



Lesson 200.2 Basic Searching



Learning Objectives

At the end of this lesson, learners will be able to:

- Describe adding data to Splunk.
- Run basic searches.
- Set the time range of a search.
- Identify the contents of search results.
- Refine searches.
- Use the timeline.
- Use time modifiers.
- Control a search job.
- Save search results.

Introduction

This lesson will introduce you to basic search concepts with Splunk. After a brief introduction on **how data enters Splunk**, we will focus on understanding and using the **search interface**, working with the **time picker**, identifying the contents of the **search results**, and using various tools to **refine** and **control** Splunk searches.

We **strongly** recommend **following along** using your own **Splunk** instance or a connection to an existing one.

Happy **Splunking**!

2.0 Adding Data to Splunk

Splunk supports a **wide** range of data types, including logs, metrics, and events, and can handle both structured and unstructured data.

The **responsibility** of adding data to Splunk typically falls on the **IT or DevOps teams** within an organization who have **permission** to upload data to Splunk. They are responsible for **configuring** the **data inputs**, such as **forwarders**, **log files**, **network devices**, or **databases** for **automatically** sending data to Splunk for indexing and analysis.

Splunk end-users **do not** usually add data to Splunk, although exceptions may happen.

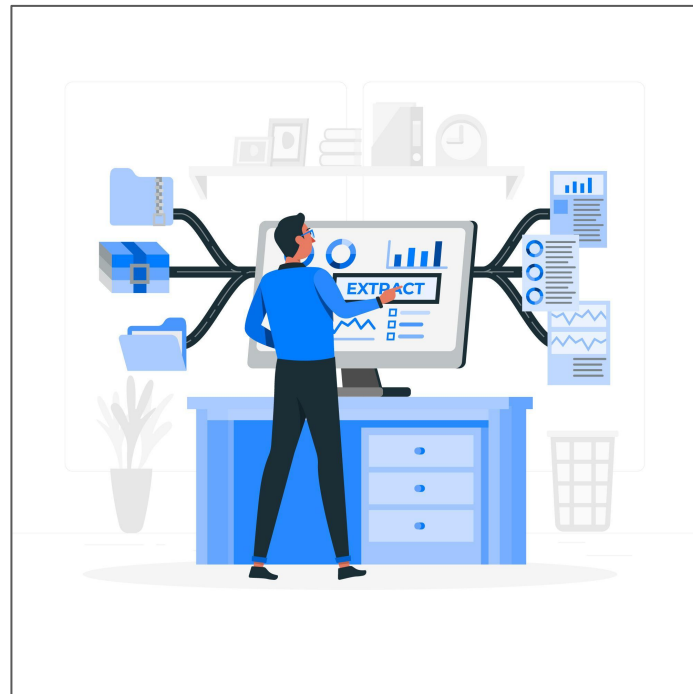


image: Freepik.com

2.0 Adding Data to Splunk (continued)

Adding data to Splunk involves **sending** the **data** to be **indexed** by Splunk.

There are **several** methods available for adding data to Splunk, including using the Splunk Web interface, the Splunk command-line interface, or by configuring data inputs to automatically collect data from various sources.

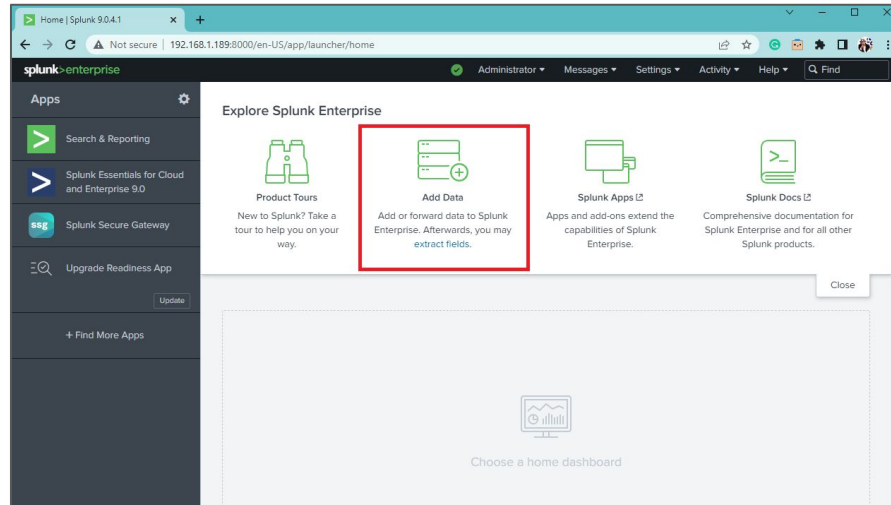


image: Screenshot of Splunk Web interface launcher window with the Add Data button highlighted.

2.0 Adding Data to Splunk (continued)

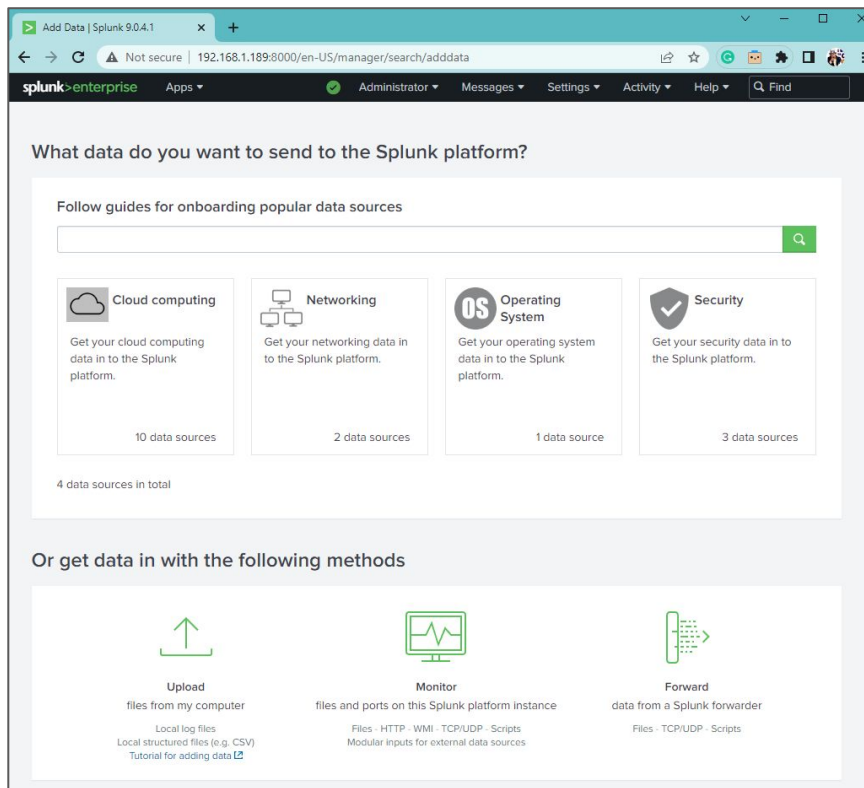


image: Screenshot of Splunk Web interface add data window displaying the various options to add data to splunk.

2.0 Adding Data to Splunk - Indexing

In Splunk, an index is a **repository** that stores the machine-generated data that is **ingested** by Splunk.

When **data is added to Splunk**, it is first **indexed**. This involves breaking it into individual **events**, parsing out relevant **fields**, and **assigning time stamps** and other metadata.

The indexed data is then stored in the appropriate index, where it can be easily searched, analyzed, and visualized.

Splunk provides several **default indexes**, such as main, _internal, and _audit, but users can also create their **own custom indexes** to organize data in a way that makes sense for their particular use case.

Indexes can be configured with **specific retention policies**, such as how long data should be stored before being rolled over or deleted, and how often data should be summarized or aggregated to improve search performance.

2.0 Adding Data to Splunk - sourcetype

In Splunk, **sourcetype** is a **metadata field** that identifies the data **source** and **format** of an event.

It is a **key** piece of information that is used by Splunk to parse and extract fields from the raw data and apply appropriate data models, tags, and other settings to it.

When **data is ingested** into Splunk, it is **assigned** a sourcetype based on its **source** and **format**, such as **access_combined** for Apache logs, **syslog** for system logs, or **JSON** for structured data.

Splunk provides a large number of **preconfigured sourcetypes** for common data sources, but users can also create their own **custom sourcetypes** if needed.

Sourcetypes play a **crucial** role in enabling users to search, analyze, and visualize their data effectively in Splunk.

By **accurately identifying** and **tagging** the **data source and format**, users can quickly find and extract meaningful insights from their data.

2.0 Adding Data to Splunk - tour

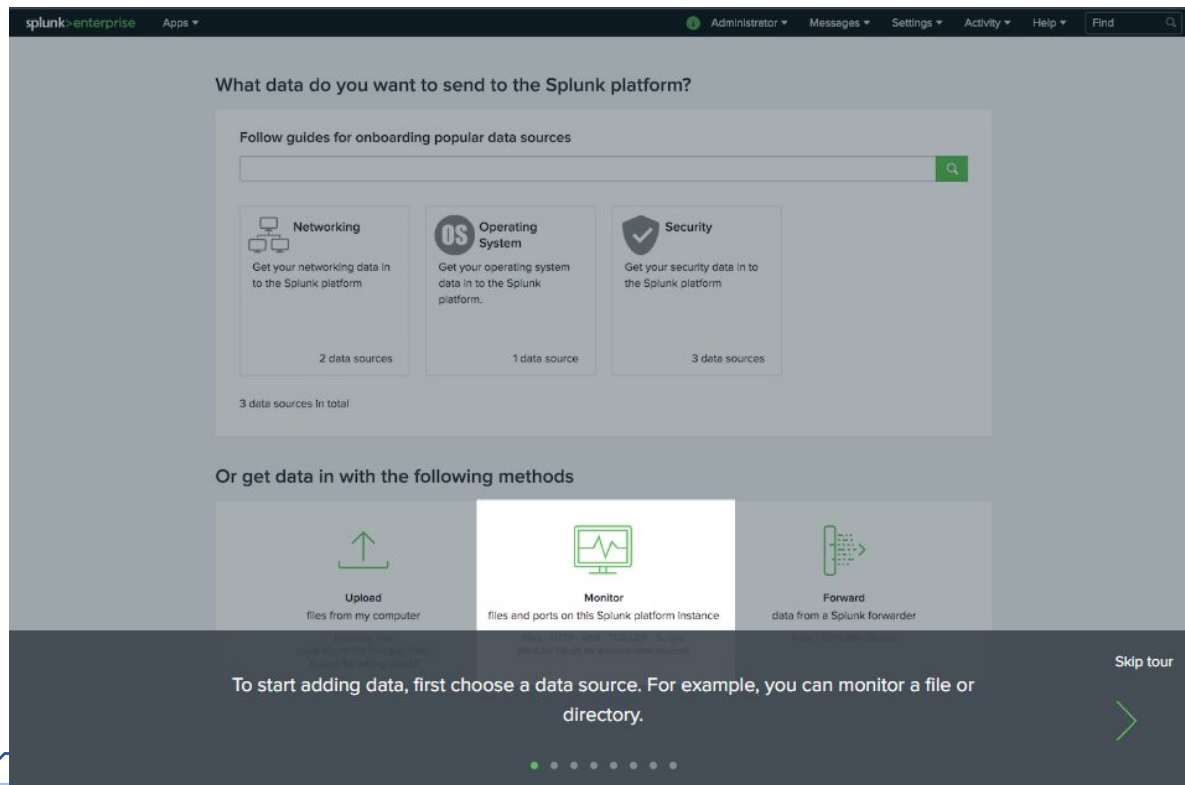


image: Screenshot of a Splunk example of adding data

2.0 Adding Data to Splunk - tour (continued)

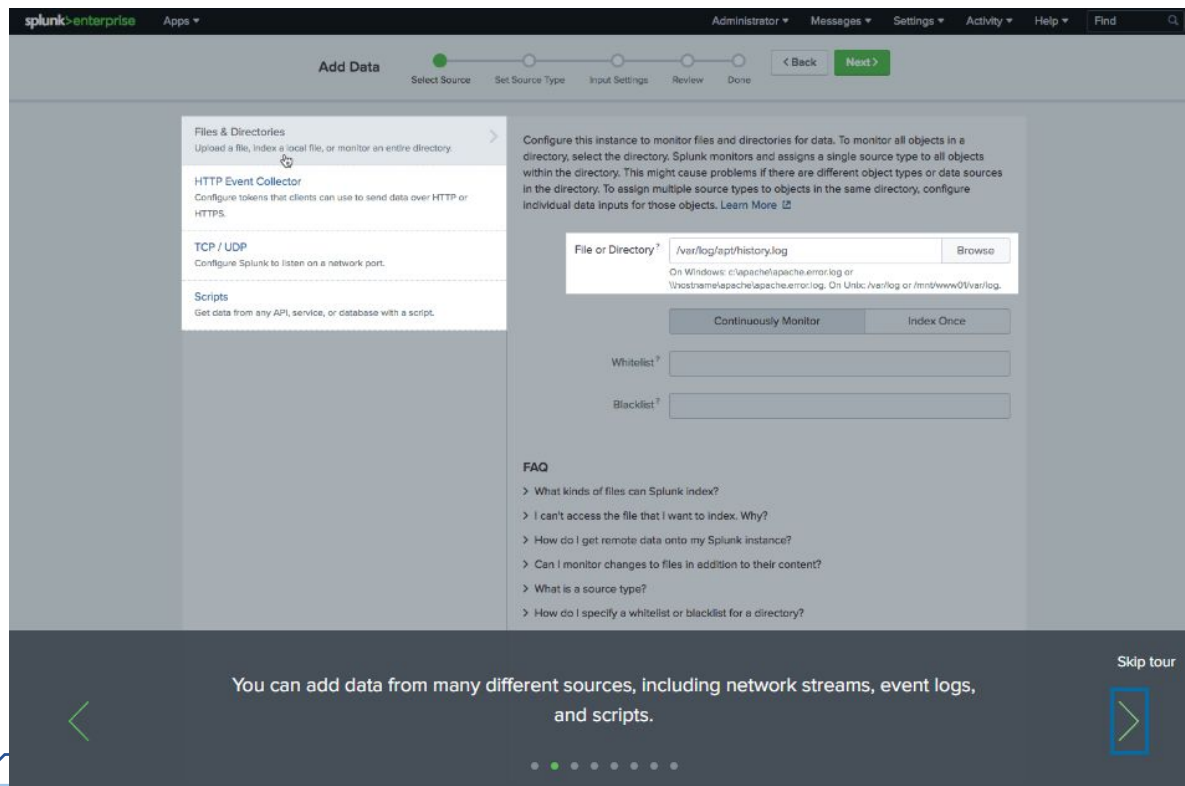
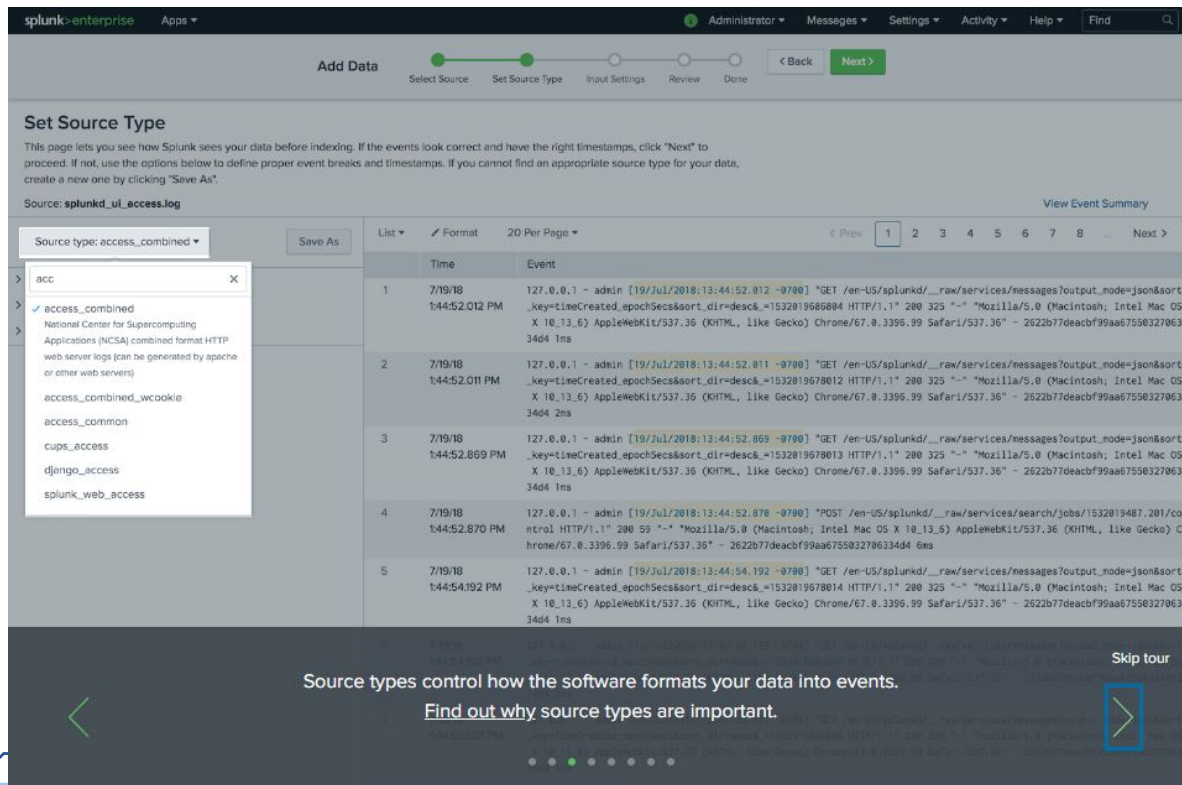


