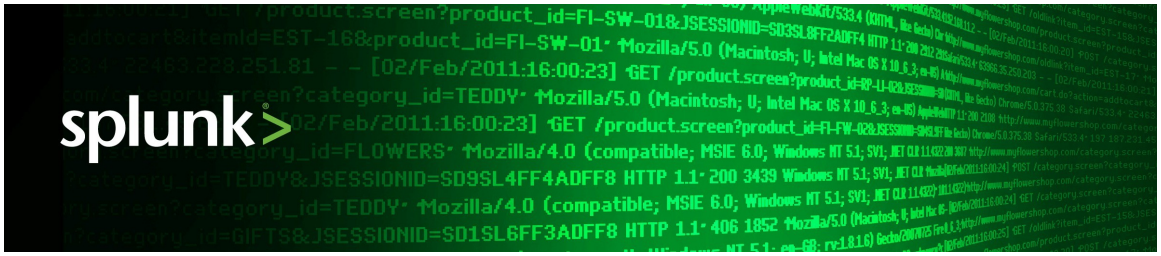


Splunk® Enterprise Search Tutorial 7.1.2

Generated: 7/24/2018 3:59 pm

Table of Contents

Table of Contents

Introduction

About the Search Tutorial

The Search & Reporting application (Search app) is the primary interface for using the Splunk software to run searches, save reports, and create dashboards. This Search Tutorial is for users who are new to the Splunk platform and the Search app.

Use this tutorial to learn how to use the Search app. Differences between Splunk Enterprise and Splunk Cloud are specified throughout this tutorial.

Already have access to Splunk software?

For this tutorial, use a free Trial version of the Splunk software.

Why? Because this tutorial uses a specific set of data to ensure consistency in your search results and the features that you are learning about. In the tutorial, you will upload this tutorial-specific data to the Splunk platform. You might not have permission to upload data in your production, work environment. Additionally, using a free Trial version of the software ensures that the tutorial data is not mixed in with your work data.

The Trial version of the software converts to a Free version after 30 days. If you have a Free version of the Splunk software, some of the features, such as changing Preferences in the User account menu, are not available. See About Splunk Free in the *Admin manual*.

The steps for downloading a free Trial version of Splunk Enterprise or Splunk Cloud are described in the tutorial.

What's in this tutorial?

You will learn how to use the Search app to add data to your Splunk deployment, search the data, save the searches as reports, and create dashboards. If you are new to the Search app, this tutorial is the place to start.

How to use this tutorial

Each Part in the Search Tutorial builds on the previous Part. For example, the searches that you create in Part 5 are used to create reports and charts in Part 7. It is important that you don't skip a Part.

- **Part 1: Getting started**
- **Part 2: Uploading the tutorial data**
- **Part 3: Using the Splunk Search app**
- **Part 4: Searching the tutorial data**
- **Part 5: Enriching events with lookups**
- **Part 6: Creating reports and charts**
- **Part 7: Creating dashboards**

Using the PDF version of the tutorial

You can copy and paste search strings or regular expressions directly into the Search & Reporting App from this online tutorial in your web browser.

Do not copy and paste search strings or regular expressions directly from the electronic PDF into the Search app. Pasting data from the PDF can cause errors in searches, because of hidden characters that are included in the PDF formatting.

See also sections

At the end of most of the topics in this tutorial is a section called **See also**. These sections contain links to Splunk documentation that is related to the information discussed in that topic.

Additional resources

See Additional resources at the end of this tutorial for information about:

- The Splunk community
- Links to the Splunk documentation
- Providing feedback

Part 1: Getting started

What you need for this tutorial

You need to create a Splunk.com account, access the free trial Splunk software, and download the tutorial data files. There might be other prerequisites, depending on which Splunk platform you use.

Create a Splunk.com account

You need a Splunk.com account to download the free trial Splunk software. If you do not already have a Splunk.com account, you need to create an account. If you already have an account, you need to log in to that account.

1. In a separate browser window, go to http://www.splunk.com/.
    - Use **CTRL+click** on the download link to open the link in a new browser tab.
    - By using a separate browser window, you keep this window with the Search Tutorial instructions open. You can switch back and forth between the browser tabs.
2. In the upper right corner of the window, click the Splunk Account icon .
    - To create an account, click **Sign Up** and complete the registration information.
    - To log in to an existing account, click **Login**.

Choose a platform

You can use this tutorial with a trial version of Splunk Cloud or Splunk Enterprise. The main difference in the trial versions is the length of the license.

Splunk Cloud

When you start a Splunk Cloud trial, you have access to Splunk Cloud for 15 days. The trial license includes all of the features in Splunk Cloud, and access to select premium applications and add-ons. You can index up to 5GB of data each day.

After 15 days, the access to your Splunk Cloud trial expires.

Splunk Enterprise

When you download Splunk Enterprise for the first time, you get a Splunk

Enterprise Trial license for 30 days. This trial license includes all of the features in Splunk Enterprise, and access to all premium applications and add-ons. You can index up to 500MB of data each day.

After 30 days, the Enterprise Trial license converts to a perpetual Free license and some of the features, such as user preferences, authentication, and alerting are disabled. The Free license also includes the 500MB daily indexing volume, but there is no expiration date. See About Splunk Free in the *Admin manual*.

System requirements

Ensure that your computer meets the system requirements for your platform.

Splunk Cloud

You must have a web browser. The latest versions of Chrome, Firefox, and Safari browsers are supported with Splunk Cloud.

Splunk Enterprise

You can use Splunk Enterprise on Linux, Windows, and Mac OS. For this tutorial, your computer must meet the specifications listed in the following table.

Requirement	Minimum supported hardware capacity
Non-Windows platforms	2-core 64-bit CPU at 2GHz or greater, 4GB RAM
Windows platforms	2-core 64-bit CPU at 2GHz or greater, 4GB RAM
Web browser	The latest versions of Chrome, Firefox, and Safari browsers are supported with Splunk Enterprise 6.0 and later

Download the tutorial data files

This tutorial uses a fictitious game store, called Buttercup Games, that sells games and related items in an online store.

You must download several data files to use with the tutorial. The data files contain web access log files, secure formatted log files, sales log files, and a

price list in a CSV file.

If you use the **Safari** browser, under **Preferences > General**, ensure that the `Open ?safe? files after downloading` option is **unchecked**. The `tutorialdata.zip` file must be compressed to upload the file successfully.

1. Download the `tutorialdata.zip` file. Do not uncompress the file.
2. Download the `Prices.csv.zip` file. Do not uncompress the file at this time.

Access the trial version of the Splunk software

For this tutorial, use the latest version of the software.

Splunk Cloud

For this tutorial, set up a trial version of Splunk Cloud.

1. In a separate browser window, setup a free trial version of Splunk Cloud.
    - Use **CTRL+click** on the download link to open the link in a new browser tab.
    - By using a separate browser window, you keep this window with the Search Tutorial instructions open. You can switch back and forth between the browser tabs.
2. Follow the prompts on the website.
3. When the trial version is created, click **View My Instance**.
4. On the Terms of Service page, check the box to confirm your agreement and click **OK**.
    - Your trial version of Splunk Cloud opens in a browser window.
    - Additionally, an email is sent to you with information about your Splunk Cloud instance. For example, if you close the browser window, the email explains how to access your Splunk Cloud instance again.
5. See Next step.

Splunk Enterprise

If you downloaded the Splunk Enterprise trial software previously, download the trial software again. It is possible that your Splunk Enterprise trial license converted to a free license. The free license has some limitations that will not allow you to complete all parts of this tutorial.

1. Identify the installer that you want use with the tutorial.

Operating system	For this tutorial	Available installers
Linux	**Use any of the installers.**	3 installers. An RPM download for RedHat, a DEB package for Debian Linux, and a TAR file installer.
Mac OSX	**Use the DMG packaged graphical installer.**	2 installers. A DMG package and a TAR file installer.
Windows	**Use the MSI file graphical installer that is appropriate for you computer.**	2 installers. An MSI file for 64-bit and an MSI file for 32-bit.

2. In a separate browser window, download the free trial version of the installer for Splunk Enterprise.
    - Use **CTRL+click** on the download link to open the link in a new browser tab.
    - By using a separate browser window, you keep this window with the Search Tutorial instructions open. You can switch back and forth between the browser tabs.
3. See Next step.

Next step

The next step depends on the Splunk platform that you are using.

Splunk Cloud

If you see a window welcoming you to the Splunk Free Cloud Trial and inviting you to **Drop your data file here**, close that window. You will upload the tutorial data In Part 2. For now, go to Navigating Splunk Web.

Splunk Enterprise

You must install Splunk Enterprise.

See also

System Requirements in the *Installation Manual*
Types of Splunk licenses in the *Admin Manual*

Install Splunk Enterprise

You can install Splunk Enterprise on the following operating systems.

- Linux installation instructions
- Windows installation instructions
- Mac OS X installation instructions

For other installers or other supported operating systems, see the step-by-step installation instructions for that platform. After installing Splunk Enterprise, you can continue to Navigating Splunk Web.

Linux installation instructions

Splunk Enterprise provides three Linux installer options: an RPM, a DEB, or a .tar file.

Prerequisite
You must have access to a command-line interface (CLI). When you type in the installation commands, replace `splunk_package_name` with the file name of the Splunk Enterprise installer that you downloaded.

Install the Splunk Enterprise RPM

You can install the Splunk Enterprise RPM in the default directory `/opt/splunk`, or in a different directory.

1. Use the CLI to install Splunk Enterprise.
   - To install into the default directory, type **`rpm -i splunk_package_name.rpm`**.
   - To install into a different directory, add the `--prefix` flag to the installation command.
     For example, type **`rpm -i --prefix=/opt/new_directory splunk_package_name.rpm`**.
2. A command line window prompts you to create an administrator password. You need this password for your initial Splunk Enterprise login.

```
This appears to be your first time running this version of Splunk.
An Admin password must be set before installation proceeds.
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
```

If you have enabled `--no prompt` in the command line, you are not prompted to create the administrator credentials needed to log into Splunk Enterprise for the first time. There are several ways you can create these credentials at startup. See Start Splunk Enterprise for the first time.

3. Go to the steps to Launch Splunk Web.

Install the Splunk Enterprise DEB package

- You can install the Splunk Enterprise DEB only into the `/opt/splunk` directory.
- This location must be a regular directory, and cannot be a symbolic link.
- You must have access to the root user or have sudo permissions to install the package.
- The package does not create environment variables to access the Splunk Enterprise installation directory. You must set those variables on your own.

If you need to install Splunk Enterprise somewhere else, or if you use a symbolic link for `/opt/splunk`, then use a TAR file to install the software.

1. In the CLI, type **`dpkg -i splunk_package_name.deb`**.
2. Go to the steps to Launch Splunk Web.

Install the Splunk Enterprise TAR file

Knowing the following items helps ensure a successful installation with a tar file:

- Some non-GNU versions of `tar` might not have the `-C` argument available. In this case, to install in `/opt/splunk`, either `cd` to `/opt` or place the tar file in `/opt` before you run the `tar` command. This method works for any accessible directory on your host file system.
- Splunk Enterprise does not create the `splunk` user. If you want Splunk Enterprise to run as a specific user, you must create the user manually before you install.
- Confirm that the disk partition has enough space to hold the uncompressed volume of the data you plan to keep indexed.

1. To install Splunk Enterprise on a Linux system, expand the TAR file into an appropriate directory using the `tar` command. The default installation directory is `splunk` in the current working directory.

   To install into `/opt/splunk`, use the following command with the `-C`

argument.

```
tar xvzf splunk_package_name.tgz -C /opt
```

2. A command line window prompts you to create an administrator password. You will need this password for you initial Splunk Enterprise login. `This appears to be your first time running this version of Splunk.`

   ```
   An Admin password must be set before installation proceeds.
   Password must contain at least:
      * 8 total printable ASCII character(s).
   Please enter a new password:
   Please confirm new password:
   ```

   If you have enabled `--no prompt` in the command line, you are not prompted to create the administrator credentials needed to log into Splunk Enterprise for the first time. There are several ways you can create these credentials at startup. See Start Splunk Enterprise for the first time.
3. Go to the steps to Launch Splunk Web.

Windows installation instructions

For this tutorial you will install Splunk Enterprise using the default installation settings, which run the software as the Local System user, `admin`.

1. Navigate to the folder or directory where the installer is located.
2. Double-click the `splunk.msi` file to start the installer.
3. In the Welcome panel, read the License Agreement and click **Check this box to accept the license agreement**.
4. Click **Next**.
5. You are prompted to specify a password for the Splunk admin user. Type and confirm the password.
   The password must be at least 8 characters in length. Do not forget this password. You will use this password to log into Splunk Web.
6. Click **Next**.
7. (Optional) You are prompted to create a shortcut on the Start Menu. If you want to do this, click **Create Start Menu shortcut**.
8. Click **Install**.
9. In the Installation Complete panel, confirm that the **Launch browser with Splunk** check box is selected.
10. Click **Finish**.
    The installation finishes, Splunk Enterprise starts, and Splunk Web launches in a browser window.
11. Go to the steps to Launch Splunk Web.

For other user options or to perform a custom installation, see the instructions for Install on Windows in the *Installation Manual.*

Mac OS X installation instructions

1. Navigate to the folder or directory where the installer is located.
2. Double-click the DMG file.
   A Finder window that contains the `splunk.pkg` opens.
3. Double-click the `Install Splunk` icon to start the installer.
4. The **Introduction** panel lists version and copyright information. Click **Continue**.
5. The **License** panel lists shows the software license agreement. Click **Continue**.
6. You will be asked to agree to the terms of the software license agreement. Click **Agree**.
7. In the **Installation Type** panel, click **Install**. This installs Splunk Enterprise in the default directory `/Applications/splunk`.
8. You are prompted to type the password that you use to login to your computer.
9. When the installation finishes, a popup informs you that an initialization must be performed. Click **OK**.
10. A terminal window appears with a prompt for you to specify a password to access Splunk Enterprise with the `admin` account. Choose a password that is at least 8 characters long. Do not forget this password. You will use this password to log into Splunk Web. Type the password and press return. The cursor will not advance as you type.
11. Confirm the new password when prompted and press return.
12. A popup appears asking what you would like to do. Click **Start and Show Splunk**. The login page for Splunk Enterprise opens in your browser window.
13. Close the **Install Splunk** window.

    The installer places a shortcut on the Desktop so that you can launch Splunk Enterprise from your Desktop any time.
14. Go to the steps to Launch Splunk Web.

Next step

Start Splunk Enterprise and launch Splunk Web

See also

Install on Linux in the *Installation Manual*.

Launch Splunk Web

After you download and install the software, you must start Splunk Enterprise and launch Splunk Web.

- Start Splunk Enterprise on Linux
- Start Splunk Enterprise on Windows
- Start Splunk Enterprise on Mac OS X

Start Splunk Enterprise on Linux

After you install Splunk Enterprise, use the Splunk CLI to start Splunk Enterprise.

Prerequisite
You need to understand how to access the CLI. See About the CLI in the *Admin Manual*.

Steps

1. Simplify the CLI access by adding a `SPLUNK_HOME` environment variable for the top-level installation directory, and adding `$SPLUNK_HOME/bin` to your shell's path.
   If you installed in the default location for Linux, then your export path looks like this:

   ```
   # export SPLUNK_HOME=/opt/splunk
   # export PATH=$SPLUNK_HOME/bin:$PATH
   ```

   If you installed in another location, use that path for the `SPLUNK_HOME` environment variable.
2. In the CLI, to start Splunk Enterprise type **`$SPLUNK_HOME/bin/splunk start`**
3. Accept the Splunk Enterprise license.
   After you run the `start` command, Splunk Enterprise displays the license agreement and prompts you to accept the license before the startup sequence continues.

   Troubleshooting: If you have problems starting Splunk Enterprise, see

Start Splunk Enterprise for the first time in the *Installation Manual*.
4. Now login to Splunk Web.

Useful CLI commands

If you need to stop, restart, or check the status of your Splunk Enterprise server, use these CLI commands:

```
$ splunk stop
$ splunk restart
$ splunk status
```

Start Splunk Enterprise on Windows

After the Windows installation finishes, Splunk Enterprise starts and opens Splunk Web in a supported browser.

If Splunk Enterprise does not start, use one of the following options to start it.

- Start Splunk Enterprise from the **Start** menu.
- Use the Windows Services Manager to start Splunk Enterprise.
- Open a `cmd` window, go to `\Program Files\Splunk\bin`, and type **`splunk start`**.

Now login to Splunk Web.

Start Splunk Enterprise on Mac OS X

In Mac OS X, you can start Splunk Enterprise from your desktop.

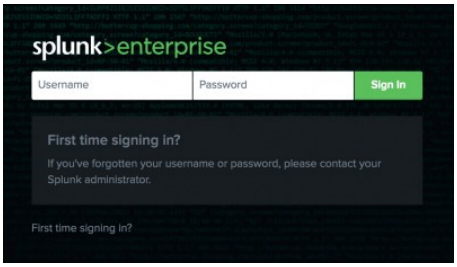
1. Double-click the **Splunk** icon on your desktop.
2. The first time you run the helper application, it notifies you that it needs to perform an initialization. Click **OK**. Splunk Enterprise initializes and sets up the trial license.
3. In the Splunk's Little Helper window, select **Start and Show Splunk**. This option starts Splunk Enterprise and directs your web browser to open a page to Splunk Web. You can also use the Splunk's Little Helper application to stop Splunk Enterprise.
4. Now login to Splunk Web.

Login to Splunk Web

Splunk Web runs by default on port 8000 of the host on which it is installed. If you use Splunk Enterprise on your local machine, the URL to access Splunk Web is `http://localhost:8000`.

When you launch Splunk Enterprise for the first time, this login screen appears.

1. Login using the username **admin** and the password that you specified when you installed Splunk Enterprise.



2. The **Help us improve Splunk software** window appears. Read each of the types of usage collection and click **OK** or **Skip**.

The first page you see is Splunk Home.

Next step

You have downloaded the tutorial data files and installed Splunk Enterprise.

Continue to Navigating Splunk Web.

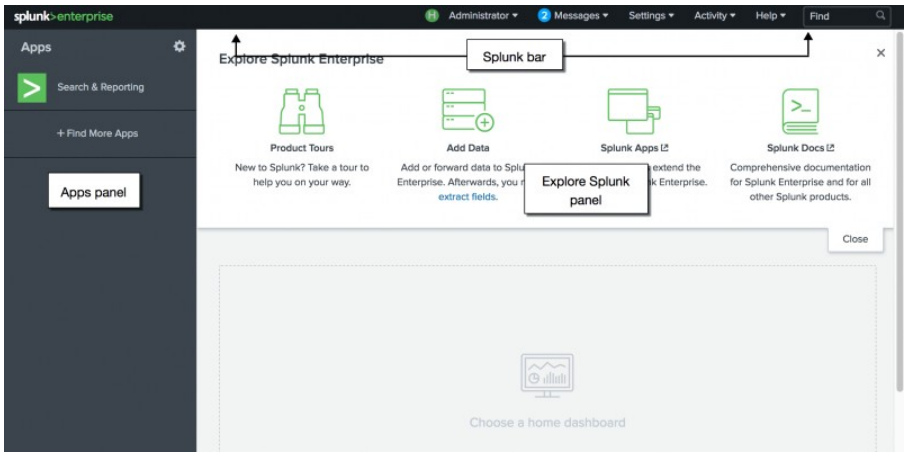
Navigating Splunk Web

Splunk Web is the primary interface for searching, problem investigation, reporting on results, and administrating Splunk deployments.

About Splunk Home

Splunk Home is the initial page in Splunk Web. Splunk Home is an interactive portal to the data and applications that you can access from your Splunk instance. The main parts of the Splunk Home page are the Apps panel, the Explore Splunk panel, and the Splunk bar.

The following screen image shows the Splunk Home page for Splunk Enterprise. Splunk Cloud has a similar Home Page.



Apps panel

The **Apps** panel lists the applications that are installed on your Splunk instance. The list shows only the apps that you have permission to view.

When you first open Splunk Web, you see **Search & Reporting** in the Apps panel. The **Search & Reporting** app is sometimes referred to as simply the **Search app**. There might be other apps listed on the Apps panel if other applications are installed on your computer.

Explore Splunk panel

The Explore Splunk panel contains links to pages where you can get help.

Splunk Cloud
: You can take a product tour or access the documentation that is used the most.

Splunk Enterprise
: You can take a product tour, add data, browse for new apps, or access the documentation.

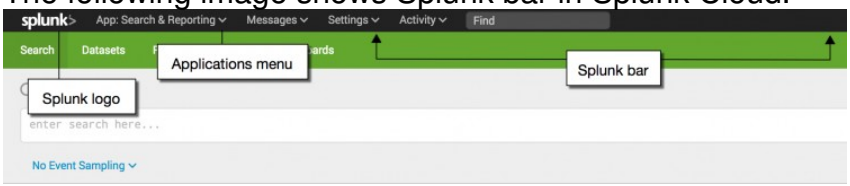
Splunk bar

The Splunk bar appears on every page in Splunk Web. You use this bar to switch between apps, configure your Splunk deployment, view system-level messages, and monitor the progress of search jobs.

1. On the Splunk Home page, click **Search & Reporting** in the Apps Panel to open the Search app.
   When you are in an app, the Applications menu displays in the Splunk bar. You can use the Applications menu to switch between apps.

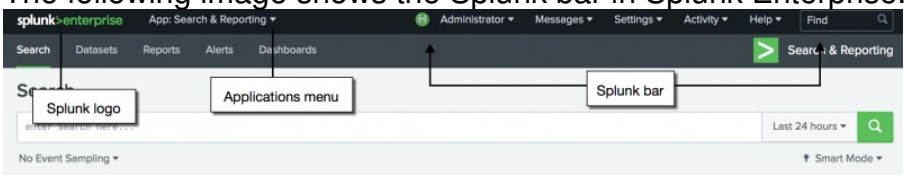
   Splunk Cloud

   The following image shows Splunk bar in Splunk Cloud.

   Splunk Enterprise

   The following image shows the Splunk bar in Splunk Enterprise.

   We will explore the Search app in detail. For now, let's return to Splunk Home.
2. Click the **Splunk** logo on the Splunk bar.
   Regardless of where you are in an app, you can always click the Splunk logo to return to Splunk Home.

Other Splunk bar menus

In addition to the Applications menu, the Splunk bar has several other menus. Let's explore a few of them.

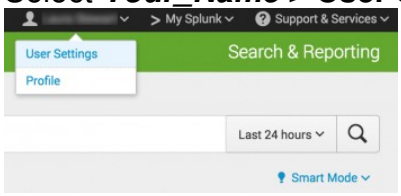
Account menu

Use the Account menu to edit your account settings, set your preferences, and to logout.

Splunk Cloud

The Account menu displays your name.

1. Select ***Your_Name*** **> User Settings**.

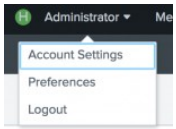


2. The **Full name** field should list your first name and surname.
   You can change the order of the names, or type a nickname. For this tutorial, we will not change the other settings.
3. Click **Save**.
4. Click the Splunk logo to return to Splunk Home.

Splunk Enterprise

The Account menu displays **Administrator** for now, but this menu is your **Account** menu. It shows **Administrator** initially, because that is the default user name for a new installation.

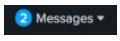
1. Select **Administrator > Account Settings**.



2. In the **Full name** field, type your first name and surname.
   For this tutorial, you will not change the other settings.
3. Click **Save**.
4. Click the Splunk logo to return to Splunk Home.

Messages menu

All system-level error messages are listed on the **Messages** menu. When you have a new message to review, a numerical notification appears next to the **Messages** menu. The notification indicates the number of messages that you have.



Assistance

The menu that you use to get help with the Splunk software depends on the Splunk platform that you are using.

Splunk Cloud
: The **Support & Services** menu contains a set of links to Splunk Answers, the Documentation home page, and the Splunk Support and Services page. You can also search the online documentation.

Splunk Enterprise
: The **Help** menu contains a set of links to the product release notes, tutorials, Splunk Answers, and the Splunk Support and Services page. You can also search the online documentation.

Other menus on the Splunk bar

You will explore the other menus on the Splunk bar later in this tutorial.

Next step

This completes Part 1 of the Search Tutorial.

You are now familiar with Splunk Web. Continue to Part 2: Uploading the tutorial data.

Part 2: Uploading the tutorial data

About uploading data

When you add data to your Splunk deployment, the data is processed and transformed into a series of individual events that you can view, search, and analyze.

What kind of data?

The Splunk platform accepts any type of data. In particular, it works with all IT streaming and historical data. The source of the data can be event logs, web logs, live application logs, network feeds, system metrics, change monitoring, message queues, archive files, and so on.

In general, data sources are grouped into the following categories.

Data source	Description
Files and directories	Most data that you might be interested in comes directly from files and directories.
Network events	The Splunk software can index remote data from any network port and SNMP events from remote devices.
Windows sources	The Windows version of Splunk software accepts a wide range of Windows-specific inputs, including Windows Event Log, Windows Registry, WMI, Active Directory, and Performance monitoring.
Other sources	Other input sources are supported, such as FIFO queues and scripted inputs for getting data from APIs, and other remote data interfaces.

