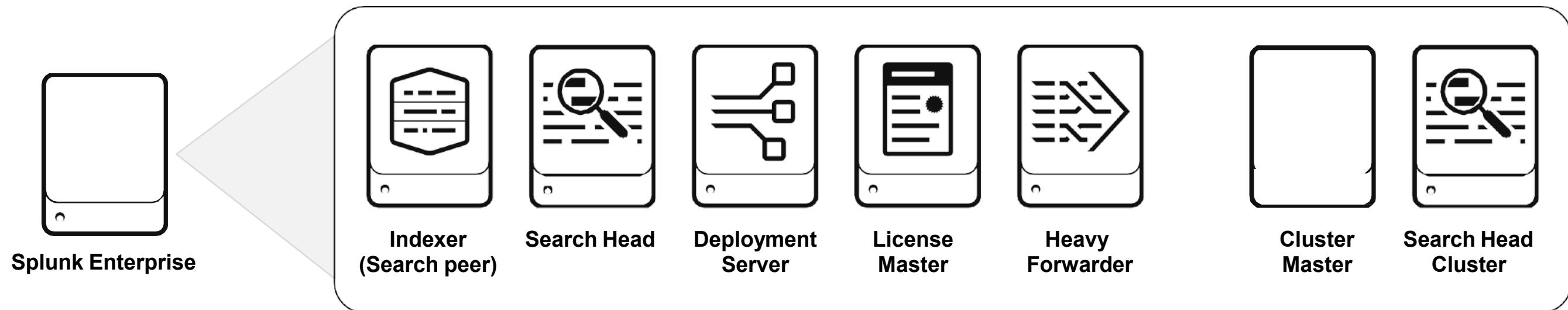
- Traditional Index Clusters:
 - Configured to replicate data
 - Prevent data loss
 - Promote availability
 - Manage multiple indexers
- Non-replicating Index Clusters
 - Offer simplified management
 - Do not provide availability or data recovery



Module 3: Installing Splunk

Splunk Enterprise Install Package

There are multiple Splunk components installed from the Splunk Enterprise package



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

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

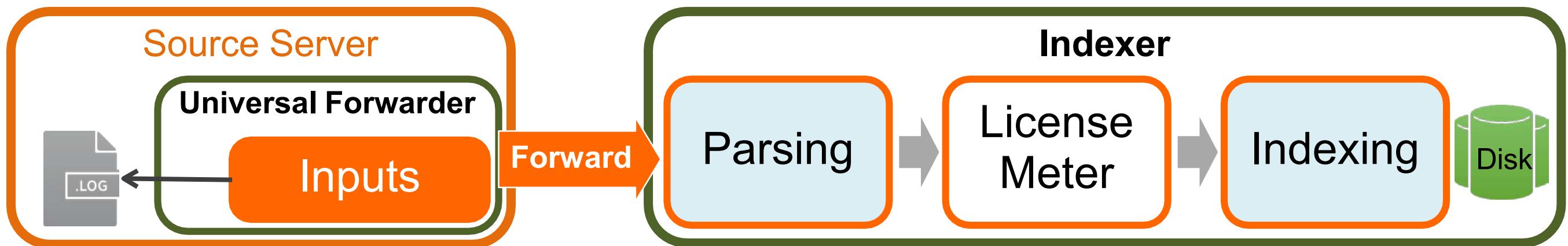
Command	Operation
splunk help	Display a usage summary
splunk [start stop restart]	Manage the Splunk processes
splunk start --accept-license	Automatically accept the license without prompt
splunk status	Display the Splunk process status
splunk show splunkd-port	Show the port that the splunkd listens on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

Module 4

Getting Data In

Splunk Index Time Process

- Splunk index time process (data ingestion) can be broken down into three phases:
 1. **Input phase:** handled at the source (usually a forwarder)
 - ? The data sources are being opened and read
 - ? Data is handled as streams and any configuration settings are applied to the entire stream
 2. **Parsing phase:** handled by indexers (or heavy forwarders)
 - ? Data is broken up into events and advanced processing can be performed
 3. **Indexing phase:**
 - ? License meter runs as data and is initially written to disk, prior to compression
 - ? After data is written to disk, it **cannot** be changed



Data Input Types

- Splunk supports many types of data input
 - **Files and directories:** monitoring text files and/or directory structures containing text files
 - **Network data:** listening on a port for network data
 - **Script output:** executing a script and using the output from the script as the input
 - **Windows logs:** monitoring Windows event logs, Active Directory, etc.
 - **HTTP:** using the HTTP Event Collector
 - And more...
- You can add data inputs with:
 - Apps and add-ons from Splunkbase
 - Splunk Web
 - CLI
 - Directly editing `inputs.conf`

Default Metadata Settings

- When you index a data source, Splunk assigns metadata values
 - The metadata is applied to the entire source
 - Splunk applies defaults if not specified
 - You can also override them at input time or later

Metadata	Default
source	Path of input file, network hostname:port, or script name
host	Splunk hostname of the inputting instance (usually a forwarder)
sourcetype	Uses the source filename if Splunk cannot automatically determine
index	Defaults to main

Adding an Input with Splunk Web

- Splunk admins have a number of ways to start the **Add Data** page
 - Click the **Add Data** icon
 - ?On the admin's **Home** page
 - ?On the **Settings** panel
 - Select **Settings > Data inputs > Add new**

The screenshot shows the Splunk Web interface. On the left, there is a navigation sidebar with a purple header containing the text "Settings ▾". Below this, under the "DATA" section, the "Data inputs" link is highlighted with a purple box and an orange circle containing the number "2". Other links in the sidebar include "Forwarding and receiving", "Indexes", "Report acceleration summaries", "Virtual indexes", and "Source types". To the right of the sidebar, the main content area has a title "Data inputs" and a sub-section "Local inputs". It displays a table with one row for "Files & Directories". The table has columns for "Type", "Inputs", and "Actions". In the "Actions" column, there is a button labeled "+ Add new" with an orange circle containing the number "3". A large gray callout box is positioned above the "+ Add new" button, containing a smaller image of the "Add Data" icon (three stacked rectangles with a plus sign) and the text "Add Data".

Add Data Menu

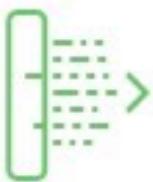
Add Data menu provides three options depending on the source to be used

Add Data

How do you want to add data?

 Upload files from my computer

 Monitor files and ports on this Splunk indexer

 Forward data from Splunk forwarder

Upload Option

Upload allows uploading local files that only get indexed once. Useful for testing or data that is created once and never gets updated. Does not create `inputs.conf`.

Monitor Option

Provides one-time or continuous monitoring of files, directories, http events, network ports, or data gathering scripts located on Splunk Enterprise instances. Useful for testing inputs.

Forward Option

Main source of input in production environments. Remote machines gather and forward data to indexers over a receiving port.

Select Source

1 Select the **Files & Directories** option to configure a monitor input

2 To specify the source:

- Enter the absolute path to a file or directory, or
- Use the **Browse** button

3 For ongoing monitoring

For one-time indexing (or testing); the **Index Once** option does not create a stanza in `inputs.conf`

Set Source Type (Data Preview Interface)

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: /opt/log/www1/access.log View Event Summary

Time	Event
11/28/17 4:58:01.000 PM	111.161.27.20 - - [28/Nov/2017:16:58:01] "GET /cart.do?action=remove&itemId=EST-19&productId=PZ-SG-G05&JSESSIONID=SD6SL1FF4ADFF4960 HTTP 1.1" 200 2708 "http://www.buttercupgames.com" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)" 728
11/28/17 4:58:03.000 PM	111.161.27.20 - - [28/Nov/2017:16:58:03] "GET /cart.do?action=changequantity&itemId=EST-19&productId=MB-AG-T01&JSESSIONID=SD6SL1FF4ADFF4960 HTTP 1.1" 200 2016 "http://www.buttercupgames.com/product.screen?productId=MB-AG-T01" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)" 418
11/28/17 4:58:09.000 PM	111.161.27.20 - - [28/Nov/2017:16:58:09] "GET /category.screen?categoryId=NULL&JSESSIONID=SD6SL1FF4ADFF4960 HTTP 1.1" 406 552 "http://www.buttercupgames.com/cart.do?action=view&itemId=EST-21" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)" 283
11/28/17 00 PM	111.161.27.20 - - [28/Nov/2017:16:58:14] "GET /search.do?items=2112&JSESSIONID=SD6SL1FF4ADFF4960 HTTP 1.1" 404 3162 "http://www.buttercupgames.com/oldlink?itemId=EST-19" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)" 126
11/28/17 00 PM	111.161.27.20 - - [28/Nov/2017:16:58:19] "GET /cart.do?action=view&itemId=EST-27&productId=WC-SH-A01&JSESSIONID=SD6SL1FF4ADFF4960 HTTP 1.1" 200 1195 "http://www.buttercupgames.com/product.screen?productId=WC-SH-A01" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)" 283

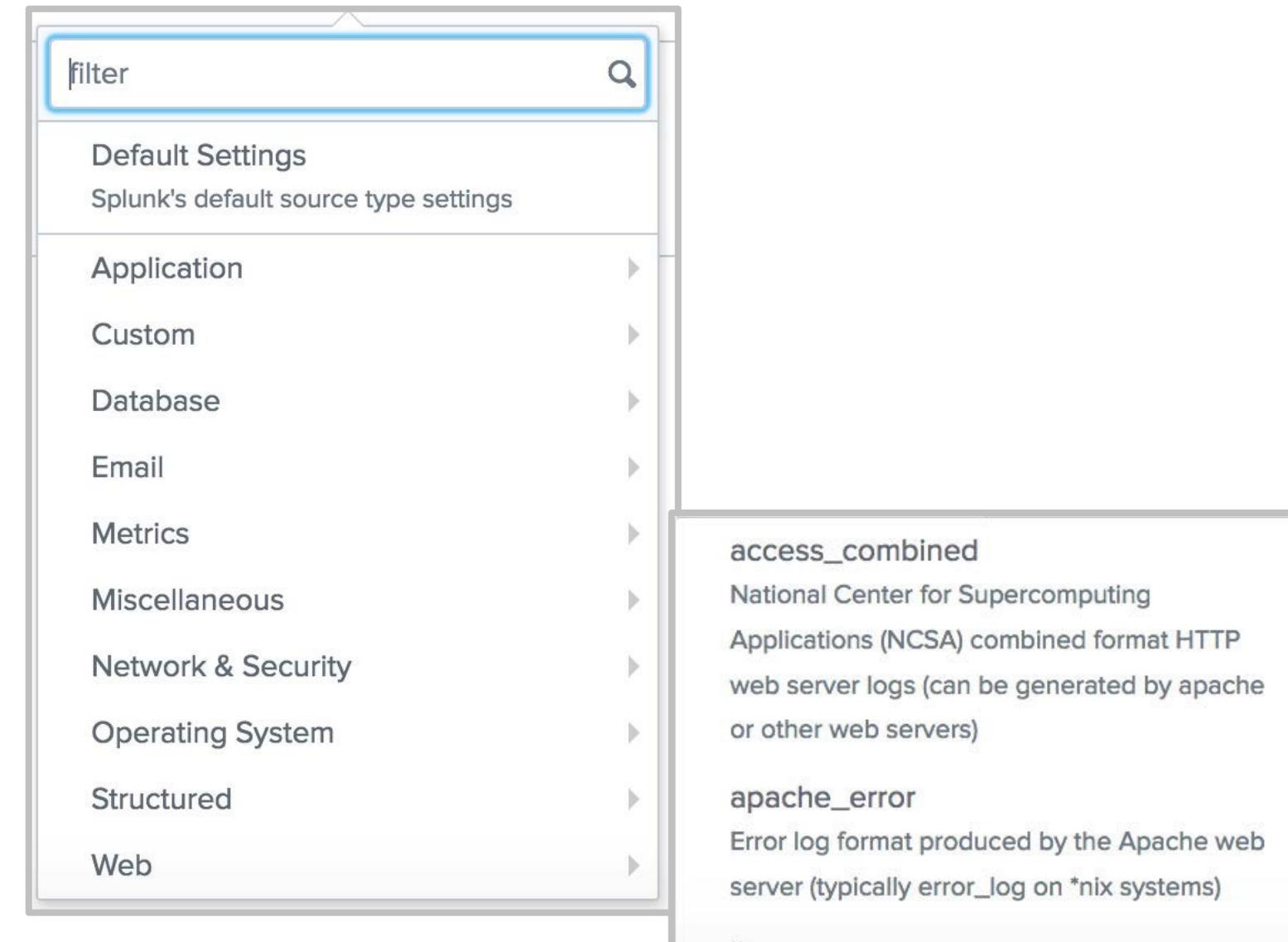
1 Source type: access_combined_wcookie ▾ **2** Web **3** filter **4** 11/28/17 4:58:01.000 PM

Set Source Type (cont.)