image: Screenshot of a Splunk example of adding data

2.0 Adding data to Splunk - tour (continued)



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: `splunkd_ui_access.log`

Source type: `access_combined` Save As

View Event Summary

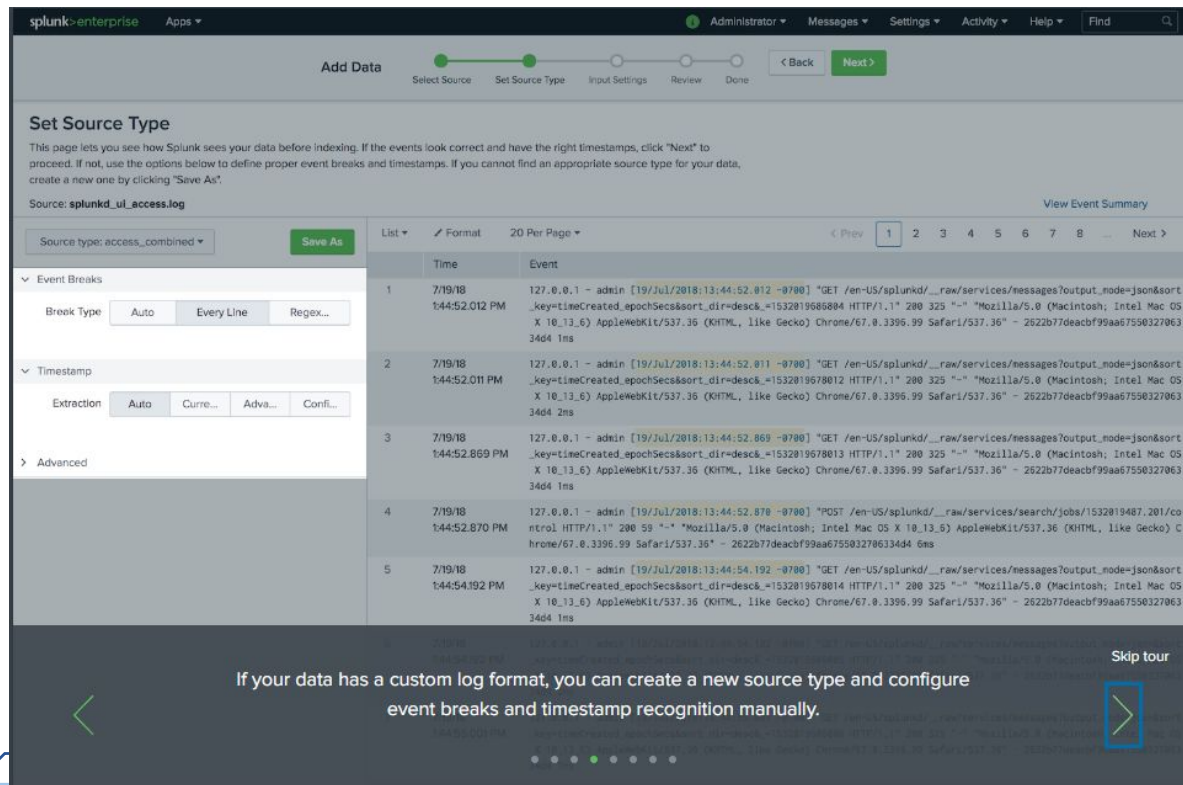
Time	Event
7/19/18 1:44:52.012 PM	127.0.0.1 - admin [19/Jul/2018:13:44:52.012 -0700] "GET /en-US/splunkd/_raw/services/messages/output_node=json&sort_key=timeCreated_epochSec&sort_dir=desc&=1532019686804 HTTP/1.1" 200 325 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36" - 2622b7deacbf99aa675503270633464 1ms
7/19/18 1:44:52.011 PM	127.0.0.1 - admin [19/Jul/2018:13:44:52.011 -0700] "GET /en-US/splunkd/_raw/services/messages/output_node=json&sort_key=timeCreated_epochSec&sort_dir=desc&=1532019678012 HTTP/1.1" 200 325 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36" - 2622b7deacbf99aa675503270633464 2ms
7/19/18 1:44:52.869 PM	127.0.0.1 - admin [19/Jul/2018:13:44:52.869 -0700] "GET /en-US/splunkd/_raw/services/messages/output_node=json&sort_key=timeCreated_epochSec&sort_dir=desc&=1532019678013 HTTP/1.1" 200 325 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36" - 2622b7deacbf99aa675503270633464 1ms
7/19/18 1:44:52.870 PM	127.0.0.1 - admin [19/Jul/2018:13:44:52.870 -0700] "POST /en-US/splunkd/_raw/services/search/jobs/1532019487.201/control HTTP/1.1" 200 59 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36" - 2622b7deacbf99aa675503270633464 6ms
7/19/18 1:44:54.192 PM	127.0.0.1 - admin [19/Jul/2018:13:44:54.192 -0700] "GET /en-US/splunkd/_raw/services/messages/output_node=json&sort_key=timeCreated_epochSec&sort_dir=desc&=1532019678014 HTTP/1.1" 200 325 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36" - 2622b7deacbf99aa675503270633464 1ms

Source types control how the software formats your data into events.
[Find out why source types are important.](#)

Skip tour

image: Screenshot of a Splunk example of adding data

2.0 Adding data to Splunk - tour (continued)



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: **splunkd_ul_access.log**

Source type: **access_combined** **Save As**

Event Breaks

Break Type: **Auto** **Every Line** **Regex...**

Timestamp

Extraction: **Auto** **Curre...** **Adva...** **Confli...**

Advanced

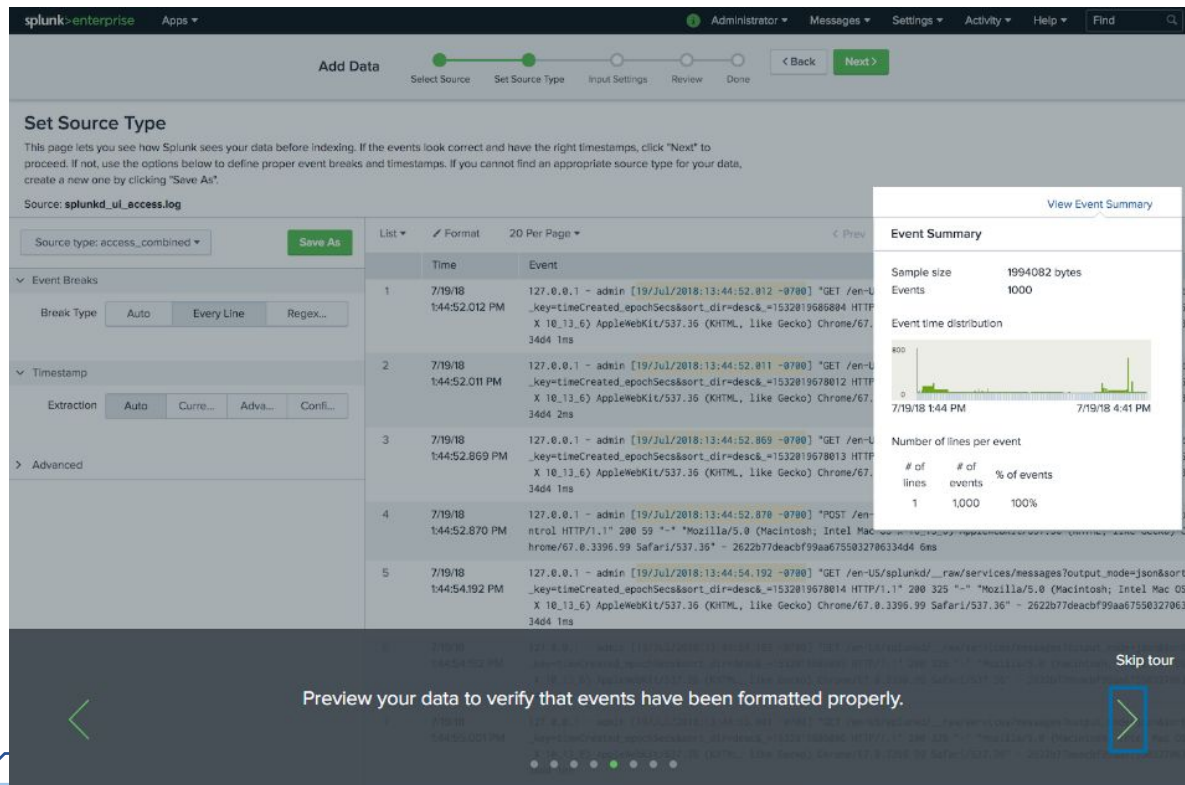
Time	Event
7/19/18 1:44:52.012 PM	127.0.0.1 - admin [19/Jul/2018:13:44:52.012 -0700] "GET /en-US/splunkd/_raw/services/messages/output_node=json&sort_key=timeCreated_epochSec&sort_dir=desc&_t=1532019686804 HTTP/1.1" 200 325 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36 - 2622b77deacbf99aa675503270633464 1ms
7/19/18 1:44:52.011 PM	127.0.0.1 - admin [19/Jul/2018:13:44:52.011 -0700] "GET /en-US/splunkd/_raw/services/messages/output_node=json&sort_key=timeCreated_epochSec&sort_dir=desc&_t=1532019678012 HTTP/1.1" 200 325 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36 - 2622b77deacbf99aa675503270633464 2ms
7/19/18 1:44:52.869 PM	127.0.0.1 - admin [19/Jul/2018:13:44:52.869 -0700] "GET /en-US/splunkd/_raw/services/messages/output_node=json&sort_key=timeCreated_epochSec&sort_dir=desc&_t=1532019678013 HTTP/1.1" 200 325 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36 - 2622b77deacbf99aa675503270633464 1ms
7/19/18 1:44:52.870 PM	127.0.0.1 - admin [19/Jul/2018:13:44:52.870 -0700] "POST /en-US/splunkd/_raw/services/search/jobs/1532019487.201/control HTTP/1.1" 200 59 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36 - 2622b77deacbf99aa675503270633464 6ms
7/19/18 1:44:54.192 PM	127.0.0.1 - admin [19/Jul/2018:13:44:54.192 -0700] "GET /en-US/splunkd/_raw/services/messages/output_node=json&sort_key=timeCreated_epochSec&sort_dir=desc&_t=1532019678014 HTTP/1.1" 200 325 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36 - 2622b77deacbf99aa675503270633464 1ms

If your data has a custom log format, you can create a new source type and configure event breaks and timestamp recognition manually.

Skip tour

image: Screenshot of a Splunk example of adding data

2.0 Adding data to Splunk - tour (continued)



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: `splunkd_ui_access.log`

Source type: `access_combined` **Save As**

Event Breaks

Break Type: ☐ Auto ☐ Every Line ☐ Regex...

Timestamp

Extraction: ☐ Auto ☐ Current ☐ Advanced ☐ Conflict...

Advanced

Time	Event
7/19/18 1:44:52.012 PM	127.0.0.1 - admin [19/Jul/2018:13:44:52.012 -0700] "GET /en-..._key=timeCreated_epochSec&sort_dir=desc._=1532019686804 HTTP X 10.13.6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.3464 1ms
7/19/18 1:44:52.011 PM	127.0.0.1 - admin [19/Jul/2018:13:44:52.011 -0700] "GET /en-..._key=timeCreated_epochSec&sort_dir=desc._=1532019678012 HTTP X 10.13.6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.3464 2ms
7/19/18 1:44:52.869 PM	127.0.0.1 - admin [19/Jul/2018:13:44:52.869 -0700] "GET /en-..._key=timeCreated_epochSec&sort_dir=desc._=1532019678013 HTTP X 10.13.6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.3464 1ms
7/19/18 1:44:52.870 PM	127.0.0.1 - admin [19/Jul/2018:13:44:52.870 -0700] "POST /en-...ntrol HTTP/1.1" 200 59 "-" Mozilla/5.0 (Macintosh; Intel Mac Chrome/67.0.3396.99 Safari/537.36" - 2622b77deacbf99aa675503270633464 6ms
7/19/18 1:44:54.192 PM	127.0.0.1 - admin [19/Jul/2018:13:44:54.192 -0700] "GET /en-US/splunkd/_raw/services/messages?output_mode=json&sort_key=timeCreated_epochSec&sort_dir=desc._=1532019678014 HTTP/1.1" 200 325 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13.6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36" - 2622b77deacbf99aa675503270633464 1ms

Event Summary

Sample size: 1994082 bytes
Events: 1000

Event time distribution

Number of lines per event

# of lines	# of events	% of events
1	1,000	100%

Preview your data to verify that events have been formatted properly.