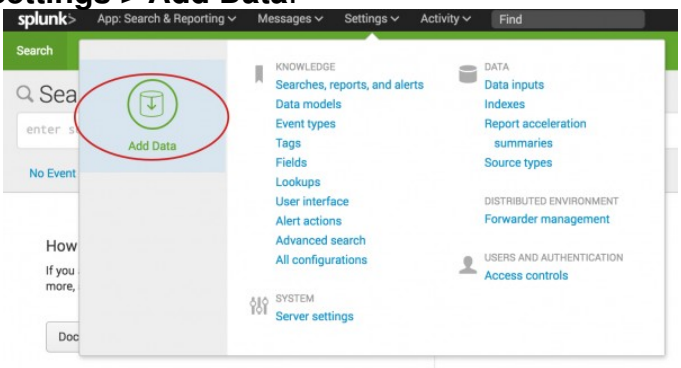
For many types of data, you can add the data directly to your Splunk deployment. If the data that you want to use is not automatically recognized by the Splunk software, you need to provide information about the data before you can add it.

Let's look at some of the data sources that are automatically recognized.

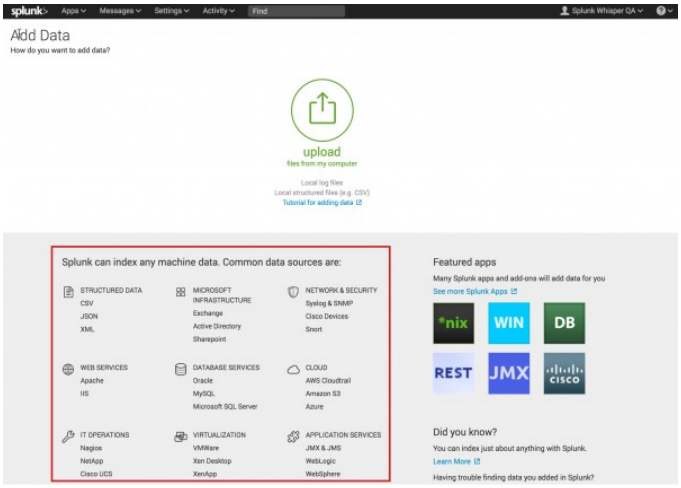
Splunk Cloud

1. If the **Welcome to the Splunk Free Cloud Trial!** window is displayed, close the window.

2. Click **Settings > Add Data**.



3. At the bottom of the screen is a list of common data sources.

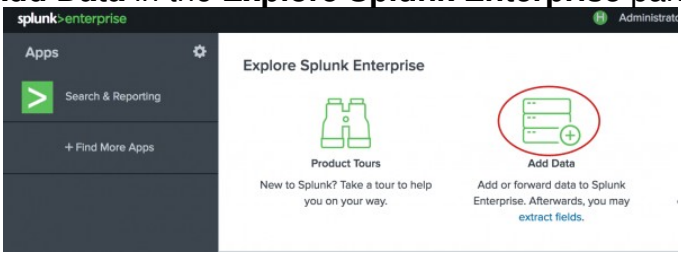


You will come back to this window in a moment.

4. Click the **Splunk** logo to return to Splunk Home.

Splunk Enterprise

1. Click **Add Data** in the **Explore Splunk Enterprise** panel.



2. Scroll down and look at the list of common data sources.

You will come back to this window in a moment.

3. Click the **Splunk** logo to return to Splunk Home.

Where is the data stored?

The process of transforming the data is called **indexing**. During indexing, the incoming data is processed to enable fast searching and analysis. The processed results are stored in the index as **events**.

The index is a flat file repository for the data. For this tutorial, the index resides on the computer where you access your Splunk deployment.

Events are stored in the index as a group of files that fall into two categories:

- Raw data, which is the data that you add to the Splunk deployment. The raw data is stored in a compressed format.
- Index files, which include some metadata files that point to the raw data.

These files reside in sets of directories, called buckets, that are organized by age.

By default, all of your data is put into a single, preconfigured index. There are several other indexes used for internal purposes.

Next step

Now that you are more familiar with data sources and indexes, let's learn about the tutorial data that you will work with.

See also

Where is my data? in *Getting Data In*
Use apps to get data into the index in *Getting Data In*
About managing indexes in *Managing Indexers and Clusters of Indexers*

What is in the tutorial data?

The tutorial data file is updated daily and contains events that are timestamped for the previous seven days. The tutorial data contains several types of information about the fictitious online store Buttercup Games. Buttercup, for those of you that don't know, is a pony and is the Splunk mascot.

The information includes access.log files, secure.log files, and vendor_sales.log files from mail servers and web accounts.

access.log file data

The raw data in the access.log file is difficult to read and analyze when you have hundreds, if not thousands, of lines of data. Each day, every day. That is where the Splunk platform comes in.

```
175.44.24.82 - - [22/Mar/2018:18:44:40] "POST
/product.screen?productId=WC-SH-A01&JSESSIONID=SD7SL9FF5ADFF5066 HTTP
1.1" 200 3067
"http://www.buttercupgames.com/product.screen?productId=WC-SH-A01"
"Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0;
BOIE9;ENUS)" 307
142.233.200.21 - - [22/Mar/2018:19:20:13] "GET
show.do?productId=SF-BVS-01&JSESSIONID=SD6SL8FF4ADFF5218 HTTP 1.1" 404
1329
"http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-13"
"Mozilla/5.0 (compatible; Googlebot/2.1;
+http://www.google.com/bot.html)" 674
```

secure.log file data

The raw data in the secure.log file looks like this:

```
Thu Mar 22 2018 00:15:06 mailsv1 sshd[60445]: pam_unix(sshd:session):
session opened for user djohnson by (uid=0)
Thu Mar 22 2018 00:15:06 mailsv1 sshd[3759]: Failed password for nagios
from 194.8.74.23 port 3769 ssh2
Thu Mar 22 2018 00:15:08 mailsv1 sshd[5276]: Failed password for invalid
user appserver from 194.8.74.23 port 3351
```

vendor_sales.log file data

The raw data in the vendor_sales.log file looks like this:

```
[22/Aug/2017:18:23:07] VendorID=5037 Code=C AcctID=5317605039838520
[22/Aug/2017:18:23:22] VendorID=9108 Code=A AcctID=2194850084423218
[22/Aug/2017:18:23:49] VendorID=1285 Code=F AcctID=8560077531775179
[22/Aug/2017:18:23:59] VendorID=1153 Code=D AcctID=4433276107716482
```

Next step

Let's upload the tutorial data to your Splunk deployment.

Upload the tutorial data

This tutorial uses a set of data that is designed to show you the features in the product. Using the tutorial data ensures that your search results are consistent with the steps in the tutorial.

Prerequisites

- You must have the tutorial data files on your computer.
- The tutorialdata.zip file must remain compressed to upload the file successfully. Some browsers automatically uncompress ZIP files.

  See Download the tutorial data files for more information.

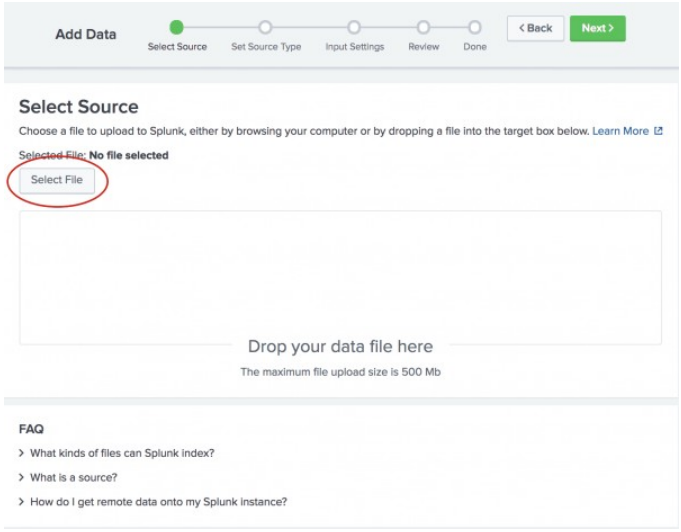
Use the Add Data wizard

1. If you are not on the Splunk Home page, click the **Splunk** logo on the Splunk bar to go to Splunk Home.
2. Locate the **Add Data** icon.

   Splunk Cloud
   a. If the **Welcome to the Splunk Free Cloud Trial!** window is displayed, close the window.
   b. Click **Settings > Add Data**.

   Splunk Enterprise
   a. In the **Explore Splunk Enterprise** panel, click **Add Data**.
3. Click **Upload**. There are other options for adding data, but for this tutorial you will upload the data files.

4. Under **Select Source**, click **Select File** to browse for the file in your download directory.

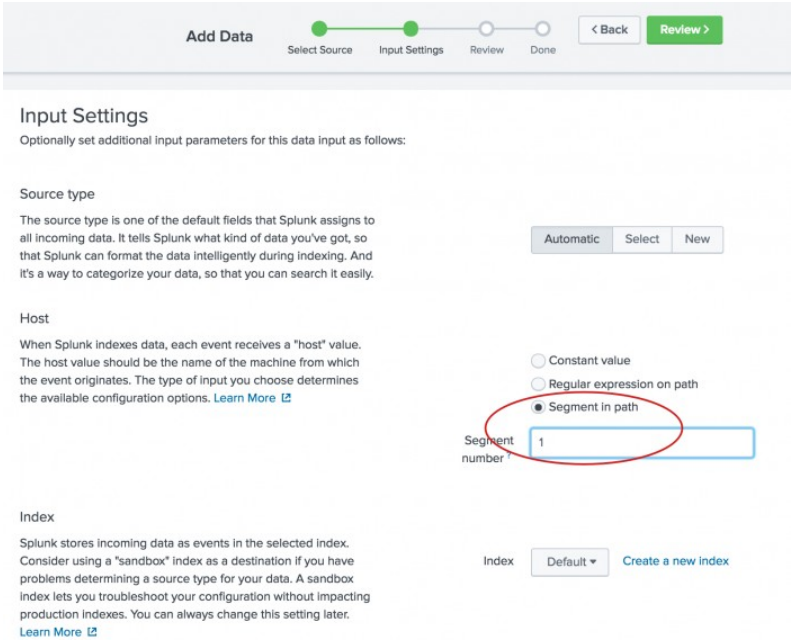


5. Select the `tutorialdata.zip` file and click **Open**.

   Because you specified a compressed file, the steps in the wizard change because the Splunk software recognizes the data source. The **Set Source Type** step is skipped. When you load data that is not in a compressed file, you will set the data source type.
6. Click **Next** to continue to **Input Settings**.
7. Under **Input Settings**, you can override the default settings for Host, Source type, and Index.
   Because this tutorial uses a ZIP file, you are going to modify the **Host** setting to assign the host values by using a portion of the path name for the files included in the ZIP file. The setting that you specify depend whether you are installing on Splunk Cloud or Splunk Enterprise, and on the operating system that you are using.

   Splunk Cloud
   a. Select **Segment in path**.
   b. Type `1` for the segment number.

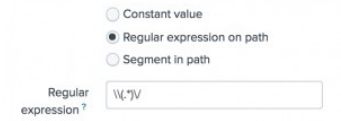
   Splunk Enterprise for Linux or Mac OS X
   a. Select **Segment in path**.
   b. Type `1` for the segment number.



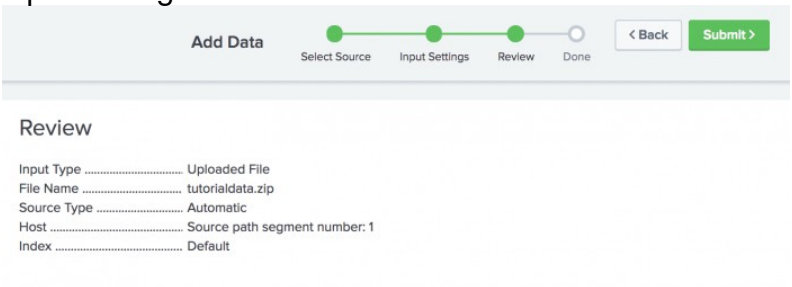
Splunk Enterprise for Windows

a. Select **Regular expression on path**.

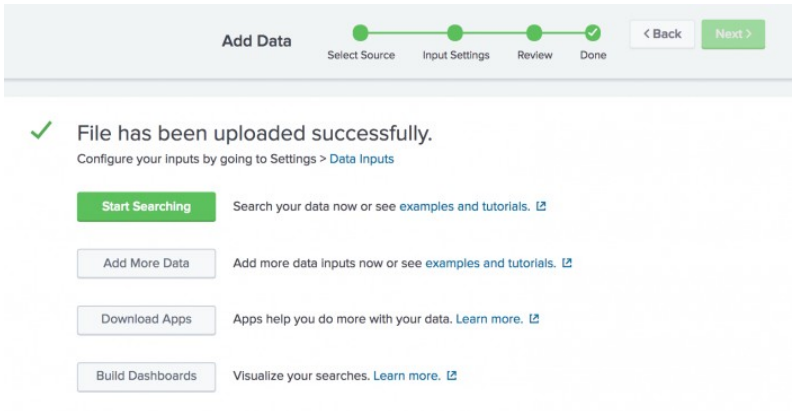
b. Type `\\(.*)\/` for the regex to extract the host values from the path.



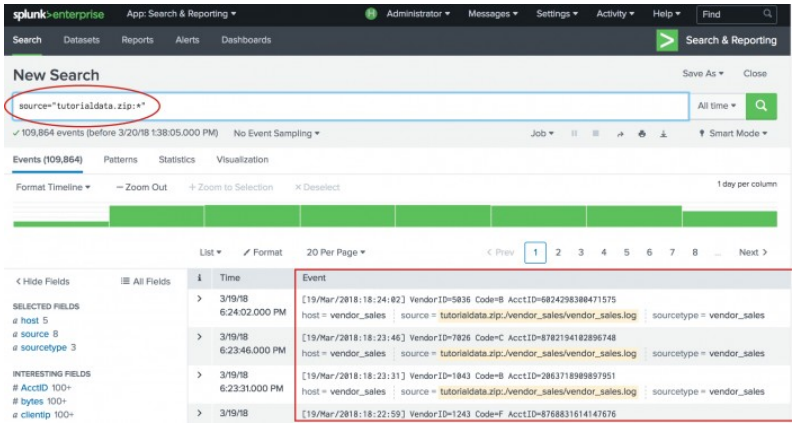
8. Click **Review**. The following screen appears where you can review your input settings.



9. Click **Submit** to add the data.



10. To see the data in the Search app, click **Start Searching**.
    You might see a screen asking if you want to take a tour. You can take the tour or click **Skip**.
    The Search app opens and a search is automatically run on the tutorial data source.



    Success! The results confirm that the data in the `tutorialdata.zip` file was indexed and that events were created.
11. Click the **Splunk** logo to return to Splunk Home.

Next step

You have completed Part 2 of the Search Tutorial.

Now you know how to add data to your Splunk platform. Next, you will begin to learn how to search that data. Continue to Part 3: Using the Splunk Search App.

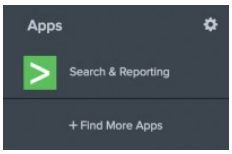
Part 3: Using the Splunk Search App

Exploring the Search views

In Part 2, you learned about the types of data that the Splunk platform works with and uploaded the tutorial data into the index. In Part 3, you will learn about the Search app.

Find Splunk Search

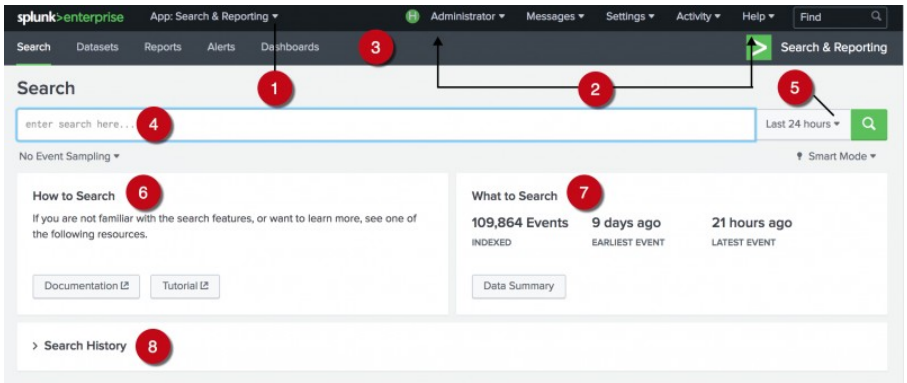
1. If you are not on the Splunk Home page, click the **Splunk** logo on the Splunk bar to go to Splunk Home.
2. From Splunk Home, click **Search & Reporting** in the **Apps** panel.



This opens the Search Summary view in the Search app.

Search Summary view

The Search Summary view includes common elements that you see on other views, including the Applications menu, the Splunk bar, the Apps bar, the Search bar, and the Time Range Picker. Elements that are unique to the Search Summary view are the panels below the Search bar: the **How to Search** panel, the **What to Search** panel, and the **Search History** panel.



Number	Element	Description
1	**Applications menu**	Switch between Splunk applications that you have installed. The current application, Search & Reporting app, is listed. This menu is on the Splunk bar.
2	**Splunk bar**	Edit your Splunk configuration, view system-level messages, and get help on using the product.
3	**Apps bar**	Navigate between the different views in the application you are in. For the Search & Reporting app the views are: Search, Datasets, Reports, Alerts, and Dashboards.
4	**Search bar**	Specify your search criteria.
5	**Time range picker**	Specify the time period for the search, such as the last 30 minutes or yesterday. The default is **Last 24 hours**.
6	**How to search**	Contains links to the *Search Manual' and the*Search Tutorial*.*
7	**What to search**	Shows a summary of the data that is uploaded on to this Splunk instance and that you are authorized to view.
8	**Search history**	View a list of the searches that you have run. The search history appears after you run your first search.

Explore the Data Summary information

Use the Data Summary to view information about your data.

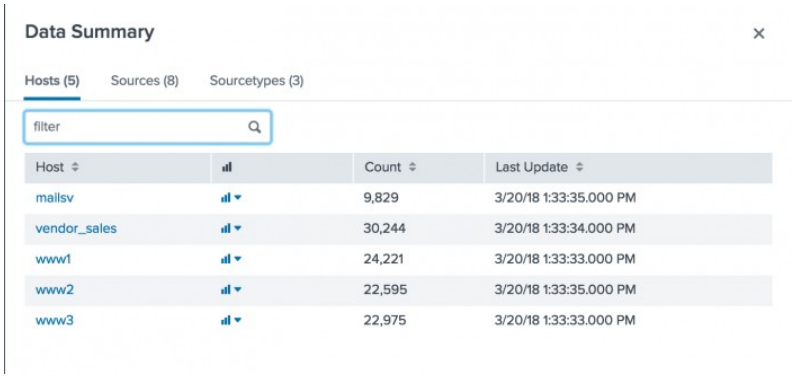
1. In the **What to Search** panel, click **Data Summary**.

   The tabs Hosts, Sources, and Sourcetypes, represent searchable fields in your data. The host, source, and source type fields describe where your data originated.

   The *host* of an event is the host name, IP address, or fully qualified domain name of the network machine from which the event originated. In a distributed environment, you can use the host field to search data from specific machines.

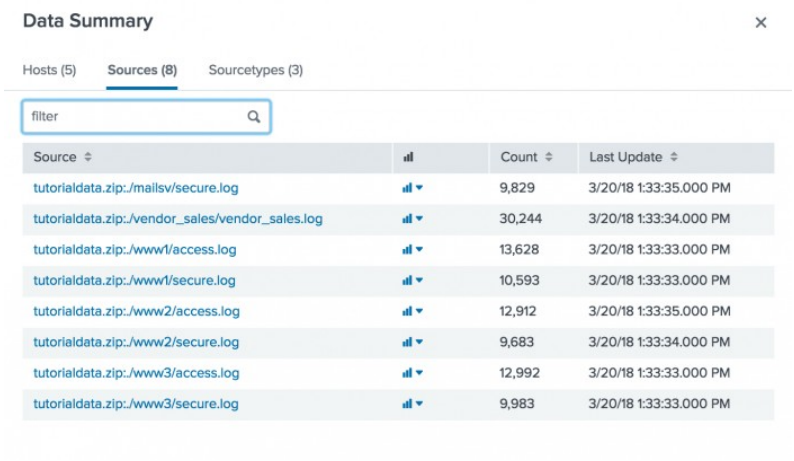
   The **Host** tab lists five hosts. These hosts were identified from the

`tutorialdata.zip` file that you added to your Splunk deployment.



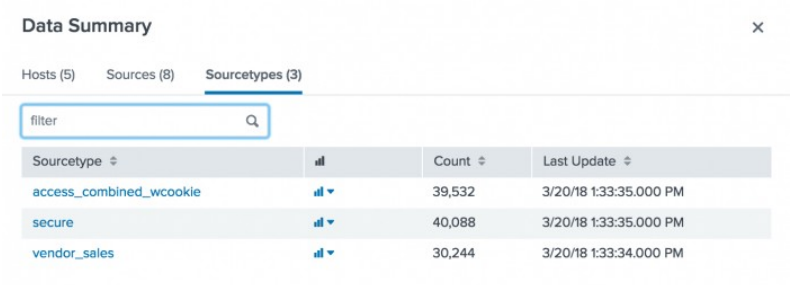
2. Click the **Sources** tab to see the eight sources listed, all of which are log files.

   The **source** of an event is the file or directory path, network port, or script from which the event originated.



3. Click the **Sourcetypes** tab. The three source types that are in the tutorial data file include the following:
   - **access_combined_wcookie**. Apache web server log files.
   - **secure**. Secure server log files.
   - **vendor_sales**. Global sales vendor information.

   The **source type** of an event tells you what kind of data it is, usually based on how the data is formatted. This classification lets you search for the same type of data across multiple sources and hosts.



Let's explore some of the data.

4. Click the **Sources** tab.
5. Click **tutorialdata.zip:./www1/access.log**.

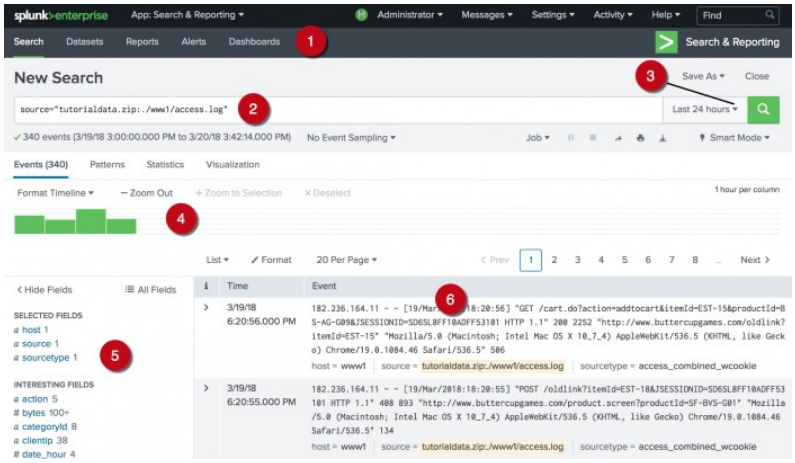
   A new search runs. The events that match the search appear in the lower portion of the screen.

   If no data is returned, expand the time range to **Last 7 days** and run the search again.

New Search view

The New Search view opens after you run a search.

Some of the elements in this view might be familiar, such as the Apps bar, the Search bar, and the time range picker. Below the Search bar, are the Timeline, the Fields sidebar, and the Events view.



Number	Element	Description
1	**Apps bar**	Navigate between the different views in the Search & Reporting app.
2		Specify your search criteria.

	Search bar	
3	**Time range picker**	Specify the time period for the search.
4	**Timeline**	A visual representation of the number of events that occur at each point in time. Peaks or valleys in the timeline can indicate spikes in activity or server downtime. The timeline options are located above the timeline. You can format the timescale, zoom out, or zoom to a selected set of events.
5	**Fields sidebar**	Displays a list of the fields discovered in the events. The fields are grouped into **Selected Fields** and **Interesting Fields**.
6	**Events viewer**	Displays the events that match your search. By default, the most recent event is listed first. In each event, the matching search terms are highlighted. To change the event view, use the **List**, **Format**, and **Per Page** options.

Explore the data source types

1. To return to the Search Summary view, click **Search** in the Apps bar.
2. Try a different search. Click **Data Summary** and click the **Sourcetypes** tab.
3. Click **vendor_sales**.

The New Search view opens and the Search bar shows the following search criteria.

```
sourcetype=vendor_sales
```

Selecting a host, source, or source type from the Data Summary dialog box is a great way to see how your data is turned into events. However, the real power of the Splunk software is in searching all of your data, not segmented parts of it.

Next step

Learn about specifying time ranges in your searches.

See also

View and interact with your Search History in the *Search Manual*
Why source types matter in *Getting Data In*

Specifying time ranges

Restricting, or filtering, your search criteria using a time range is the easiest and most effective way to optimize your searches.