- ➊ Splunk automatically determines the source type for major data types when there is enough data
- ➋ You can choose a different source type from the dropdown list
- ➌ Or, you can create a new source type name for the specific source
- ➍ **Data preview** displays how your processed events will be indexed
 - If the events are correctly separated and the right timestamps are highlighted, you can move ahead
 - ?
 - If not, you can select a different source type from the list or customize the settings

Pretrained Source Types

- Splunk has default settings for many types of data
- The docs also contain a list of source types that Splunk automatically recognizes
- Splunk apps can be used to define additional source types



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

Input Settings

Add Data ● Select Source ● Set Source Type ● Input Settings ○ Review ○ Done

Input Settings

Optionaly 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 you choose determines the available configuration 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](#)

App Context: **Search & Reporting (search)**

Host field value: **splunk01**

Index: **itops** [Create a new index](#)

- The app context determines where your input configuration is saved
- In this example, it will be saved in:
SPLUNK_HOME/etc/apps/search/local

By default, the default host name in **General settings** is used

- Select the index where this input should be stored
- To store in a new index, first create the new index

Review

- Review the input configuration summary and click **Submit** to finalize

Add Data

Review

Input Type File Monitor
Source Path /opt/log/www1/access.log
Continuously Monitor Yes
Source Type access_combined_wcookie
App Context search
Host splunk01
Index itops

What Happens Next?

- Indexed events are available for immediate search
 - However, it may take a minute for Splunk to *start* indexing the data
- You are given other options to do more with your data

Add Data

Select Source Set Source Type Input Settings Review Done

< Back Submit >

Review

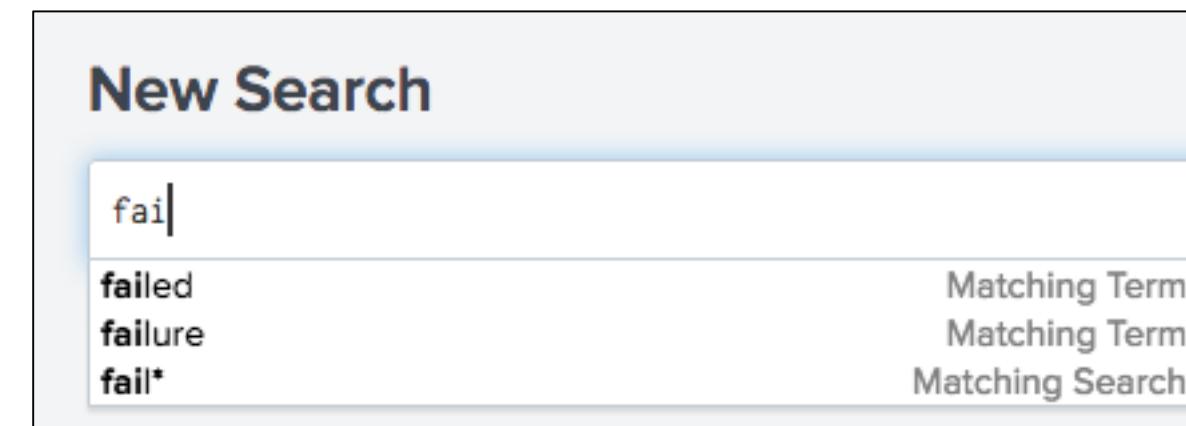
Input Type	File Monitor
Source Path	/opt/log/www1/access.log
Continuously Monitor	Yes
Source Type	access_combined_wcookie
App Context	search
Host	splunk01
Index	test

Module 5:

Basic Search

Search Assistant

- Search Assistant provides selections for how to complete the search string
- Before the first pipe (|), it looks 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



Search Assistant (cont.)

- After the first pipe, the Search Assistant shows a list of commands that can be entered into the search string
- 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**

A

New Search

failed | cha

chart
sichart
timechart
sitimechart

Events (1,942) **chart**
Returns results in a tabular output for charting.
Example:
... | chart max(delay) over foo

Format Ti

Command
Command
Command
Command

Learn More ↗

B

New Search

failed | chart cou

count
chart count by host
chart count by src_ip
chart count by user
chart count(_raw) by action
chart count(_raw) by saved_search

Events (1,942) **chart**
Returns results in a tabular output for charting.
Example:
... | chart max(delay) over foo

Format Timeline

Command Args
Command History
Command History
Command History
Command History
Command History

Learn More ↗

Search Assistant (cont.)

- Search Assistant is enabled by default in the **SPL Editor** user preferences
- By default, **Compact** is selected
- To show more information, choose **Full**

Compact Mode

New Search

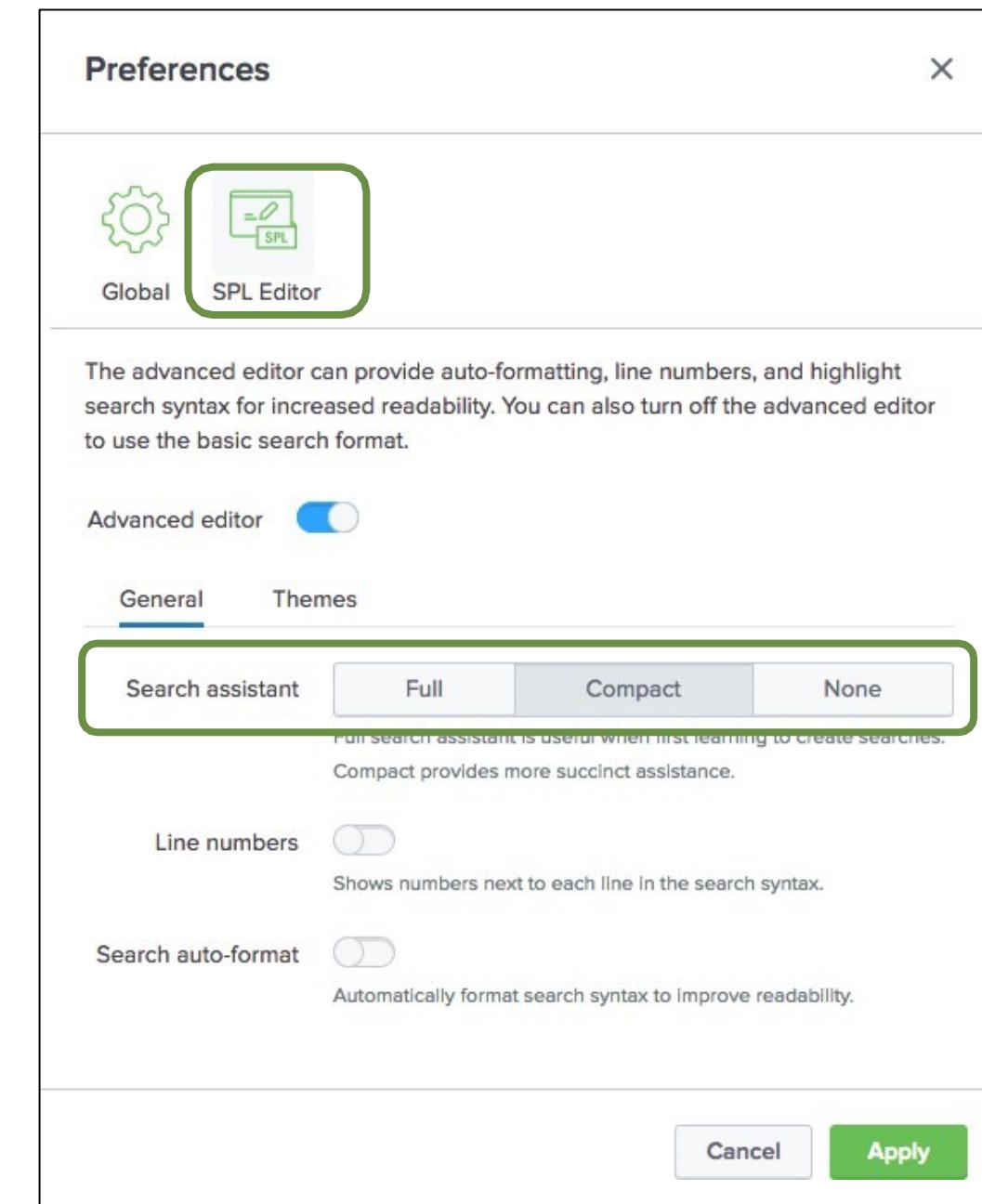
failed | chart cou

✓ 1,942 events (1/1)

Events (1,942)

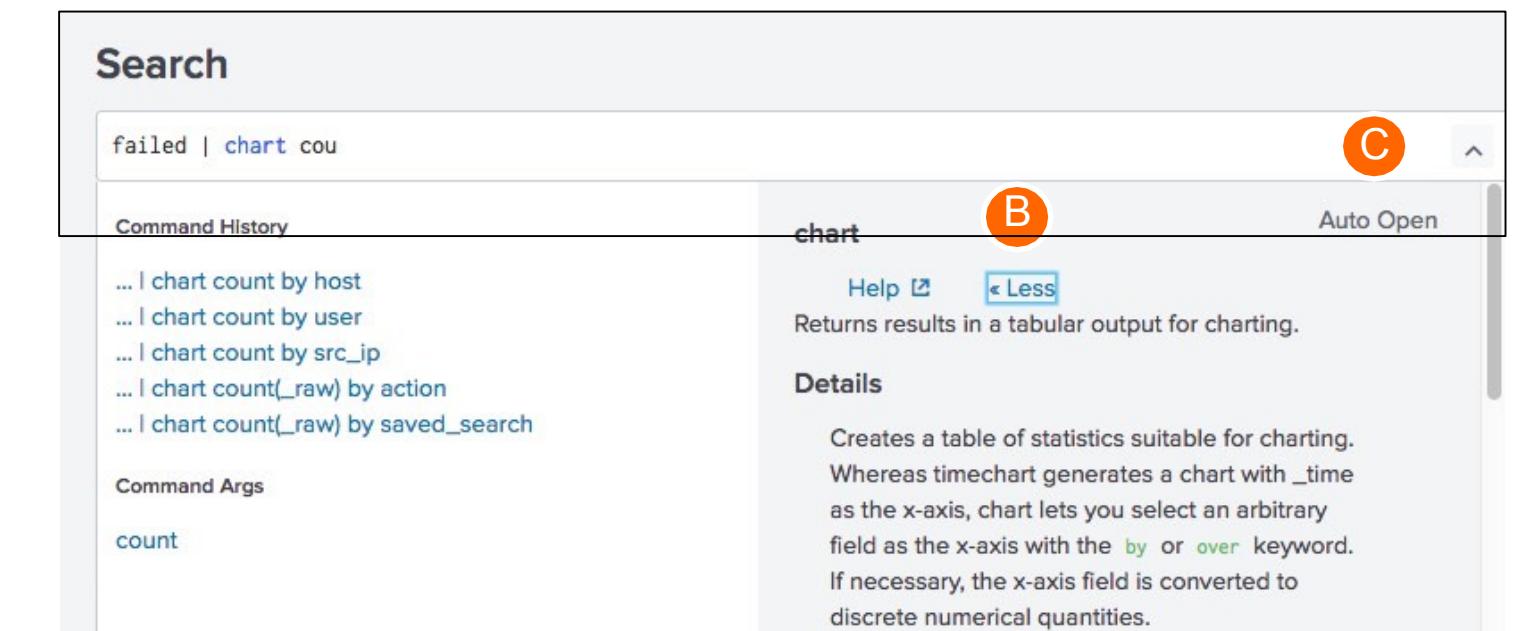
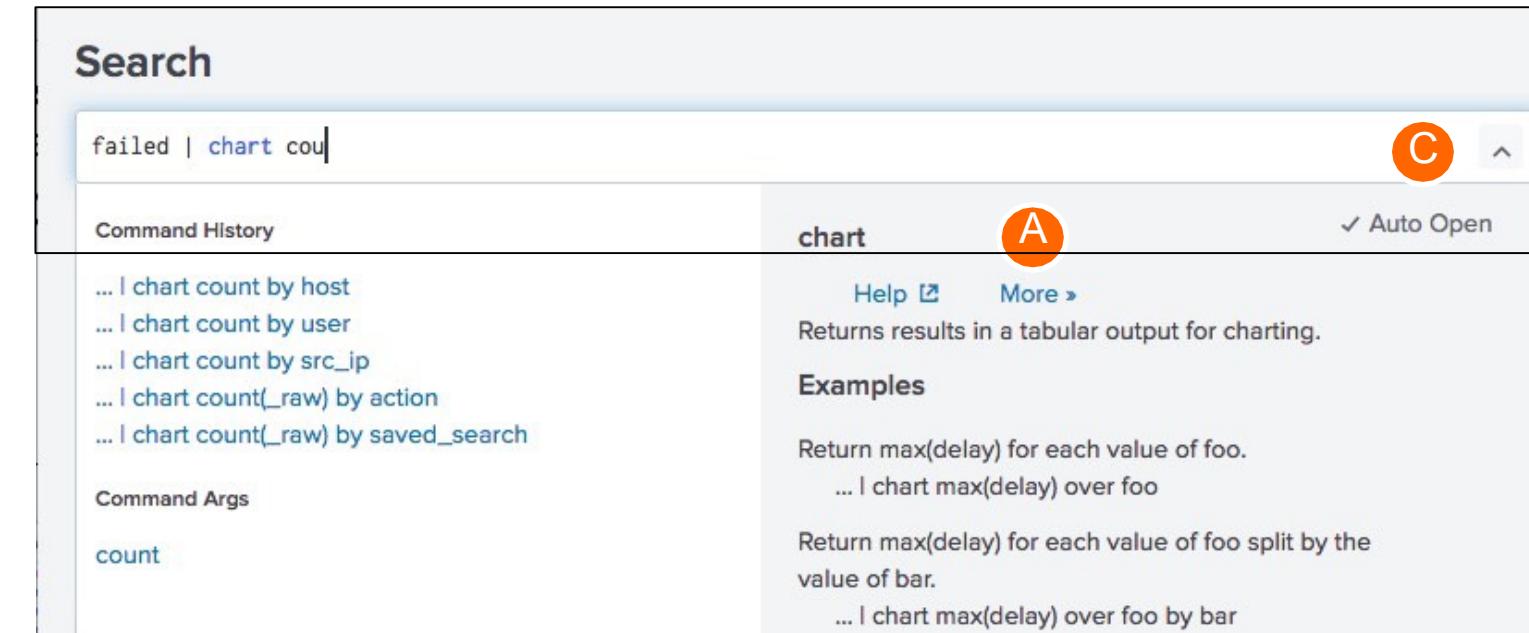
Format Timeline