Skip tour

image: Screenshot of a Splunk example of adding data

2.0 Adding data to Splunk - tour (continued)

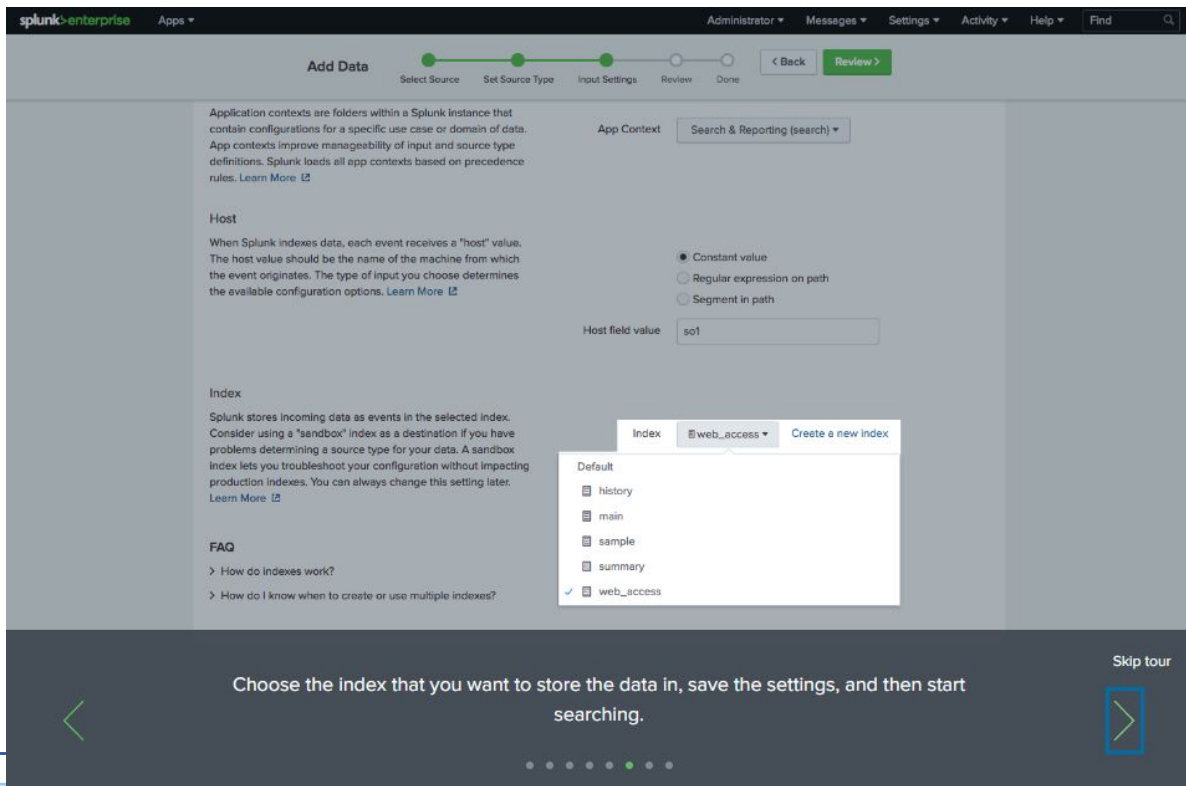
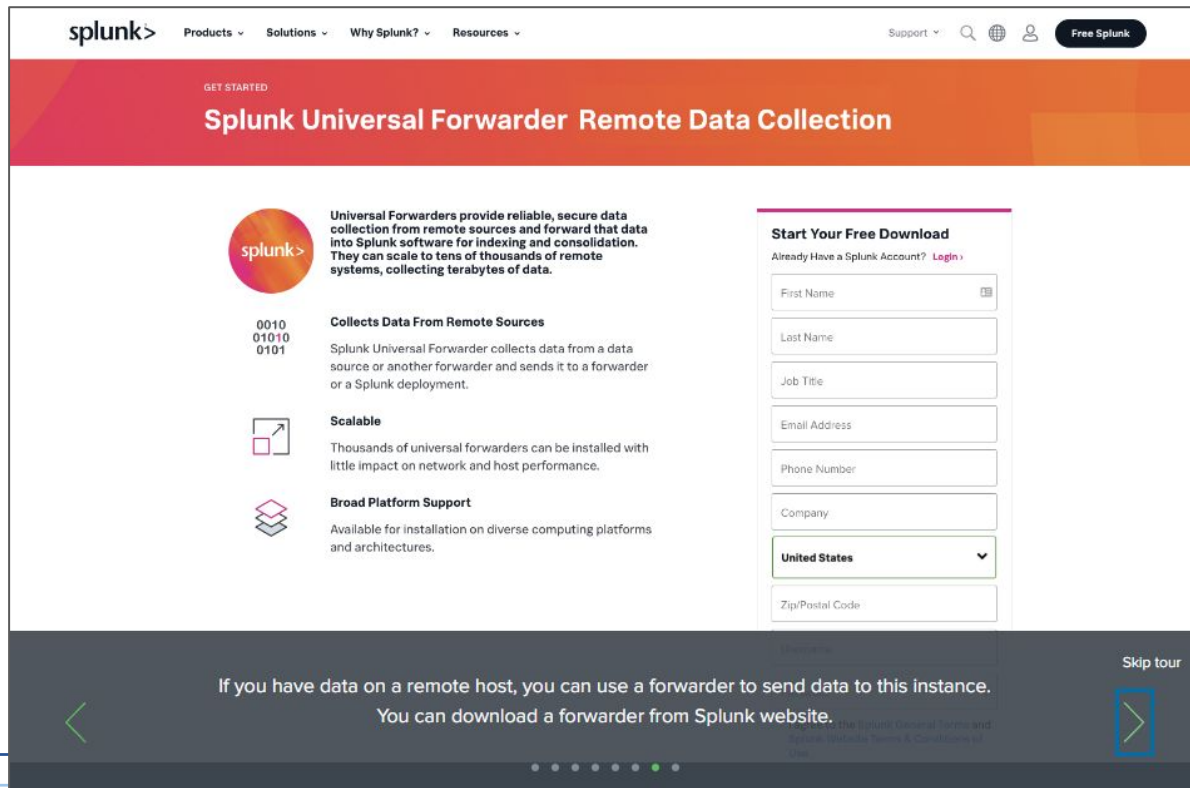


image: Screenshot of a Splunk example of adding data

2.0 Adding data to Splunk - tour (continued)



splunk> Products Solutions Why Splunk? Resources Support Free Splunk

GET STARTED

Splunk Universal Forwarder Remote Data Collection

Universal Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk software for indexing and consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data.

Collects Data From Remote Sources
Splunk Universal Forwarder collects data from a data source or another forwarder and sends it to a forwarder or a Splunk deployment.

Scalable
Thousands of universal forwarders can be installed with little impact on network and host performance.

Broad Platform Support
Available for installation on diverse computing platforms and architectures.

Start Your Free Download
Already Have a Splunk Account? [Login](#)

First Name

Last Name

Job Title

Email Address

Phone Number

Company

United States

Zip/Postal Code

If you have data on a remote host, you can use a forwarder to send data to this instance.
You can download a forwarder from Splunk website.

Skip tour

image: Screenshot of a Splunk example of adding data

2.0 Adding Data to Splunk - tour (continued)

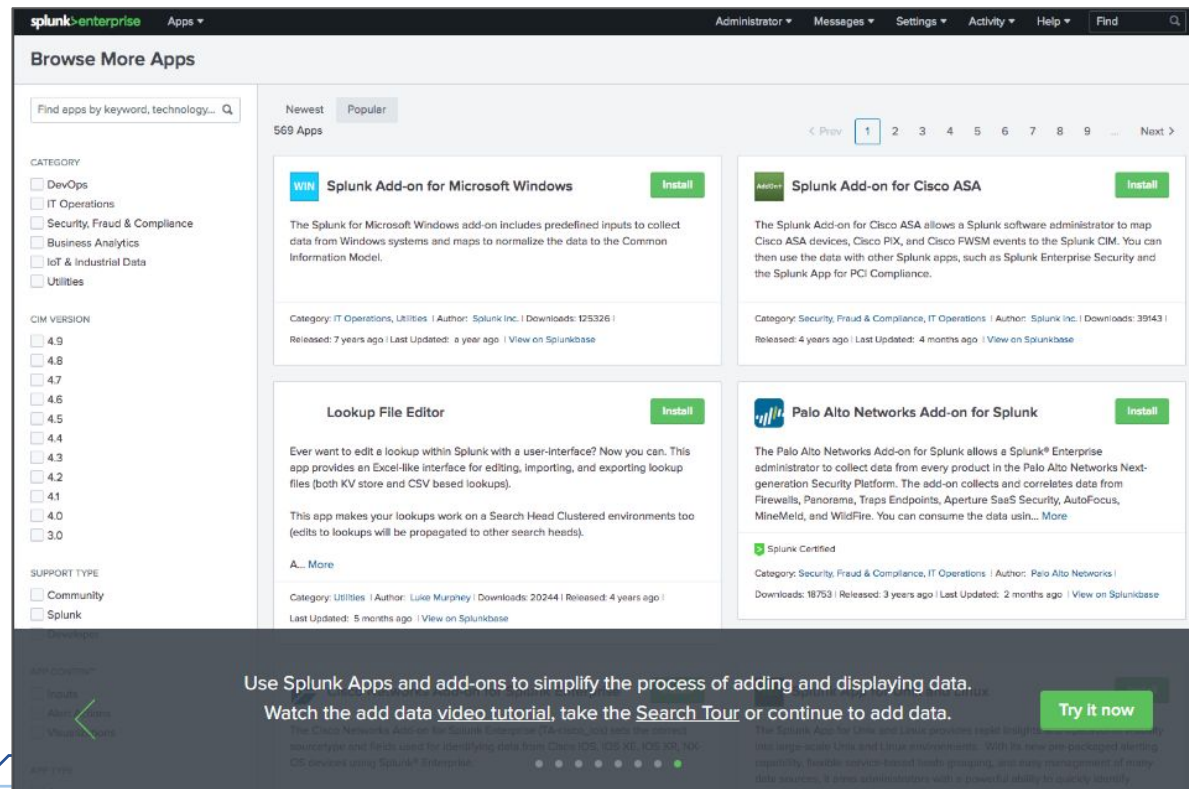


image: Screenshot of a Splunk example of adding data

2.0 Adding Data to Splunk - Summary

Adding data to Splunk involves **directing the data to an index**, which is a storage location for the data.

The index is identified by a **unique name** and is used to **quickly locate the data** when it is searched.

When data is added to an index, it needs to be identified by a **sourcetype**, which specifies the **format** of the data and the type of processing that is required.

The sourcetype helps Splunk to correctly **parse** the data and apply field extractions to it, making it easier to search and analyze.

By properly indexing and identifying the sourcetype of the data, Splunk can help to provide valuable insights and intelligence from the data.

2.1 Run Basic Searches

Searching in Splunk involves using the **search bar** in the Splunk web interface to query the indexed data.

The search language used in Splunk is based on **SPL (Splunk Processing Language)**. Users can search for specific **keywords**, **phrases**, or **patterns** within the indexed data, and **filter** results based on various criteria such as **time range**, **index**, **sourcetype**, and more.

The search results are presented in a **tabular** format, and users can also create **visualizations** such as **charts** and **graphs** to better analyze the data.

Splunk's search functionality includes a range of **operators** and **functions** that allow users to **manipulate** and **analyze** the data, and the search results can also be saved as **reports** or **alerts** for future reference.

2.1 Run Basic Searches (continued)

Access the **Search & Reporting app** by selecting the app from the App bar.

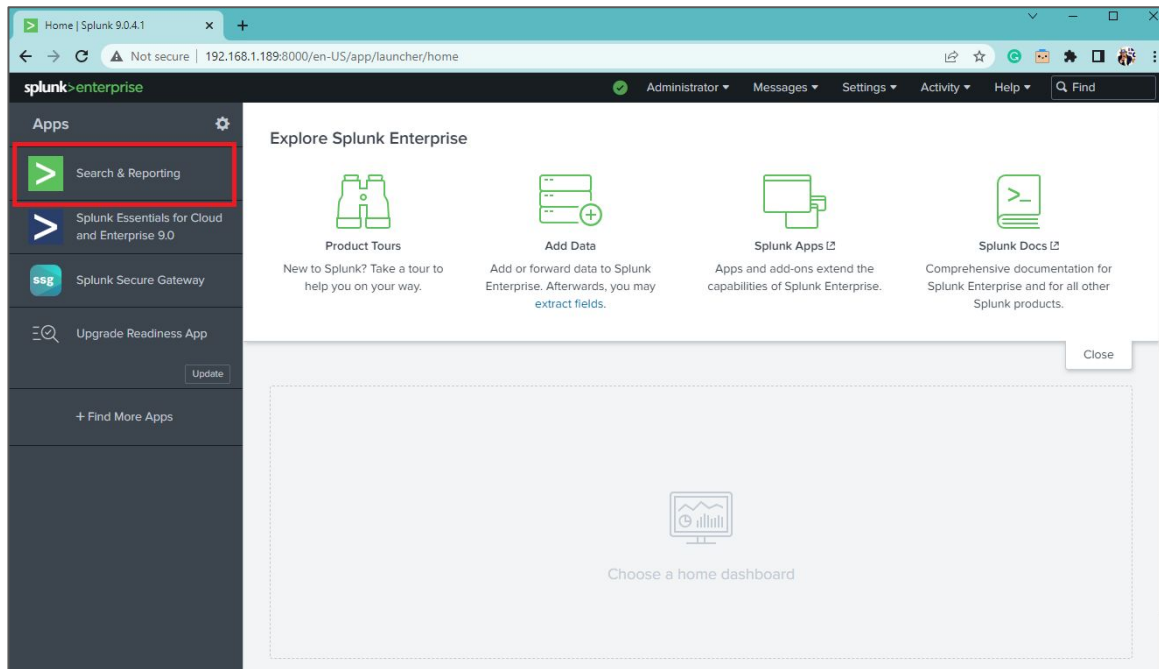


image: Screenshot Splunk launcher page with highlighted Search & Reporting app link.

2.1 Run Basic Searches (continued)

Instructor Demo- Interface Layout:

Number	Element	Description
1	Apps bar	Switch between different views in the Search & Reporting app, including Search, Analytics, Datasets, Reports, Alerts, and Dashboards
2	Search bar	Enter search queries.
3	Time range picker	Set the time period for the search.
4	Search mode menu	Choose between Smart (default), Fast, and Verbose.
5	How to Search	Documents and tutorials to help searching.
6	Table Views	GUI to search and analyze data.