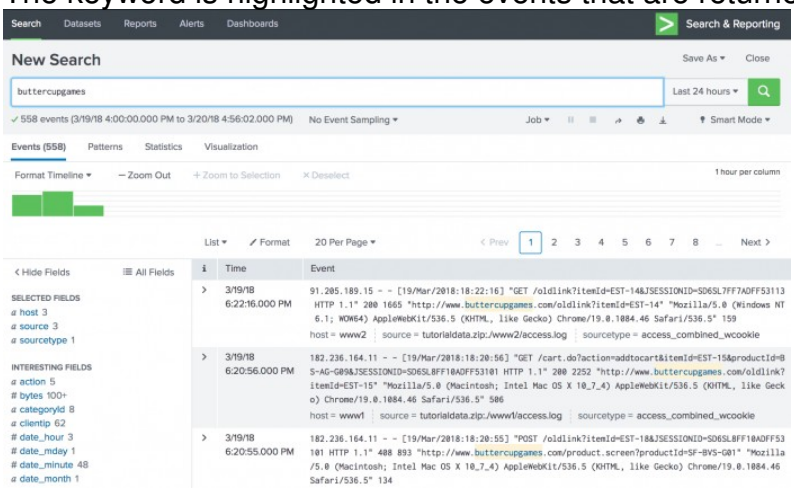
You can use time ranges to troubleshoot an issue, if you know the approximate timeframe when the issue occurred. Narrow the time range of your search to that timeframe. For example, to investigate an incident that occurred sometime in the last hour, you can select **Today**, but a better option is **Last 60 minutes**.

Let's explore the data from the Buttercup Games online store using the different time ranges.

1. To start a new search, click **Search** in the Apps bar.
2. To search for a keyword in your events, type **`buttercupgames`** in the Search bar and press **Enter**.

   ```
   buttercupgames
   ```

   The keyword is highlighted in the events that are returned.



Notice that hundreds of events are returned.

You use the time range picker, which is to the right of the Search bar, to set time boundaries on your searches. The default time range is **Last 24 hours**. You can restrict the search to one of the preset time ranges, or use a custom time range.

Time ranges and the tutorial data

When you run a search using the tutorial data, if no events are returned, it is probably because you downloaded the `tutorialdata.zip` file more than one day ago. When you download the ZIP file, timestamps are generated and added to the data.

The tutorial data for the Buttercup Games store contains events for a seven day period. The dates of the events are based on the date that you downloaded the tutorial data file. For example, if you download the file today, the dates for the events begin the previous week. If today is a Wednesday, the events have a timestamp starting the previous Wednesday. The last events are from yesterday. There are no events from today. Searching for events using **Today** or any time less than the last 24 hours will return no events.

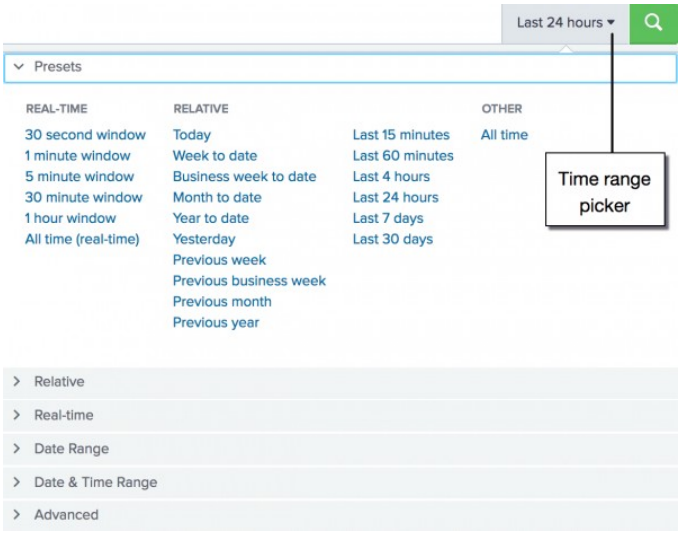
For all of your searches that use the tutorial data files, you need to adjust the search time range based on when you downloaded the tutorial data files. If you downloaded the tutorial data file 3 days ago, there are no events from the last 3 days. Try a different Relative time range, such as **Previous week** or **Last 7 days**.

Preset time ranges

The time range picker has many preset time ranges that you can select from.

1. Click the time range picker to see a list of the time range options.
   The **Presets** option contains **Real-time**, **Relative**, and **Other** time ranges.
   - **Real-time searches** display a live, streaming view of events. You can specify a window over which to retrieve events.
   - **Historical searches** display events from the past. You can restrict your search by specifying a relative time range or a specific date and time range.

   Because the data for the Buttercup Games online store is a snapshot of historical data, you will not use the "'Real-time"' preset time ranges in this tutorial.



2. In the Presets option in the **Relative** list, click **Yesterday**.

   The number of events returned should be larger. You changed the time range from **Last 24 hours** to **Yesterday**.

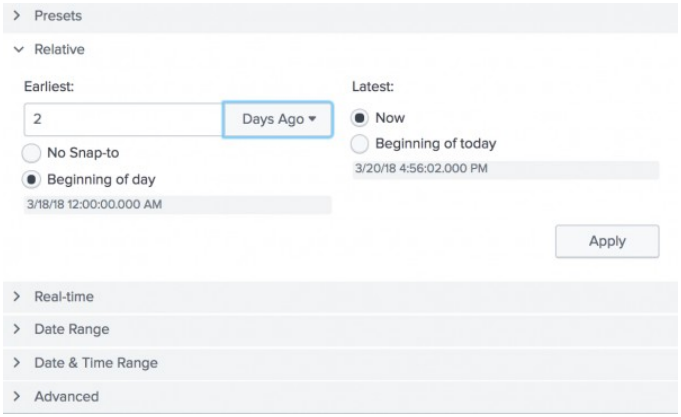
Custom time ranges

Use a custom time range when one of the preset time ranges is not precise enough for your search.

Specify relative time ranges

You can use the **Relative** option to specify a custom time range.

1. Open the time range picker.
2. To run a search over the last two days, select the **Relative** time range option.



3. For **Earliest**, type 2 in the field, and select **Days Ago** from the drop-down

list.

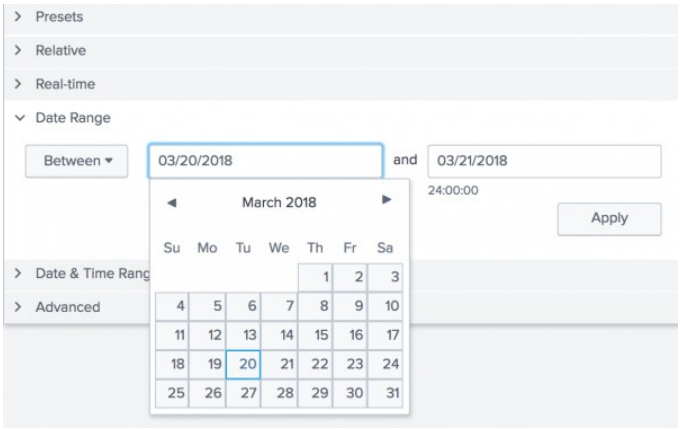
4. For **Latest**, the default is **Now**. Select **Beginning of today**.
5. Click **Apply**.
   The timestamps that appear below the radio buttons adjust based on your selections in the Relative list of time ranges.
   As mentioned before, if no events are returned, select a different time range, such **4 Days Ago** or **1 Week Ago**.

Specify date and time ranges

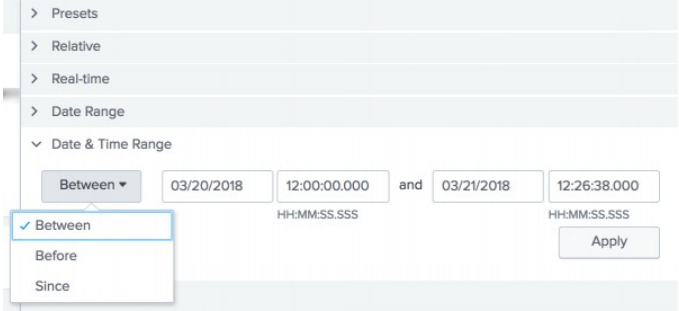
You can also use the **Date Range** and **Date & Time Range** options to specify a custom time range.

- Use **Between** to specify that events must occur between an earliest and latest date.
- Use **Before** to specify that events must occur before a date.
- Use **Since** to specify that events must occur after a date.

You use the **Date Range** option to specify dates. The following screen image shows the calendar that you can use to select a date.



You use the **Date & Time Range** option when you want to specify both a date and a time. The following screen image shows the "Between", "Before", or "Since" options.



For example, to troubleshoot an issue that took place March 20, 2018 at 10:02 AM, specify the earliest time of 03/20/2018 10:00:00.000 and the latest time of 03/20/2018 10:05:00.000 to show the events immediately before and after the issue took place.

Next step

This completes Part 3 of the Search Tutorial.

You have explored the Search app views and learned how important it is to specify time ranges with your searches. Continue to Part 4: Searching the tutorial data.

See also

Change the default time range in the *Search Manual*

Part 4: Searching the tutorial data

Basic searches and search results

In this section, you create searches that retrieve events from the index.

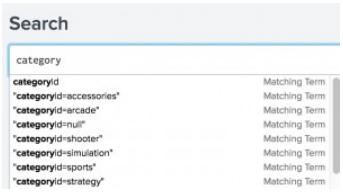
The data for this tutorial is for the Buttercup Games online store. The store sells games and other related items, such as t-shirts. In this tutorial, you will primarily search the Apache web access logs, and correlate the access logs with the vendor sales logs.

Prerequisite
Complete the steps, Upload the tutorial data, in Part 2.

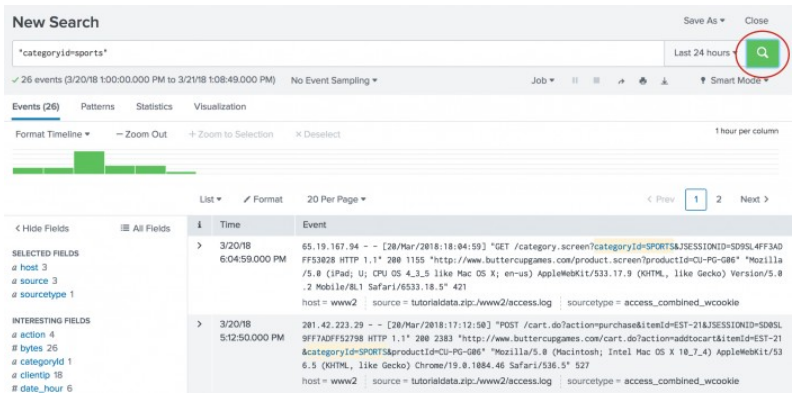
Using the Search Assistant

The Search Assistant is a feature in the Search app that appears as you type your search criteria. The Search Assistant is like autocomplete, but so much more.

1. Click **Search** in the App bar to start a new search.
2. Type `buttercup` in the Search bar.
   When you type a few letters into the Search bar, the Search Assistant shows you terms in your data that match the letters that you type in.
3. Click **Search** in the App bar to start a new search.
4. Type `category` in the Search bar. The terms that you see are in the tutorial data.



5. Select **"categoryid=sports"** from the Search Assistant list.
6. Press **Enter**, or click the **Search icon** on the right side of the Search bar, to run the search.



Matching Searches

The Search Assistant also returns matching searches, which are based on the searches that you have recently run. The Matching Searches list is useful when you want to run the same search from yesterday, or a week ago. Your search history is retained when you log out.

The Search Assistant is more useful after you start learning the search language. When you type search commands, the Search Assistant displays command information.

Retrieve events from the index

Let's try to find out how many errors have occurred on the Buttercup Games website.

To retrieve events that mention errors or failures, you type the keywords in your search criteria. If you use multiple keywords, you must specify Boolean operators such as AND, OR, and NOT.

The AND operator is implied when you type in multiple keywords.

For example, typing **`buttercupgames error`** is the same as typing **`buttercupgames AND error`**.

1. Start a new search.
2. Change the time range to **All time**.
3. To search for the terms error, fail, failure, failed, or severe, in the events that also mention buttercupgames, run the following search.

```
buttercupgames (error OR fail* OR severe)
```

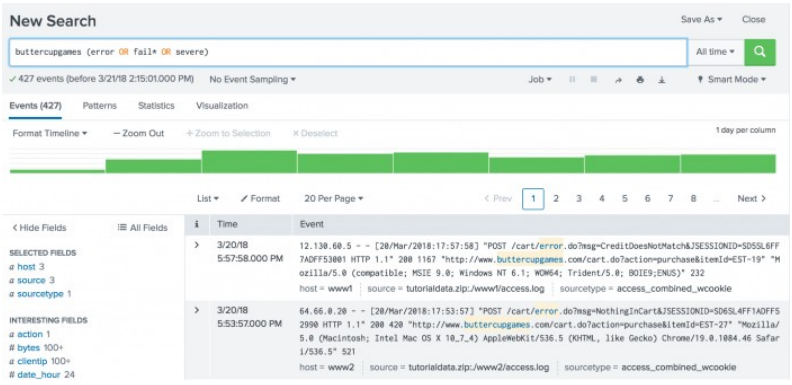
Tip: Instead of typing the search string, you can copy and paste the search from this tutorial directly into the Search bar.

4. Click the Search icon to the right of the time range picker to run the search.

Notice that you must capitalize Boolean operators. The asterisk (*) character is used as a wildcard character to match `fail`, `failure`, `failed`, `failing`, and so forth.

When evaluating Boolean expressions, precedence is given to terms inside parentheses. NOT clauses are evaluated before OR clauses. AND clauses have the lowest precedence.

This search retrieves 427 matching events.

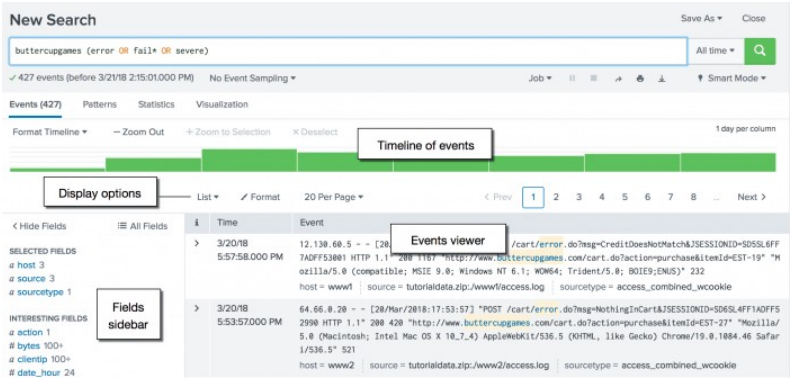


Understanding search results

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. In the early parts of this tutorial, you will work with the **Events** tab. Later in this tutorial, you will learn about the other tabs.

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



By default, the events appear as a list that is ordered starting with the most recent event. In each event, the matching search terms are highlighted. The **List** display option shows the event information in three columns.

Column	Description
i	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.

Change the display of the Events viewer

1. Select the **List** option and click **Table**.
   The display changes to show the event information column, the timestamp column, and columns for each of the **Selected fields**. You will learn more about the Selected fields later in the tutorial.
2. Change the display back to **List**.

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.

Fields sidebar

When you add data to the Splunk platform the data is indexed. 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 sourcetype 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.

Patterns, Statistics, and Visualizations

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. The keyword search for "buttercupgames" does not show results in this tab because the search does not include any transforming commands.

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 in the tutorial.

Next step

Learn to use fields to search your data.

See also

Help building searches using the Search Assistant in the *Search Manual*

Identify event patterns with the Patterns tab in the *Search Manual*

Use fields to search

To take advantage of the advanced search features in the Splunk software, you must understand what fields are and how to use them.

What are fields?

Fields exist in machine data in many forms. Often, a field is a value with a fixed, delimited position on a line, or a name and value pair, where there is a single value to each field name. A field can be multivalued, that is, a field in a single event can have multiple values in a field.

- Some examples of fields are `clientip` for IP addresses accessing your Web server, `_time` for the timestamp of an event, and `host` for domain name of a server.
- One of the more common examples of multivalue fields is email address fields. While the `From` field will contain only a single email address, the `To` and `Cc` fields have one or more email addresses associated with them.

Fields are searchable name and value pairings that distinguish one event from another. Not all events have the same fields and field values. Use fields to write more tailored searches to retrieve the specific events that you want.

Extracted fields

The Splunk software extracts fields from event data at index time and at search time.

Index time
: The time span from when the Splunk software receives new data to when the data is written to an index. During index time, the data is parsed into segments and events. Default fields and timestamps are extracted, and transforms are applied.

Search time
: The period of time beginning when a search is launched and ending when the search finishes. During search time, certain types of event processing take place, such as search time field extraction, field aliasing, source type renaming, event type matching, and so on.

The default fields and other indexed fields are extracted for each event when your data is indexed.

Search with fields

When you search for fields, you use the syntax `field_name=field_value`.

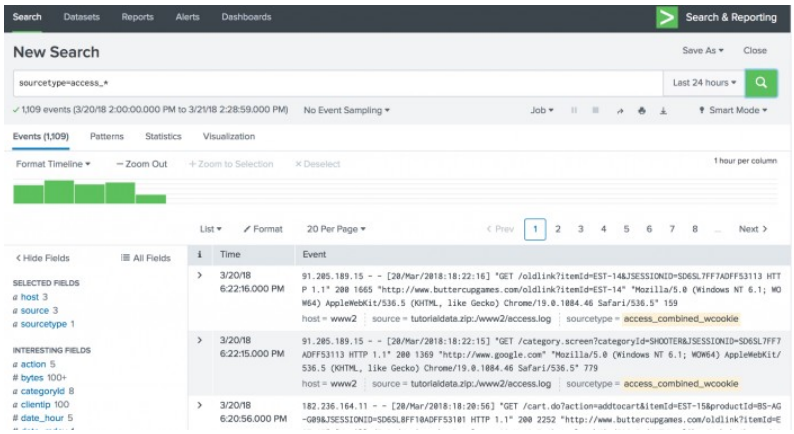
- Field names are case sensitive, but field values are not.
- You can use wildcards in field values.
- Quotation marks are required when the field values include spaces.

1. Click **Search** in the App bar to start a new search. Notice that the time range is set back to the default "Last 24 hours".
2. To search the **sourcetype** field for any values that begin with **access_**, run the following search.

   ```
   sourcetype=access_*
   ```

   This search indicates that you want to retrieve only events from your web access logs and nothing else.

   This search uses a wildcard character, `access_*`, in the field value to match any Apache web access `sourcetype`. The source types can be access_common, access_combined, or access_combined_wcookie.

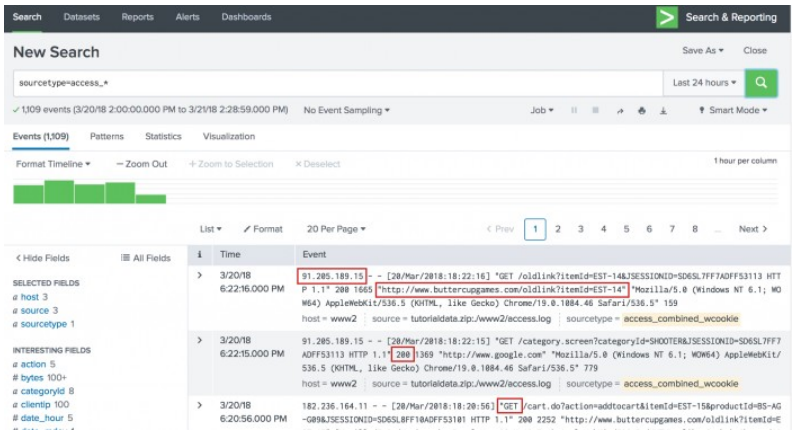


3. Scroll through the list of events in your search results.

If you are familiar with the access_combined format of Apache logs, you might recognize some of the information in each event, such as:

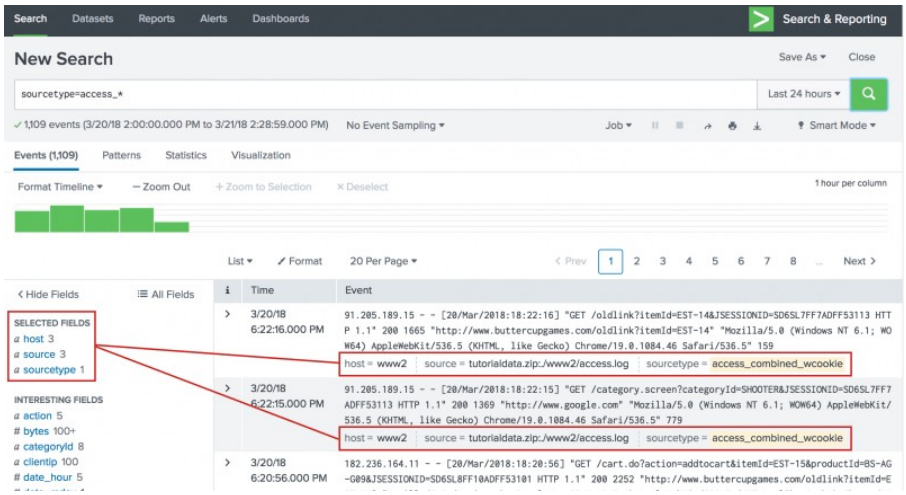
- IP addresses for the users accessing the website.
- URIs and URLs for the pages requested and referring pages.

- HTTP status codes for each page request.
- GET or POST page request methods.



These are events for the Buttercup Games online store, so you might recognize other information and keywords in the search results, such as Arcade, Simulation, productId, categoryId, purchase, addtocart, and so on.

To the left of the events list is the Fields sidebar. As events are retrieved that match your search, the Fields sidebar updates the **Selected Fields** and **Interesting Fields** lists. These are the fields that the Splunk software extracts from your data.



When you first run a search the **Selected Fields** list contains the default fields host, source, and sourcetype. The default fields appear in every event.

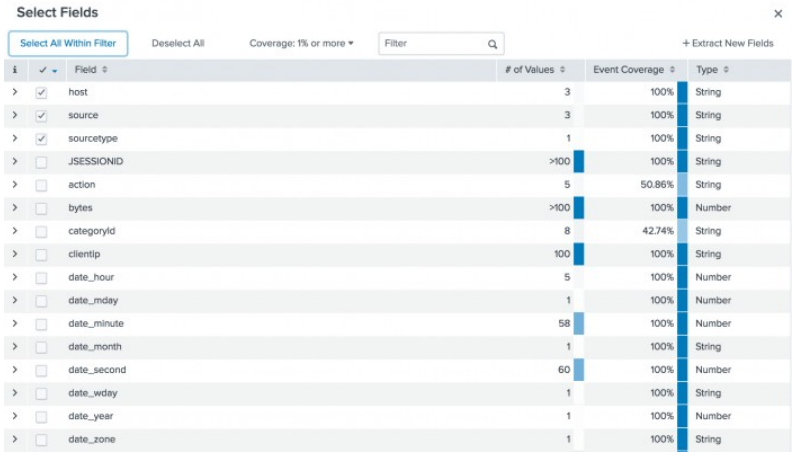
Interesting Fields are fields that appear in at least 20% of the events.

Specify additional selected fields

You can designate other fields to appear in the **Selected Fields** list. When you add a field to the **Selected Fields** list, the field name and field value are included in the search results.

1. To add fields to the **Selected Fields** list, click **All Fields** at the top of the Fields sidebar.

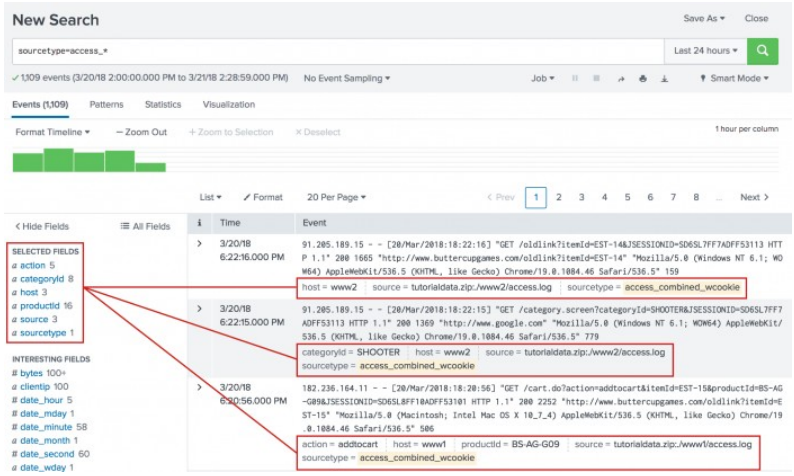
   The Select Fields dialog box shows a list of fields in your events. The **# of Values** column shows the number of unique values for each field in the events. Because your search criteria specifies the source type, the **sourcetype** field has just 1 value.



   The list contains additional default fields, fields that are unique to the source type, and fields that are related to the Buttercup Games online store.