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



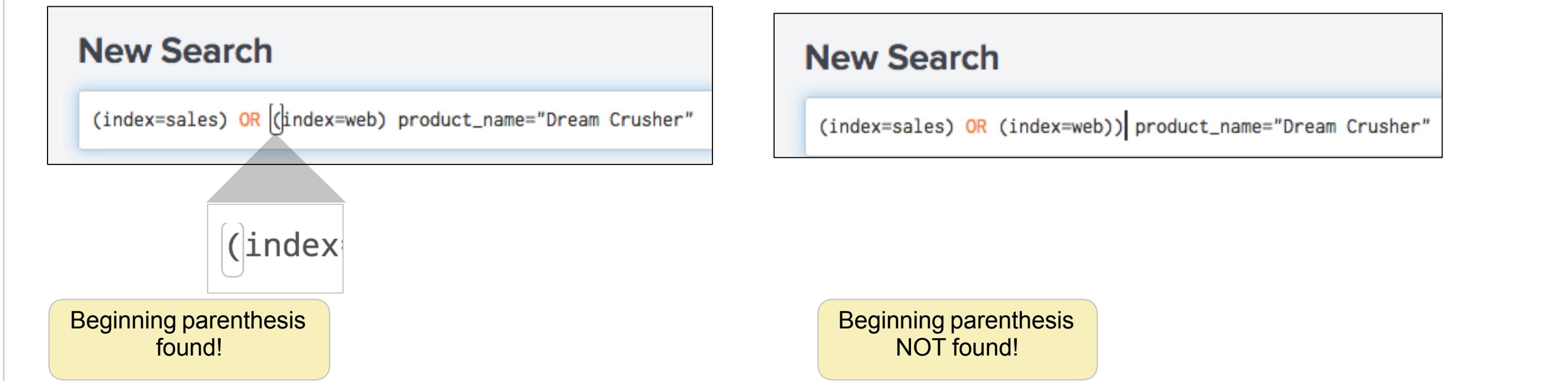
Search Assistant – Full Mode

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



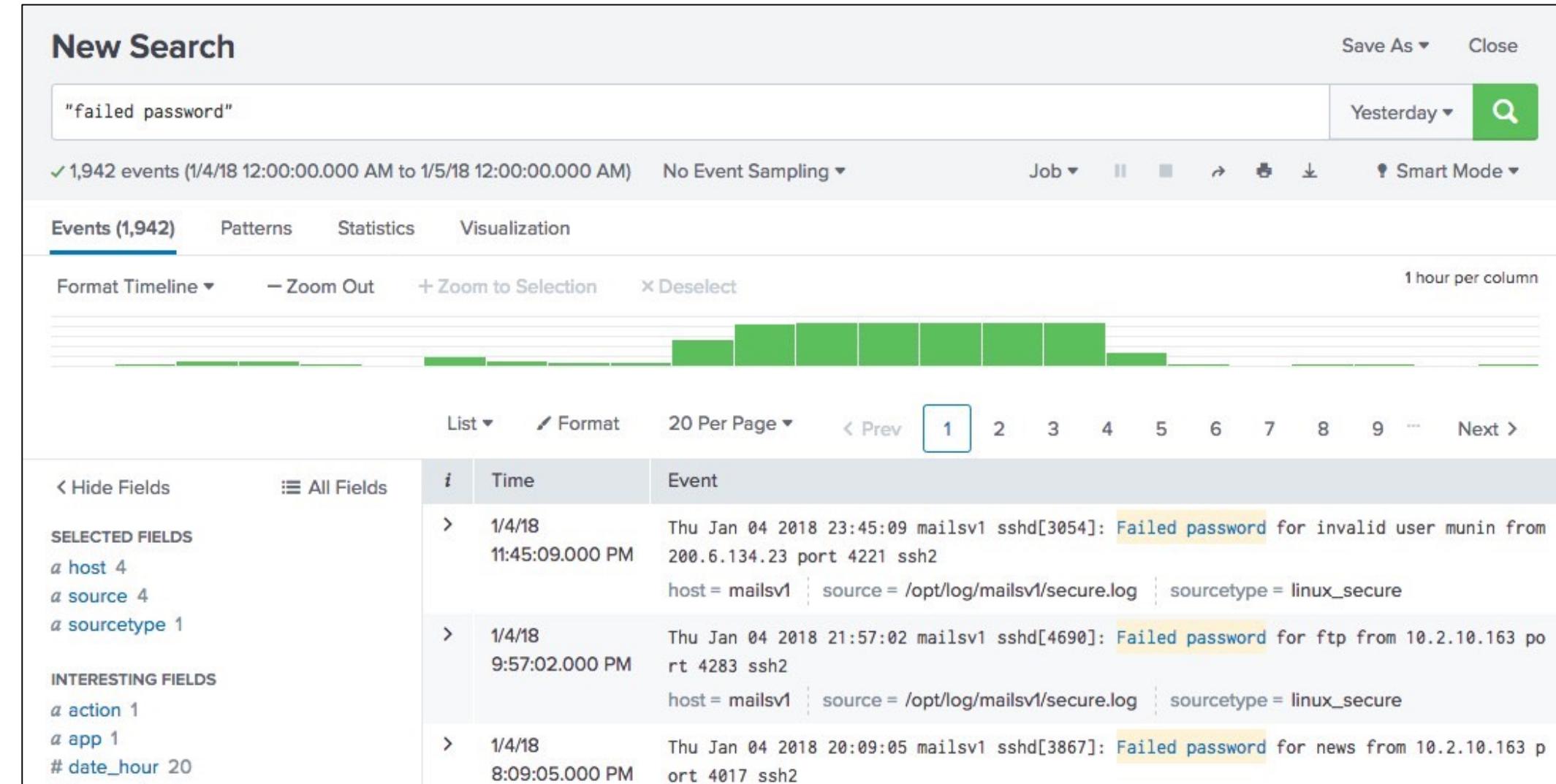
Search Assistant – Parentheses

- 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



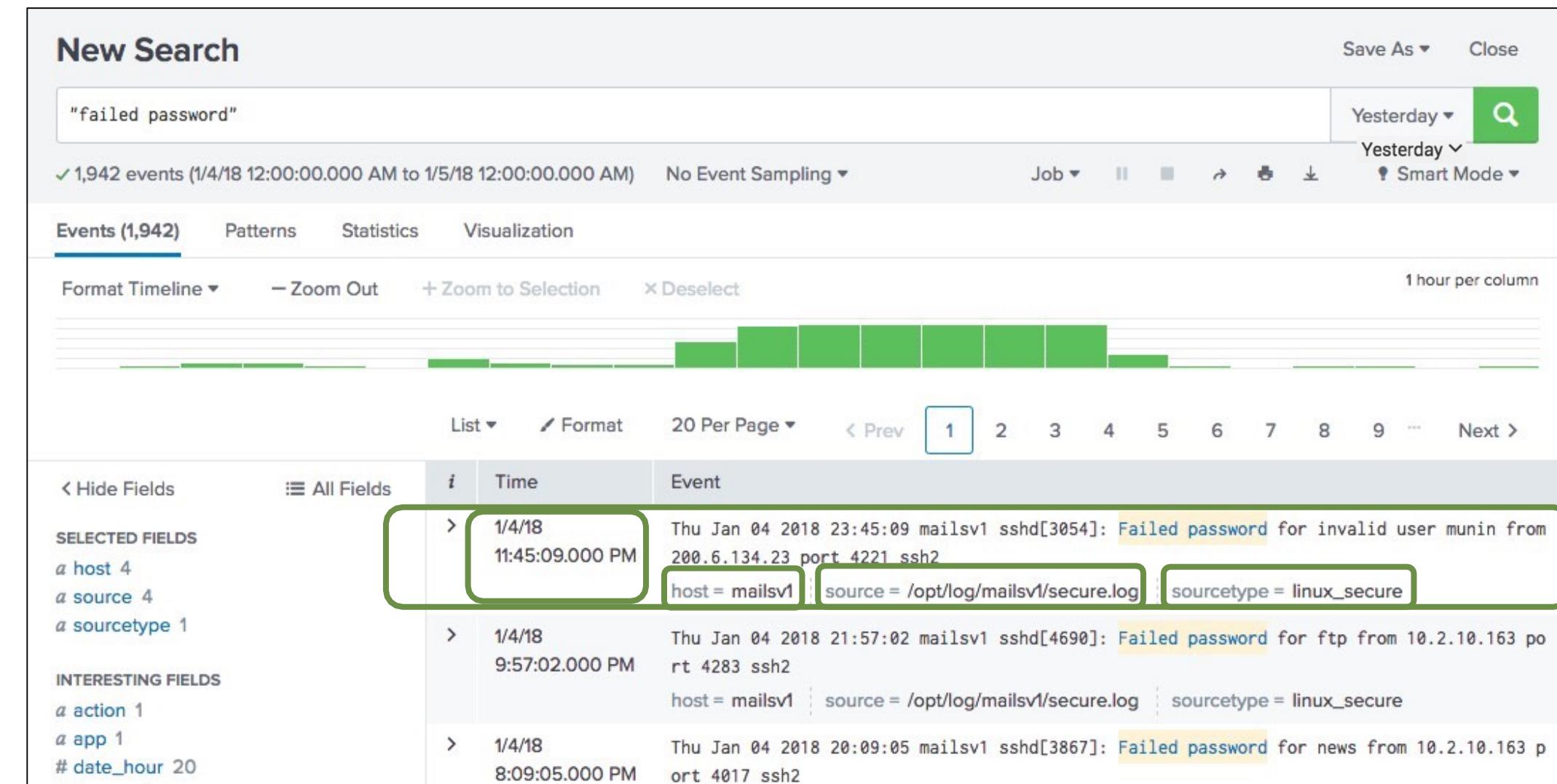
Viewing Search Results

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



Viewing Search Results (cont.)

- Splunk parses data into individual events, extracts time, and assigns metadata
- Each event has:
 - timestamp
 - host
 - source
 - sourcetype
 - index



Viewing Search Results (cont.)

The screenshot shows the Splunk interface for viewing search results. A search query "failed password" has been run, resulting in 1,942 events found between 1/4/18 and 1/5/18.

Annotations highlight various UI elements:

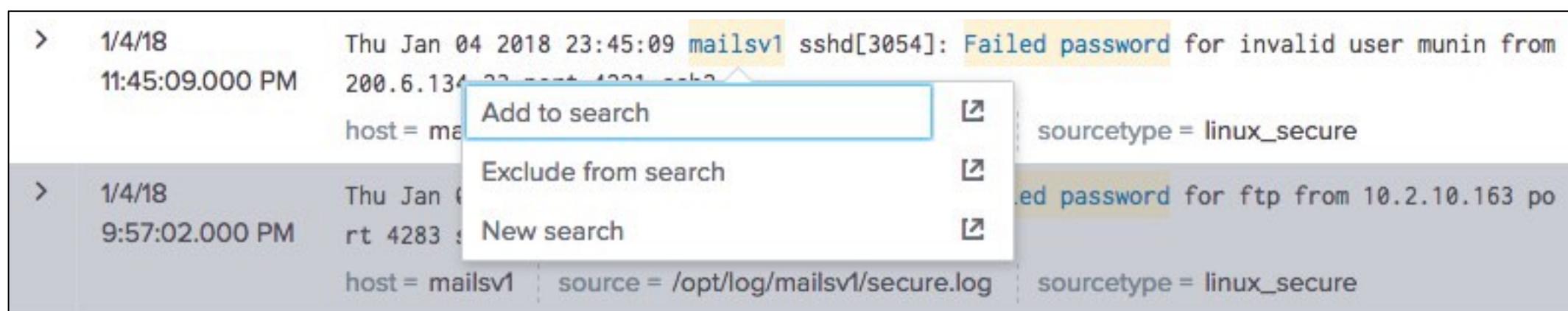
- time range picker**: Located at the top right, with a green arrow pointing to the "Save As" and "Close" buttons.
- search mode**: Located at the top right, with a green arrow pointing to the "Smart Mode" dropdown.
- Events (1,942)**: The selected tab in the navigation bar, with a green arrow pointing to it.
- timeline**: The visualization mode currently selected, with a green arrow pointing to it.
- paginator**: The pagination controls at the bottom of the search results table, with a green arrow pointing to the page number 1.
- Fields sidebar**: A sidebar on the left containing "SELECTED FIELDS" (host, source, sourcetype) and "INTERESTING FIELDS" (action, app, date_hour).
- timestamp**: The timestamp column header in the search results table, with a green box highlighting the "1/4/18 11:45:09.000 PM" entry.
- selected fields**: A box highlighting the event details for the first result, showing host=mailsv1, source=/opt/log/mailsv1/secure.log, and sourcetype=linux_secure.
- events**: A large green box enclosing the list of search results, which include multiple entries for failed password attempts on mailsv1.