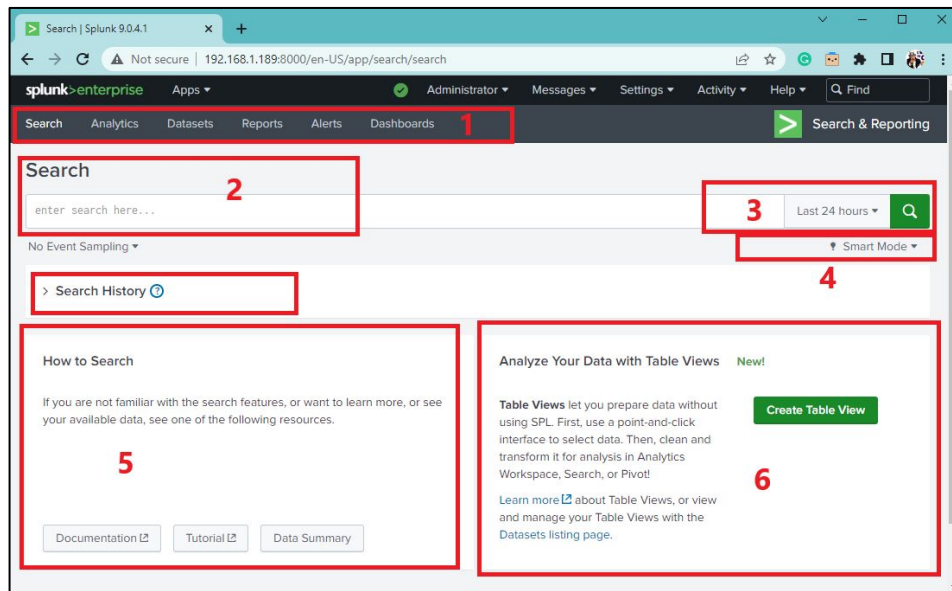


image: screenshot, splunk Search & Reporting app

2.1 Run Basic Searches - key-value pairs

In Splunk, **key-value pairs** are used to represent the **structured data** in the **events** being indexed.

Each key-value pair is separated by an **equal sign (=)**, and each pair is separated by a **space or a comma**.

For example, in a log event, the key could be "**source**" and the value could be **"/var/log/syslog,"** which would be represented as "**source=/var/log/syslog**" in Splunk.

The **key** is case-sensitive when it comes to key-value pairs, which means that if a key is defined with a **specific capitalization**, it must be **matched exactly** in the data for Splunk to extract the associated value.

As such, **source=/var/log/syslog** and **Source=/var/log/syslog** **would be treated as two separate keys** and return different search results.

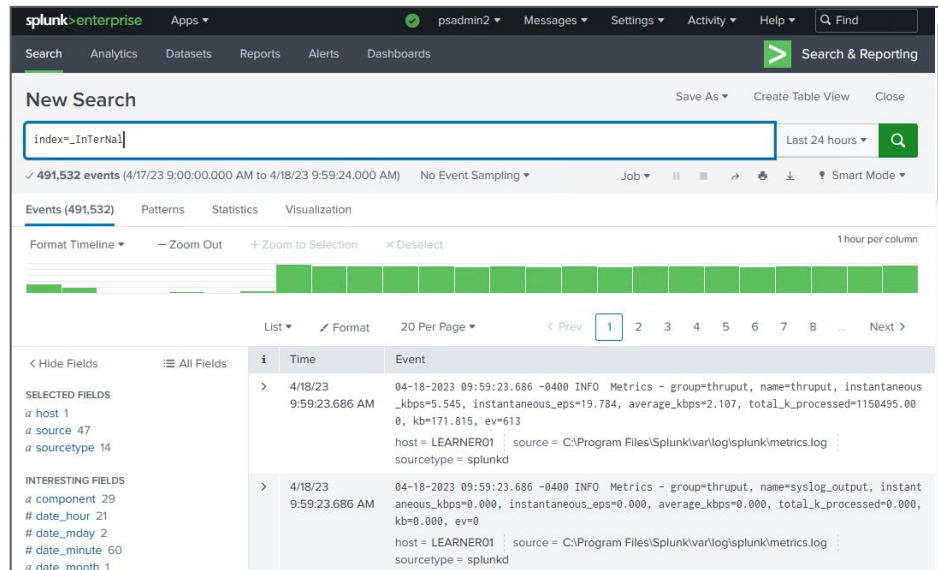
2.1 Run Basic Searches - key-value pairs

The **value** is **not case-sensitive**.

Therefore, `source=/var/log/syslog` and `source=/VaR/lOg/sYslog` would be treated as the **same value** and return similar search results.

Note that you can also search for values that are **not** part of a key-pair.

Searching for **specific key-value pairs** in the search bar, is more efficient, and users can **quickly** filter and find **relevant** events.



The screenshot shows the Splunk Search & Reporting app interface. The search bar contains the query `index=_internal`. The results show 491,532 events from 4/7/23 9:00:00.000 AM to 4/18/23 9:59:24.000 AM. The interface includes a timeline visualization and a table of events.

i	Time	Event
>	4/18/23 9:59:23.686 AM	04-18-2023 09:59:23.686 -0400 INFO Metrics - group=thruput, name=thruput, instantaneous_kbps=5.545, instantaneous_eps=19.784, average_kbps=2.107, total_k_processed=1150495.000, kb=171.815, ev=613 host = LEARNER01 source = C:\Program Files\Splunk\var\log\splunk\metrics.log sourcetype = splunkd
>	4/18/23 9:59:23.686 AM	04-18-2023 09:59:23.686 -0400 INFO Metrics - group=syslog_output, instantaneous_kbps=0.000, instantaneous_eps=0.000, average_kbps=0.000, total_k_processed=0.000, kb=0.000, ev=0 host = LEARNER01 source = C:\Program Files\Splunk\var\log\splunk\metrics.log sourcetype = splunkd

image: screenshot, splunk Search & Reporting app

2.1 Run Basic Searches - key-value pairs

Certification Question example:

What syntax is used to link key/value pairs in search strings?

- A. action+purchase
- B. action=purchase
- C. action | purchase
- D. action equal purchase

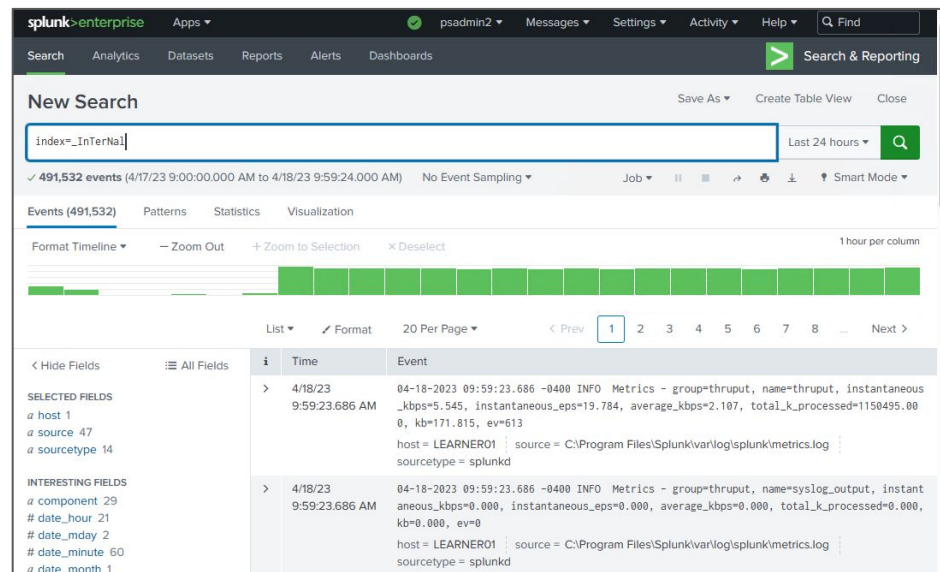


image: screenshot, splunk Search & Reporting app

2.1 Run Basic Searches - wildcards

- In Splunk the **asterisk** (*) character is the **wildcard** used to **match** an unlimited number of characters in a string.
- Use **wildcards** to match a **range** of field **values**.

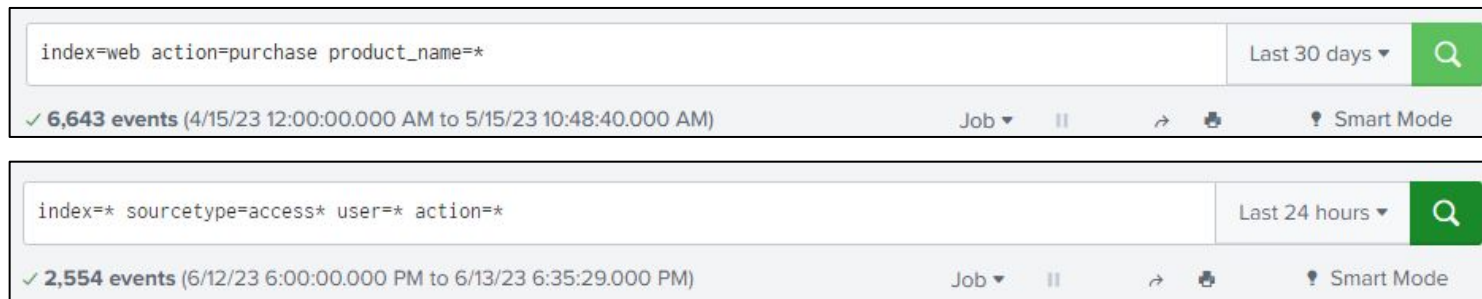


image: screenshot, splunk Search & Reporting app

2.1 Run Basic Searches - search operators

Splunk **search operators**, such as **AND**, **OR**, and **NOT**, can be used to combine key-value pairs in search queries to refine the search results.

The **AND** operator is used to search for results that **match both conditions** or key-value pairs.

For example, if we want to search for events that contain both "**error**" and "**webserver**," we can use the **AND** operator as follows:

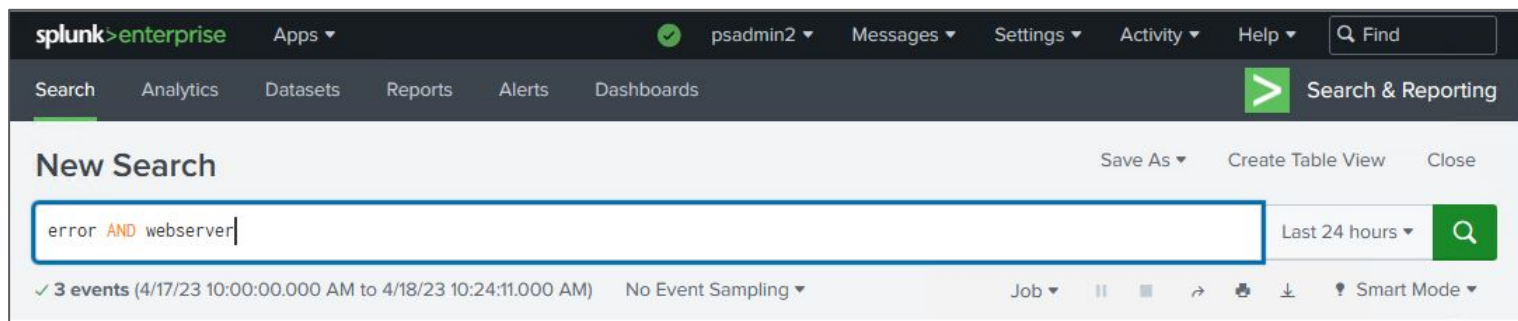


image: screenshot, splunk Search & Reporting app

2.1 Run Basic Searches - search operators

(continued)

The **OR** operator is used to search for results that match **at least one** of the conditions or key-value pairs.

For example, if we want to search for events that contain **either "error" or "warning,"** we can use the **OR** operator as follows:

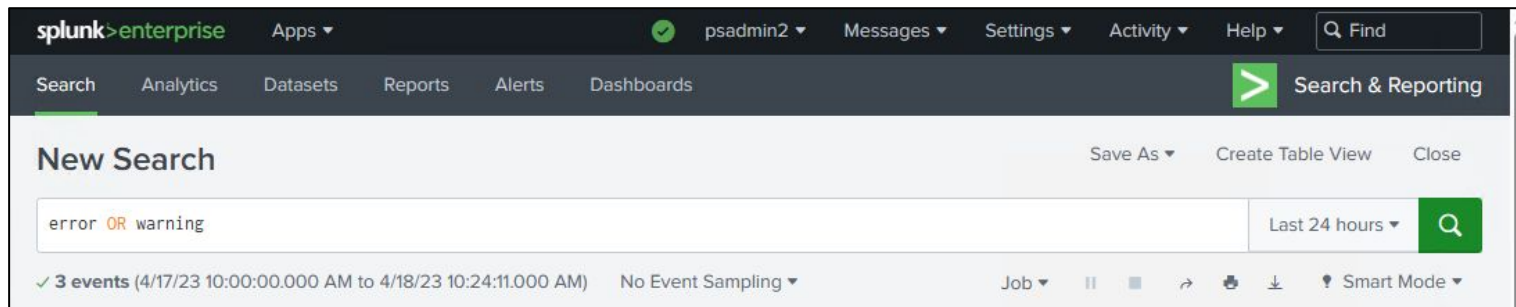


image: screenshot, splunk Search & Reporting app

2.1 Run Basic Searches - search operators

(continued)

The **NOT** operator is used to **exclude results** that match a certain condition or key-value pair.

For example, if we want to search for events that contain "**error**" but not "**database**," we can use the **NOT** operator as follows:

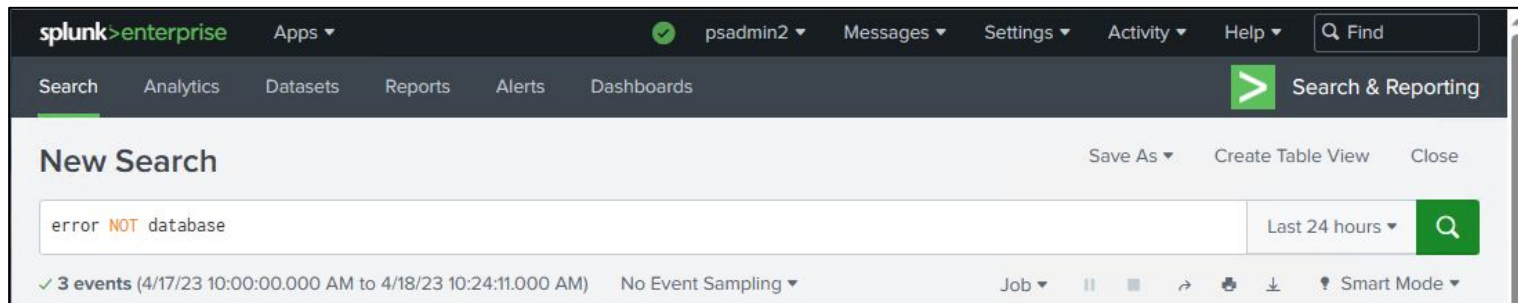


image: screenshot, splunk Search & Reporting app

2.1 Run Basic Searches - search operators

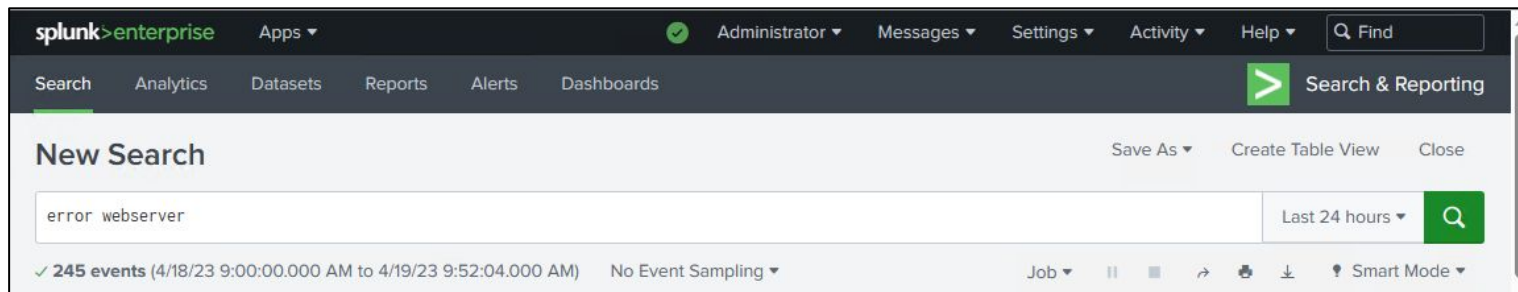
(continued)

If **no operator** is mentioned between the search items, Splunk will operate **by default** as if there was an **AND** operator present.