   - In addition to the three default fields that appear automatically in the list of Selected Fields, there are other default fields that are created when your data is indexed. For example, fields that are based on the event `timestamp` begin with `date_*`). The field that identifies data that contains punctuation is the `punct` field. The field that specifies the location of the data in your Splunk deployment is the `index` field.
   - Other field names apply to the web access logs that you are searching. For example, the `clientip`, `method`, and `status` fields. These are not default fields. They are extracted at search time.
   - Other extracted fields are related to the Buttercup Games online store. For example, `action`, `categoryId`, and `productId`.
2. Select the `action`, `categoryId`, and `productId` fields.
3. Close the Select Fields dialog box.

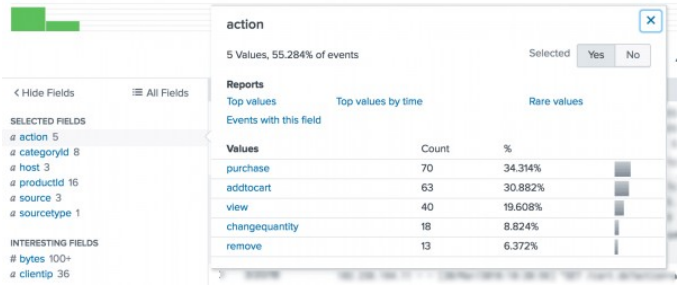
The three fields that you selected appear under **Selected Fields** in the Fields sidebar. The selected fields also appear in the events in your search results, if those fields exist in that particular event. Every event might not have all of the selected fields, as shown in the following image.



Identifying field values

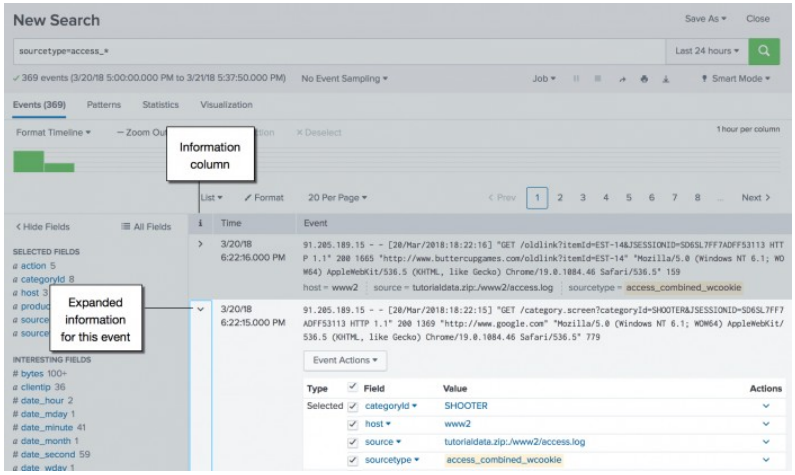
The Fields sidebar displays the number of unique values for each field in the events. These are the same numbers that appear in the Select Fields dialog box.

1. Under **Selected Fields**, notice the number 5 next to the `action` field.
2. Click the `action` field.
   The field summary for the action field opens.



   In this set of search results there are five values for `action`. The `action` field appears in over 50% of your search results.
3. Close the action field summary window.
4. Review the other two fields you added to the Selected fields. The `categoryId` field identifies the types of games or other products that are sold by the Buttercup Games online store. The `productId` field contains the catalog numbers for each product.
5. Scroll through the events list.

6. The *i* column contains event information. In the *i* column, click the arrow (>) next to an event to expand the event information.



You can use this expanded panel to view all the fields in a particular event, and select or deselect individual fields for an individual event.

Run targeted searches

The following examples are searches that use fields.

Search for purchases

Search for successful purchases from the Buttercup Games store.

1. Start a new search.
2. In the time range picker, select **Yesterday** from the Presets list.
3. Run the following search.

   ```
   sourcetype=access_* status=200 action=purchase
   ```

   This search uses the HTTP status field, `status`, to specify successful requests and the `action` field to search only for purchase events.

   You can also search for failed purchases in a similar manner using `status!=200`, which looks for all events where the HTTP status code is not equal to 200.
4. Change the `status` portion of the search to `status!=200` and run the search again.

   ```
   sourcetype=access_* status!=200 action=purchase
   ```

Search for errors

The way that errors are designed in events varies from source to source. To search for errors, your search must specify these different designations.

Use Boolean operators to specify different error criteria. Use parenthesis to group parts of your search string.

1. Start a new search.
2. Change the time range to **All time**.
3. Run the following search.

   ```
   (error OR fail* OR severe) OR (status=404 OR status=500 OR
   status=503)
   ```
4. Click on **sourcetype** in the Selected Fields list.
   This search does not specify a source type. The search retrieves events from both the secure log files and the web access log files.

Search for sales of a specific product

Search for how many simulation style games were bought yesterday.

1. Change the time range to **Yesterday**.

   If you downloaded the `tutorialdata.zip` file more than one day ago, there are no events that have a timestamp for yesterday. Instead, change the time range picker to **All time** and run the previous search. In the search results, look at the dates. Use the **Date Range** option in the time range picker to specify one of the dates in your results.
2. Run the following search.

   ```
   sourcetype=access_* status=200 action=purchase
   categoryId=simulation
   ```

   As you type the search, the Search Assistant shows you a list of your previous searches that start with "sourcetype". You can select the search that you ran earlier to search for successful purchases. Then add `categoryId=simulation` to the end of that search.

   The count of events returned are the number of simulation games purchased.
3. Find the number of purchases for each type of product sold on the Buttercup Games online store.

    1. Remove `categoryId=simulation` from your search criteria and run the search again.
    2. Locate the unique categoryId values by clicking on the **categoryId** field in the **Selected Fields** list.
    3. Click on a categoryId name, such as ACCESSORIES. The categoryId is added to your search and the search is automatically run again. The results show the number of purchases for that product.
4. For the number of purchases made each day of the previous week, run the search again for each time range.

Next step

You can use your knowledge about fields to take advantage of the Splunk search processing language to generate statistics and build charts.

Let's learn how to use the search language.

See also

In the *Knowledge Manager Manual*

About fields
Use default fields
When Splunk Enterprise extracts fields

Use the search language

The searches that you have run to this point have retrieved events from your Splunk index. You were limited to asking questions that could only be answered by the number of events returned.

For example, you ran the following search to determine how many simulation games were purchased:

```
sourcetype=access_* status=200 action=purchase categoryId=simulation
```

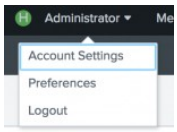
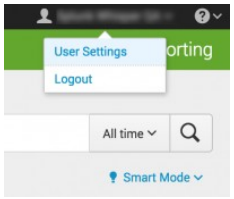
To find this number for the days of the previous week, you need to run it against the data for each day of that week. To see which products are more popular than the other, run the search for each of the eight `categoryId` values and compare the results.

Splunk developed the Search Processing Language (SPL) to use with Splunk software. SPL encompasses all the search commands and their functions, arguments, and clauses. One way to learn the SPL language is by using the Search Assistant.

Learn with the Search Assistant

There are two modes for the Search Assistant: Compact and Full. The default mode is Compact, which you were introduced to in the Basic searches and search results topic in this tutorial.

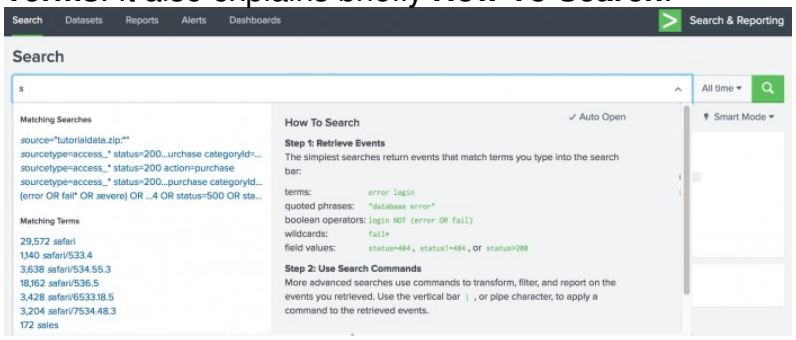
This section shows you how to change the Search Assistant mode. You will use the Search Assistant to learn about the SPL and to construct searches. If you have a Splunk Free license, you will not be able to change the Search Assistant mode. See Choose a platform to learn about difference between the Splunk Trial and Splunk Free licenses.

Splunk platform	Step	Example
Splunk Enterprise	1. Select **Administrator > Preferences**. 2. Click **SPL Editor**. 3. On the **General** tab next to Search assistant, click **Full**. The default setting is Compact. You can tell which mode is set by the dark gray background on the mode. The Full mode provides more information as you type commands in the Search bar. 4. Click **Apply**.	
Splunk Cloud	1. Select ***Your_Name*** **> User Settings**. 2. Scroll down to the **Search** section and change the Search assistant to **Full**. The Full mode provides more information as you type commands in the Search bar. 3. Click **Save**.	

Let's explore the benefits of the Full mode and creating searches using the SPL commands.

1. Click **Search** in the App bar to start a new search.
2. Change the time range to **All time**.

3. Type the letter **s** in the Search bar.
   The Search Assistant shows a list of **Matching Searches** and **Matching Terms**. It also explains briefly **How To Search**.

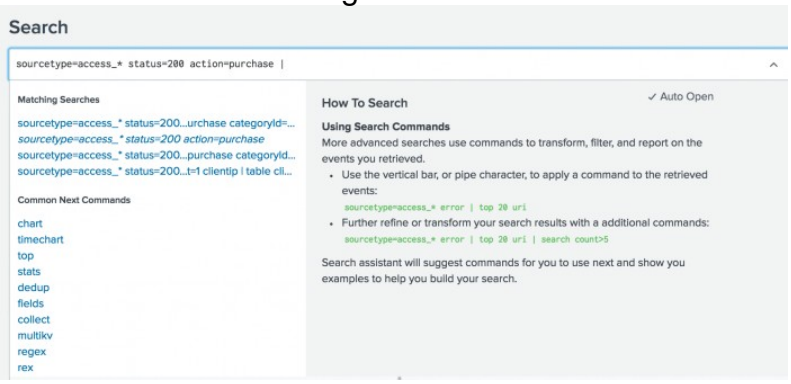


4. Select the following search from the **Matching Searches** list, or type the search into the Search bar.

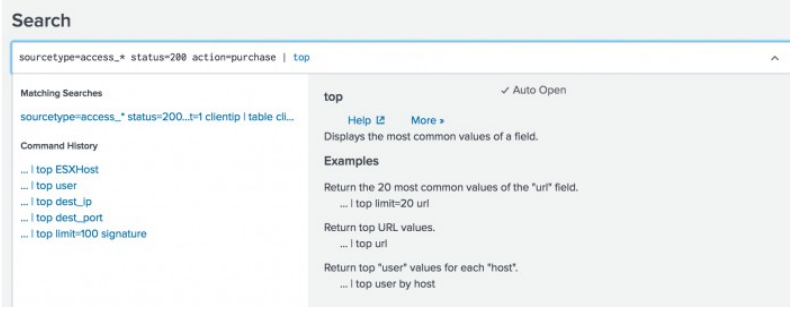
   ```
   sourcetype=access_* status=200 action=purchase
   ```

5. After **action=purchase**, type a pipe character (|) into the Search bar.
   The pipe character indicates that you are about to use a command. The results of the search to the left of the pipe are used as the input to the command to the right of the pipe. You can pass the results of one command into another command in a series, or **pipeline**, of search commands.

   Notice that the Search Assistant changes to show a list of **Common Next Commands**.



   You want the search to return the most popular items bought at the Buttercup Games online store.
6. Under **Common Next Commands**, select **top**.
   The `top` command is appended to your search string.



7. Type **`categoryId`** into the Search bar.
   The following search is the complete search string.

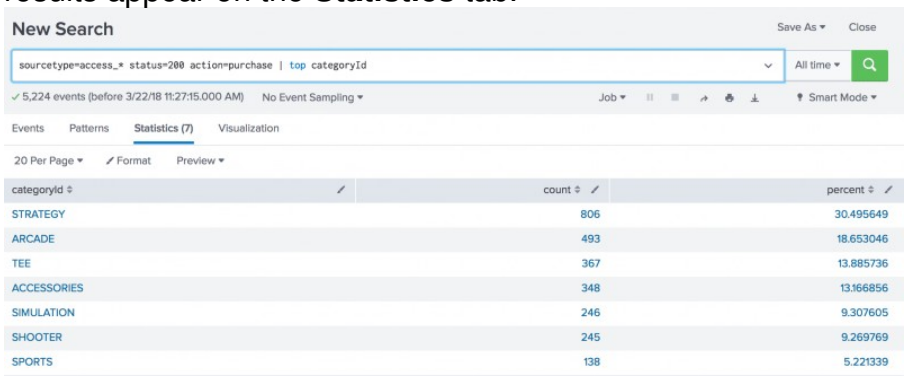
   ```
   sourcetype=access_* status=200 action=purchase | top categoryId
   ```

   - The search criteria before the pipe character, `sourcetype=access_* status=200 action=purchase`, locates events from the access control log files, that were successful (HTTP status is 200), and that were a purchase of a product.
   - The search criteria after the pipe character, `top categoryId`, takes the events located and returns the `categoryId` field for the most common values.
8. Run the search.
   The results of the `top` command appear in the **Statistics** tab.

View results in the Statistics tab

The `top` command is a **transforming command**. Transforming commands organize the search results into a table. Use transforming commands to generate results that you can use to create visualizations such as column, line, area, and pie charts. You will learn more about visualizations later in this tutorial.

Because transforming commands return your search results in a table format, the results appear on the **Statistics** tab.



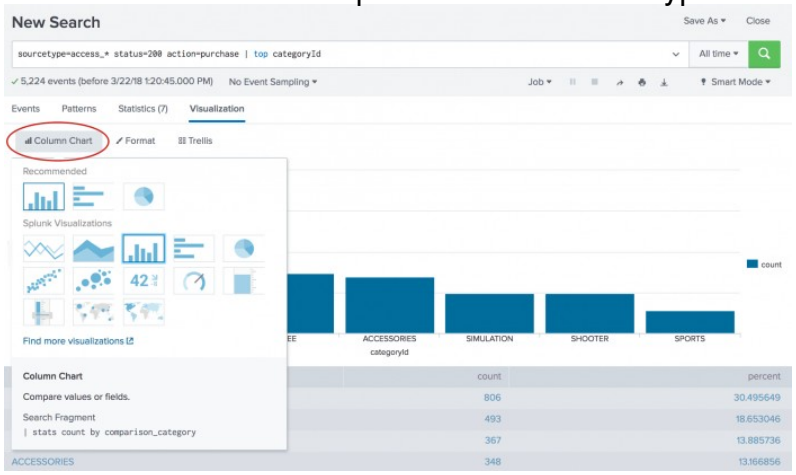
In this search for successful purchases, seven different category IDs were found. The list shows the category ID values from highest to lowest, based on the frequency of the category ID values in the events.

Many of the transforming commands return additional fields that contain useful statistical information. The `top` command returns two new fields, `count` and `percent`.

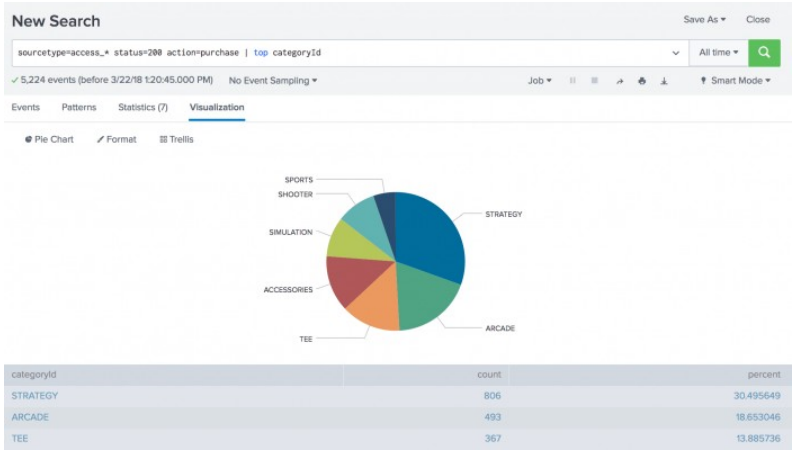
- The `count` field specifies the number of times each value of the `categoryId` field occurs in the search results.
- The `percent` field specifies how large the count is compared to the total count.

View and format results on the Visualization tab

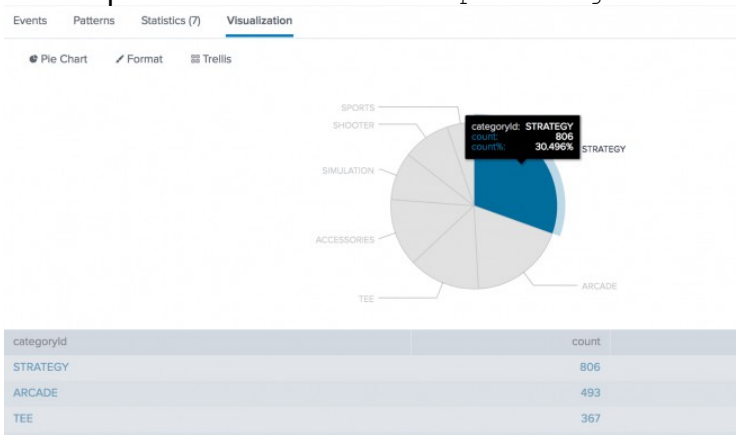
You can also view the results of transforming searches on the **Visualization** tab, where you can format the chart type.

1. Click the **Visualization** tab.
   By default, the **Visualization** tab opens with a Column chart.
2. Click **Column Chart** to open the visualization type selector.
   

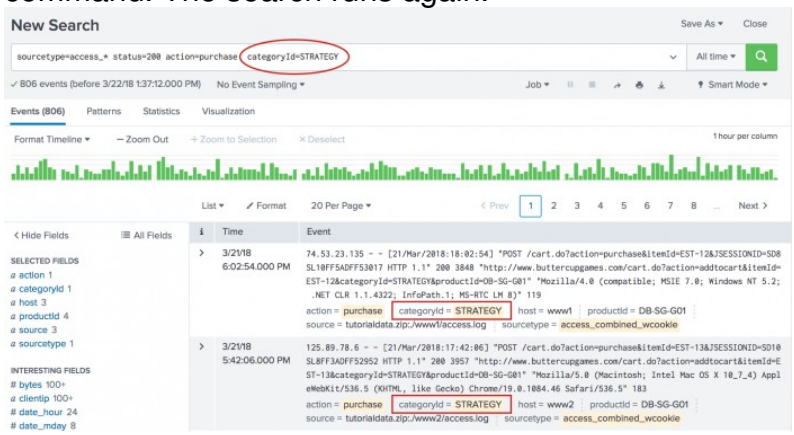
   Column, Bar, and Pie charts are listed as the Recommended chart type for this data set.
3. Select the **Pie** chart.
   Now, your visualization looks like the following pie chart.



4. Hover over each slice of the pie to see the `count` and `percentage` values for each `categoryId`.



5. Click on the STRATEGY slice.
`categoryId=STRATEGY` is added to your search string, replacing the `top` command. The search runs again.



Next step

Learn about correlating events with subsearches.

See also

The top command in the *Search Reference*
Use drilldown for dashboard interactivity in the *Dashboards and Visualizations*

Use a subsearch

In this section you will learn how to correlate events by using subsearches.

A subsearch is a search that is used to narrow down the set of events that you search on. The result of the subsearch is then used as an argument to the primary, or outer, search. Subsearches are enclosed in square brackets within a main search and are evaluated first.

Let's find the single most frequent shopper on the Buttercup Games online store, and what that shopper has purchased.

The following examples show why a subsearch is useful. Example 1 shows how to find the most frequent shopper without a subsearch. Example 2 shows how to find the most frequent shopper with a subsearch.

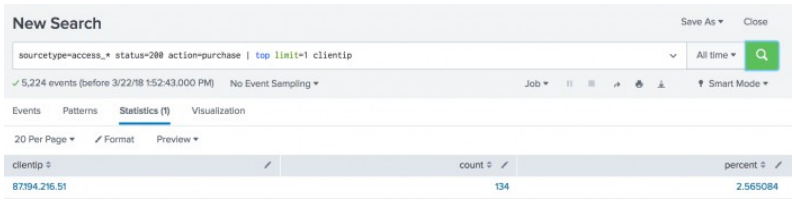
Example 1: Search without a subsearch

You want to find the single most frequent shopper on the Buttercup Games online store and what that shopper has purchased. Use the `top` command to return the most frequent shopper.

1. Start a new search.
2. Change the time range to **All time**.
3. To find the shopper who accessed the online shop the most, use this search.

   ```
   sourcetype=access_* status=200 action=purchase | top limit=1
   clientip
   ```

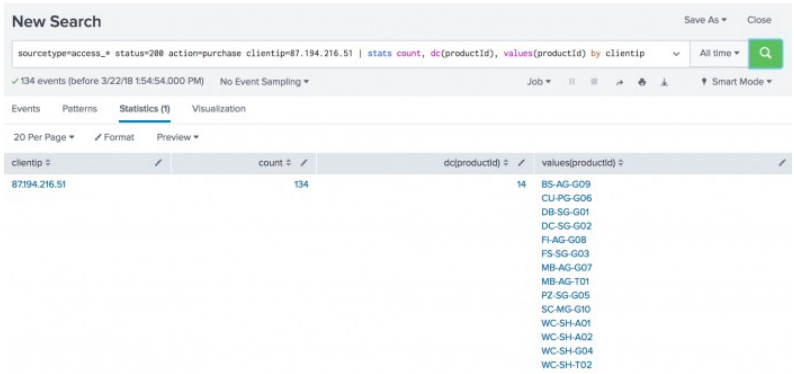
   The `limit=1` argument specifies to return 1 value. The `clientip` argument specifies the field to return.



This search returns one `clientip` value, 87.194.216.51, which you will use to identify the VIP shopper.

4. You now need to run another search to determine how many different products the VIP shopper has purchased. Use the `stats` command to count the purchases by this VIP customer.

```
sourcetype=access_* status=200 action=purchase
clientip=87.194.216.51 | stats count, dc(productId),
values(productId) by clientip
```



This search uses the `count()` function to return the total count of the purchases for the VIP shopper. The `dc()` function is the distinct_count function. Use this function to count the number of different, or unique, products that the shopper bought. The `values` function is used to display the distinct product IDs as a multivalue field.

The drawback to this approach is that you have to run two searches each time you want to build this table. The top purchaser is not likely to be the same person at any given time range.

Example 2: Search with a subsearch

Let's start with our first requirement, to identify the single most frequent shopper on the Buttercup Games online store.

1. Copy and paste the following search into the Search bar and run the search. Make sure the time range is **All time**.

```
sourcetype=access_* status=200 action=purchase | top limit=1
clientip | table clientip
```

This search returns the clientip for the most frequent shopper, `clientip=87.194.216.51`. This search is almost identical to the search in Example 1 Step 1. The difference is the last piped command, `| table clientip`, which displays the clientip information in a table.

To find what this shopper has purchased, you run a search on the same data. You provide the result of the most frequent shopper search as one of the criteria for the purchases search.

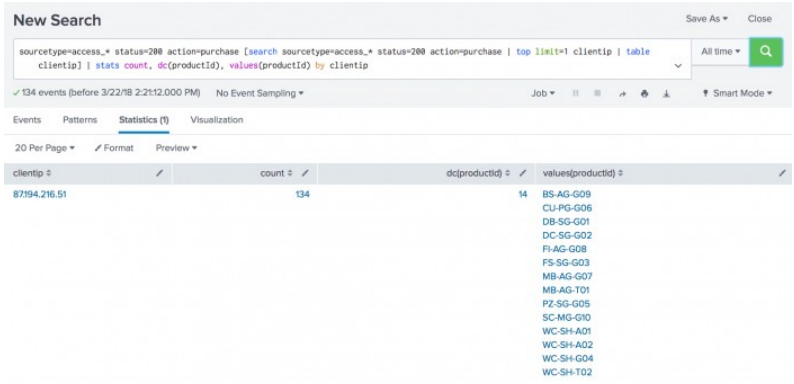
The most frequent shopper search becomes the **subsearch** for the purchases search. The purchases search is referred to as the **outer** or primary search. Because you are searching the same data, the beginning of the outer search is identical to the beginning of the subsearch.

A subsearch is enclosed in square brackets [ ] and processed first when the search is parsed.

2. Copy and paste the following search into the Search bar and run the search.

```
sourcetype=access_* status=200 action=purchase [search
sourcetype=access_* status=200 action=purchase | top limit=1
clientip | table clientip] | stats count, dc(productId),
values(productId) by clientip
```

Because the `top` command returns the **count** and **percent** fields, the `table` command is used to keep only the `clientip` value.



These results should match the result of the two searches in Example 1, if you run it on the same time range. If you change the time range, you might see different results because the top purchasing customer will be

different.

The performance of this subsearch depends on how many distinct IP addresses match `status=200 action=purchase`. If there are thousands of distinct IP addresses, the `top` command has to keep track of all of those addresses before the top 1 is returned, impacting performance. By default, subsearches return a maximum of 10,000 results and have a maximum runtime of 60 seconds. In large production environments, it is possible that the subsearch in this example will timeout before it completes. The best option is to rewrite the query to limit the number of events that the subsearch must process. Alternatively, you can increase the maximum results and maximum runtime parameters.