Search results table (partial view):

Time	Event
1/4/18 11:45:09.000 PM	Thu Jan 04 2018 23:45:09 mailsv1 sshd[3054]: Failed password for invalid user munin from 200.6.134.23 port 4221 ssh2 host = mailsv1 source = /opt/log/mailsv1/secure.log sourcetype = linux_secure
9:57:02.000 PM	mailsv1 sshd[4690]: Failed password for ftp from 10.2.10.163 po rt 4283 ssh2 host = mailsv1 source = /opt/log/mailsv1/secure.log sourcetype = linux_secure
> 1/4/18 8:09:05.000 PM	Thu Jan 04 2018 20:09:05 mailsv1 sshd[3867]: Failed password for news from 10.2.10.163 p ort 4017 ssh2

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



Changing Search Results View Options

You have several layout options for displaying your search results

The screenshot shows a Splunk search interface for a query of "failed password". The search results are displayed in three different formats:

- Raw View:** Shows raw log entries. The first entry is highlighted:

```
11:45:09.000 PM |> Thu Jan 04 2018 23:45:09 mailsv1 sshd[3054]: Failed password for invalid user munin from 200.6.134.23 port 4221 ssh2
```
- List View:** Shows a list of events. The first two entries are highlighted:

Time	Event
11:45:09.000 PM	Thu Jan 04 2018 23:45:09 mailsv1 sshd[3054]: Failed password for invalid user munin from 200.6.134.23 port 4221 ssh2 host = mailsv1 source = /opt/log/mailsv1/secure.log sourcetype = linux_secure
9:57:02.000 PM	Thu Jan 04 2018 21:57:02 mailsv1 sshd[4690]: Failed password for ftp from 10.2.10.163 port 4283 ssh2 host = mailsv1 source = /opt/log/mailsv1/secure.log sourcetype = linux_secure
- Table View:** Shows a table of events. The first two entries are highlighted:

Time	host	source	sourcetype
11:45:09.000 PM	mailsv1	/opt/log/mailsv1/secure.log	linux_secure
9:57:02.000 PM	mailsv1	/opt/log/mailsv1/secure.log	linux_secure

The interface includes a sidebar with selected fields and interesting fields, and a bottom navigation bar with a "Raw" button.

Selecting a Specific Time

The diagram illustrates five methods for selecting a specific time, grouped on the left, and a detailed time selector on the right.

Left Column (Custom Time Ranges):

- Relative:** Set Earliest to 7 Days Ago and Latest to Now. Options include No Snap-to and Beginning of day.
- Real-time:** Set Earliest to 7 Days Ago and Latest to now. Options include Days Ago ▾ and Apply.
- Date Range:** Set Between 12/29/2017 and 01/05/2018, and 00:00:00 and 24:00:00. Options include Between ▾ and Apply.
- Date & Time Range:** Set Between 12/29/2017 at 11:00:00.000 and 01/05/2018 at 11:26:07.000. Options include Between ▾ and Apply.
- Advanced:** Set Earliest to -24h@h and Latest to now. Options include -24h@h, now, Apply, and Documentation ↗.

Right Column (Presets):

- Presets:** A dropdown menu containing:
 - REAL-TIME:** 30 second window, 1 minute window, 5 minute window, 30 minute window, 1 hour window, All time (real-time)
 - RELATIVE:** Today, Week to date, Business week to date, Month to date, Year to date, Yesterday, Previous week, Previous business week, Previous month, Previous year
 - OTHER:** Last 15 minutes, Last 60 minutes, Last 4 hours, Last 24 hours, Last 7 days, Last 30 days, All time
- Last 7 days ▾** (highlighted with a green box)
- Search icon** (highlighted with a green box)

Annotations:

- A yellow callout box labeled **custom time ranges** points to the five methods on the left.
- A yellow callout box labeled **preset time ranges** points to the Presets section on the right.

Time Range Abbreviations

- Time ranges are 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`

`earliest=-2d@ latest=@d
d`

`earliest=6/15/2017:12:30
:00`

looks back one hour

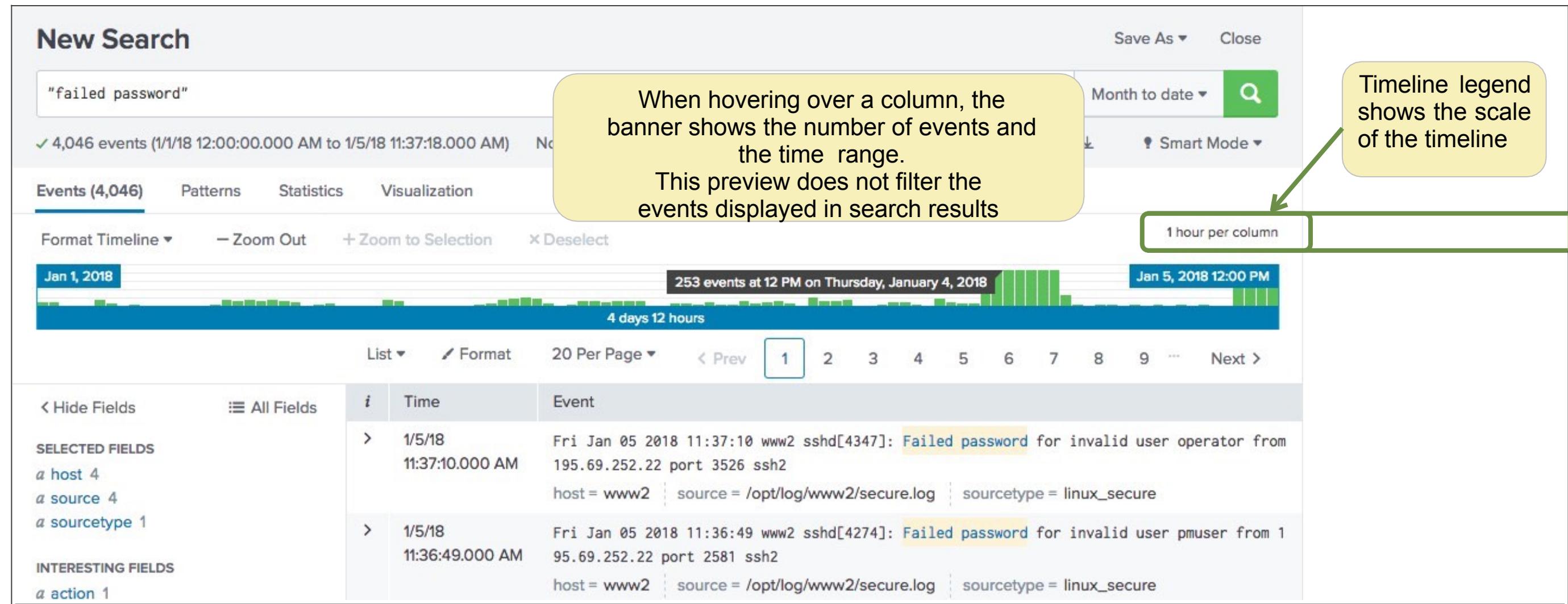
looks back from two days ago, up to the beginning of today looks back to specified time

Note

If time specified, it must be in MM/DD/YYYY:HH:MM:SS format.

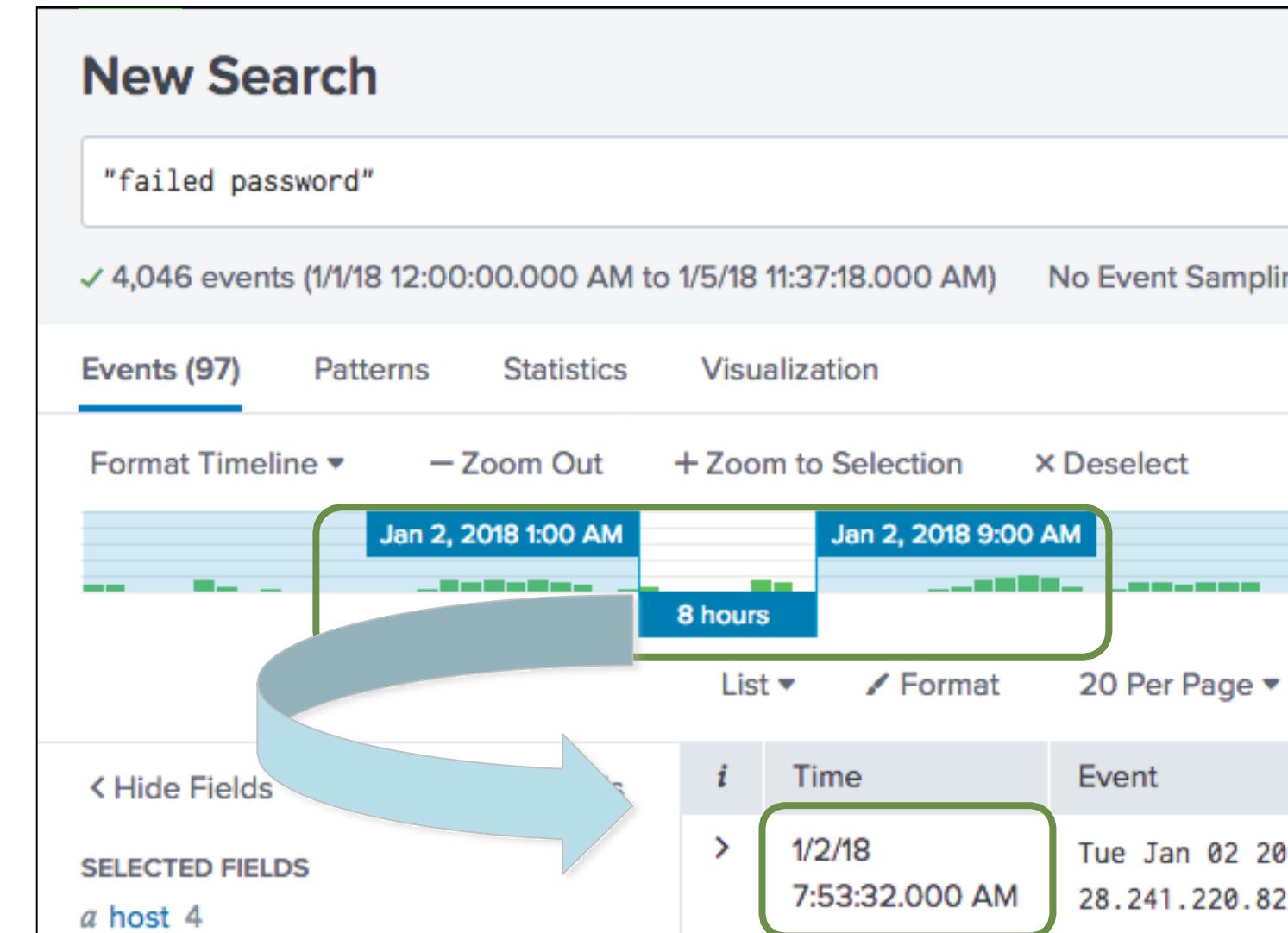
Viewing the Timeline

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



Viewing 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)