Certification Question example:

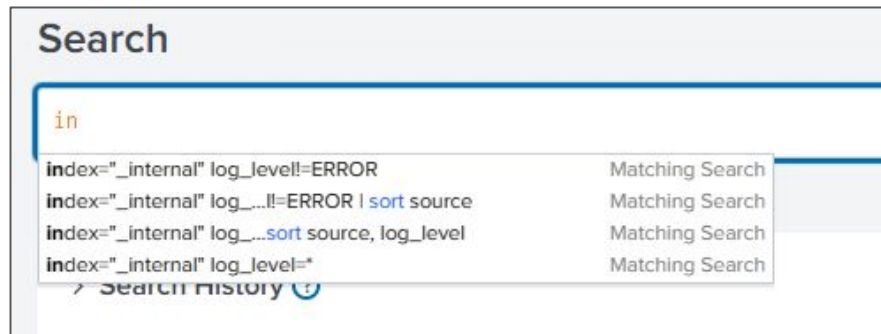
Which search matches the events containing the terms "error" and "webserver"?

- A. index=security Error Webserver
- B. index=security error OR webserver
- C. index=security "error web server"
- D. index=security NOT error NOT webserver



2.1 Run Basic Searches - the Search Assistant

- The Search Assistant in Splunk is a feature that provides **suggestions** for search terms and syntax **as you type** in the search bar.
- It uses machine learning algorithms to analyze the data in real time and **suggests potential search terms, field names, and command options**.
- It is a useful tool for beginners who may not be familiar with the search language or for more experienced users who want to speed up their searches and discover new fields and commands.



2.1 Run Basic Searches - Search History

- **Search history** in Splunk is a feature that allows users to view and access their **previously executed searches**.
- Each time a user performs a search in Splunk, the **search query is added to their search history**. This can be useful for **quickly referencing and re-executing previous searches**, as well as tracking the progress of a long-running search.
- The search history is accessed by clicking on the **Search history button** located under the Search Bar

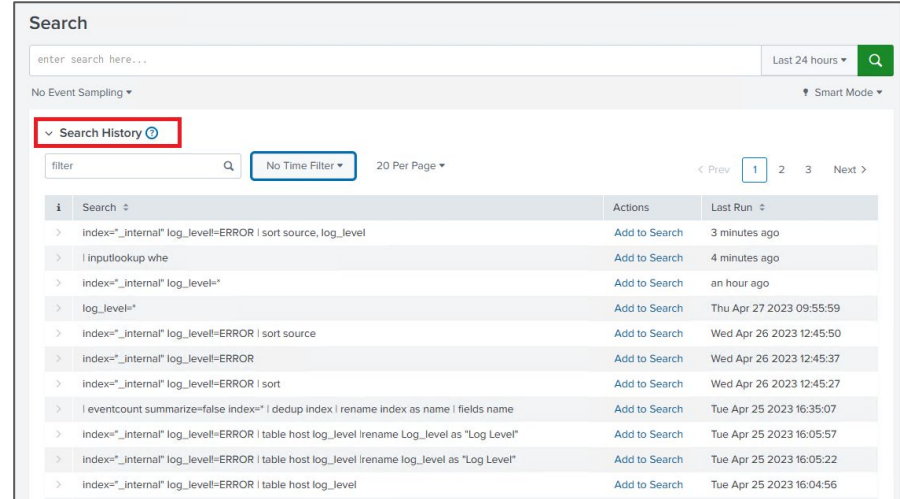


image: screenshot, splunk Search & Reporting app

2.1 Run Basic Searches - How to Search

- The **How to Search** section on the **Search & Reporting** app provides **additional resources** such as **Documentation** and a **Tutorial** To help users.
- With the **Data Summary** feature, you can determine data **sources**, **source types**, and the **hosts** that generated the data.
- This is the most comprehensive way of learning **what data is present in a Splunk deployment**.

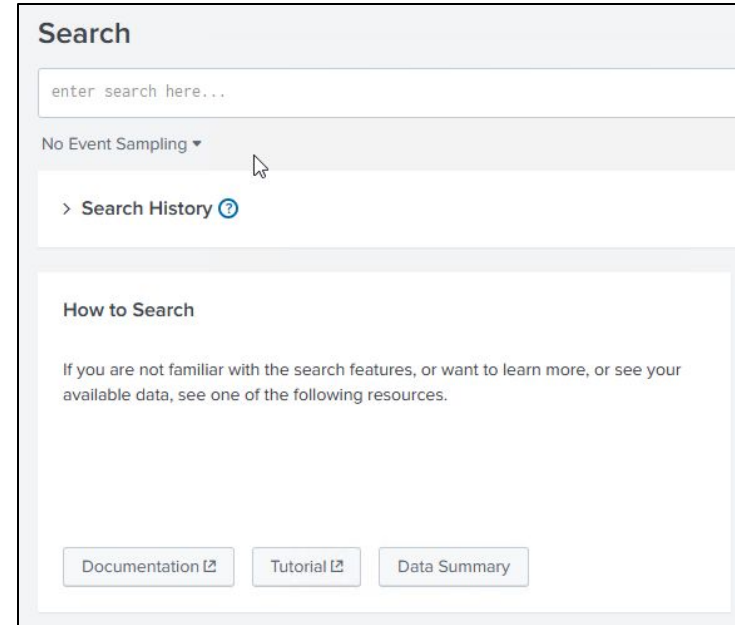


image: screenshot, splunk Search & Reporting app

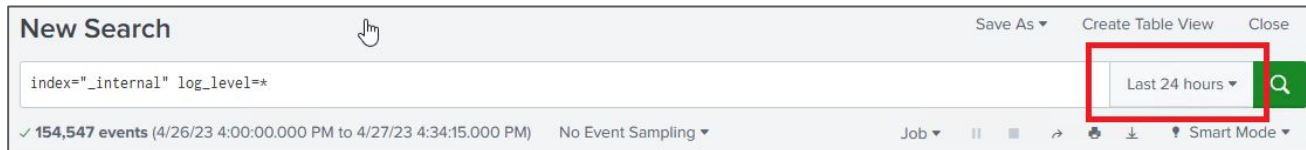
2.1 Run Basic Searches - Summary

- In Splunk, key-value pairs are used to represent the structured data in the events being indexed.
- The key is case sensitive; the value is not.
- Splunk search operators, such as AND, OR, and NOT, can be used to combine key-value pairs in search queries to refine the search results.
- In Splunk the asterisk (*) character is the wildcard used to match an unlimited number of characters in a string.
- When using wildcards, ensure to follow the wildcard usage best practices.
- Quotation marks are required when the field values include spaces.
- Splunk provides search helping tools such as the Search Assistant and Search History.

2.2 Set the Time Range of a Search

Specifying time ranges:

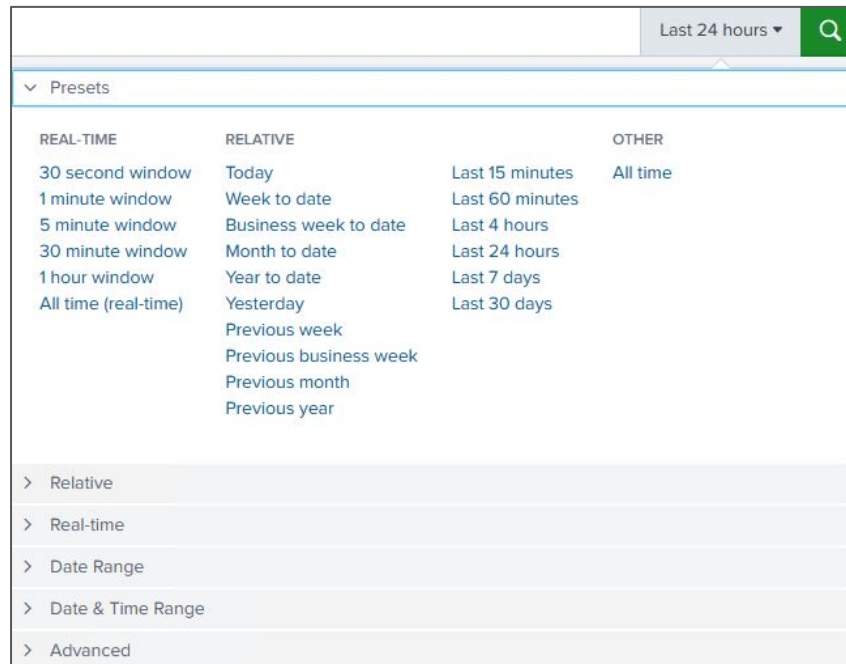
- Restricting, or filtering your search criteria **using a time range is the easiest and most effective way to optimize your searches.**
- You can use time ranges to **troubleshoot an issue** if you know the **approximate time frame** when the issue occurred. Narrow the time range of your search to that timeframe.
 - For example, to investigate an incident that occurred sometime in the last hour, you can use the default time range: "Last 24 hours," but a better option is **Last 60 minutes**.
- Use the **Time Range Picker** to set a time range for a search.



2.2 Set the Time Range of a Search (continue)

The Time Range Picker

- Clicking the Time Range Picker will open a drop-down menu containing the following sections:
 - Presets
 - Relative
 - Real Time
 - Date Range
 - Date and Time Range
 - Advanced



2.2 Set the Time Range of a Search (continued)

Instructor Demo - Time Range Picker:

Use a live Splunk environment to **introduce** and **experience** the **various options and sections** of the Time Range Picker.

Certification Question example:

Which user interface component allows for time selection?

- A. Time summary
- B. Time range picker
- C. Search time picker
- D. Data source time statistics

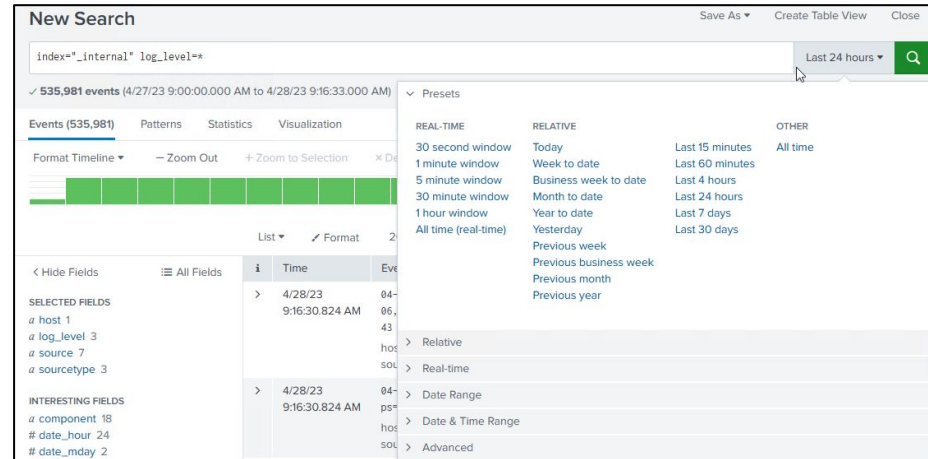


image: screenshot, splunk Search & Reporting app

Note:

You can also specify time modifiers by typing them into your search string.

We will dedicate a separate section for this.

2.2 Set the Time Range of a Search - Summary

- You can use the **Time Range Picker** interface to set the time range for a Splunk search.
- The interface provides many **different tools** for selecting the **time range** such as **Presets**, **Relative**, **Real-time**, **Date Range**, and more.
- **Restricting**, or **filtering**, your **search criteria using a time range** is the easiest and most **effective** way to **optimize** your searches.

2.3 Identify the Contents of Search Results

Understanding Search Results:

Below the **Search bar** are four tabs: **Events**, **Patterns**, **Statistics**, and **Visualization**.

The **type of search** commands that you use **determines which tab** the search results **appear** on.

The **Events** tab displays the **Timeline of events**, the **Display options**, the **Fields sidebar**, and the **Events viewer**.

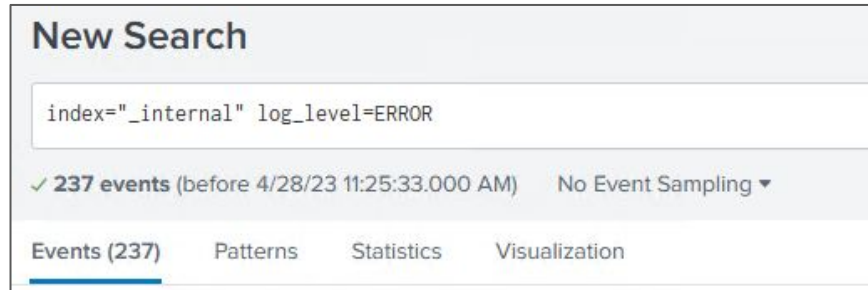
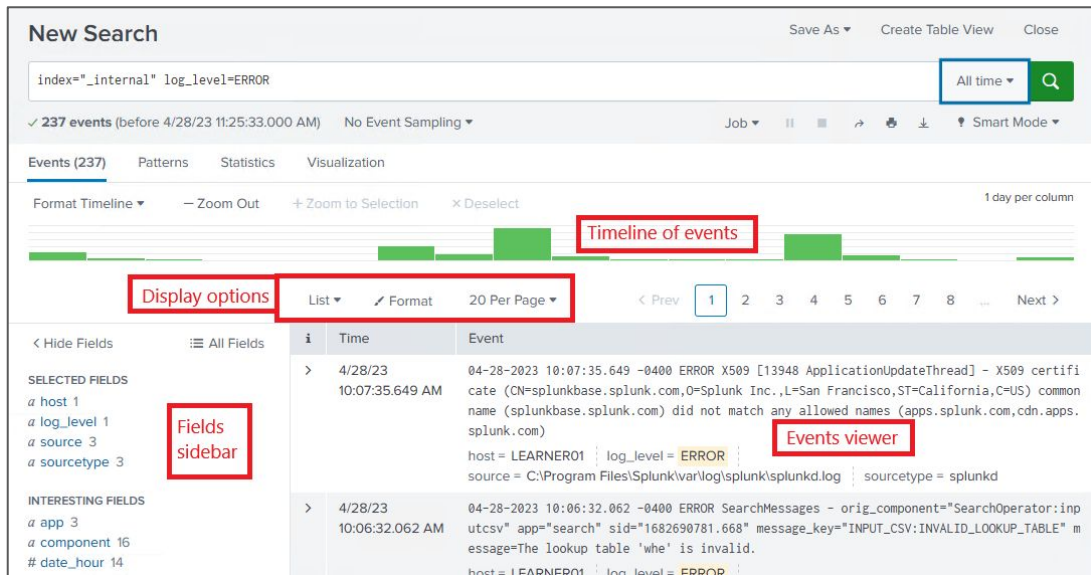


image: screenshot, splunk Search & Reporting app

2.3 Identify the Contents of Search Results

(continued)

Understanding search results - Events



The screenshot shows the Splunk Search & Reporting app interface. The search bar contains the query `index='_internal' log_level=ERROR`. Below the search bar, it indicates 237 events. The interface is divided into several sections:

- Timeline of events:** A horizontal bar chart showing the distribution of events over time.
- Display options:** A dropdown menu showing 'List' and 'Format' options, and a '20 Per Page' setting.
- Fields sidebar:** A sidebar on the left showing 'SELECTED FIELDS' (host, log_level, source, sourcetype) and 'INTERESTING FIELDS' (app, component, date_hour).
- Events viewer:** A table displaying the search results, with columns for Time and Event. The first event is highlighted.