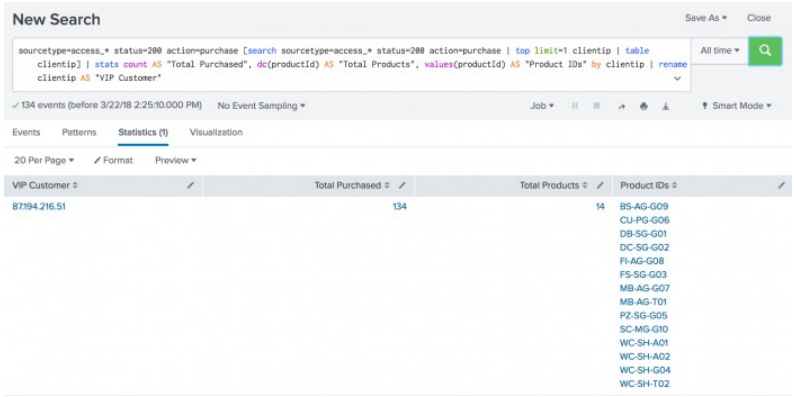
You can make the information more understandable by renaming the columns.

Column	Rename
count	Total Purchased
dc(productId)	Total Products
values(productId)	Product IDs
clientip	VIP Customer

You rename columns by using the AS operator on the fields in your search. If the rename that you want to use contains a space, you must enclose the rename in quotation marks.

3. To rename the fields, copy and paste the following search into the Search bar and run the search.

```
sourcetype=access_* status=200 action=purchase [search
sourcetype=access_* status=200 action=purchase | top limit=1
clientip | table clientip] | stats count AS "Total Purchased",
dc(productId) AS "Total Products", values(productId) AS "Product
IDs" by clientip | rename clientip AS "VIP Customer"
```



4. Experiment with this search. What happens when you run the search over different time periods? What if you wanted to find the top product sold and how many people bought it?

Next step

This completes Part 4 of the Search Tutorial.

You have learned how to use fields, the Splunk search language, and subsearches to search your data. Continue to Part 5: Enriching events with lookups.

See also

About subsearches in the *Search Manual*
The top command in the *Search Reference*
The stats command in the *Search Reference*

Part 5: Enriching events with lookups

Enabling field lookups

The events used in this tutorial data contain fields with the product codes and product IDs. Those codes and IDs do not tell you much about the products themselves, such as the product names. Being able to display the actual product names in reports and dashboards is useful to anyone who reads those reports or dashboards. That is where lookup files come in.

Lookup files contain data that does not change very often. This can include information about customers, products, employees, equipment, and so forth. For this tutorial, you will use a CSV lookup file that contains product IDs, product names, regular prices, sales prices, and product codes.

With a lookup file, you can match the codes or IDs in the Buttercup Games store events with the codes or IDs in a lookup file. This matching is referred to as *field lookups*. After the field lookups are configured, you can add any of the fields from the lookup file to your search. The lookup files are sometimes referred to as *lookup tables* or *lookup table files*.

There are five key steps to enabling fields lookups:

1. Upload the lookup file
2. Share the uploaded file with the applications
3. Create a lookup definition
4. Share the lookup definition
5. Optional. Make the lookup definition automatic

The remaining Parts in this tutorial dependent on you completing the steps in this section.
If you do not configure the field lookup, the searches will not produce the correct results.

Uncompress the lookup file

In Part 1 of this tutorial, you downloaded two data files. One of the files was `Prices.csv.zip`. You will use this file as the lookup file for the remaining sections of the tutorial.

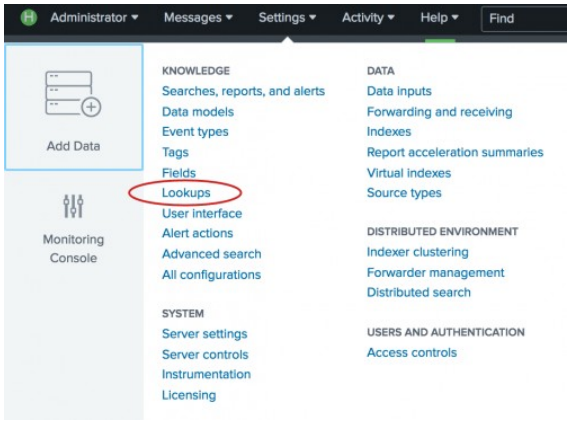
1. Uncompress the `Prices.csv.zip` file. There is only one file in the ZIP file, `prices.csv`.

   The `prices.csv` file contains the product names, price, and code. For example:

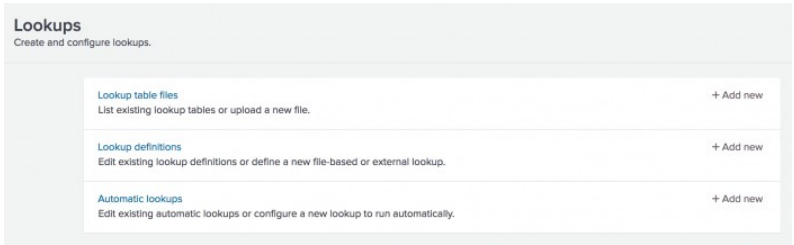
productId	product_name	price	sale_price	Code
DB-SG-G01	Mediocre Kingdoms	24.99	19.99	A
DC-SG-G02	Dream Crusher	39.99	24.99	B
FS-SG-G03	Final Sequel	24.99	16.99	C
WC-SH-G04	World of Cheese	24.99	19.99	D

Find the Lookups manager

1. In the Splunk bar, click **Settings**.
2. In the **Knowledge** section, click **Lookups**.



   The Lookups manager opens, where you can create new lookups or edit existing lookups.



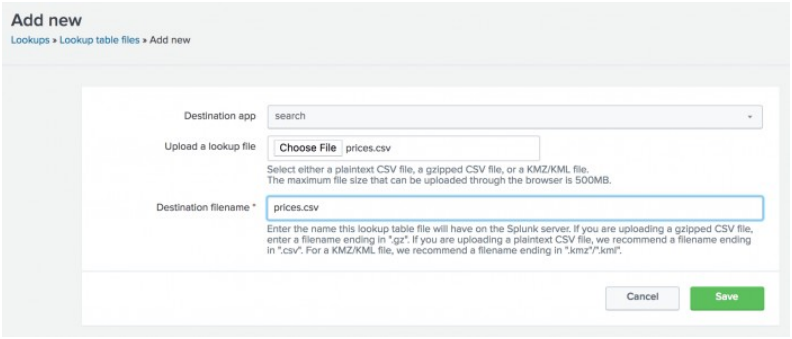
You can view and edit existing lookups by clicking on the links in the Lookups

manager. In the next few sections of this tutorial, you will upload a lookup table file, create a lookup definition, and create an automatic lookup.

Upload the lookup table file

To use a lookup table file, you must upload the file to your Splunk platform.

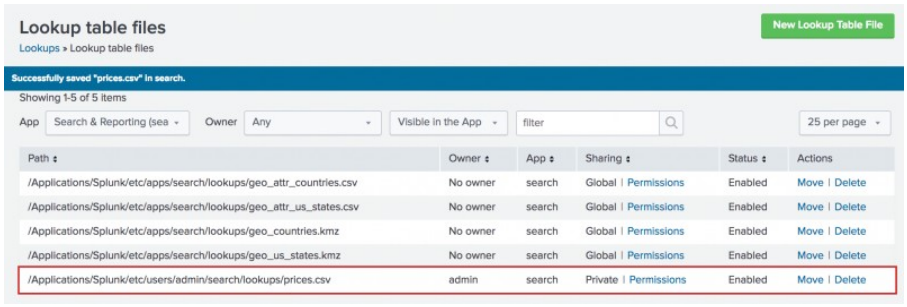
1. In the Lookups manager, locate **Lookup table files** and click **Add new**. You use the **Add new** view to upload the CSV file that you want to as a lookup table.



2. The **Destination app** field specifies which app you want to upload the lookup table file to. To upload the file in the Search app, you do not need to change anything. The default value is **search**.
3. Under **Upload a lookup file**, click **Choose File** and browse for the **prices.csv** file.
4. Under **Destination filename**, type `prices.csv`.
   This is the name that you will use when you create a lookup definition.
5. Click **Save**.
   This uploads your lookup file to the Search app and displays the lookup table files list.

If the Splunk software does not recognize or cannot upload the file, you can take the following actions.

- Check that the file is uncompressed.
- If an error message indicates that the file does not have line breaks, the file has become corrupted. This can happen if the file is opened in Microsoft Excel before it is uploaded. You should delete the `Prices.csv.zip` and `prices.csv` files. Then download the ZIP file again, and uncompress the file.

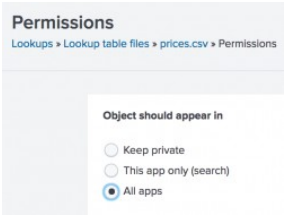


The other lookup table files in the list are included with the Splunk software.

Share the lookup table file

When you upload a lookup table file, the default sharing setting is **Private**. To use the file with other applications or with specific roles, you need to change the permissions to the file. For this tutorial, you are going to share the lookup table file with all applications.

1. In the **Lookup table files** list, locate the `prices.csv` file at the bottom of the **Path** list.
2. In the **Sharing** column, notice that `prices.csv` is listed as **Private**.
3. To share the lookup table file, click **Permissions**.
4. In the Permissions dialog box, under **Object should appear in**, select **All apps**.

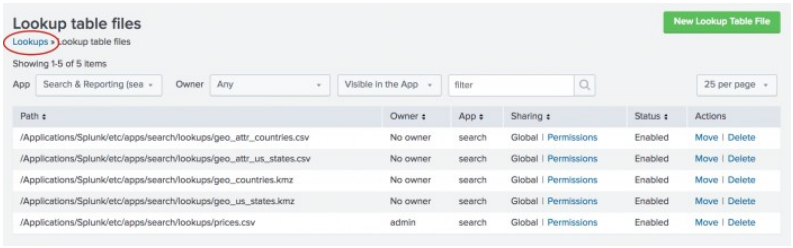


5. Click **Save**.
   The Sharing setting for the prices.csv lookup table is set to **Global**.

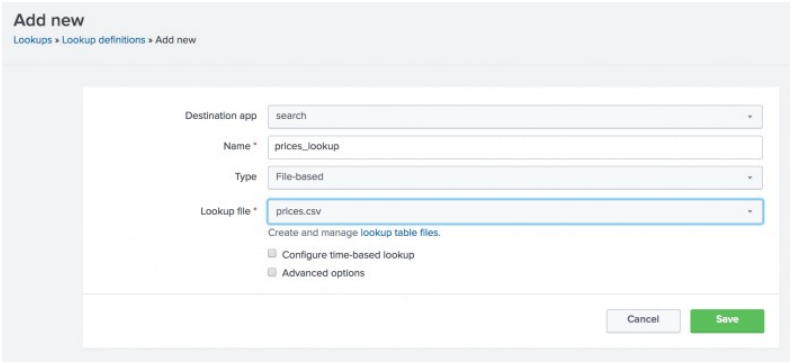
Add the field lookup definition

It is not sufficient to share the lookup table file with an application. You must define the information in the lookup table file and how that information relates to the fields in your events. This is called a **lookup definition**.

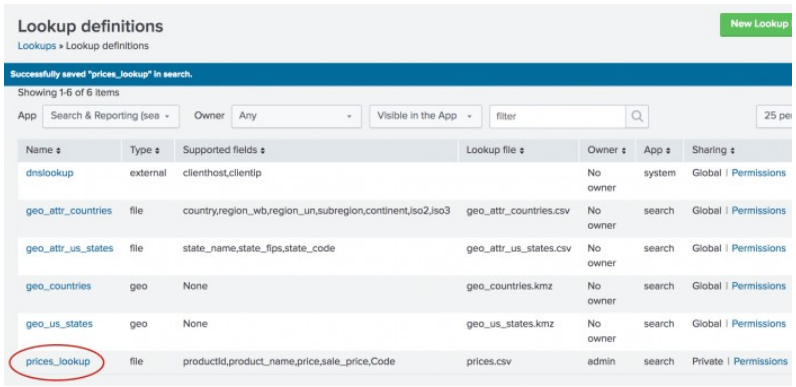
1. In the Lookup table file dialog box, select **Lookups** in the breadcrumbs to return to the Lookups manager.



2. For **Lookup definitions**, click **Add New**.
   The Add new lookups definitions page opens, where you define the field lookup.
3. There is no need to change the **Destination app** setting. It is already set to **search**, referring to the Search app.
4. For **Name**, type `prices_lookup`.
5. For **Type**, select **File-based**.
   A file-based lookup is typically a static table, such as a CSV file.
6. For **Lookup file**, select **prices.csv**, which is the name of the lookup table file that you created.



7. Leave the check boxes for **Configure time-based lookup** and **Advanced options** unchecked.
8. Click **Save**.
   The **prices_lookup** is now defined as a file-based lookup.

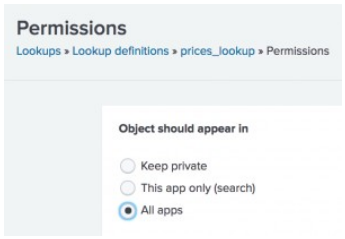


Notice the **Supported fields** column in the Lookup Definitions page. The Splunk software automatically interprets the first row in a CSV lookup table file as the field names, or column headings, for the lookup table.

Share the lookup definition with all apps

Now that you have created the lookup definition, you need to specify in which apps you want to use the lookup table.

1. In the Lookup definitions list, for the prices_lookup, click **Permissions**.
2. In the Permissions dialog box, under **Object should appear in**, select **All apps**.



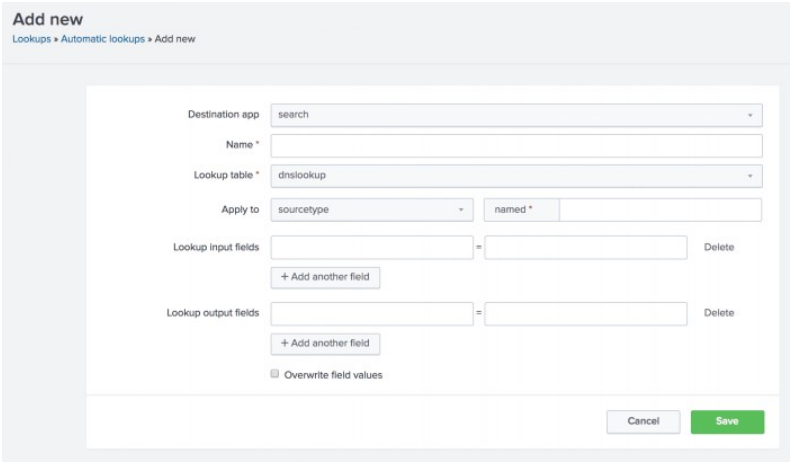
3. Click **Save**.
   In the Lookup definitions page, prices_lookup now has **Global** permissions.

You can use this field lookup to add information from the lookup table file to your events. You use the field lookup by specifying the `lookup` command in a search. Or, you can set the field lookup to run automatically.

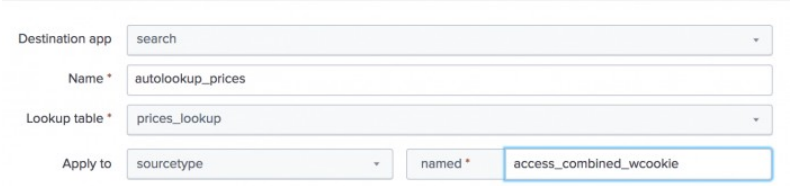
Make the lookup automatic

Instead of using the `lookup` command in your search when you want to apply a field lookup to your events, you can set the lookup to run automatically.

1. In the Lookup table file dialog box, select **Lookups** in the breadcrumbs to return to the Lookups manager.
2. In the Lookups manager, for **Automatic lookups**, click **Add New**.
   This takes you to the Add new automatic lookups view, where you configure the lookup to run automatically.



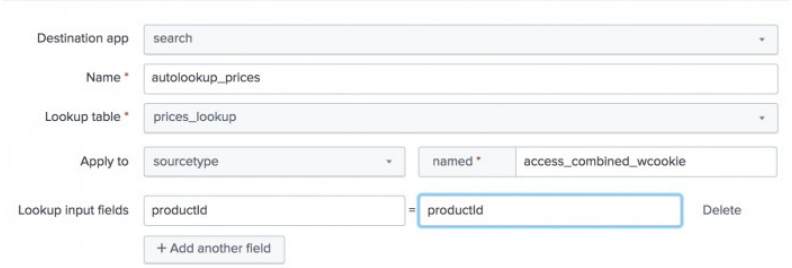
3. There is no need to change the **Destination app** setting. It is already set to **search**, referring to the Search app.
4. For **Name**, type **`autolookup_prices`**.
5. For **Lookup table**, select **prices_lookup**.
   The other options are lookup table files that come with the product.
6. For **Apply to**, the value **sourcetype** is already selected. For **named**, type **`access_combined_wcookie`**.



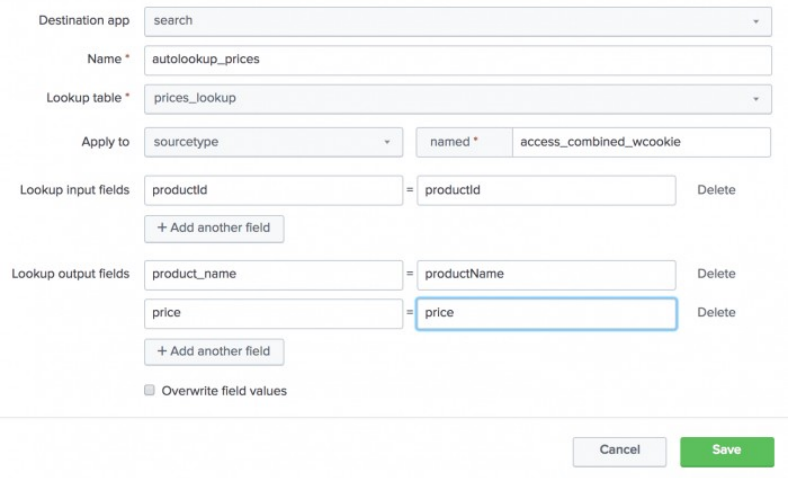
7. For **Lookup input fields**, type **`productId`** in both text boxes.

   The lookup input fields are the fields that the lookup table and the events have in common. The lookup input fields are used to associate, or link, the fields from the lookup table file with fields in your events.
   - The first text box specifies the field name in the lookup table file.
   - The second text box specifies the field name in your events.

   The lookup table file has a **productId** column that contains values that match the values in the **productId** field in the events.

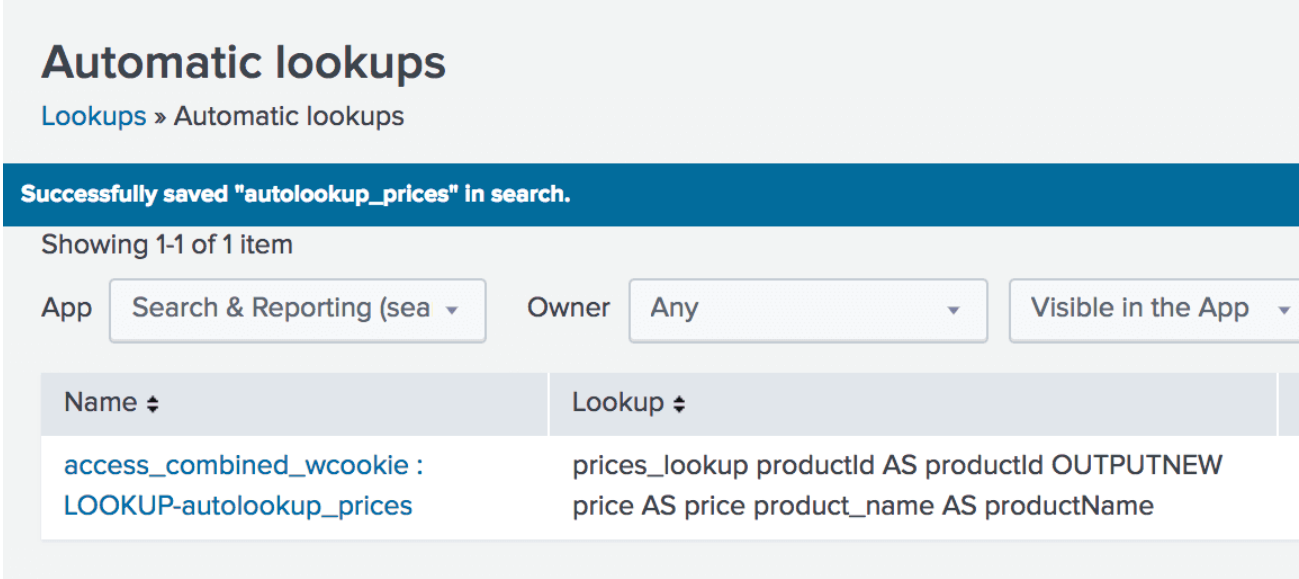


8. For **Lookup output fields**, specify the names of the fields from the lookup table file that you want to add to your event data. You can specify different names.
   The lookup table file has several fields. You will specify two of the fields in the lookup table to appear in your events.
   1. In the first text box, type **`product_name`**. This is the field in the `prices.csv` file that contains the descriptive name for each productId.
   2. In the second text box, after the equal sign, type **`productName`**. This is the name of the field that will appear in your events for the descriptive name of the product.
   3. Click **Add another field** to add another field after the first one.
   4. Type **`price`** in the first text box. This is the field in the `prices.csv` file that contains the price for each productId. Let's use the same name for the field that will appear in your events. Type **`price`** in the second text box.



9. Keep **Overwrite field values** unchecked.
10. Click **Save**.
    The Automatic lookup view appears and the lookup that you configured,

autolookup_prices, is in the list. The full name is **access_combined_wcookie : LOOKUP-autolookup_prices**.



Next step

You have setup the Search app to automatically retrieve information from your lookup table definition.
Now, you will search using those lookup definitions.

Search with field lookups

Now that you have defined the `prices_lookup`, you can see the fields from that lookup in your search results.

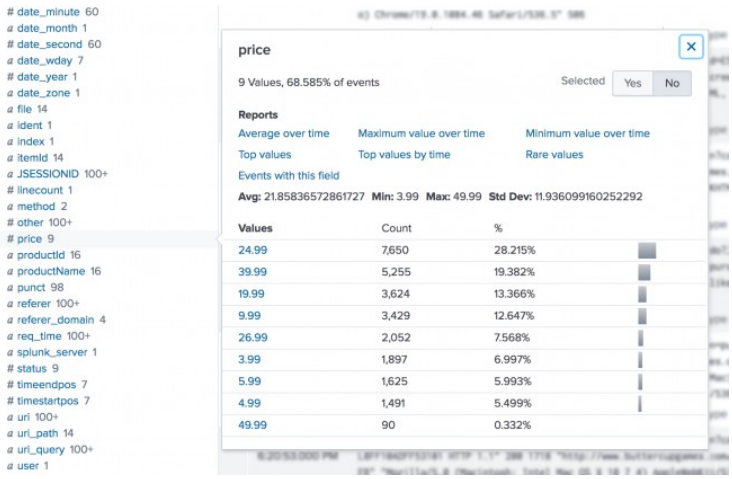
Show the lookup fields in your search results

Because the `prices_lookup` is an automatic lookup, the fields from the lookup table will automatically appear in your search results.

1. From the Automatic Lookups window, click the **Apps** menu in the Splunk bar.
2. Click **Search & Reporting** to return to the Search app.
3. Change the time range to **All time**.
4. Run the following search to locate all of the web access activity.

`sourcetype=access_*`

5. Scroll through the list of **Interesting Fields** in the Fields sidebar, and find the `price` field.
   This field is added to your events from the automatic lookup you created.
6. Click **price** to open the summary dialog box for that field.



   The summary dialog box contains a lot of information about the price field. For example, the price field appears in more than 50% of the events. There are a set of built-in reports that you can access. Several aggregate calculations, such as average, minimum, and standard deviation, are listed. Along with a count and percentage of how many events each price appears in.
7. Next to **Selected**, click **Yes**. This moves the **prices** field from the list of **Interesting Fields** to the list of **Selected Fields** in the Fields sidebar.
8. Close the dialog box.
9. Scroll through the list of **Interesting Fields** in the Fields sidebar, and find the `productName` field.
10. Click **productName** to open the summary dialog box for the field.
11. Next to **Selected**, click **Yes**.
12. Close the dialog box.

Both the `price` and the `productName` fields appear in the Selected Fields list and in the search results.

Notice that not every event shows the `price` and the `productName` fields.

Search with the new lookup fields

When you setup the automatic lookup, you specified that the `productId` field in your indexed events corresponds to the `productId` field in the `prices.csv` file.

When you run a search, the Splunk software uses that relationship to retrieve, or lookup, data from the `prices.csv` file.