Using Other Timeline Controls

- **Format Timeline**

- Hides or shows the timeline in different views

- **Zoom Out**

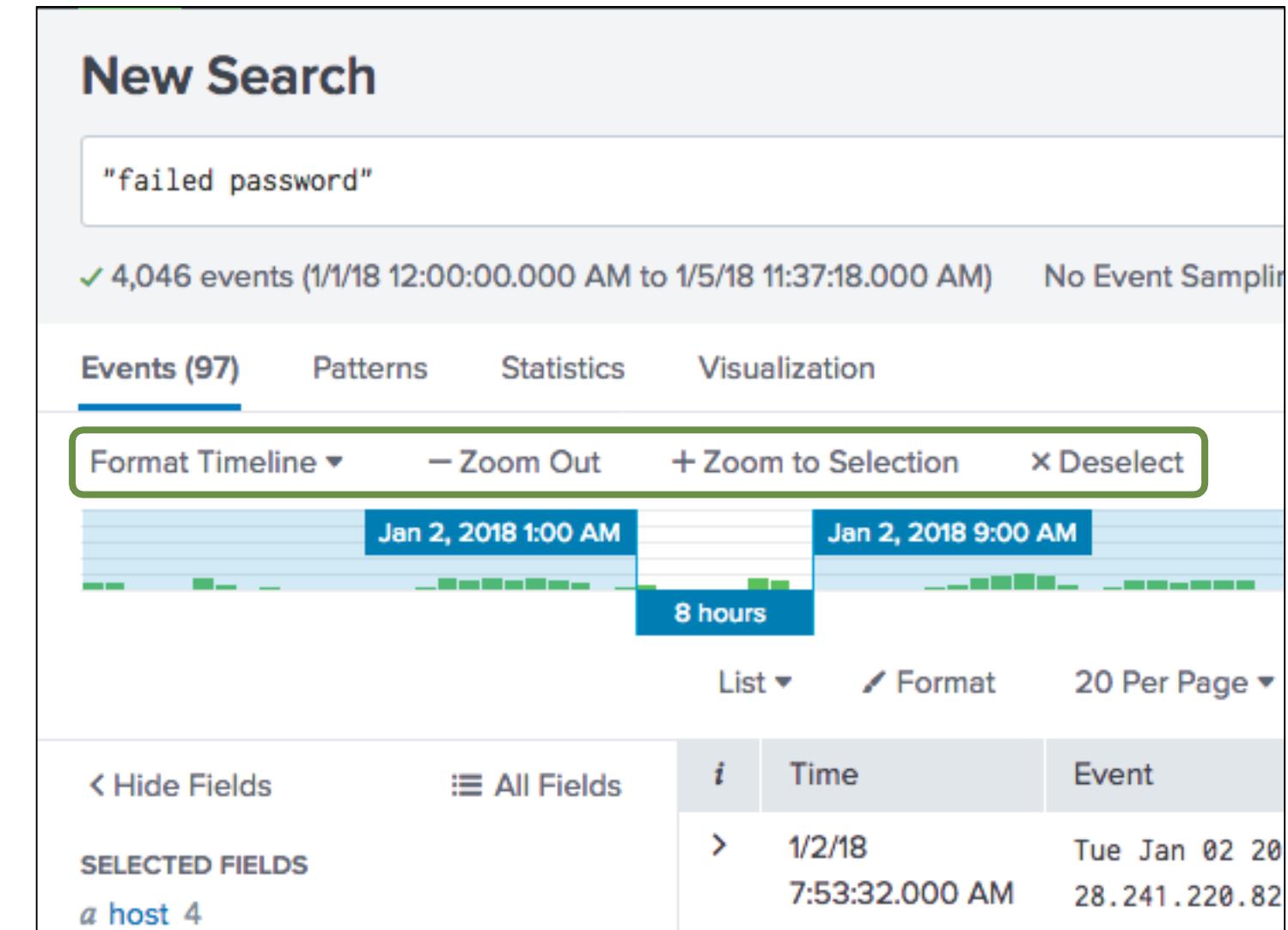
- Expands the time focus and re-executes the search

- **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



Controlling and Saving 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

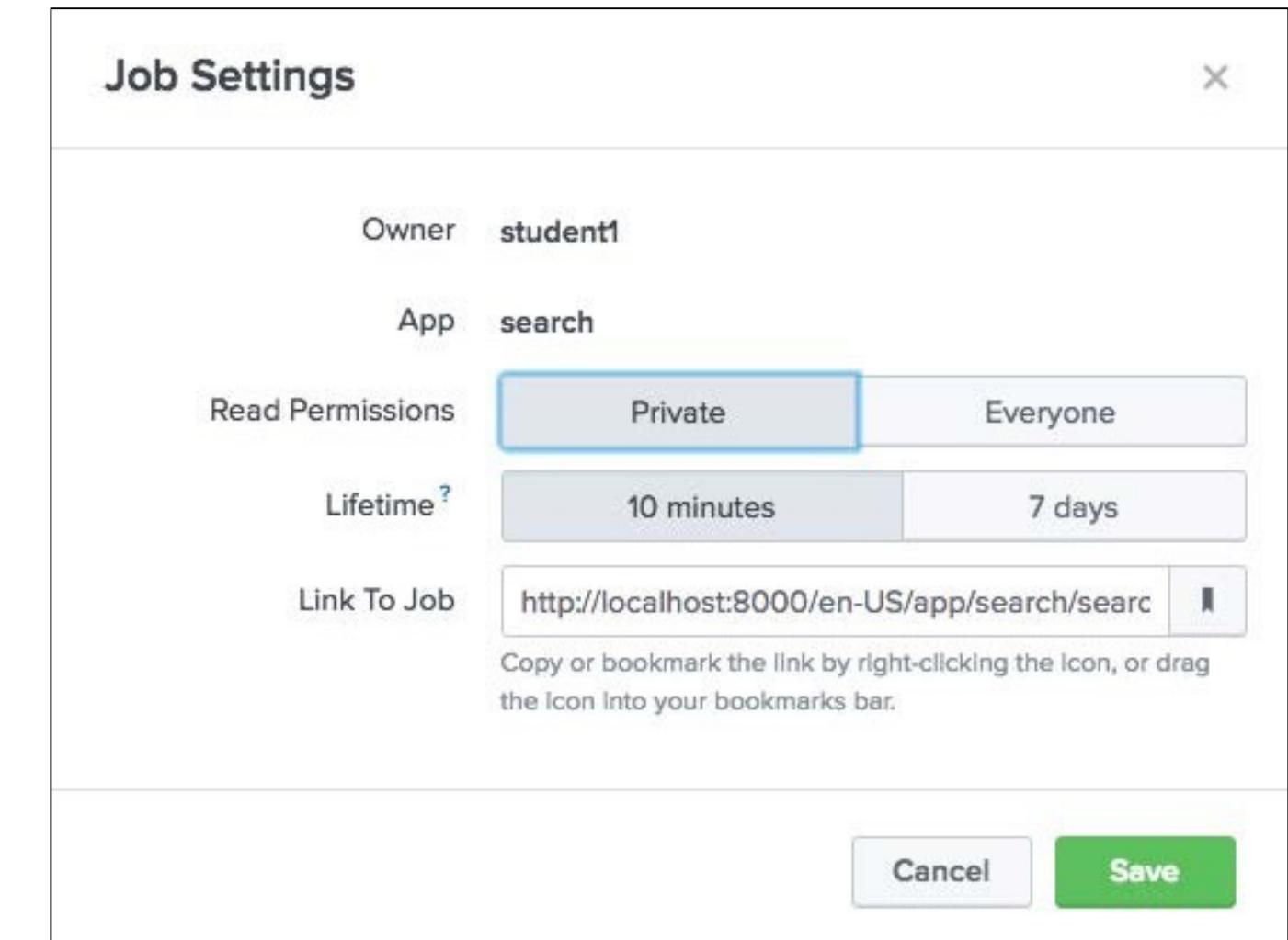
The screenshot shows the Splunk interface for a "New Search" titled "failed password". The search bar contains the query "failed password". Below it, a message indicates "4,128 events (1/18 12:00:00.000 AM to 1/5/18 11:56:03.000 AM)" and "No Event Sampling". The "Events (4,128)" tab is selected. A "Job" button in the top right is highlighted with a green box. A dropdown menu from this button includes "Edit Job Settings..." which is also highlighted with a green box. To the right of the search results, a "Job Settings" dialog box is open, also highlighted with a green box. The dialog box displays the following information:

- Owner: student1
- App: search
- Read Permissions: Private (selected)
- Lifetime: 10 minutes
- Link To Job: http://localhost:8000/en-US/app/search/searc

A green arrow points from the "Edit Job Settings..." item in the dropdown to the "Edit Job Settings..." item in the dialog box.

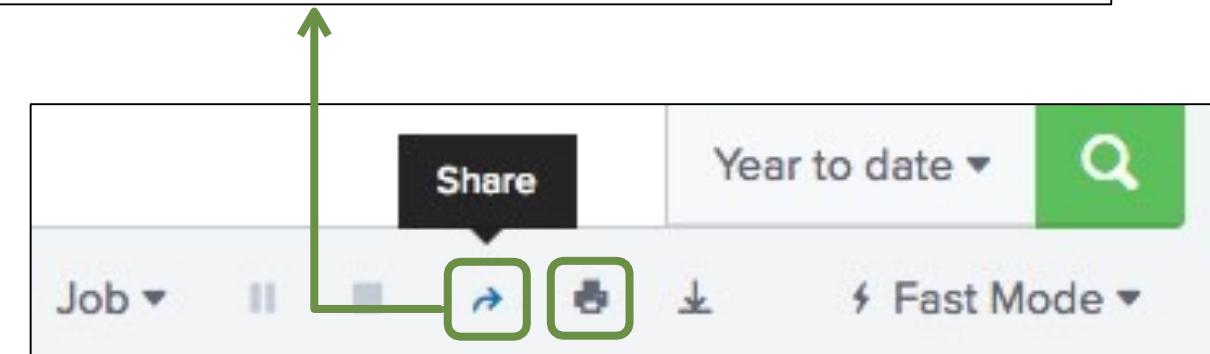
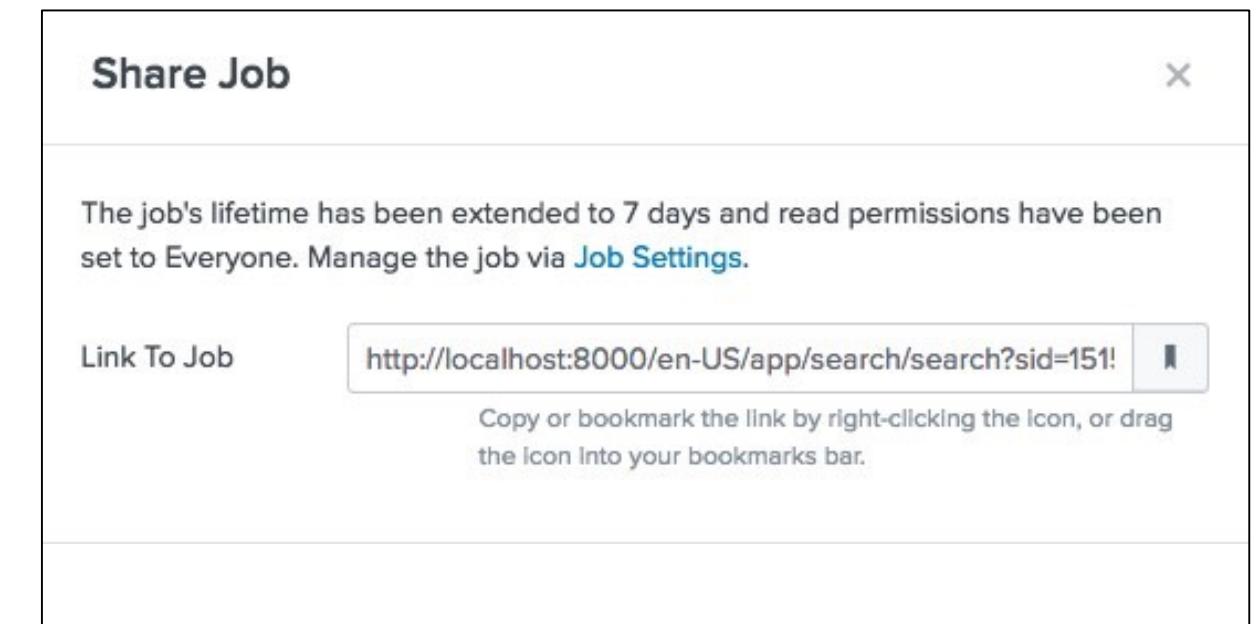
Setting Permissions

- **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



Sharing Search Jobs

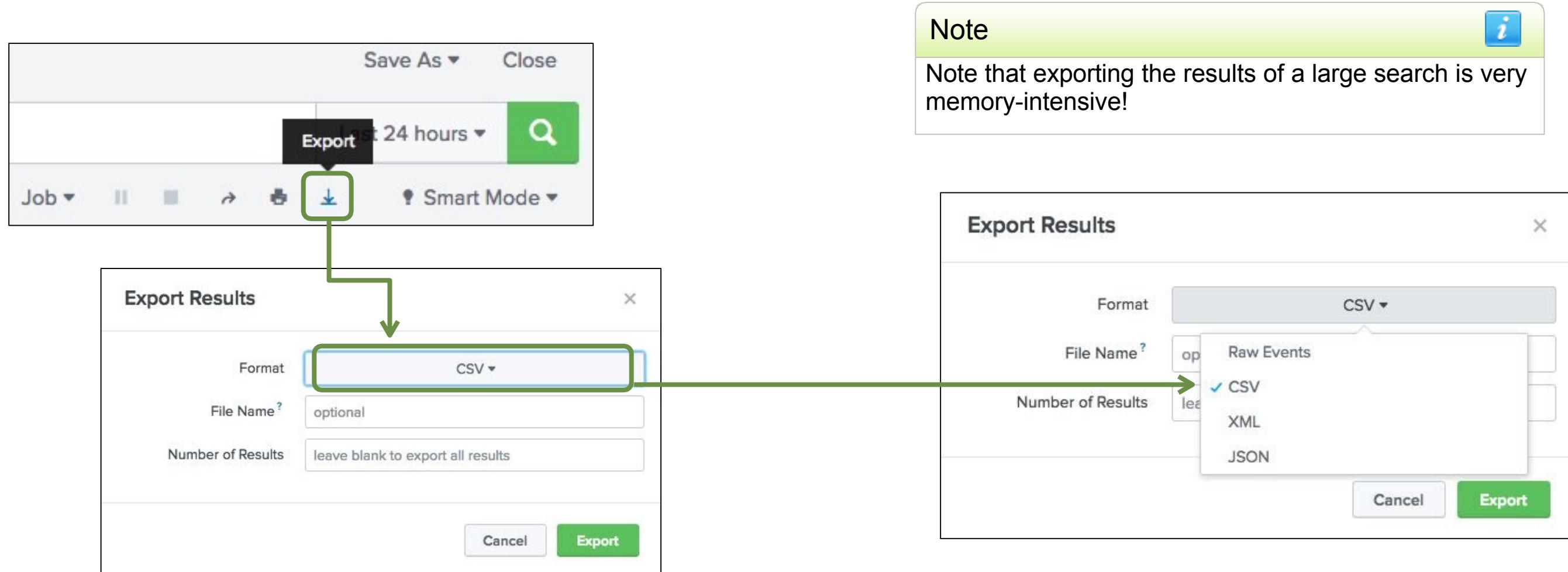
- Use the Share button next to the Job bar to quickly:
 - Give everyone read permissions
 - Extend results retention to 7 days
 - Get a sharable link to the results
- Sharing search allows multiple users working on same issue to see same data
 - More efficient than each running search separately
 - Less load on server and disk space used



- Can also click printer icon to print results or save as PDF

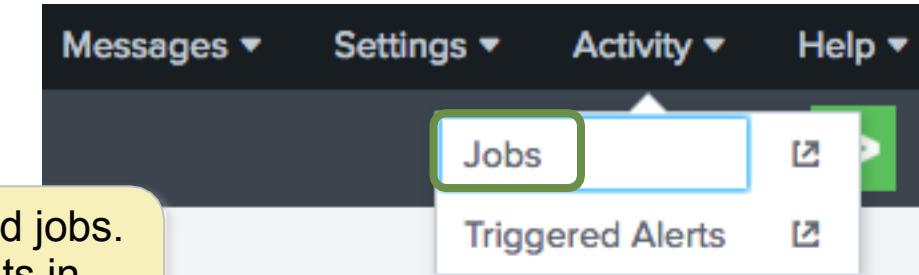
Exporting Search Results

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



Viewing Your Saved Jobs

- 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.)