Time	Event
4/28/23 10:07:35.649 AM	04-28-2023 10:07:35.649 -0400 ERROR X509 [13948 ApplicationUpdateThread] - X509 certificate (CN=splunkbase.splunk.com,O=Splunk Inc.,L=San Francisco,ST=California,C=US) common name (splunkbase.splunk.com) did not match any allowed names (apps.splunk.com,cdn.apps.splunk.com) host = LEARNER01 log_level = ERROR source = C:\Program Files\Splunk\var\log\splunk\splunkd.log sourcetype = splunkd
4/28/23 10:06:32.062 AM	04-28-2023 10:06:32.062 -0400 ERROR SearchMessages - orig_component="SearchOperator:inp utcsv" app="search" sid="1682690781.668" message_key="INPUT_CSV:INVALID_LOOKUP_TABLE" m essage="The lookup table 'wh' is invalid. host = LEARNER01 log_level = ERROR

image: screenshot, splunk Search & Reporting app

- By default, the **events** appear as a **list** that is ordered starting with the **most recent event** (reverse chronological order).
- An event refers to a **single line of data** that contains **timestamped data** along with any other relevant information.
- In each event, the **matching search terms are highlighted**.

2.3 Identify the Contents of Search Results

(continued)

Understanding Search Results - the Events list:

- The **List** display option shows the event information in **three** columns.

Column	Description
/	Use the event information column to expand or collapse the display of the event information. By default the display is collapsed. Click the greater than (>) symbol to expand the display.
Time	The timestamp for the event. When events are indexed, the timestamp in the event is extracted. If the event does not contain a timestamp, the indexing process adds a timestamp that is the date and time the event was indexed.
Event	The raw event data. The Selected fields from the Fields sidebar appear at the bottom of each event.

image: <https://docs.splunk.com/Documentation/Splunk/9.0.4/SearchTutorial/Startsearching>

- Other **Events Viewer display options** are **Raw**, and **Table**.

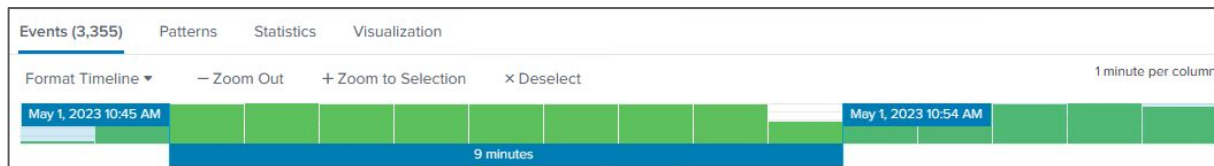
2.3 Identify the Contents of Search Results

(continued)

Understanding Search Results - Timeline of events

- The **Timeline of events** is a visual representation of the number of events that occur at each point in time.
- As the timeline **updates with your search results**, there are clusters or patterns of bars. The **height** of each bar indicates the **count of events**.
- **Peaks or valleys** in the timeline can indicate **spikes** in activity or server **downtime**. The timeline highlights patterns of events, or peaks and lows in event activity.
- The timeline options are located above the timeline. **You can zoom in, zoom out, and change the scale of the timeline chart.**

Source: <https://docs.splunk.com/Documentation/Splunk/9.0.4/SearchTutorial/Startsearching>

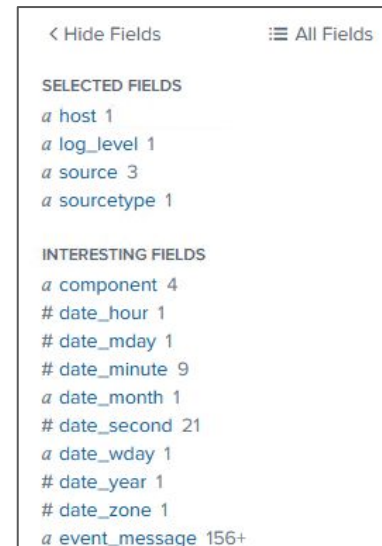


2.3 Identify the Contents of Search Results

(continued)

Understanding Search Results - Fields sidebar

- As part of the **index** process, information is **extracted** from your data and formatted as **name and value pairs**, called **fields**.
- When you run a search, the **fields** are identified and **listed** in the **Fields sidebar** next to your search results. The fields are divided into two categories.
 - Selected fields** are visible in your search results. By default, **host**, **source**, and **what is the percentage** appear. You can select other fields to show in your events.
 - Interesting fields** are other fields that have been extracted from the events in your search results.
- You can **hide** the fields sidebar to maximize the results area.



2.3 Identify the Contents of Search Results

Understanding Search Results - Patterns, Statistics, and Visualizations

(continued)

- The **Patterns** tab displays a list of the most **common patterns** among the set of events returned by your search. Each of these patterns represents **events that share a similar structure**.
- The **Statistics** tab populates when you run a search with **transforming commands** such as **stats**, **top**, **chart**, and so on.
- Searches with **transforming commands** also populate the **Visualization** tab. The results area of the Visualizations tab includes a **chart** and the **statistics table** that is used to generate the chart. You will learn about transforming commands, and use the Statistics and Visualizations tabs later.

Source: <https://docs.splunk.com/Documentation/Splunk/9.0.4/SearchTutorial/Startsearching>



image: screenshot, splunk Search & Reporting app

2.3 Identify the Contents of Search Results - Summary

This section covered various options that users can utilize in the **Search & Reporting** app, and provided an **overview** of the **fundamental concepts** of search results.

The **Timeline of events**, the **Fields sidebar**, and the **Events viewer** are important components that aid in searching and analyzing data in Splunk.

To prepare for the **certification** exam, it is crucial to be **proficient** and well-versed in using these features.

2.4 Refine Searches

The amount of **time** it takes to **complete a search** in Splunk can vary depending on several factors, such as the **complexity** of the search query, the **amount** of **data** being searched, and the resources available on the machine running Splunk.

Searches can take just a few **seconds** for small amounts of data, or several **minutes** or even **hours** for very large datasets.

We refine searches in Splunk to **narrow down the results** and focus on **specific information** that we are interested in.



image: Freepik.com

2.4 Refine Searches (continued)

By **adding more search terms**, and using **filters** and refining search syntax, we can **reduce** the number of **events** in the search results and make it easier to find the **relevant information**.

Refining searches can also help to **eliminate false positives** or **irrelevant data** from the results, making the analysis process more efficient and accurate.

Some basic ways to refine a search are to **drill-down** into the search results, use different **search modes**, and utilize **comparison operators**.

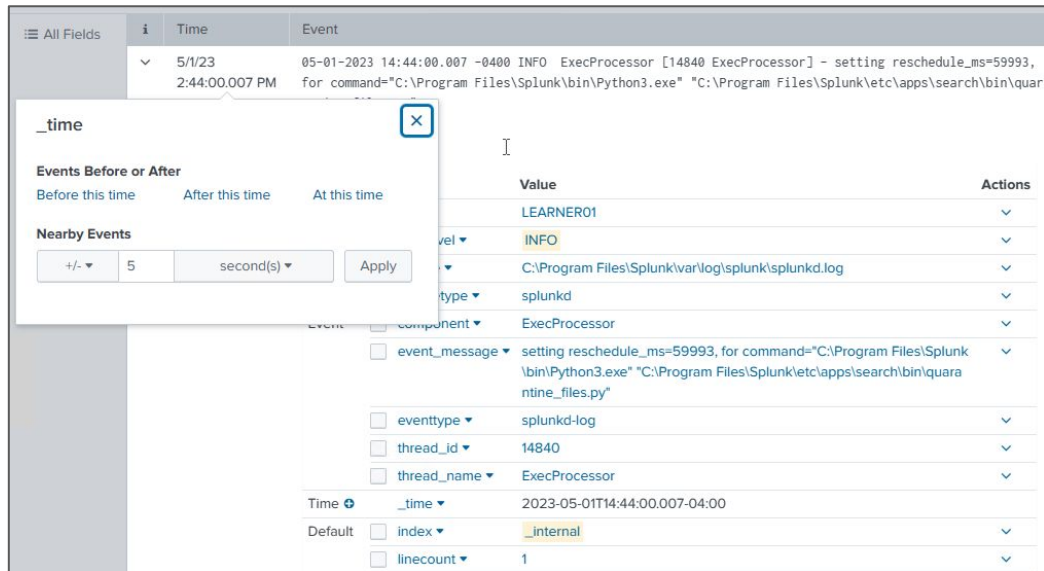
2.4 Refine Searches (continued)

Refining Searches - Drill-down the search results

Once the event viewer is **populated** with events, **drilling down** into an event can help **narrow** the search.

Using the **i** column, expand a single event.

Clicking on the **timestamp** allows easy access to searching **nearby events**.



The screenshot shows the Splunk Search & Reporting app interface. The top bar displays 'All Fields', 'i' (expand), 'Time', and 'Event'. The main table shows a search result for '05-01-2023 14:44:00.007 -0400 INFO ExecProcessor [14840 ExecProcessor] - setting reschedule_ms=59993, for command="C:\Program Files\Splunk\bin\Python3.exe" "C:\Program Files\Splunk\etc\apps\search\bin\quarantine_files.py"'. A drill-down menu is open, showing 'Nearby Events' and 'Events Before or After' options. The 'Nearby Events' section includes a search bar, a time range selector (set to 5 seconds), and an 'Apply' button. The 'Events Before or After' section includes a search bar and a 'Close' button. The main table also shows a list of fields with their values and actions, including 'event_message', 'eventtype', 'thread_id', 'thread_name', 'Time', 'Default', 'index', and 'linecount'.

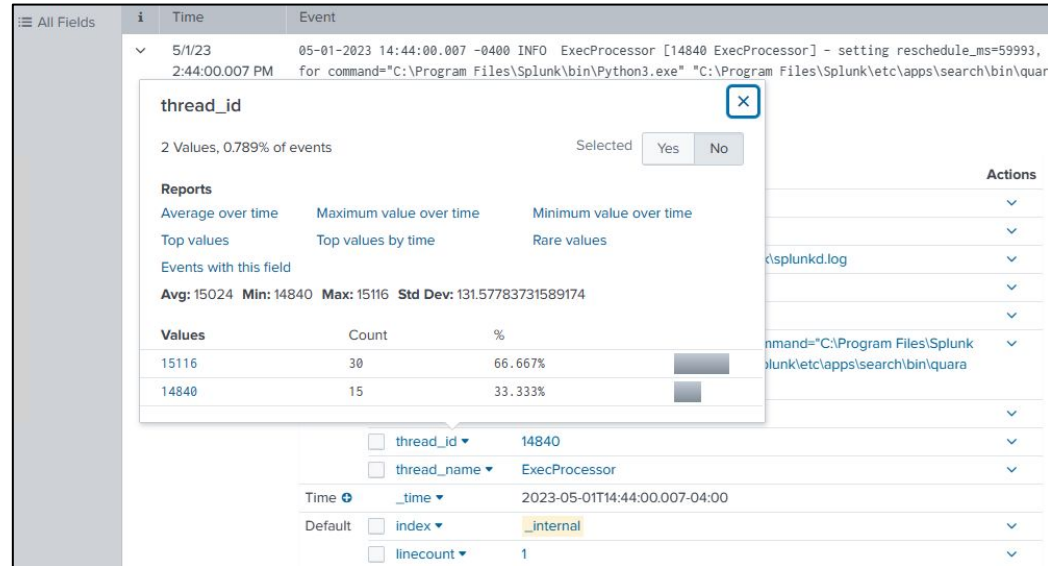
Field	Value	Actions
event_message	setting reschedule_ms=59993, for command="C:\Program Files\Splunk\bin\Python3.exe" "C:\Program Files\Splunk\etc\apps\search\bin\quarantine_files.py"	▼
eventtype	splunkd-log	▼
thread_id	14840	▼
thread_name	ExecProcessor	▼
Time	_time ▼ 2023-05-01T14:44:00.007-04:00	
Default	index ▼ _internal	▼
	linecount ▼ 1	▼

2.4 Refine Searches (continued)

Refining Searches - Drill-down the search results

Clicking on a **key** (field name), of a key-pair provides **quick access** to refining the search by generating **statistical reports**, or searching for events that contain the **same field**.

It will also provide **instant data** regarding **unique values** contained in this field.



The screenshot shows the Splunk Search & Reporting app interface. A search result is displayed with the following details:

- Time:** 5/1/23 2:44:00.007 PM
- Event:** 05-01-2023 14:44:00.007 -0400 INFO ExecProcessor [14840 ExecProcessor] - setting reschedule_ms=59993, for command="C:\Program Files\Splunk\bin\Python3.exe" "C:\Program Files\Splunk\etc\apps\search\bin\quara"

A drill-down menu for the field **thread_id** is open, showing the following information:

- thread_id** (2 Values, 0.789% of events)
- Reports:**
 - Average over time
 - Maximum value over time
 - Minimum value over time
 - Top values
 - Top values by time
 - Rare values
 - Events with this field
- Summary:** Avg: 15024 Min: 14840 Max: 15116 Std Dev: 131.57783731589174
- Values:**

Values	Count	%
15116	30	66.667%
14840	15	33.333%

Below the drill-down menu, the search results are filtered by the selected field **thread_id** with the value **14840**. The search results show the following details:

- thread_id:** 14840
- thread_name:** ExecProcessor
- Time:** 2023-05-01T14:44:00.007-04:00
- Default:**
 - index:** _internal
 - linecount:** 1

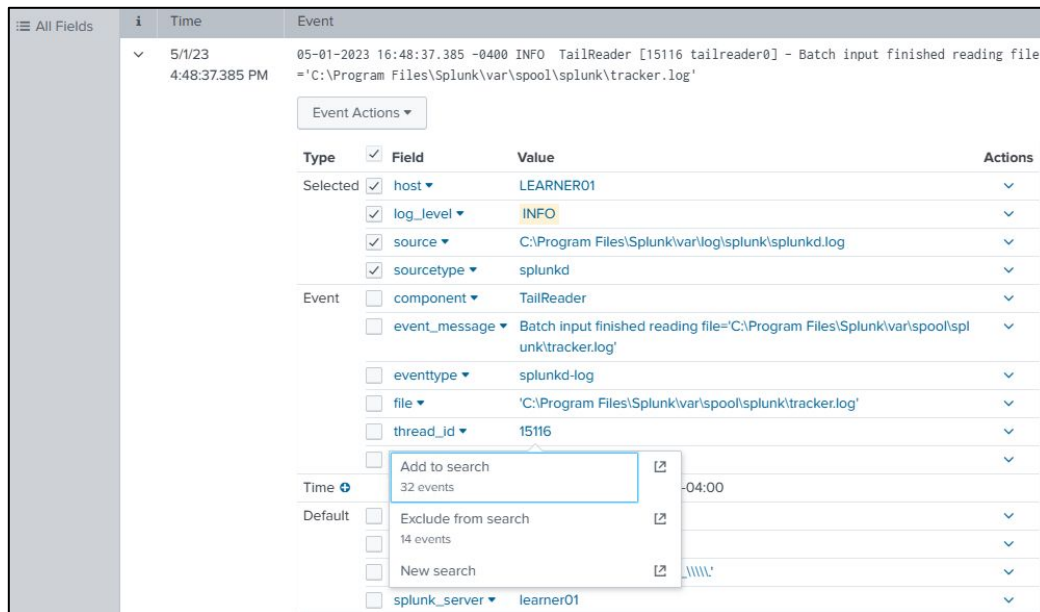
2.4 Refine Searches (continued)

Refining Searches - Drill-down the search results

Clicking on a **value** of a field provides **quick access** to refining the search by **adding** or **removing** the value to or from the search.