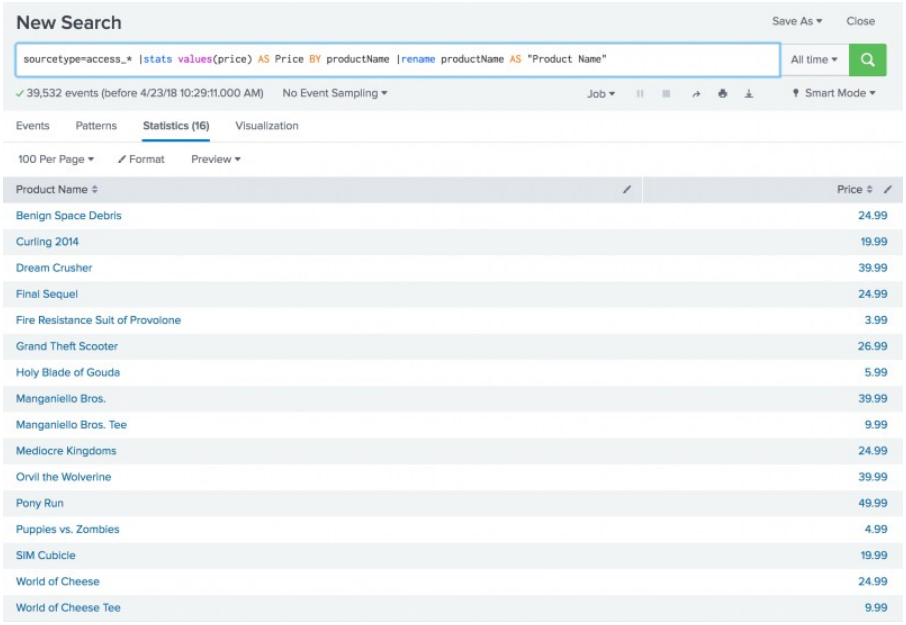
This enables you to specify the `productName` and `price` fields in your search criteria. The product name and price information does not exist in your indexed fields. This information exists in the lookup file, `prices.csv`.

Example: Display the product names and prices

You can show a list of the Buttercup Games product names and the corresponding prices by using the `stats` command to output a table that lists the prices by product. The search also uses the AS keyword and the `rename` command.

1. Run the following search.

```
sourcetype=access_* |stats values(price) AS Price BY
productName |rename productName AS "Product Name"
```

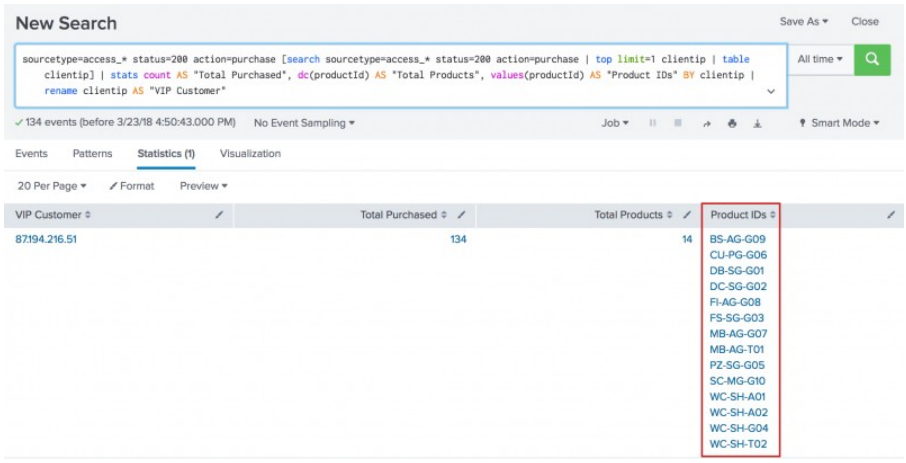


Example: Display the VIP client purchases

In Part 4 of this tutorial about subsearches, you created the following search that returned the product IDs of the products that a VIP client purchased.

```
sourcetype=access_* status=200 action=purchase [search
sourcetype=access_* status=200 action=purchase | top limit=1 clientip |
table clientip] | stats count AS "Total Purchased", dc(productId) AS
"Total Products", values(productId) AS "Product IDs" BY clientip |
rename clientip AS "VIP Customer"
```

The results of that search are shown in the following image.

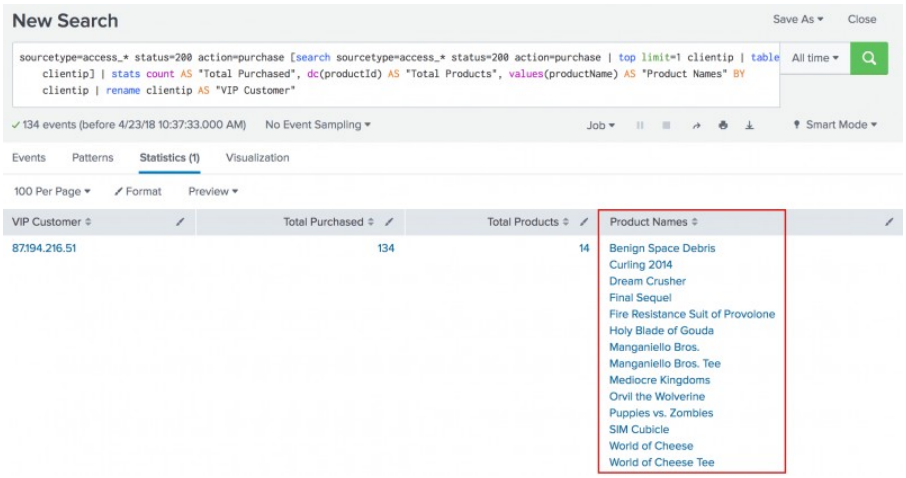


The events return the product IDs because that is the only data in your events about the product. However, now that you have defined the automatic lookup, you can return the actual product names.

1. Make sure that the time range is set to **All time**.
2. Using the same search, change **values(productId)** to **values(productName)**.
3. Run the search.

```
sourcetype=access_* status=200 action=purchase [search
sourcetype=access_* status=200 action=purchase | top
limit=1 clientip | table clientip] | stats count AS "Total
Purchased", dc(productId) AS "Total Products",
values(productName) AS "Product Names" BY clientip | rename
clientip AS "VIP Customer"
```

The results, like the previous search, show the purchases by the VIP customer. However, the results are more meaningful because the product names, which are coming from the lookup table, appear instead of the more cryptic product IDs.



Next step

This completes Part 5 of the Search Tutorial.

You have learned how to use field lookups in your searches. As you run more searches, you want to be able to save those searches, or share the searches with other people. Continue to Part 6: Creating reports and charts.

Part 6: Creating reports and charts

Save and share your reports

In the last few Parts of this tutorial, you learned the basics of searching using the Splunk software, how to use a subsearch, and how to add fields from lookup tables. Part 6 shows you how to save and share your searches and explores more detailed search examples.

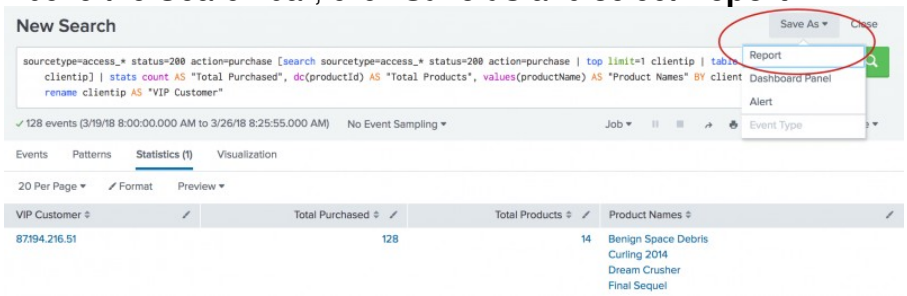
Save a search as a report

Reports are created whenever you save a search. After you create a report, you can do a lot with it.

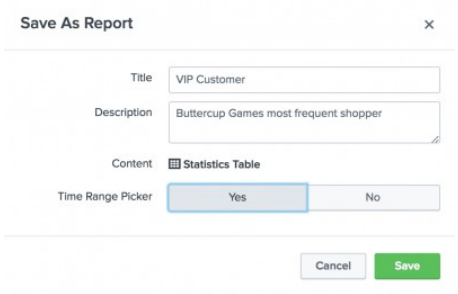
1. Set the time range to **Last 7 days** and run the following search. This is the same search that you ran in the section Search with field lookups.

   ```
   sourcetype=access_* status=200 action=purchase [search
   sourcetype=access_* status=200 action=purchase | top limit=1
   clientip | table clientip] | stats count AS "Total Purchased",
   dc(productId) AS "Total Products", values(productName) AS
   "Product Names" BY clientip | rename clientip AS "VIP Customer"
   ```

   If your search does not return results, increase the time range of the search. For example, you can run this search over the time range **Last 30 days** or **All Time**.
2. Above the Search bar, click **Save as** and select **Report**.

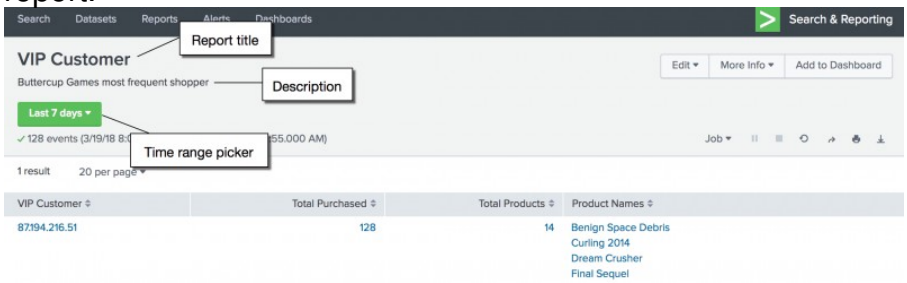


3. In the Save As Report dialog box for **Title** type `VIP Customer`.
4. For **Description**, type `Buttercup Games most frequent shopper`.



5. For **Time Range Picker**, click **Yes**.
   When you include a Time range picker in a report, it gives you the option of running the report with a different time range.
6. Click **Save**.
   A confirmation dialog box opens confirming that your report has been created. From this dialog box you can perform the following actions.
   - **Continue Editing**. To refine the search and report format.
   - **Add to Dashboard**. To add the report to a new or existing dashboard.
   - **View**. To view the report.

7. Click **View.**
   The title and description that you specified appear at the top of the report. Time range picker is also included at the top of the report. If you specified some other time range for the search, that time range appears in the report.

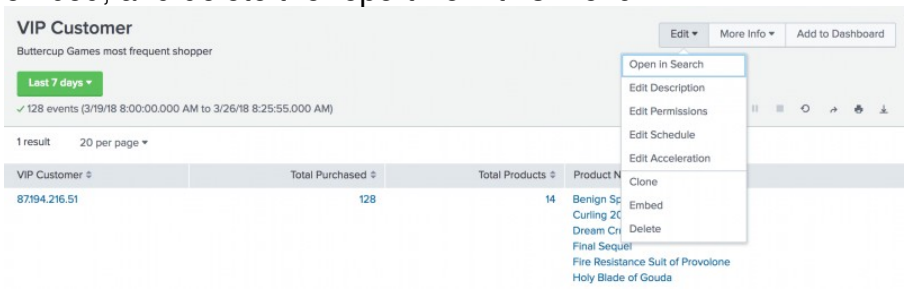


View and edit reports

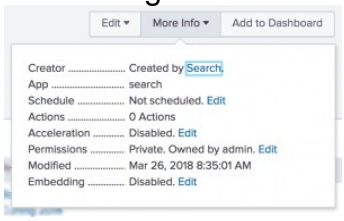
You can view and edit reports that you have saved. You edit a report directly from within the report.

1. In the VIP Customer report, click **Edit**.
   The options are to open the report in the Search view, or to edit the report

description, permissions, schedule, and acceleration. You can also clone, embed, and delete the report from this menu.

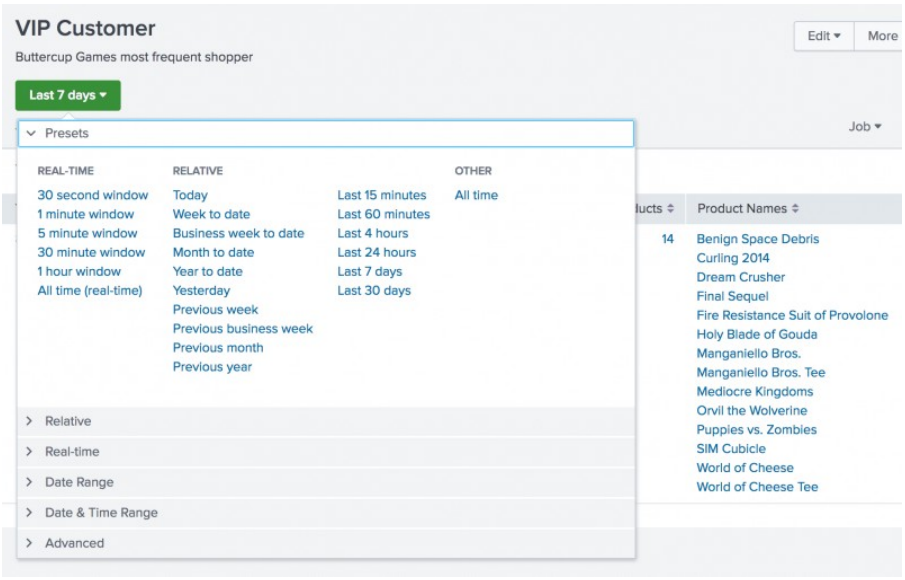


2. Click **More Info** to view information about the report.
   From the **More Info** menu, you can view and edit different properties of the report, including its schedule, acceleration, permissions, and embedding.



3. Look at the time range picker, located at the upper left corner of the window.

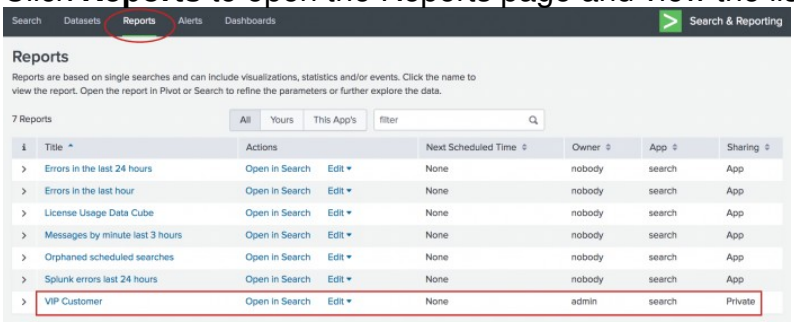
   With the Time range picker, you can change the time period to run this search. For example, you can use the time range picker to run this search for the VIP Customer **Week to date**, **Last 60 minutes**, or **Last 24 hours** just by selecting the Preset time range or defining a custom time range.



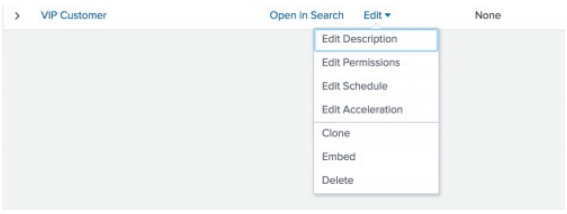
Find and share reports

You can access your reports using the App bar.

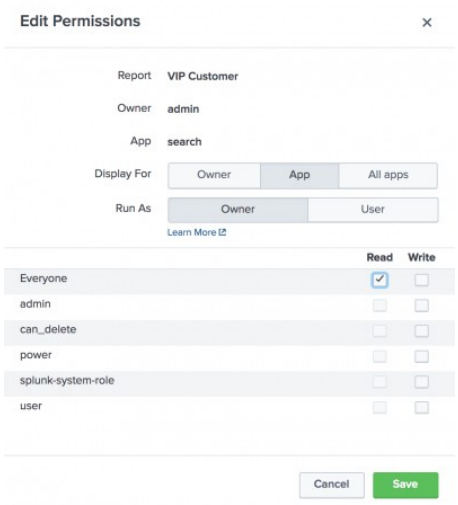
1. Click **Reports** to open the Reports page and view the list of reports.



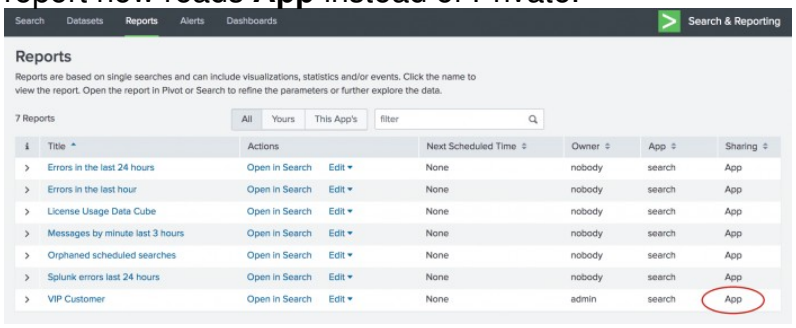
   When you save a report, **Sharing** is set to **Private**. Only you can view and edit the report. You can allow other apps to view, edit, or both view and edit the report by changing the report permission.
2. For the **VIP Customer** report, under **Actions** click **Edit**.
3. Select **Edit Permissions**.



4. In the Edit Permissions dialog box, set **Display For** to **App**.
   The display expands to show more settings.
5. For **Everyone**, mark the check box under **Read**.
   This action gives everyone who has access to this app the permission to view the report.



6. Click **Save**.
   The Reports page appears. The **Sharing** setting for the VIP Customer report now reads **App** instead of Private.



Next step

Let's explore some other search examples, work with chart visualizations, and save the searches as reports, starting with Create a basic chart.

See also

In the *Reporting Manual*

About reports
Accelerate reports

Create a basic chart

In this example you compare the counts of user actions by calculating information about the actions customers have taken on the online store website.

- The number of times each product is viewed
- The number of times each product is added to the cart
- The number of times each product is purchased

Prerequisite
This example requires the `productName` field from the Enabling field lookups section. You must complete all of those steps before continuing with this section.

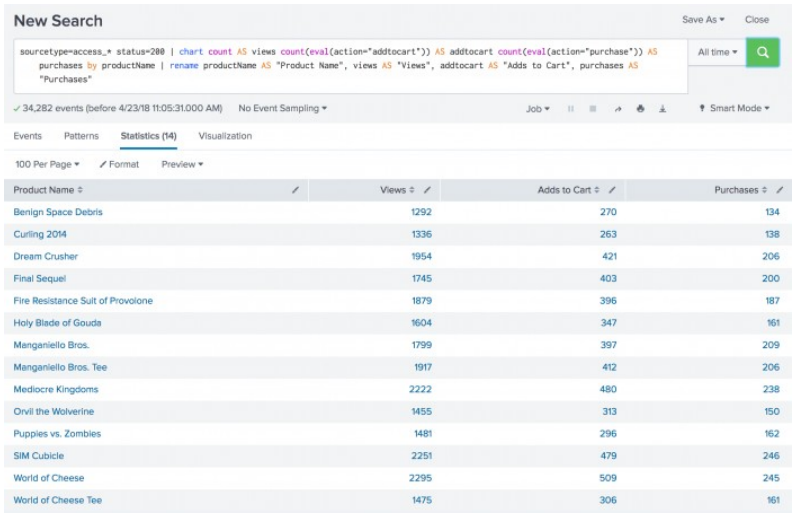
Steps

1. Start a new search.
2. Set the time range to **All time**.
3. Run the following search.

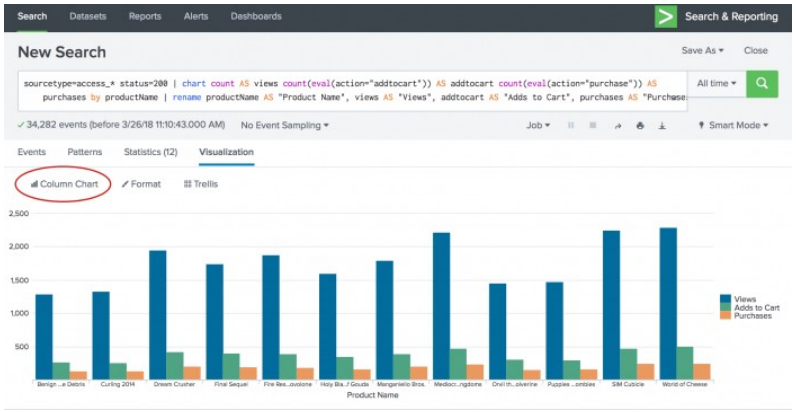
```
sourcetype=access_* status=200 | chart count AS views
count(eval(action="addtocart")) AS addtocart
count(eval(action="purchase")) AS purchases by productName |
rename productName AS "Product Name", views AS "Views", addtocart
AS "Adds to Cart", purchases AS "Purchases"
```

This search uses the `chart` command to count the number of events that are `action=purchase` and `action=addtocart`. The search then uses the `rename` command to rename the fields that appear in the results.

The `chart` command is a transforming command. The results of the search appear on the **Statistics** tab.



4. Click the **Visualization** tab. The search results appear in a Pie chart.
5. Change the display to a **Column** chart.



Next step

Create an overlay chart and explore visualization options

See also

chart command in the *Search Reference*
rename command in the *Search Reference*
Transforming commands in the *Search Manual*

Create an overlay chart and explore visualization options

In this example, you create a chart that overlays two data series as lines over three data series as columns. The overlay chart will show the Actions and the Conversion Rates.

You will use the `stats` command to count the user actions. The `eval` command is used to calculate the conversion rates for those actions. For example, how often someone who viewed a product also added the product to their cart.

Prerequisite
This example uses the `productName` field from the Enabling field lookups section of this tutorial. You must complete all of those steps before continuing with this section.

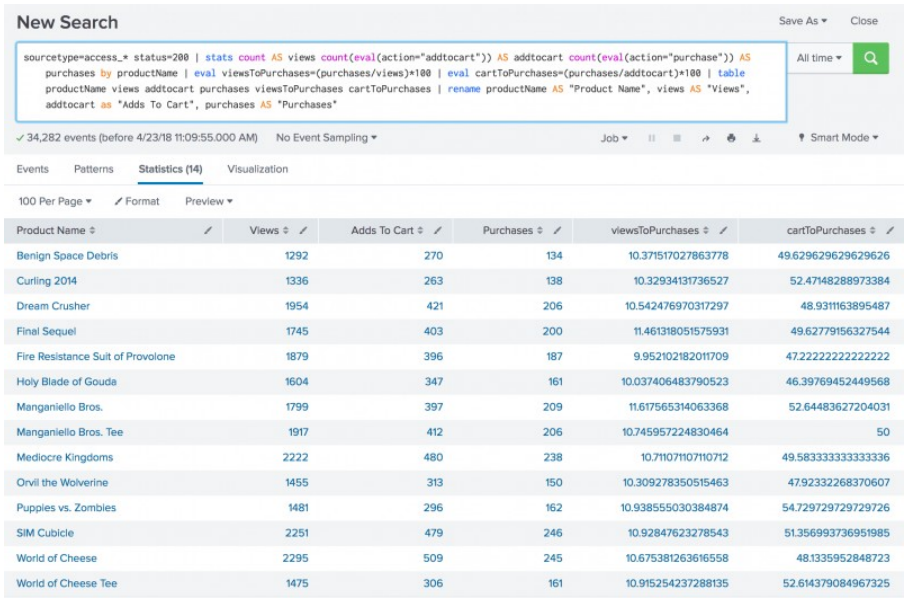
Steps

1. Start a new search.
2. Change the time range to **All time**.
3. Run the following search.

```
sourcetype=access_* status=200 | stats count AS views
count(eval(action="addtocart")) AS addtocart
count(eval(action="purchase")) AS purchases by productName | eval
viewsToPurchases=(purchases/views)*100 | eval
cartToPurchases=(purchases/addtocart)*100 | table productName
views addtocart purchases viewsToPurchases cartToPurchases |
rename productName AS "Product Name", views AS "Views", addtocart
as "Adds To Cart", purchases AS "Purchases"
```

   The `eval` command is used to define two new fields. These fields contain the conversion rates.

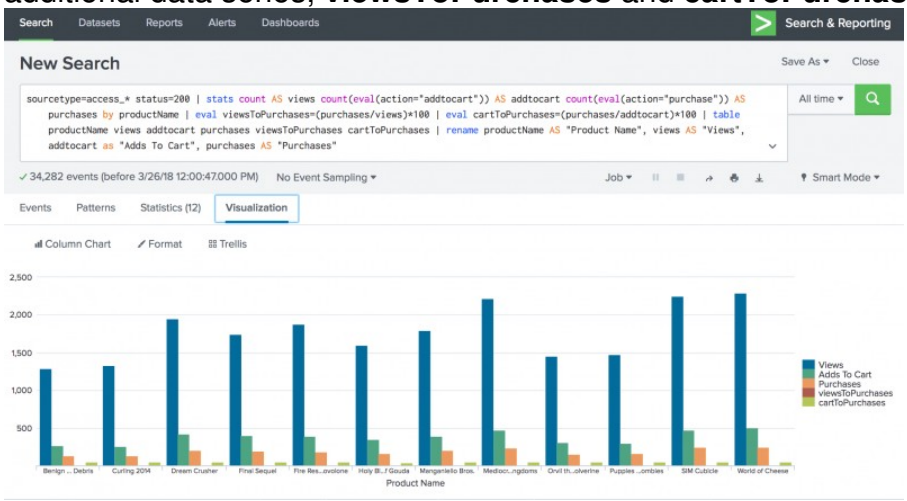
   - The **viewToPurchases** field calculates the number of customers who viewed the product to the number of customers who purchased the product. The calculation returns a percentage.
   - The **cartToPurchases** field calculates the number of customers who added the product to their cart to the number of customers who purchased the product. The calculation returns a percentage.