The screenshot shows a table titled '3 Jobs' under the 'App: Search & Reporting (search) ▾'. The table has columns for Owner, Application, Events, Size, Created at, Expires, Runtime, Status, and Actions. One row is visible, showing 'student1' as the owner, 'search' as the application, 2,449 events, 616 KB size, created on Jan 5, 2018 at 12:45:47 PM, and expired on Jan 5, 2018 at 1:02:50 PM. The runtime is 00:00:01 and the status is Done. The 'Actions' column shows a Job link with a green border and a download icon. A tooltip for the 'failed password' link in the 'Events' column reads: "failed password" [14/18 12:00:00.000 PM to 1/5/18 12:45:47.000 PM]."

	<input type="checkbox"/>	Owner	Application	Events	Size	Created at	Expires	Runtime	Status	Actions
>	<input type="checkbox"/>	student1	search	2,449	616 KB	Jan 5, 2018 12:45:47 PM	Jan 5, 2018 1:02:50 PM	00:00:01	Done	Job ▾

Viewing 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

The screenshot shows the Splunk Search & Reporting interface. At the top, there are tabs for Search, Datasets, Reports, Alerts, and Dashboards. On the right, a green icon with a right arrow and the text "Search & Reporting" is visible. Below the tabs is a search bar with placeholder text "enter search here...". To the right of the search bar is a "Last 24 hours" dropdown and a magnifying glass icon. Further right are "Smart Mode" and a gear icon.

The main area is titled "Search" and features a "How to Search" section with links to "Documentation" and "Tutorial". To the right is a "What to Search" summary: 537,902 Events indexed from 3 months ago to a few seconds ago, with the earliest event being 20 days ago and the latest event being a few seconds ago.

A callout box labeled "1" highlights the "Search History" button, which is part of a dropdown menu titled "Search History". This menu includes a "filter" input field and a "No Time Filter" button, which is highlighted with a green border and a callout box labeled "2". Below this are buttons for "20 Per Page" and "All".

A third callout box labeled "3" points to the first item in the search history list, which is a long search query starting with "(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". To the left of this query is an "i" icon. To the right are "Actions" and "Last Run" columns.

Actions	Last Run
Add to Search	a few seconds ago
Add to Search	25 minutes ago
Add to Search	2 hours ago
Add to Search	3 hours ago

3. Click the > icon in the leftmost column to expand long queries to display the full text

Module 6: Using Fields in Searches

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, AND is implied unless otherwise specified

The screenshot shows a log search interface with four search terms listed vertically:

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

A purple arrow points to the second term, "action=purchase".

Field Discovery

- Splunk automatically discovers many fields based on sourcetype and key/value pairs found in the data
- Prior to search time, some fields are already stored with the event in the index:
 - Meta fields, such as `host`, `source`, `sourcetype`, and `index`
 - Internal fields such as `_time` and `_raw`
- At search time, *field discovery* discovers fields directly related to the 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.

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
>	1/5/18 1:21:10.000 PM	192.162.19.179 - - [05/Jan/2018:13:21:10] "POST /cart/success.do?JSESSIONID=SD1SL6FF4ADFF4964 HT TP 1.1" 200 966 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-26" "Mozilla/5 .0 (iPad; U; CPU OS 4_3_5 like Mac OS X; en-us) AppleWebKit/533.17.9 (KHTML, like Gecko) Version /5.0.2 Mobile/8L1 Safari/6533.18.5" 552

Note



For more information, please see: <http://docs.splunk.com/Documentation/Splunk/latest/Data/Listofpretrainedsourcetypes>

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)

indicates the field's values are alpha-numeric

indicates that the majority of the field values are numeric

New Search
"failed password"

✓ 2,406 events (1/4/18 1:00:00.000 PM to 1/5/18 1:36:10.000 PM) No Event Sampling ▾

Events (2,406) Patterns Statistics Visualization

Format Timeline ▾ List ▾ Format 20 Per Page ▾

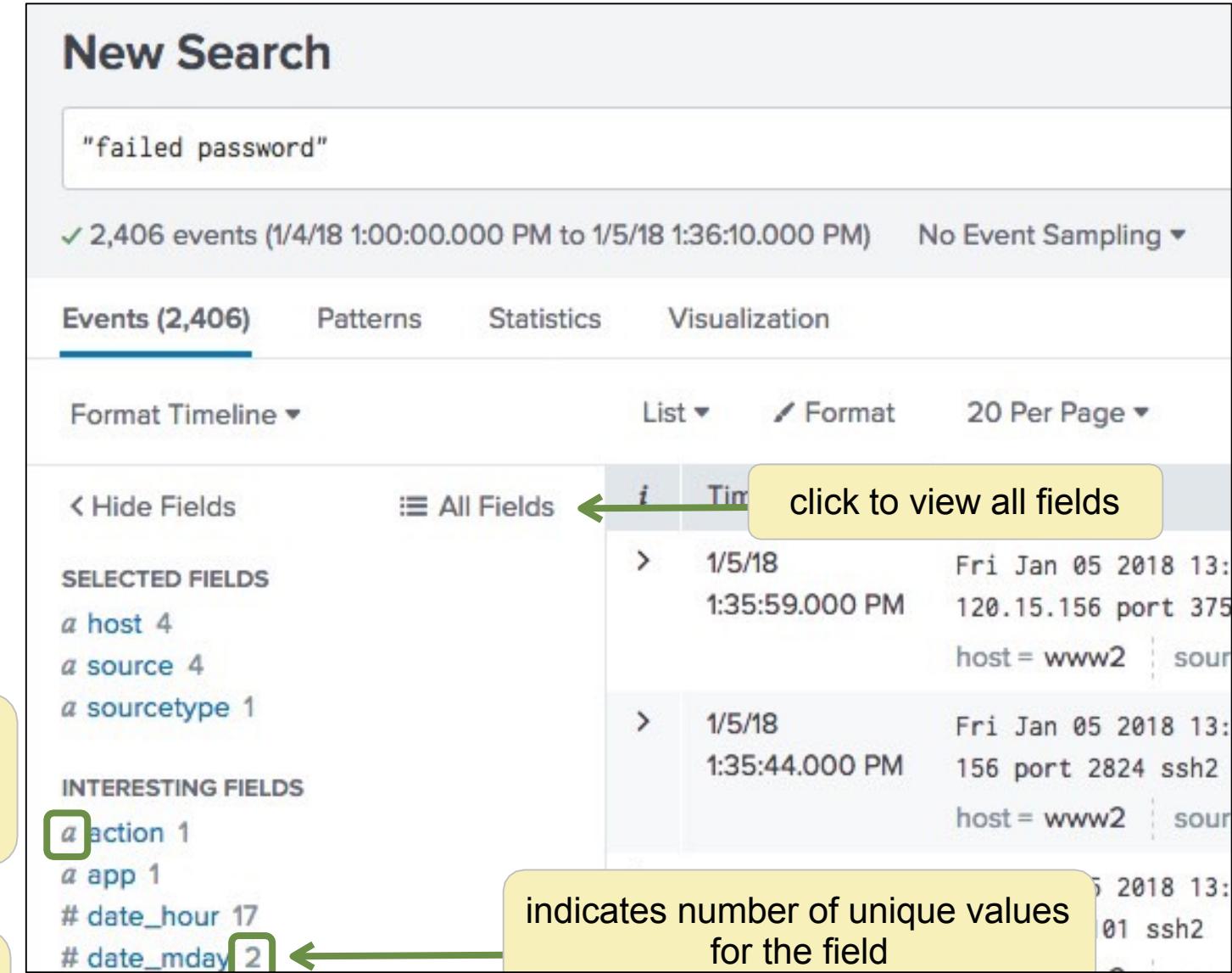
◀ Hide Fields ⌂ All Fields i Tim click to view all fields

	Date	Time	Host	Source
>	1/5/18	Fri Jan 05 2018 13:13:59.000 PM	120.15.156	port 375
			host = www2	sour
>	1/5/18	Fri Jan 05 2018 13:13:44.000 PM	156	port 2824 ssh2
			host = www2	sour

SELECTED FIELDS
a host 4
a source 4
a sourcetype 1

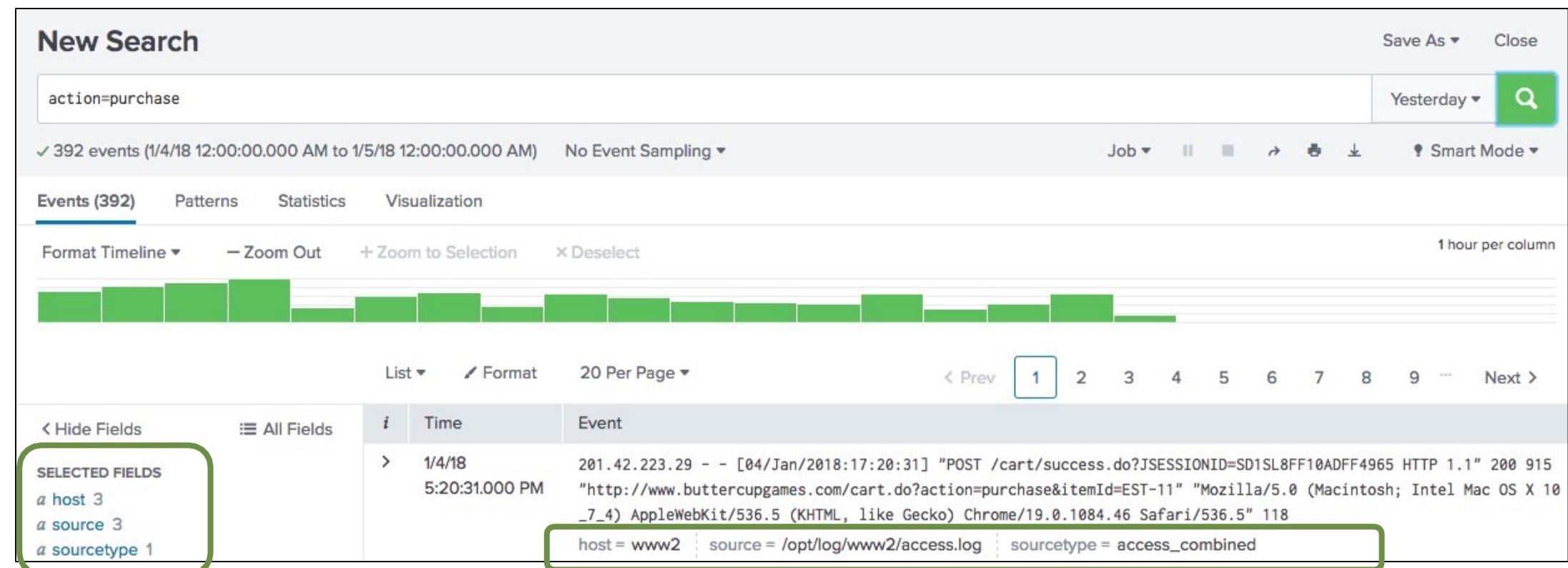
INTERESTING FIELDS
a action 1
a app 1
date_hour 17
date_mday 2
date_minute 60

indicates number of unique values for the field



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



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
- Note that a selected field appears:
 - In the Selected Fields section of the Fields sidebar
 - Below each event where a value exists for that field

The screenshot illustrates the process of selecting an interesting field as a selected field in Splunk. It shows two panels: a field dialog and a search results table.