It will display the **number of events** for each option.

It also allows for executing a **new search** based on that value.



The screenshot shows the Splunk Search & Reporting app interface. The top section displays a search result for 'TailReader' with a timestamp of '05-01-2023 16:48:37.385 -0400'. The event message is 'Batch input finished reading file = 'C:\Program Files\Splunk\var\spool\splunk\tracker.log''. Below the event, there is a table of fields and values, and a dropdown menu for refining the search.

Type	Field	Value	Actions
Selected	host	LEARNER01	▼
	log_level	INFO	▼
	source	C:\Program Files\Splunk\var\log\splunk\splunkd.log	▼
	sourcetype	splunkd	▼
Event	component	TailReader	▼
	event_message	Batch input finished reading file='C:\Program Files\Splunk\var\spool\splunk\tracker.log'	▼
	eventtype	splunkd-log	▼
	file	'C:\Program Files\Splunk\var\spool\splunk\tracker.log'	▼
	thread_id	15116	▼

The dropdown menu for refining the search shows the following options:

- Add to search: 32 events
- Exclude from search: 14 events
- New search
- splunk_server: learner01

2.4 Refine Searches (continued)

Refining Searches - Search modes

In Splunk, there are three **search modes**:

1. **Fast Mode**: This mode is designed to return search results as quickly as possible, sacrificing some accuracy and completeness for speed.
2. **Smart Mode**: This mode **automatically switches** between **Fast** and **Verbose** modes depending on the size and complexity of the search. It attempts to provide the best balance between speed and accuracy, and is the default search mode in Splunk.
3. **Verbose Mode**: This mode is designed to provide the **most accurate** and **complete** search results, even if it **takes longer** to execute. It performs a detailed analysis of all of the events in the data, and can be useful for debugging and troubleshooting purposes.

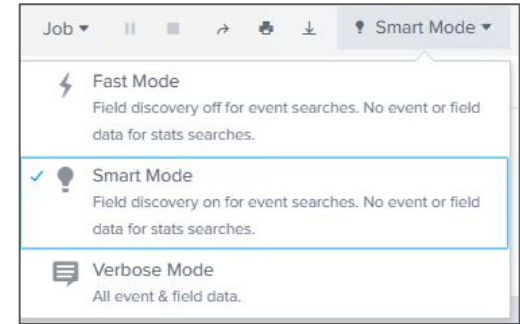


image: screenshot, splunk Search & Reporting app

2.4 Refine Searches - Summary

Refining searches in Splunk can help to **narrow down** the search results and find **relevant** information.

This can be done by adding **more** search terms, using **filters**, and refining search syntax.

Different **search modes** in Splunk affect the way results are returned.

Refining searches can also help to **eliminate irrelevant data** or false positives, leading to more efficient and accurate analysis.

Basic ways to refine a search include **drill-down** into the search results, using different **search modes**, and **comparison operators**.

2.5 Use the Timeline

Use the timeline to investigate events-

The **timeline** is a **visual representation** of the **number of events** in your search results that occur at each point in time.

The timeline shows the **distribution of events over time**.

When you use the timeline to investigate events, you are not running a new search; you are filtering the existing search results.

You can use the timeline to **highlight patterns or clusters of events** or **investigate** peaks (spikes in activity) and lows (possible server downtime) in event activity.

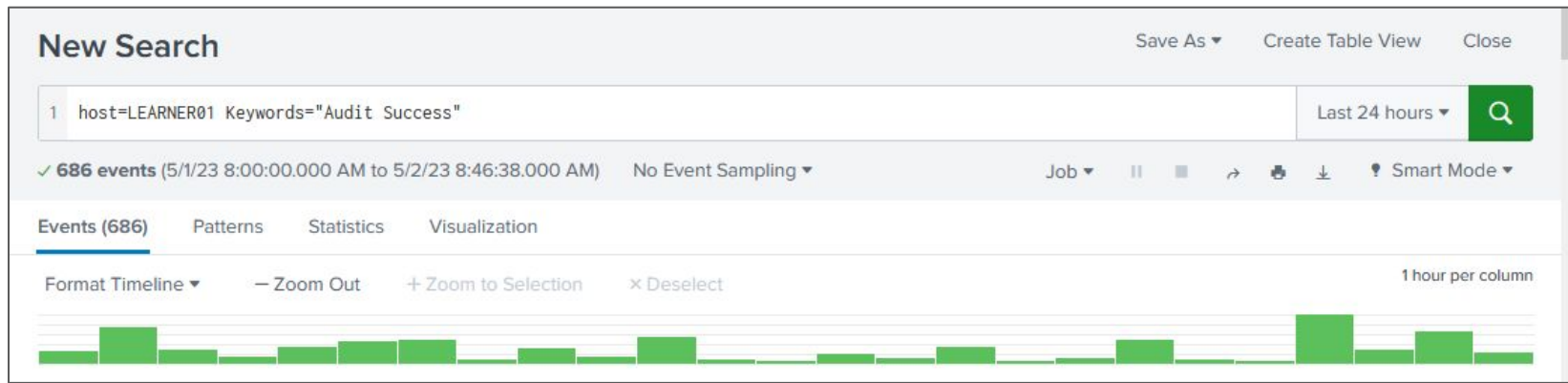
Position your mouse over a **bar** to see the count of events. **Click** on a bar to **drill down** to that time range.

2.5 Use the Timeline

Change the timeline format-

The **timeline** is a **visual representation** of the **number of events** in your search results that occur at each point in time.

The timeline shows the **distribution of events over time**.



2.5 Use the Timeline (continued)

Change the timeline format-

Format options are located in the **Format Timeline menu**:

You can **hide the timeline** or **display** a **Compact** or **Full** view of the timeline.

You can also **toggle the timeline scale** between **Linear** scale or **Log** scale (logarithmic).

When **Full** is selected, the timeline view is **taller** to accommodate the labels on the axis. The count is on the Y-axis and time is on the X-axis.

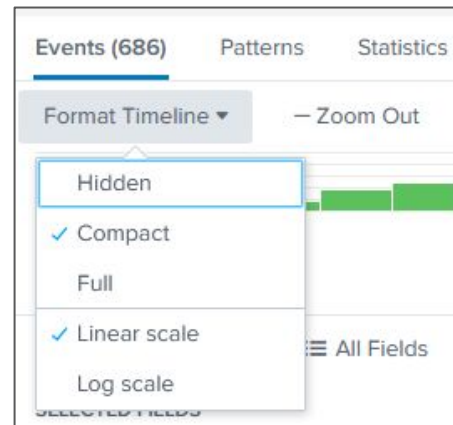


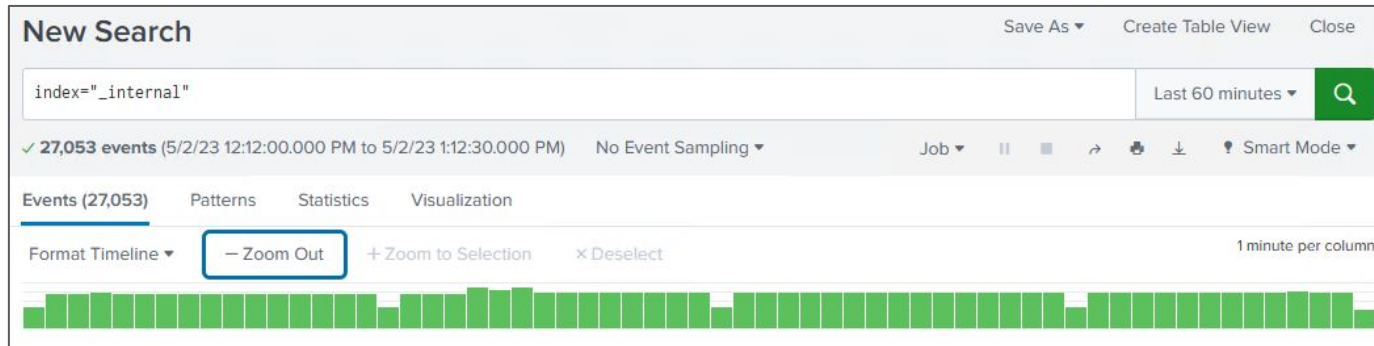
image: screenshot, splunk Search & Reporting app

2.5 Use the Timeline (continued)

Zoom in and zoom out to investigate events.

Above the timeline are the **zoom** options.

By **default**, the timeline is **zoomed in**. When in **Full view** and **zoomed in**, the **Zoom Out** option is available.



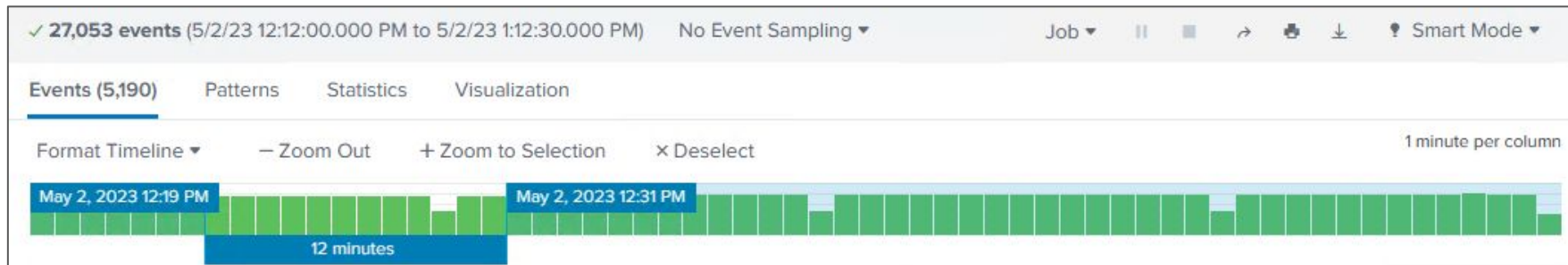
When you use the Zoom In/Out to Selection buttons, Splunk will run a new search with a new time frame.

2.5 Use the Timeline (continued)

Zoom to a selection-

When you **mouse over, and select bars** in the timeline, the **Zoom to Selection** or **Deselect** options above the timeline become **available**. Additionally, the **events list** updates to display **only the events** that occurred in that **selected time range**.

You can cancel this selection by clicking **Deselect**.



2.5 Use the Timeline - Summary

In Splunk, the **timeline** is a **visual representation** of the **events** that **match** a particular **search**.

It shows the **distribution of events over a period of time** and allows the user to **easily** identify **patterns** and **trends**.

The timeline can be used to **refine searches** by zooming in on **specific time periods** and identifying events that occurred within that time frame.

Selecting a time range on the timeline will **filter** the events on the search results **without running a new search**. **Zooming** in or **zooming to a selection** will **run a new search**.

It is a **powerful** tool for analyzing and visualizing time-based data in Splunk.

Use Time Modifiers in Your Search

Time modifiers-

When **searching** or saving a search, you can specify **absolute** and **relative** time ranges using **time modifiers**.

- An **absolute** time range uses specific dates and times (e.g., from 12 A.M. April 1, 2023 to 12 A.M. April 13, 2023).
- A **relative** time range is dependent on **when the search is run**. For example, a relative time range of **-60m** means **60 minutes ago**. If the current time is 3 P.M., the search returns events from the **last 60 minutes**, or 2 P.M. to 3 P.M. today.
- The current time is referred to as "**now**."
- Set the start of the time range using the **earliest=** command.
- Set the end of the time range using the **latest=** command.

earliest=<time_modifier>
latest=<time_modifier>

Use Time Modifiers in Your Search (continued)

Time modifiers and the Time Range Picker-

- A **time range** that you specify in the **Search bar**, or in a saved search, **overrides** the time range that is selected in the **Time Range Picker**.
- If you specify a time range of **Last 24 hours in the Time Range Picker** and in the **Search bar** you specify **earliest=-30m latest=now**, the search only **looks at events** that have a timestamp within the **last 30 minutes**.
- This applies to **any of the options** you can select in the **Time Range Picker**.
- Time ranges that you specify **directly in the Search bar** apply only to **that portion** of the search.
 - The time ranges specified in the **main search** do not apply to **subsearches**.
 - Time time ranges specified in a **subsearch** applies **only to that subsearch**. The time range does not apply to the **main** search or any other **subsearch**.

Use Time Modifiers in Your Search (continued)

Specify absolute time ranges-

- For **exact time ranges**, the syntax for the time modifiers is **%m/%d/%Y:%H:%M:%S**.
- The following search specifies a time range from 12 A.M. April 19, 2023 to 12 A.M. April 27, 2023.
 - **earliest=04/19/2023:00:00:00 latest=04/27/2023:00:00:00**
- If you specify **only the earliest** time modifier, the **latest** is set to the **current time now by default**.
- If you specify a **latest** time modifier, you **must** also specify an **earliest** time.

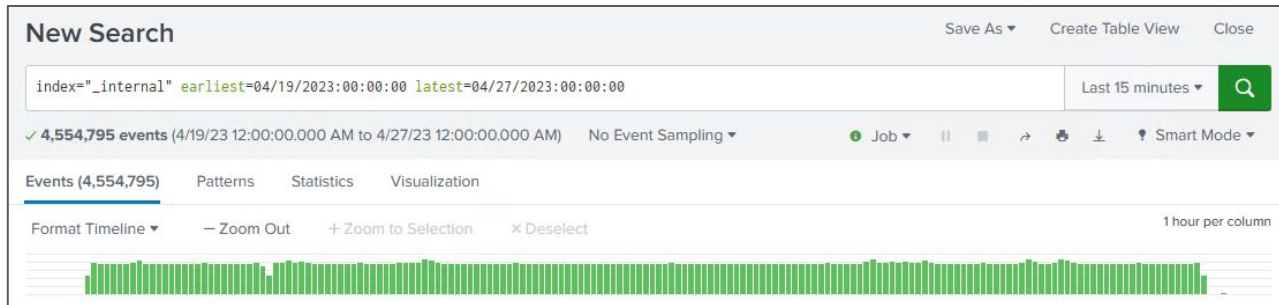


image: screenshot, splunk Search & Reporting app

Use Time Modifiers in Your Search (continued)

Specify relative time ranges-

- You define the **relative time** in your search by using a **string** of characters that indicate the **amount of time**.
- The syntax is an **integer** and a **time unit**:
 - Begin your string with a **minus (-)** or a **plus (+)** to indicate the offset **before** or **after** the time amount.
 - Specify the **amount of time** by using a **number** and a **time unit**.
 - When specifying relative time, use **now** to refer to the **current** time.