Product Name	Views	Adds To Cart	Purchases	viewsToPurchases	cartToPurchases
Benign Space Debris	1292	270	134	10.371517027863778	49.629629629629626
Curling 2014	1336	263	138	10.32934131736527	52.47148288973384
Dream Crusher	1954	421	206	10.542476970317297	48.9311163895487
Final Sequel	1745	403	200	11.461318051575931	49.62779156327544
Fire Resistance Suit of Provolone	1879	396	187	9.952102182011709	47.22222222222222
Holy Blade of Gouda	1604	347	161	10.037406483790523	46.39769452449568
Manganiello Bros.	1799	397	209	11.617565314063368	52.6448362720403 1
Manganiello Bros. Tee	1917	412	206	10.745957224830464	50
Mediocre Kingdoms	2222	480	238	10.711071107110712	49.583333333333336
Orvil the Wolverine	1455	313	150	10.309278350515463	47.92332268370607
Puppies vs. Zombies	1481	296	162	10.938555030384874	54.729729729729726
SIM Cubicle	2251	479	246	10.92847623278543	51.356993736951985
World of Cheese	2295	509	245	10.675381263616558	48.1335952848723
World of Cheese Tee	1475	306	161	10.915254237288135	52.614379084967325

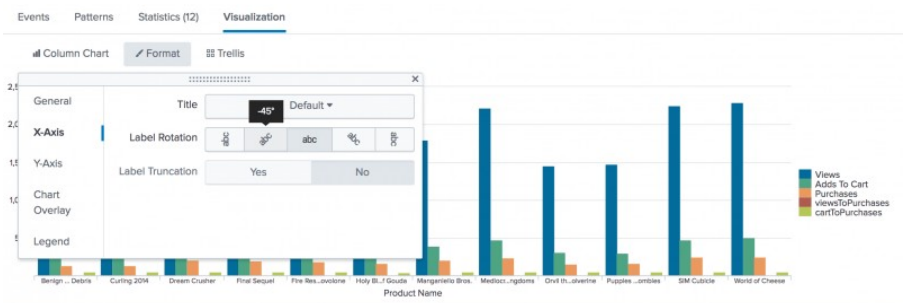
The next few steps reformat the chart visualization to overlay the two data series for the conversion rates, onto the three data series for the actions.

4. Click the **Visualization** tab.
   This is the same chart in the section Create a basic chart, with two additional data series, **viewsToPurchases** and **cartToPurchases**.

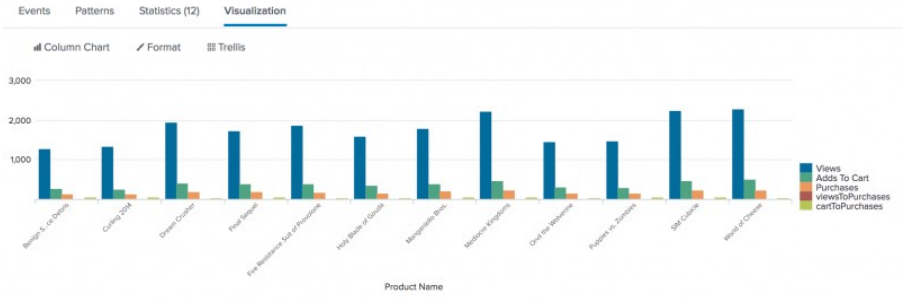


Notice that the labels on the X-Axis are truncated. Because there are so many products, the labels are truncated making them difficult to read. Let's fix that.

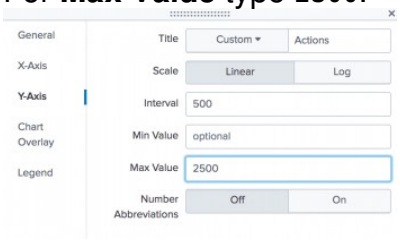
5. Click **Format** and **X-Axis**.
   1. For **Label Rotation** select the second option, which is **-45** degrees.



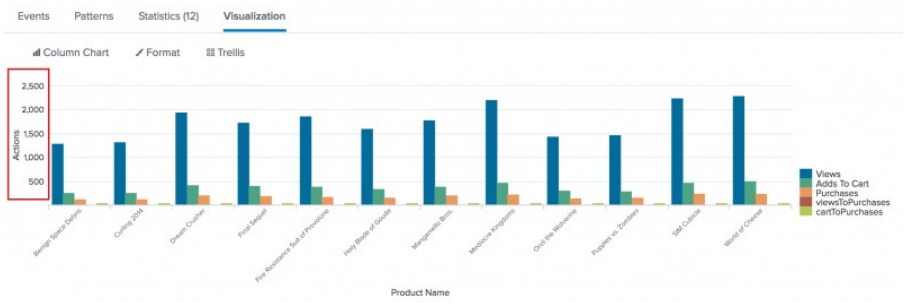
2. Close the Format dialog box.
   Notice the change in the labels on the X-Axis.



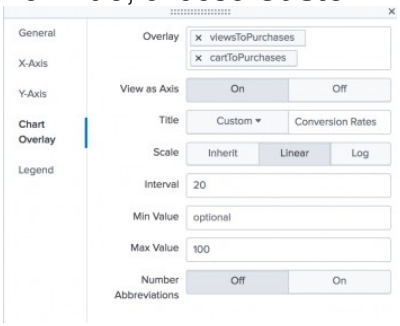
6. Look at the numbers on the Y-Axis. The numbers range from 1000 to 3000. Click **Format** and **Y-Axis**.
   To make the chart easier to read, add a title and specify different number intervals on the Y-Axis.
   1. For **Title**, choose **Custom** and type `Actions`.
   2. For **Interval** type `500`.
   3. For **Max Value** type `2500`.



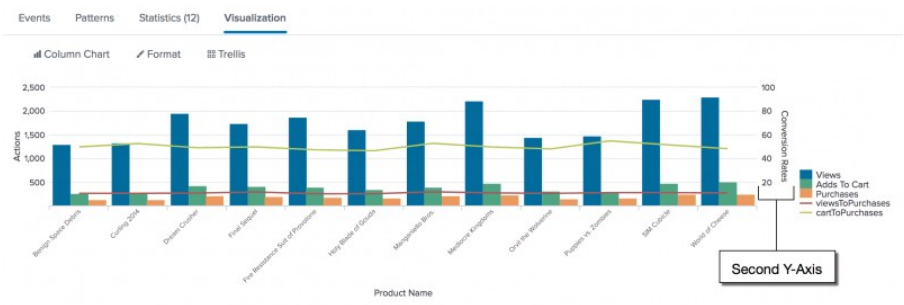
4. Close the Format dialog box. Notice the changes to the label and values on the Y-Axis.



7. Look at the legend. It shows that some of the columns represent **actions** such as Views and Purchases, and some columns represent **conversion rates** such as viewsToPurchases. The actions are counts of the values in specific fields. The conversion rates are percentages. These two types of information should be shown separately.
8. To fix this issue, click **Format** and **Chart Overlay**.
   To separate the actions from the conversion rates, you can overly one set of values over another set of values. In this example you will overlay the conversion rates, as lines, over the actions, which will remain as columns.
   1. For **Overlay**, click inside the box. Begin and select **viewsToPurchase**. Click inside the box again and select **cartToPurchase**. This identifies the two series that you want to overlay on to the column chart.
   2. For **View as Axis**, click **On**.
   3. For **Title**, choose **Custom**

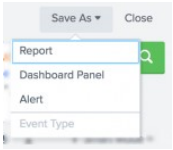


   4. Type `Conversion Rates`.
   5. For **Scale**, click **Linear**.
   6. For the **Interval** type `20`. For the **Max Value** type `100`.
   7. Close the Format dialog box. Notice that the conversion rates now appear as lines in the chart.



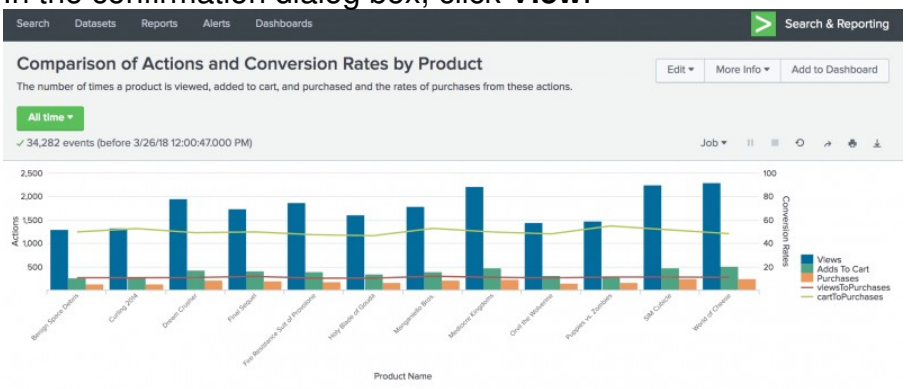
The axis on the right side of the chart is called a **second Y-Axis**. The label and values for the line series appear on this axis.

- Click **Save As** and select **Report**.



1. In the Save Report As dialog box, for **Title** type `Comparison of Actions and Conversion Rates by Product.`
2. For **Description**, type `The number of times a product is viewed, added to cart, and purchased and the rates of purchases from these actions.`

- Click **Save**
- In the confirmation dialog box, click **View**.



Next step

Create a report from a custom chart

See also

stats command in the *Search Reference*
eval command in the *Search Reference*
Chart overview in *Dashboards and Visualizations*

Create a report from a custom chart

In this example, you create a report that charts which products were purchased over a period of time. This example uses the `timechart` command and chart options to create and customize a chart.

Prerequisite
This example requires the `productName` field from the Enabling field lookups section. You must complete all of those steps before continuing with this section.

Steps

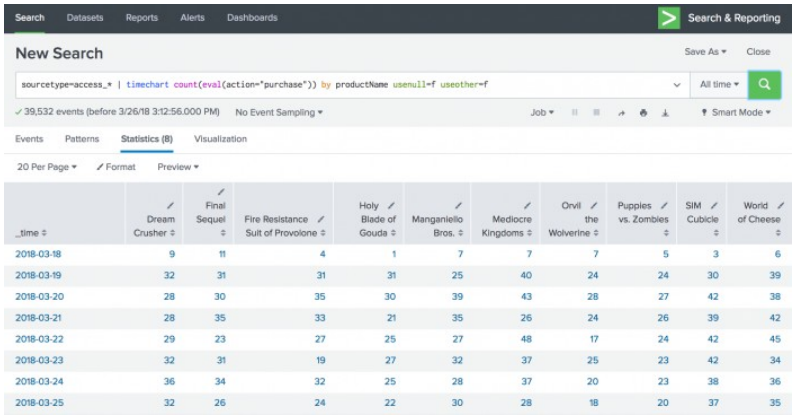
1. Start a new search.
2. Change the time range to **All time**.
3. Run the following search.

   ```
   sourcetype=access_* | timechart count(eval(action="purchase")) by
   productName usenull=f useother=f
   ```

   This search uses the `count()` function to count the number of events that have the field `action=purchase`.

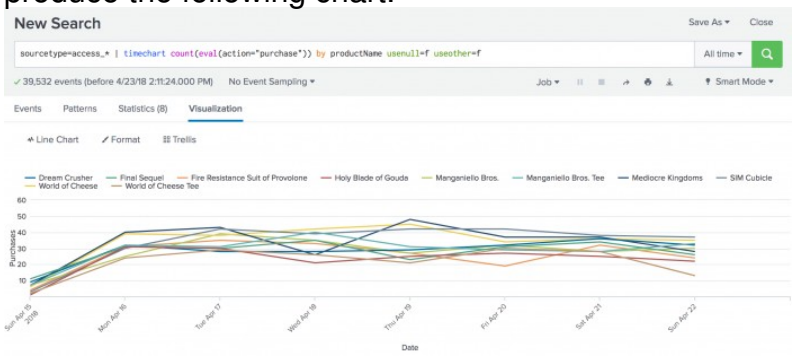
   The search also uses the `usenull` and `useother` arguments to ensure that the `timechart` command counts events that have a value for `productName` Events that have null values for productName are not included.

   The following table appears on the **Statistics** tab.



_time	Dream Crusher	Final Sequel	Fire Resistance Suit of Provolone	Holy Blade of Gouda	Manganiello Bros.	Mediocre Kingdoms	Orvil the Wolverine	Puppies vs. Zombies	SIM Cubicle	World of Cheese
2018-03-18	9	11	4	1	7	7	7	5	3	6
2018-03-19	32	31	31	31	25	40	24	24	30	39
2018-03-20	28	30	35	30	39	43	28	27	42	38
2018-03-21	28	35	33	21	35	26	24	26	39	42
2018-03-22	29	23	27	25	27	48	17	24	42	45
2018-03-23	32	31	19	27	32	37	25	23	42	34
2018-03-24	36	34	32	25	28	37	20	23	38	36
2018-03-25	32	26	24	22	30	28	18	20	37	35

4. Click the **Visualization** tab.
5. Change the chart type to a **Line chart**.
6. Use the **Format** drop-down to format the **X-Axis**, **Y-Axis**, and **Legend** to produce the following chart.



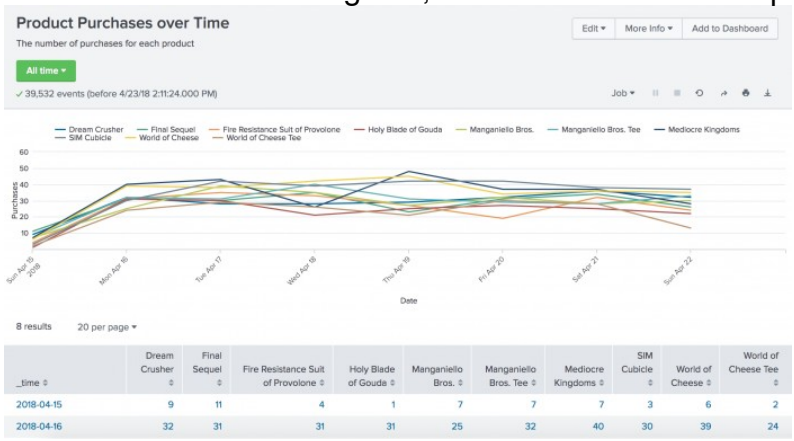
This table lists the changes made to the chart.

Chart changes	Setting or value
Chart type	Line
X-Axis CustomTitle	Date
X-Axis Labels	-45 degree angle
Y-Axis Custom Title	Purchases
Y-Axis Interval	10
Legend Position	Top

7. Click **Save As** and select **Report**.
    1. In the **Save Report As** dialog box, for **Title** type `Product Purchases over Time`.
    2. For **Description**, type `The number of purchases for each product.`
    3. For **Content**, select the first option **Line Chart and Statistics Table**.

4. For **Time Range Picker**, keep the default setting **Yes**.

8. Click **Save**.
9. In the confirmation dialog box, click **View** to see the report.



Next step

Create a report from a sparkline chart

See also

timechart command in the *Search Reference*
Chart overview in *Dashboards and Visualizations*
About reports in the *Reporting Manual*

Create a report from a sparkline chart

In this example, you create a report that shows the trends in the number of purchases made over time. This example uses sparkline charts. **Sparklines** are inline charts that appear in the search results table and are designed to display time-based trends associated with the primary key of each row.

For searches that use the `stats` and `chart` commands, you can add sparkline charts to the results table.

Prerequisite

This example requires the `productName` field from the Enabling field lookups section. You must complete all of those steps before continuing with this section.

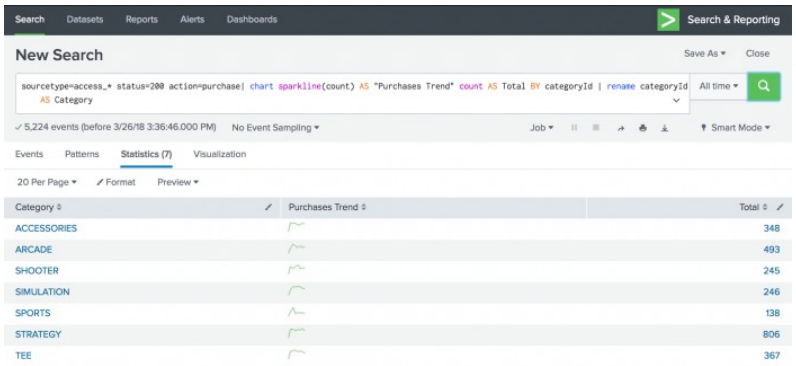
Steps

1. Start a new search.
2. Set the time range to **All time**.
3. Run the following search.

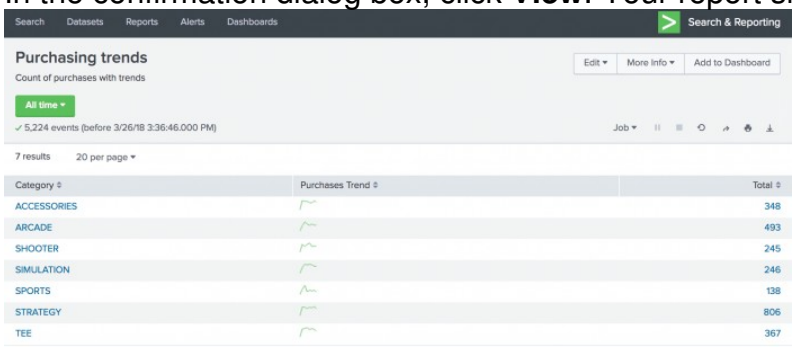
```
sourcetype=access_* status=200 action=purchase| chart
sparkline(count) AS "Purchases Trend" count AS Total BY
categoryId | rename categoryId AS Category
```

This search uses the `chart` command to count the number of purchases by using `action="purchase"`. The search specifies the purchases made for each product by using `categoryId`. The difference is that the count of purchases is now an argument of the `sparkline()` function.

When you rename a column using the AS keyword, names that are more than one word need to be in quotation marks. In this search quotation marks are around the name **Purchases Trend** but not around the name **Category**.



4. Click **Save As** and select **Report**.
5. In the **Save Report As** dialog box, for **Title** type **`Purchasing trends`**.
6. For **Description**, type **`Count of purchases with trends`**.
7. Click **Save**.
8. In the confirmation dialog box, click **View**. Your report should look like this.



Next step

This completes Part 6 of the Search Tutorial.

Up to now, you have saved searches as Reports. Continue to Part 7: Creating dashboards, where you learn how to save searches and reports as dashboard panels.

See also

chart command in the *Search Reference*
Add sparklines to your search results in the *Search Manual*

Part 7: Creating dashboards

About dashboards

Dashboards are views that are made up of panels. The panels can contain modules such as search boxes, fields, charts, tables, and lists. Dashboard panels are usually connected to reports.

After you create a search visualization or save a report, you can add it to a new or existing dashboard. There is also a Dashboard Editor that you can use to create and edit dashboards. The Dashboard Editor is useful when you have a set of saved reports that you want to quickly add to a dashboard.

Change dashboard permissions

You can grant access to a dashboard from the Dashboard Editor. However, your user role and capabilities defined for that role, might limit the type of access you can define.

If your Splunk user role is admin (with the default set of capabilities), then you can create dashboards that are private, visible in a specific app, or visible in all apps. You can also provide access to other Splunk user roles, such as user, admin, and other roles with specific capabilities.

Change dashboard panel visualizations

After you create a panel with the Dashboard Editor, use the Visualization Editor to change the visualization type in the panel, and to specify how the visualization displays and behaves.

Edit the XML configuration of a dashboard

You can edit the panels in a dashboard by editing the XML configuration for the dashboard. This provides access to features not available from the Dashboard Editor. For example, you can edit the XML configuration to change the name of dashboard, or you can specify a custom number of rows in a table.

Next step

Now let's create dashboards and dashboard panels that are based on searches and reports.

See also

In *Dashboards and Visualizations*:

Dashboards Quick Reference Guide
Visualization reference
Data structure requirements for visualizations

In the *Admin Manual*:

Manage knowledge object permissions

Create dashboards and panels

In this section, you will save a search as a dashboard panel and add an input element to the dashboard.

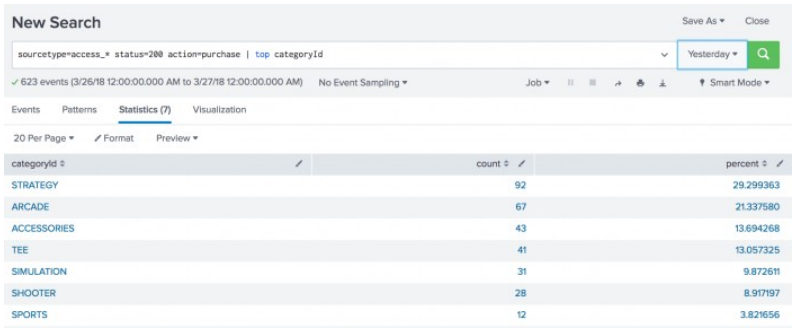
Save a search as a dashboard panel

1. Start a new search.
2. Change the time range to **Yesterday**.
3. Run the following search.

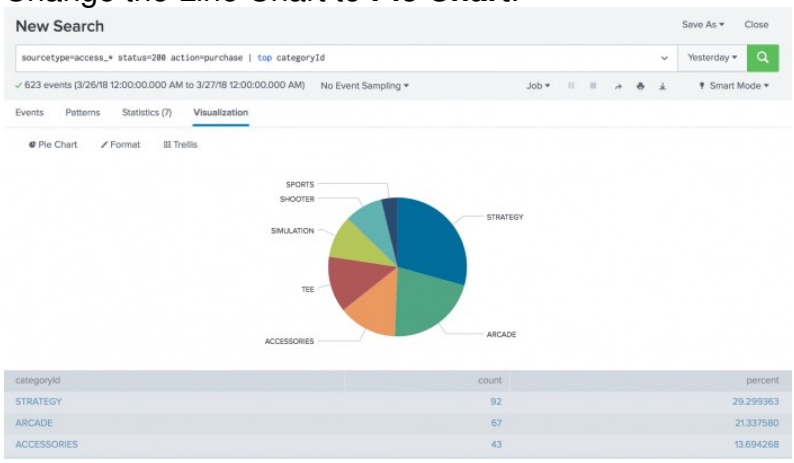
```
sourcetype=access_* status=200 action=purchase | top categoryId
```

If no results are returned, expand your time range to **Previous week**.

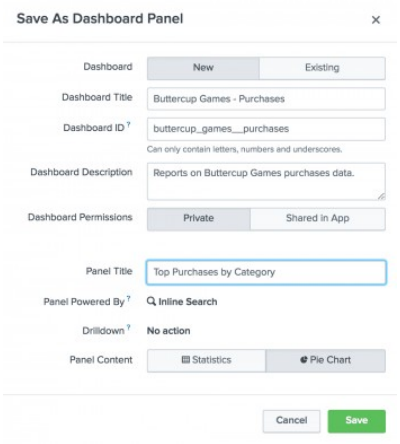
This search returns events from web server access log files for successful (status=200) purchases. The `top` command automatically returns the count and the percent.



4. Click the **Visualization** tab. The displays shows a Line Chart.
5. Change the Line Chart to **Pie Chart**.



6. Click **Save As** and select **Dashboard Panel**.
7. Define a new dashboard and dashboard panel.
    1. For **Dashboard**, click **New**.
    2. For **Dashboard Title**, type `Buttercup Games - Purchases`.
       The **Dashboard ID** field displays **buttercup_games__purchases**.
    3. For **Dashboard Description**, type `Reports on Buttercup Games purchases data.`
    4. For **Dashboard Permissions**, keep the default setting **Private**.
    5. For **Panel Title**, type `Top Purchases by Category`.
    6. For **Panel Content**, keep the setting for **Pie Chart**.



8. Click **Save**.
9. In the confirmation dialog box, click **View Dashboard**.

You now have a dashboard with one report panel. To add more report panels, you can either run new searches and save them to this dashboard, or you can add saved reports to this dashboard. You will add more panels to this dashboard in the next section.

For now, let's spend a little bit more time on this dashboard panel.