Field Dialog: On the left, a sidebar lists "SELECTED FIELDS" (a host 3, a source 3, a sourcetype 1) and "INTERESTING FIELDS" (a action 1, # bytes 100+, a categoryId 8, a clientip 100+, # date_hour 18, # date_mday 1, # date_minute 59, a date_month 1). The "a action 1" item is highlighted with a green box and has a red circle with the number "1" above it. On the right, a detailed view of the "action" field shows "1 Value, 100% of events". A "Selected" checkbox is checked, and a "Yes" button is highlighted with a green box and a red circle with the number "2".

Search Results: On the right, the search results table shows 392 events from 1/4/18 to 1/5/18. The "Events (392)" tab is selected. The "Selected Fields" sidebar at the bottom includes "a action 1" (highlighted with a blue box), "a host 3", "a source 3", and "a sourcetype 1". The "INTERESTING FIELDS" sidebar includes "# bytes 100+". The first event in the table is highlighted with a yellow box and shows "action = purchase", "host = www2", and "source = /opt/log/www2/access.log".

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 Splunk interface for managing selected fields. On the left, there's a sidebar with buttons for 'Hide Fields' and 'All Fields'. The 'All Fields' button is highlighted with a green border. On the right, a modal window titled 'Select Fields' displays a list of discovered fields. The 'action' field is selected, indicated by a checked checkbox. Other fields listed include host, source, sourcetype, JSESSIONID, bytes, and categoryid. The main pane below shows event details: timestamp (5:20:31.000 PM), offset (0 915), URL ("http://www.butte"), operating system (Mac OS X 10_7_4), and browser (AppleW). The event also contains the selected field 'action = purchase'.

	Field	# of Values	Event Coverage	Type
>	action	1	100%	String
>	host	3	100%	String
>	source	3	100%	String
>	sourcetype	1	100%	String
>	JSESSIONID	>100	100%	String
>	bytes	>100	100%	Number
>	categoryid	8	50.77%	String

SELECTED FIELDS

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

5:20:31.000 PM 0 915 "http://www.butte
Mac OS X 10_7_4) AppleWebKit/537.36 (KHTML, like Gecko)
action = purchase | host
> 1/4/18 201.42.223.29 - - [04/J

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

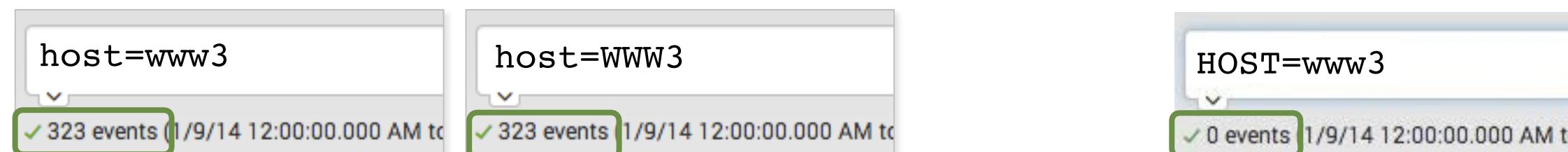
Value	Count	%
failure	1,942	49.923%
view	440	11.311%
purchase	392	10.077%
addtocart	377	9.692%
success	230	5.912%
TCP_REFRESH_HIT	189	4.859%
remove	100	2.602%
TCP_DENIED	43	1.105%

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="202.201.1.0/24  
"
```

```
clientip="202.201.1.  
*"
```

- 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)
```

- Use relational operators

With numeric fields

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

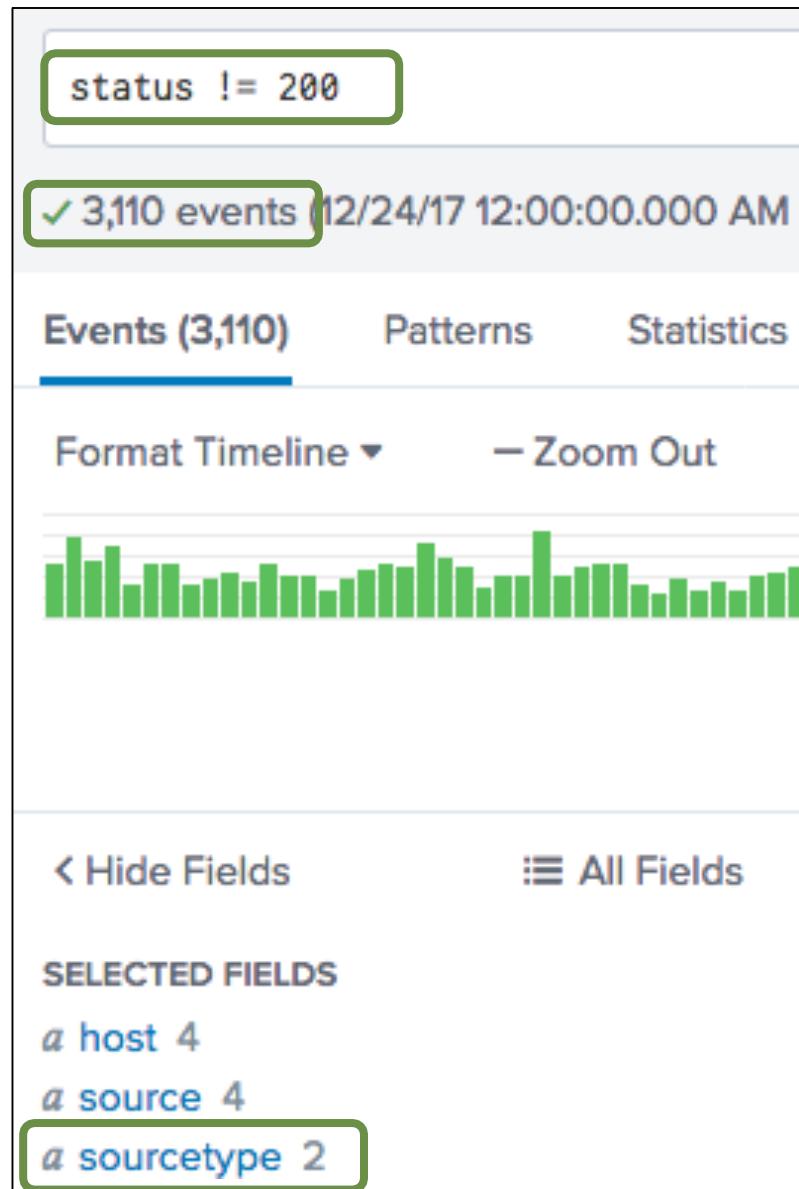
With alphanumeric fields

```
host!  
=www3
```

`!=` vs. `NOT`

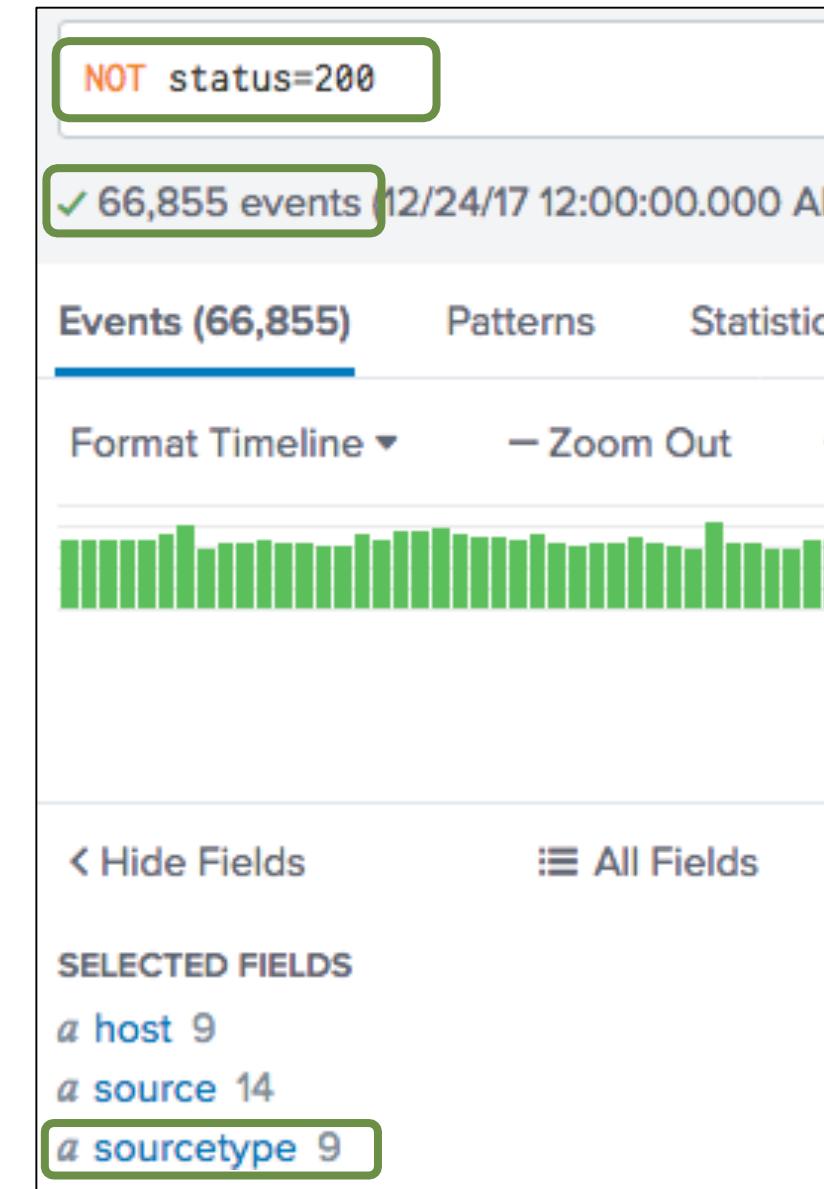
- Both `!=` field expression and `NOT` operator exclude events from your search, but produce different results
- Example: `status != 200`
 - Returns events where `status` field exists and value in field doesn't equal 200
- Example: `NOT status = 200`
 - Returns events where `status` field exists and value in field doesn't equal 200 -- **and** all events where `status` field **doesn't** exist

$!=$ vs. NOT (cont.)



- In this example:
- `status != 200` returns **3,110** events from **2 sourcetypes**
 - `NOT status=200` returns **66,855** events from **9 sourcetypes**

Note
The results from a search using `!=` are a **subset** of the results from a similar search using `NOT`.

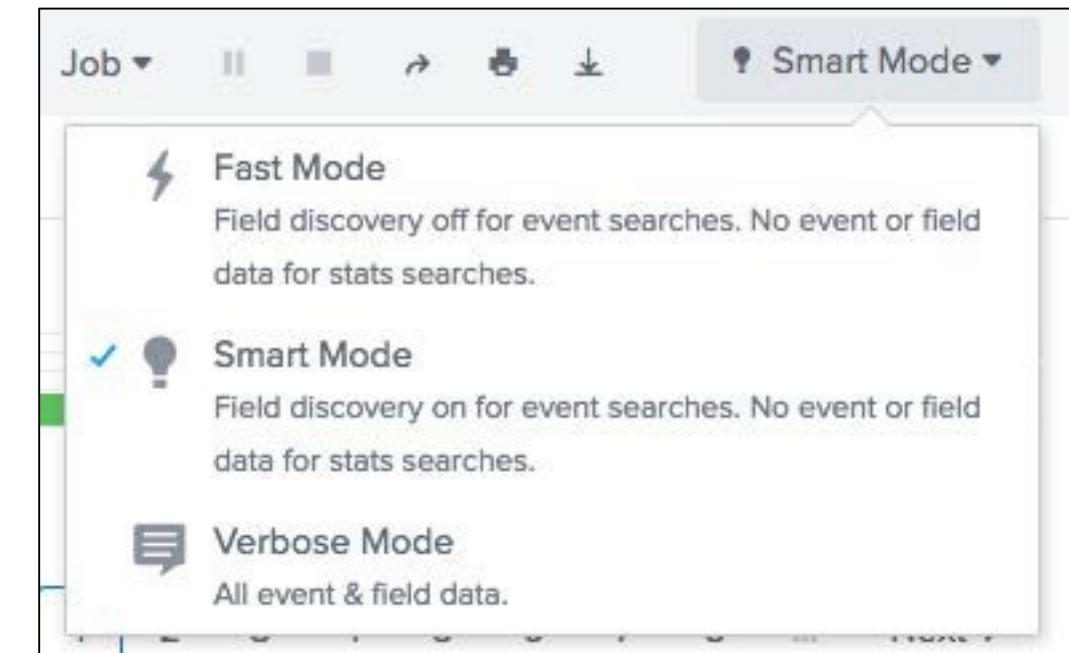


`!=` vs. `NOT` (cont.)

- Does `!=` and `NOT` ever yield the same results?
 - Yes, if you know the field you're evaluating always exists in the data you're searching
 - For example:
 - `?index=web sourcetype=access_combined status!=200`
 - `?index=web sourcetype=access_combined NOT status=200`
- yields same results because `status` field always exists in `access_combined` sourcetype

Search Modes: Fast, Smart, Verbose

- Fast: emphasizes speed over completeness
- Smart: balances speed and completeness (default)
- Verbose:
 - Emphasizes completeness over speed
 - Allows access to underlying events when using reporting or statistical commands (in addition to totals and stats)



Note



You'll discuss statistical commands later in this course.

Module 7

Best Practices

Search Best Practices

- Time is the most efficient filter
- Specify one or more index values at the beginning of your search string
- Include as many search 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
- Make your search terms as specific as possible
 - Searching for "access denied" is always better than searching for "denied"
- Inclusion is generally better than exclusion
 - Searching for "access denied" is faster than searching for NOT "access granted"

Search Best Practices (cont.)