Time range	Valid values
seconds	s, sec, secs, second, seconds
minutes	m, min, minute, minutes
hours	h, hr, hrs, hour, hours
days	d, day, days
weeks	w, week, weeks
months	mon, month, months
quarters	q, qtr, qtrs, quarter, quarters
years	y, yr, yrs, year, years

Use Time Modifiers in Your Search (continued)

Relative time modifiers that snap to a time-

- With **relative time**, you can specify a **snap to time**, which is an **offset from the relative time**.
- The snap to time unit **rounds down to the nearest or latest time** for the time amount that you specify.
- To do this, **separate** the **time amount** from the **snap to time** unit with an "@" character.
 - For example, the current time is **15:45:00** and the **snap to time** is **earliest=-h@h**. The time modifier snaps to **14:00**.
- You can also define the relative time modifier using **only the snap to time** unit. To snap to a **specific day** of the week, use **@w0** (or **@w7**) for **Sunday**, **@w1** for **Monday**, and so forth.
- To search for events in the **previous month**, specify **earliest=-mon@mon latest=@mon**. This example begins at the **start** of the **previous month** and ends at the **start** of the **current month**.

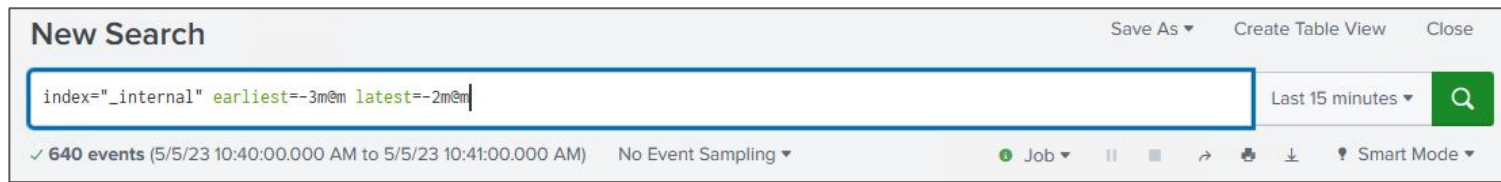
Use Time Modifiers in Your Search - Summary

An absolute time range refers to a **specific range of time** that is defined by a **start** time and an end **time**, in a **specific** date and time format:

- **earliest=04/19/2023:00:00:00 latest=04/27/2023:00:00:00**

A **relative time range**, is a range of time that is defined in **relation to the current time** or to a **specific time point**. This type of range is usually defined using time units such as **minutes**, **hours**, **days**, or **weeks**, and can be expressed as a **positive** or **negative** value.

Snap to time is an **offset** from the **relative time** and **rounds down to the nearest or latest time** for the time amount that you specify using the "@" character.



2.7 Control a Search Job

About jobs and job management-

Each time you run a **search**, create a pivot, open a report, or load a dashboard panel, the Splunk software **creates a job** in the system.

When you run a search, you are creating an **ad hoc search**. Pivots, reports, and panels are powered by **saved** searches.

A **job** is a **process that tracks information** about the ad hoc search or saved search.

The information that is tracked includes the **owner** of the job, the **app** that the job was run on, how many **events** were returned, and how **long the job took to run**.



designed by  freepik.com

image: Freepik.com

2.7 Control a Search Job (continued)

Inspecting jobs and managing jobs-

There are **several** ways that you can look at information about your **jobs**.

You can **inspect** a job or you can **manage** a job.

Search Job Inspector

- Use the **Search Job Inspector** to view **information** about the **current job**, such as job **execution costs** and job **properties**.

Search job inspector

This search has completed and has returned **26,741** results by scanning **26,741** events in **1.757** seconds

(SID: 1683059916.1327) [search.log](#) [Job Details Dashboard](#)

Execution costs

Duration (seconds)	Component	Invocations	Input count	Output count
0.00	command.fields	15	26,741	26,741
0.38	command.search	15	-	26,741
0.03	command.search.expand_search	2	-	-
0.00	command.search.calcfields	14	26,741	26,741
0.00	command.search.evalfilter	14	26,741	26,741
0.00	command.search.expand_search.calcfield	2	-	-
0.00	command.search.expand_search.fieldalias	2	-	-
0.00	command.search.expand_search.indexed_fields	2	-	-
0.00	command.search.expand_search.kv	2	-	-

2.7 Control a Search Job (continued)

Inspecting jobs and managing jobs-

Job Details dashboard

- The **Job Details dashboard** provides a clear and concise overview of a search job process.
- You can access the **Job Details dashboard** through the Search Job Inspector.

Job Details Dashboard				
<p>This dashboard displays properties of a search job. Use it to gain insight into search job performance and troubleshoot search efficiency issues. Provide a Search ID for a job that has not expired.</p> <p>Learn more</p>				
<p>Search ID (SID)</p> <input type="text" value="1683059916.1327"/>				
Summary				
Search Duration	Total Events Scanned	Total Events Matched	Result Count	Events Scanned Per Second
1.76s	26,741	26,741	26,741	15,220
Search Status	Search User	Search Mode		
done	psadmin	Learn more smart		

2.7 Control a Search Job (continued)

Inspecting jobs and managing jobs-

Jobs manager page

- Use the **Jobs manager page** to view information about recent jobs.
- If you have the **Admin** role or a role with an equivalent set of capabilities, you can **manage** the search jobs run by **other users**.

52 Jobs App: Search & Reporting (search) Owner: All Status: All filter 10 Per Page

Edit Selected < Prev 1 2 3 4 5 6 Next >

i	<input type="checkbox"/>	Owner	Application	Events	Size	Created at	Expires	Runtime	Status	Actions
>	<input type="checkbox"/>	psadmin	search	5	92 KB	May 2, 2023 4:51:11 PM	May 2, 2023 5:01:56 PM	00:00:01	Done	Job ▾ ■ ↻ ⬇
index="_introspection" sourcetype=search_telemetry search_id="1683059916.1327" spath path=search_commands .name output=command spath ...										
>	<input type="checkbox"/>	psadmin	search	1	88 KB	May 2, 2023 4:50:57 PM	May 2, 2023 4:55:56 PM	00:00:01	Done	Job ▾ ■ ↻ ⬇
index="_introspection" sourcetype=search_telemetry search_id="1683059916.1327" spath path=search_commands .name output=command spath ...										
>	<input type="checkbox"/>	psadmin	search	1	88 KB	May 2, 2023 4:50:57 PM	May 2, 2023 4:55:56 PM	00:00:01	Done	Job ▾ ■ ↻ ⬇
index="_introspection" sourcetype=search_telemetry search_id="1683059916.1327" spath path=search_commands .name output=command spath ...										
>	<input type="checkbox"/>	psadmin	search	1	88 KB	May 2, 2023 4:50:57 PM	May 2, 2023 4:55:56 PM	00:00:01	Done	Job ▾ ■ ↻ ⬇

2.7 Control a Search Job (continued)

Job menu-

- After you run a search or open a report in Splunk Web, you can **access and manage** information about the **search job** without leaving the **Search** page.

- On the **Job menu**, the following options are available:



image: screenshot, splunk Search & Report app

- **Edit the job settings.** Select this to open the Job Settings dialog, where you can change the job read permissions, extend the job lifetime, and get a URL for the job.
- **Send the job to the background.** Select this if the search job is slow to complete and you want to work on other Splunk activities, including running a new search job. The job continues to run in the background.
- **Inspect the job.** Opens a separate window and displays information and metrics for the search job using the Search Job Inspector.
- **Delete the job.** Use this to delete a job that is currently running, is paused, or which has finalized. After you delete the job, you can still save the search as a report.

2.7 Control a Search Job (continued)

Edit search job settings

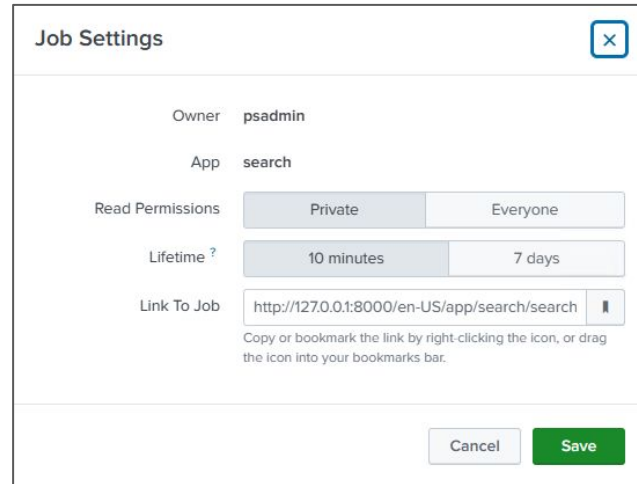
- You can open the Job Settings dialog when a search job is running, paused, or finalized. Just click Job and select **Edit Job Settings**.

Sharing jobs

- There are several ways to share a job with other Splunk users. You can change the job permissions or send a link to the job.

Job lifetimes

- When you run a new search, a job is retained in the system for a period of time, called the job lifetime.




Job Settings

Owner psadmin

App search

Read Permissions Private Everyone

Lifetime ? 10 minutes 7 days

Link To Job 

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

Cancel Save

image: screenshot, splunk Search & Reporting app

The default lifetime is 10 minutes. The lifetime starts from the moment the job is run.

2.7 Control a Search Job - Summary

A **search job** is the process of executing a search request and retrieving the results.

When you **initiate** a **search** in Splunk, it creates a **search job** that runs in the background to fetch and process the data, while this is happening, you can **stop** or **pause** the process.

The **Search Job Inspector**, **Job Details dashboard**, **Jobs manager page**, and the **Job menu** allow you to **inspect** and **manage** search jobs.

The **Edit search job settings**, option allows you to **share** the job, edit the job's **permissions**, and change the job's **lifetime**.

The **default lifetime of a job is 10 minutes**. Using the job settings menu you can **extend the job's lifetime to 7 days**.

2.8 Save Search Results

In Splunk, users have the option to **save** search results for later use or to share with others.

Saving search results allows users to **easily access relevant data** without having to **re-run** the search.

A user can also **export** the search results in several **different formats**.



image: Freepik.com

2.8 Save Search Results (continued)

Saving the search results.

There are **several** ways to **save search results** in Splunk.

Using the **Save As** drop-down menu, any search can be saved as a **Report** or an **Alert**.

Search results (especially searches that include statistical analysis) can, via this menu, serve as data drivers for **new** or **existing Dashboards**.

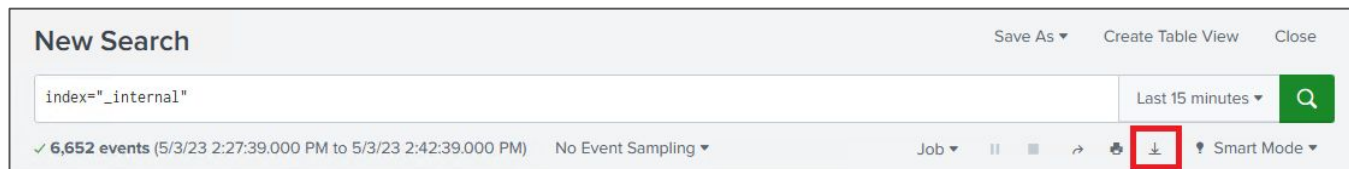
We will cover Reports, Alerts, and Dashboards in more detail later in this course.

Save as option	Description	More information
Report	When you create a search that you would like to run again, you can save the search as a report.	See Create and edit reports in the <i>Reporting Manual</i> . If you are using reports, also referred to as "saved searches," in the Splunk Dashboard Studio see, Use reports and saved searches with ds.savedSearch in the <i>Splunk Dashboard Studio</i> manual for information on how to use them.
Dashboard panel	You can also save a search as a dashboard panel. Dashboards can have one or more panels which can show search results in tables or in graphical visualizations.	See Getting started in the <i>Dashboards and Visualizations</i> manual. These searches are also referred to as "ad hoc" searches. If you are using these searches in the Splunk Dashboard Studio, see, Create search-based visualizations with ds.search in the <i>Splunk Dashboard Studio</i> manual.
Alert	Some searches provide timely information that you want to be notified about. You can save a search as an alert. An alert is an action that a saved search triggers, based on the results of the search. The action might be to send an email or run a script.	See About alerts in the <i>Alerting Manual</i> .
Event type	You can save a search as an event type. Event types are a categorization system to help you make sense of your data. Event types let you sift through huge amounts of data, find similar patterns, and create alerts and reports.	See About event types in the <i>Knowledge Manager Manual</i> .

2.8 Save Search Results (continued)

Export the search results.

To export the search results to a file, use the **Export button** next to the Job toolbar.



When exporting, the following file formats are available:

- Raw Events
- CSV
- XML
- JSON

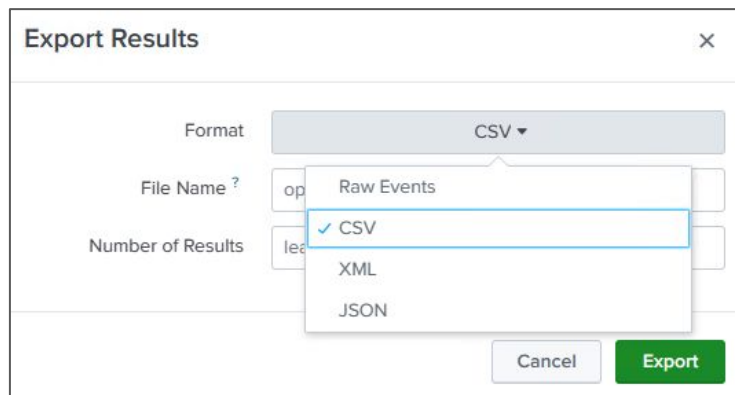


image: screenshot, splunk Search & Report app

2.8 Save Search Results - Summary

Saving a search, be it a **report**, **alert** or **dashboard**, is a way to **preserve** and **share** a predefined **view of data** that has been extracted and analyzed from a search query.

You can also **export** search results to a file in any of the following formats:

- **Raw events**
- **CSV**
- **XML**
- **JSON**

Knowledge check.

- What syntax is used to link key/value pairs in search strings?
- What does the "earliest=-72h@h latest=@d" time range do?
- What is the function of the timeline located under the search bar?
- What can be configured using the Edit Job Settings menu?
- What user interface component allows for time selection?
- By default, how long does Splunk retain a search job?
- Which Boolean operator is implied between search terms, unless otherwise specified?
- What character is used as a wildcard in Splunk?
- What is the easiest and most effective way to optimize your searches?
- What is an event?
- What are the three search modes in Splunk?