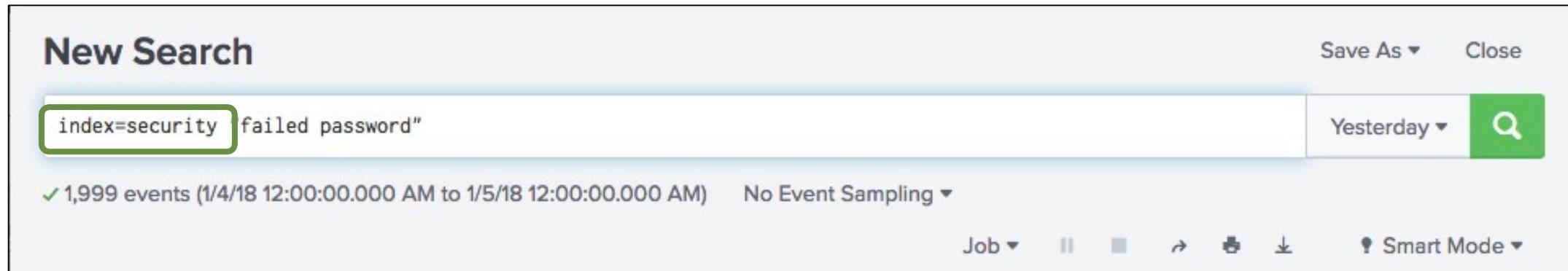
- Filter as early as possible
 - For example, remove duplicate events, then sort
- Avoid using wildcards at the beginning or middle of a string
 - Wildcards at *beginning* of string scan all events within timeframe
 - Wildcards in *middle* of string may return inconsistent results
 - So use fail* (not *fail or *fail* or f*il)
- When possible, use OR instead of wildcards
 - For example, use (user=admin **OR** user=administrator) instead of user=admin*

Note 

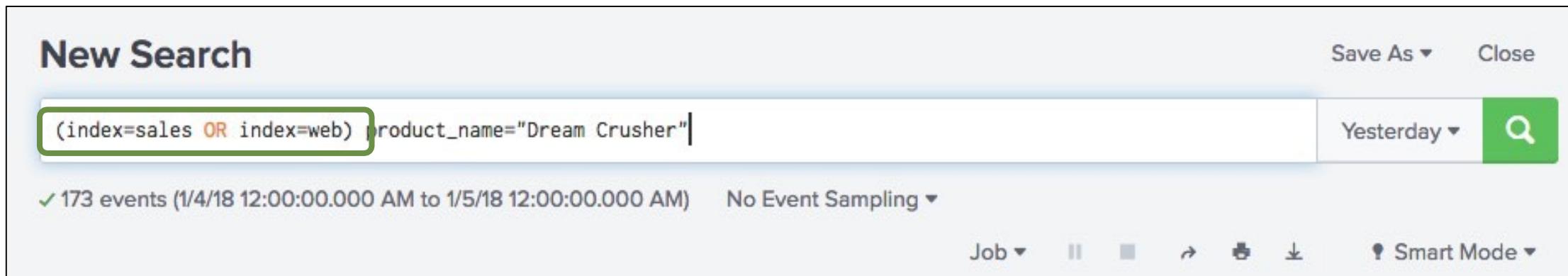
Remember, field names are case *sensitive* and field values are case *insensitive*.

Working with Indexes

- This search returns event data from the security index

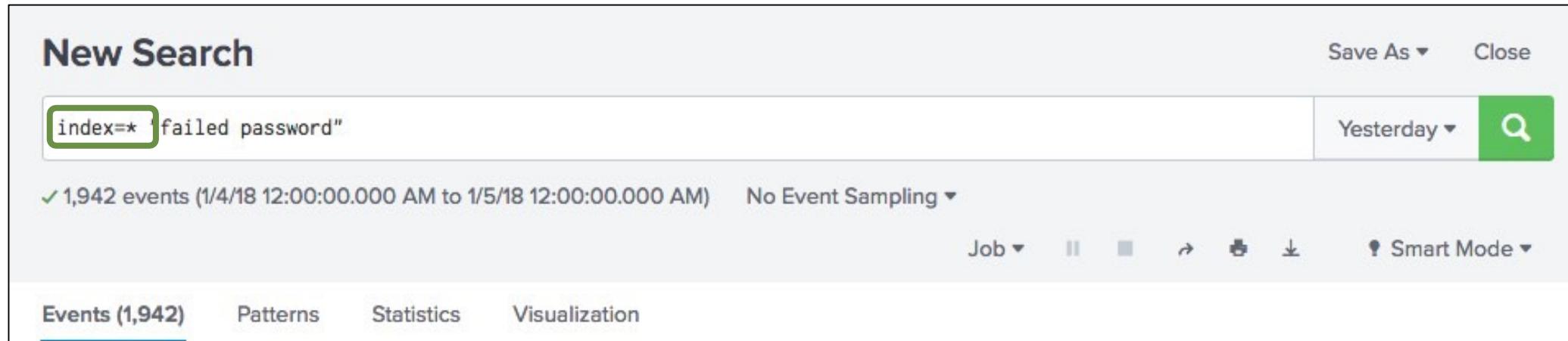


- It's possible to specify multiple index values in a search



Working with Indexes (cont.)

- It's possible to use a wildcard (*) in index values



- It's also possible to search *without* an index—but that's inefficient and **not recommended**

Note 1 i

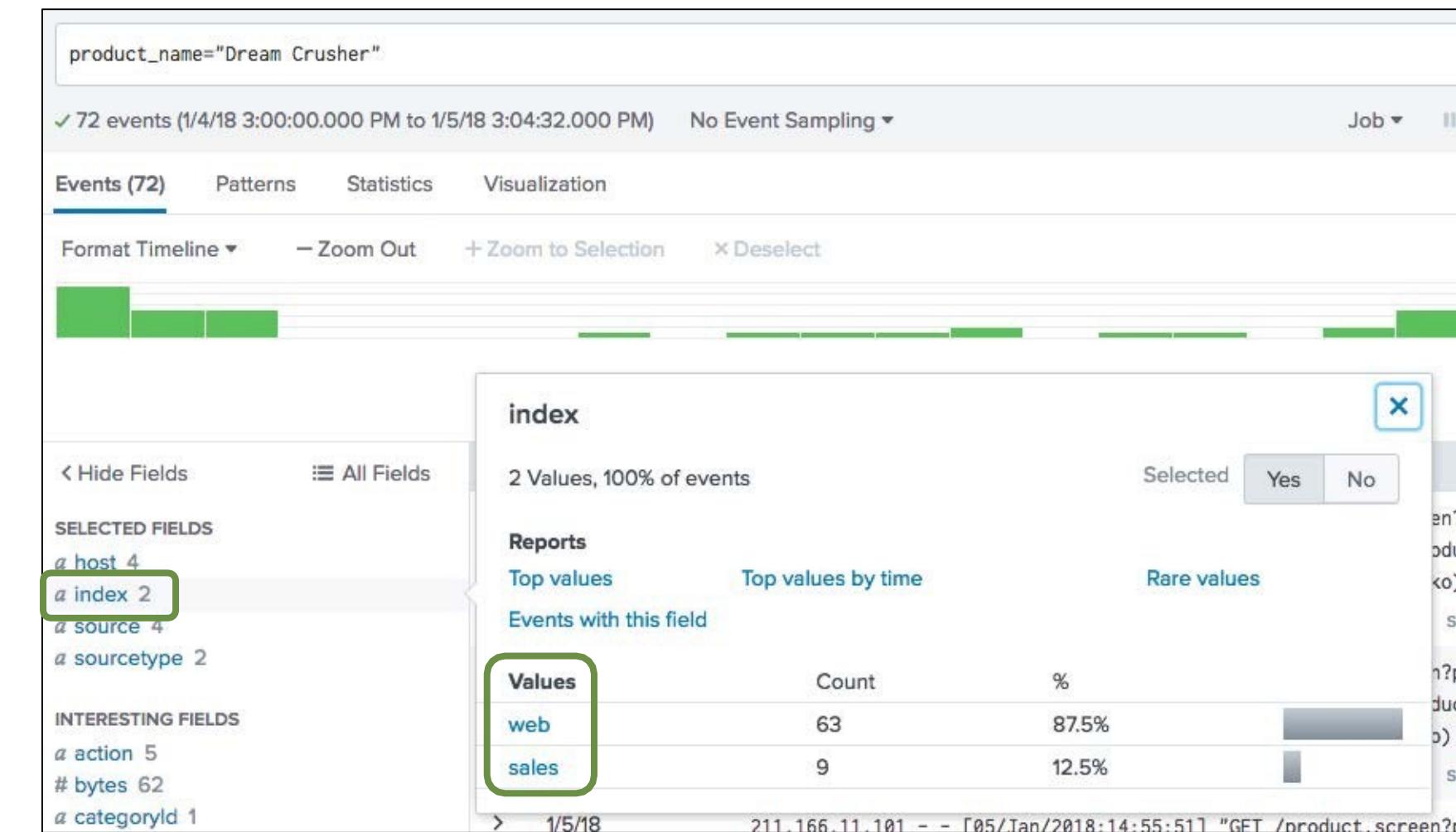
Although `index=*` is a valid search, better performance is always obtained by specifying one or more specific index values.

Note 2 i

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

Viewing the Index Field

- The *index* always appears as a field in search results
- In the search shown here, no index was indicated in the search, so data is returned from two indexes: web and sales
- Remember, this practice is **not** recommended—it's always more efficient to specify one or more indexes in your search

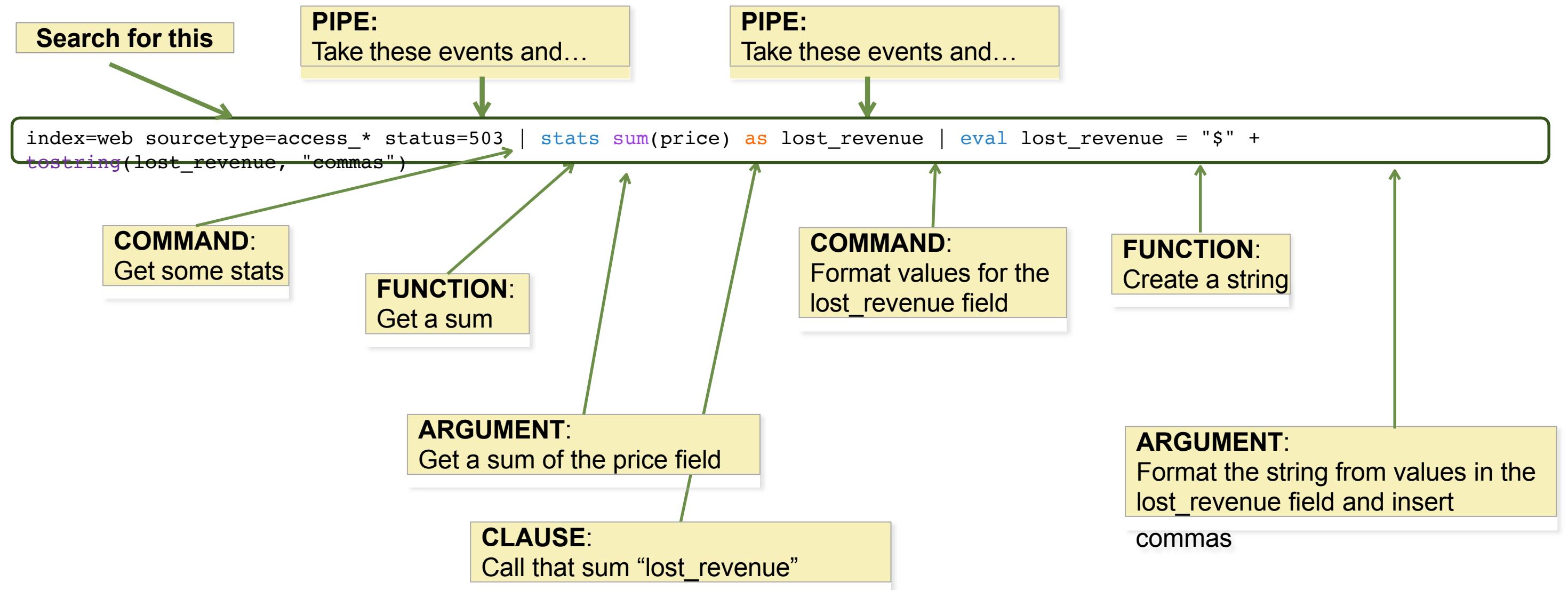


Module 8:

Splunk's Search Language

Search Language Syntax

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



Search Language Syntax Components

- Searches are made up of 5 basic components
 1. **Search terms** – what are you looking for?
 - Keywords, phrases, Booleans, etc.
 2. **Commands** – what do you want to do with the results?
 - Create a chart, compute statistics, evaluate and format, etc.
 3. **Functions** – how do you want to chart, compute, or evaluate the results?
 - Get a sum, get an average, transform the values, etc.
 4. **Arguments** – are there variables you want to apply to this function?
 - Calculate average value for a specific field, convert milliseconds to seconds, etc.
 5. **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