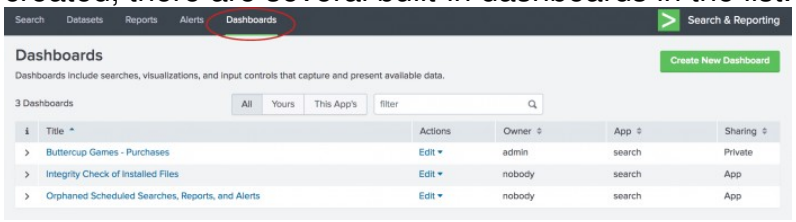
View and edit dashboard panels

There is a separate view to see a list of the dashboards that you have access to. From this view, you can create dashboards, and make changes to dashboards and dashboard panels.

1. Click **Dashboards** in the App bar to see the Dashboards view.

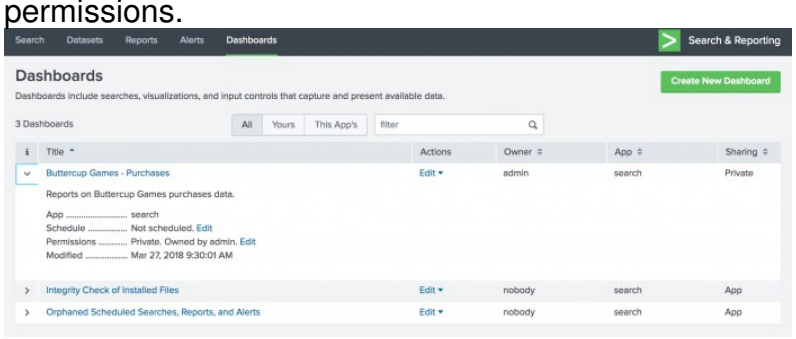
   You might see a pop-up dialog box asking if you want to take a tour about dashboards. If you take the tour, there is an option at the end of the tour to try dashboards yourself. This option displays the Dashboards view.

In addition to the **Buttercup Games - Purchases** dashboard that you created, there are several built-in dashboards in the list.



2. For the **Buttercup Games - Purchases** dashboard, click the arrow (>) symbol in the **i** column to expand the dashboard information.

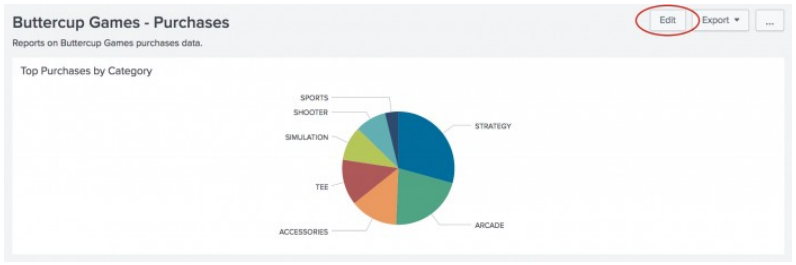
   You can see information about the app that this dashboard is associated with, whether or not the dashboard is scheduled, and the dashboard permissions.



Add controls to a dashboard

You can add input controls, such as the Time range picker, to dashboard panels.

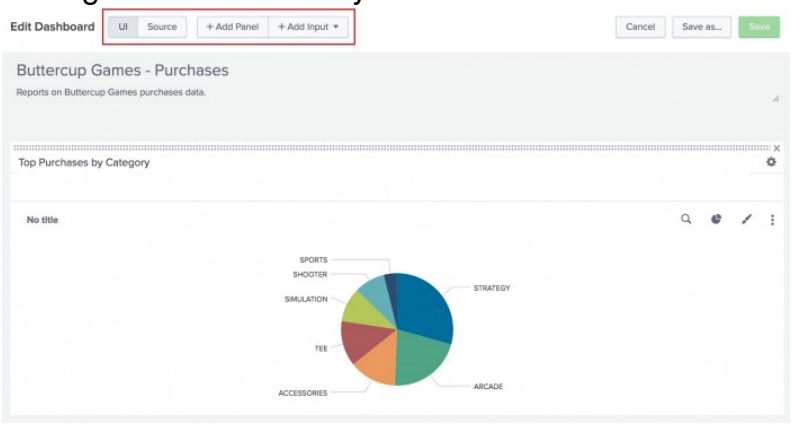
1. In the **Dashboards** list, click **Buttercup Games - Purchases** to display that dashboard.
2. Click **Edit**.



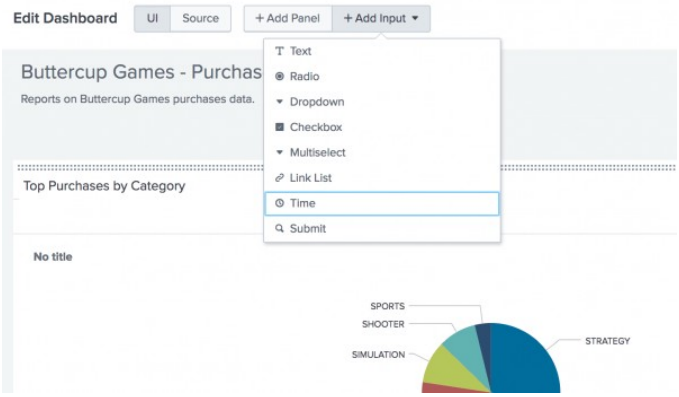
   You can either edit the dashboard using the UI or the Source. With the UI option you can add panels and inputs to the dashboard.

- Use the **Add Panel** option to create a new panel, add a report as a panel, or clone from an existing dashboard.
- Use the **Add Input** option to choose from a list of controls to add to the dashboard, including text, a checkbox, and a time range picker.

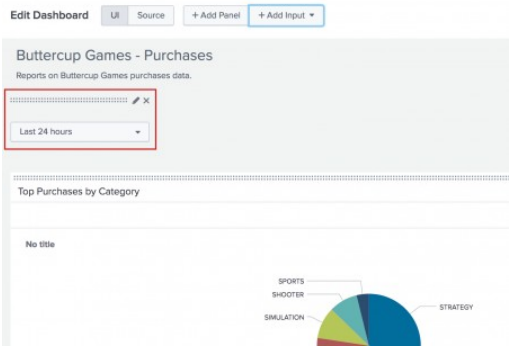
With the Source option, you can edit the XML source for the panel directly. Editing the source directly is not discussed in this tutorial.



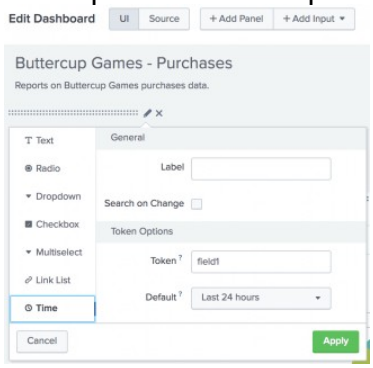
3. Click **Add Input**, and select **Time**.



The Time range picker input control appears on the dashboard.



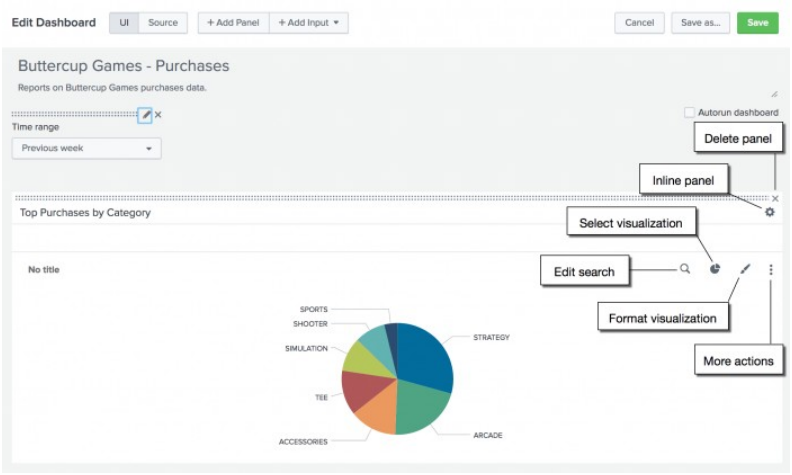
4. Click the **Edit Input** icon for the Time range picker. The icon looks like a pencil.
   This opens a set of input controls. The **Time** input type is selected.



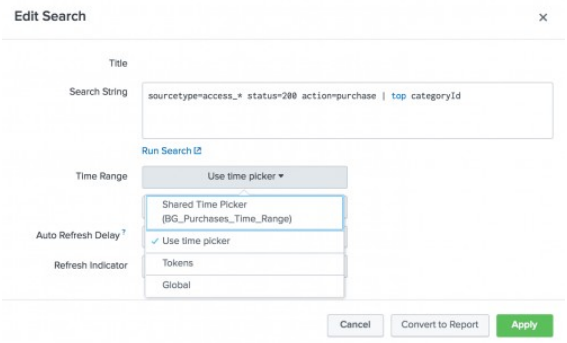
   1. For **Label**, type **`Time range`**
   2. For **Token**, replace the default token name `field1`. Type **`BG_Purchases_Time_Range`**.

      The controls that you add to a dashboard have identifiers called **input tokens**. This step redefines the name of the input token for the Time range picker. The default names for input tokens are field1, field2, field3, and so on. You can change the input tokens when you add controls to your dashboard. Naming the tokens makes it easier to understand which input you are working with. In this example you are using a token name that includes the a short version of the dashboard title.
   3. For **Default**, change the default time range to **Previous week**.
   4. Click **Apply**.

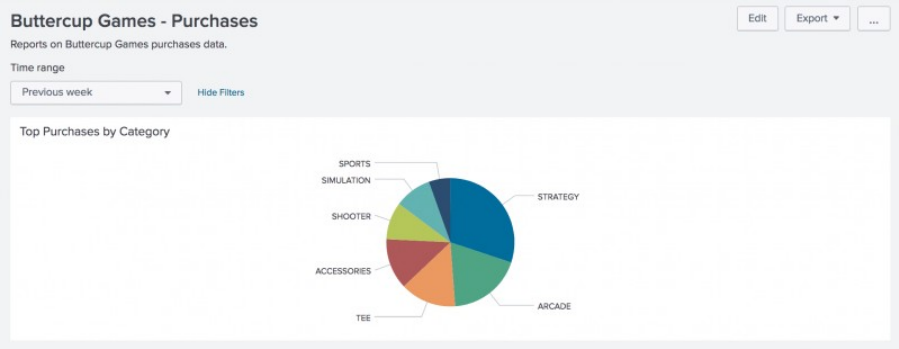
   The input controls that you add to a dashboard are independent from the dashboard panels. If you want the chart on the panel to refresh when you change the time range, you need to connect the dashboard panel to the Time range picker input control.
5. In the dashboard panel, click the **Edit Search** icon.



6. In the Edit Search dialog box, for **Time range** the default selection is **Use time picker**. Click to see the options. You want to select **Shared Time Picker (BG_Purchases_Time_Range)**.



7. Click **Apply**.
8. In the **Edit Dashboard** window, click **Save** to save the changes to the dashboard.
   The panel is now connected to the Time range picker input control in the dashboard. This Time range picker is referred to as the **shared time picker**. The inline search that powers the panel now uses the time range that is specified in the shared time picker.



You can have dashboards that contain a mix of panels. Panels that are connected to the shared Time range picker, and panels that show data for the time range specified in the search that the panel is based on.

You will learn more about connecting other panels to the shared time picker in the next section.

Next step

Learn about adding more panels to a dashboard.

See also

About the Dashboard Editor in *Dashboards and Visualizations*

Add more panels to dashboards

Earlier in this tutorial you ran searches and saved them as reports. In this section, you add the saved reports to an existing dashboard. You will also add more panels based on ad hoc searches.

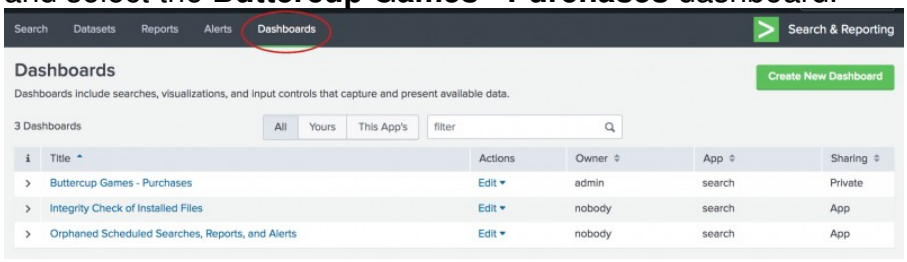
Add saved reports to a dashboard

Prerequisite

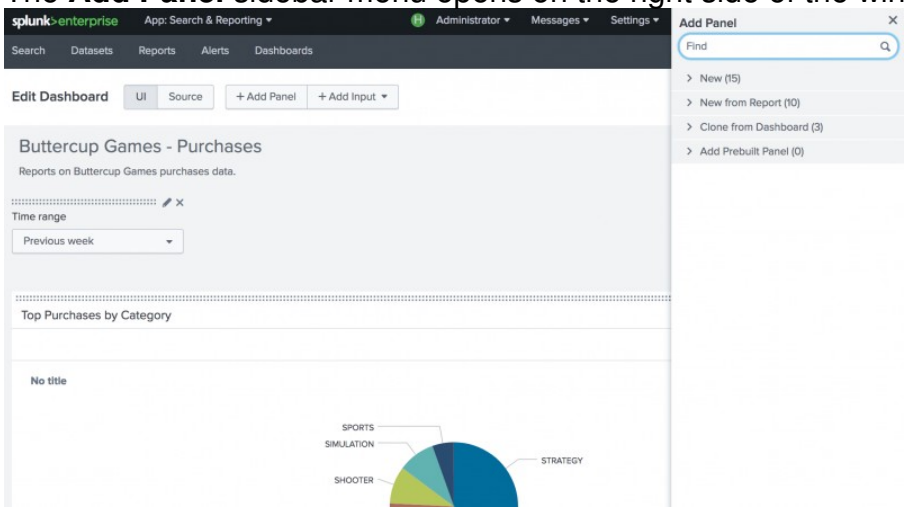
Ensure that you have created the **Buttercup Games - Purchases** dashboard created. This is the dashboard that was created and edited in the previous section of this tutorial, Create dashboards and panels.

Steps

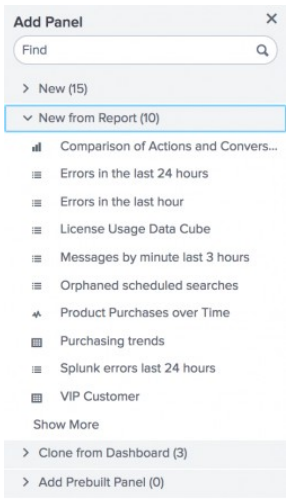
1. To display a list of your dashboards, click **Dashboards** on the Apps bar and select the **Buttercup Games - Purchases** dashboard.



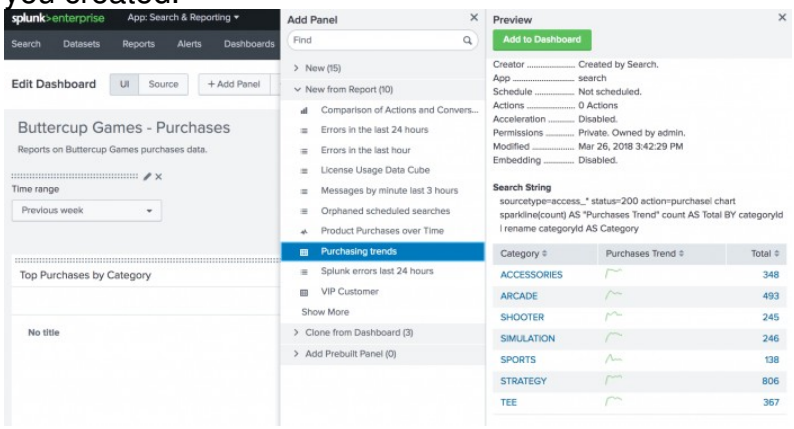
2. In the **Actions** column, click **Edit** and select **Edit Panels**. The Edit Dashboard page opens.
3. Click **Add Panel**.
   The **Add Panel** sidebar menu opens on the right side of the window.



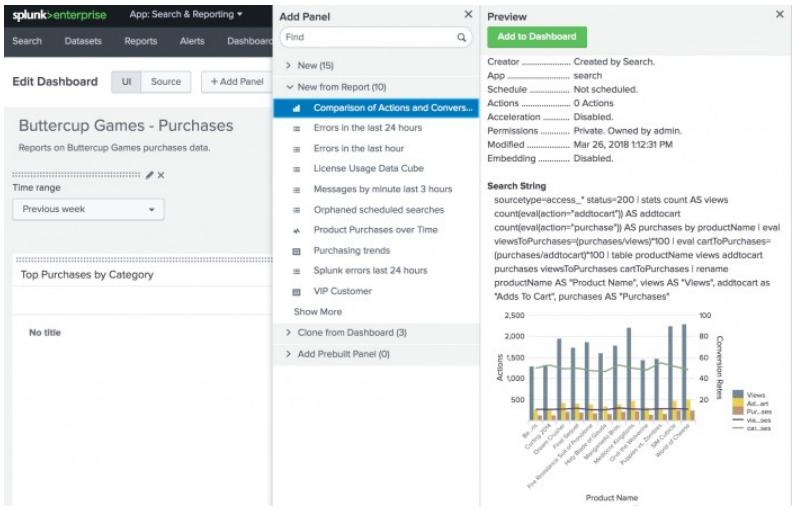
4. To add a new panel from an existing report, click **New from Report**.
   The list expands to show reports that you created and saved and built-in reports.



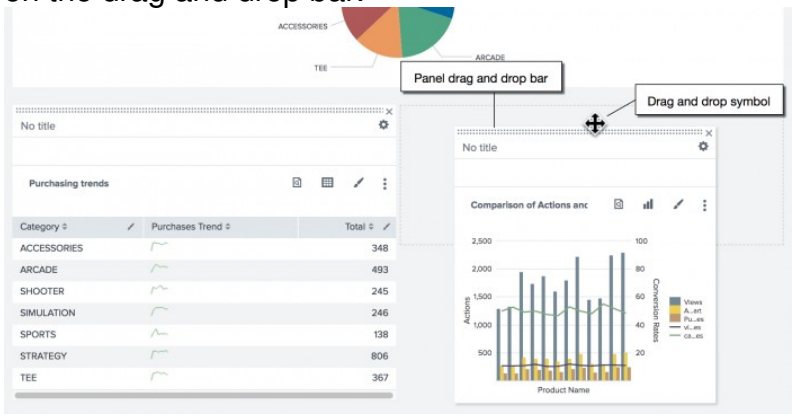
5. Select **Purchasing trends**.
   Next to the Add Panel sidebar, the Preview sidebar appears. The preview includes information about the report, the search that the report is based on, and preview of the report itself. This is the sparkline chart report that you created.



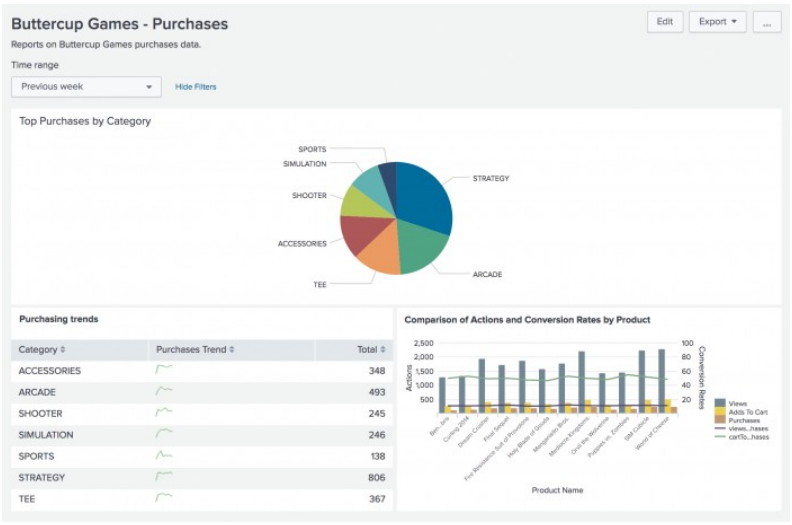
6. Click **Add to Dashboard**.
   The new panel is placed at the bottom of the dashboard.
7. From the Add Panel sidebar menu, select the report **Comparison of Actions and Conversion Rates by Product** and add it to the dashboard.



8. Close the **Add Panel** sidebar.
9. Rearrange the panels on the dashboard.
   Drag and drop a panel by the panel drag and drop bar, which is at the top of the panel. When you drag a panel, a four pointed arrow symbol appears on the drag and drop bar.



10. In the Edit Dashboards window, click **Save** to save your changes to the dashboard.
    Your finished dashboard should look like the following image.



Adding a search to an existing dashboard

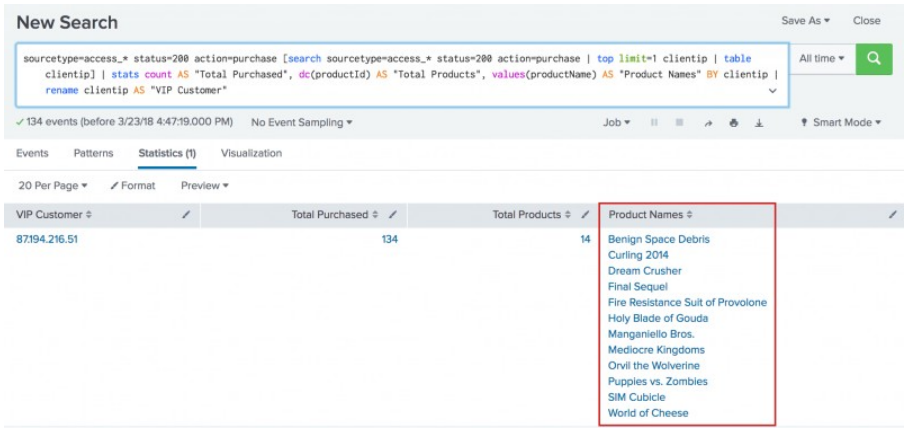
You can save an **ad hoc search** as a panel in an existing dashboard.

In the Enabling field lookups section in this tutorial, you created the `prices_lookup`. Let's use that lookup to run the following search.

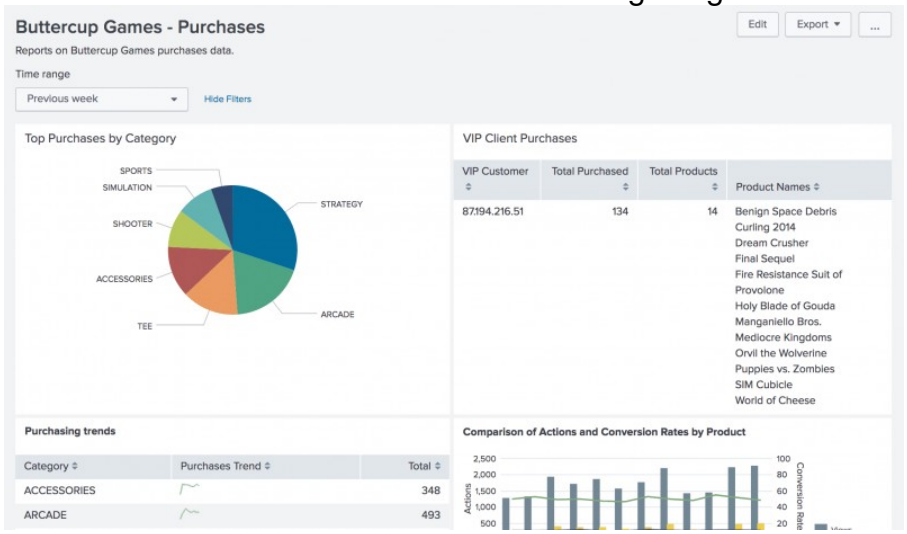
1. Click **Search** in the Apps bar to start a new search.
2. Make sure that the time range is set to **All time**.
3. Run the following search to determine the VIP client and the products that the client purchased.

```
sourcetype=access_* status=200 action=purchase [search
sourcetype=access_* status=200 action=purchase | top limit=1
clientip | table clientip] | stats count AS "Total Purchased",
dc(productId) AS "Total Products", values(productName) AS
"Product Names" BY clientip | rename clientip AS "VIP Customer"
```

The following image shows the results of the search.



4. Click **Save As** and choose **Dashboard panel**.
5. For Dashboard, click **Existing** and select **Buttercup Games - Purchases**.
6. For Panel title, type **VIP Client Purchases**.
7. Click **Save**.
8. Click **View Dashboard**.
9. Click **Edit**.
10. In the dashboard editor, drag the **VIP Client Purchases** panel next to the **Top Purchases by Category** pie chart.
11. Click **Save**.
    Your dashboard should look like the following image.



Connecting panels to a shared Time Range Picker

The type of panel that you add to a dashboard determines whether you can connect the panel to the shared Time Range Picker.

The **Buttercup Games - Purchases** dashboard now contains the panels listed in the following table.

Panel name	Panel source
Top Purchases by Category	Ad hoc search
Purchasing Trends	Report
VIP Client Purchases	Ad hoc search
Comparison of Actions and Conversion Rates by Product	Report

If the panel is based on an **ad hoc search**, you can connect the panel to the shared Time Range Picker. If the panel is a **report**, you cannot connect it to the shared Time Range Picker. Reports can be scheduled to run at a set time interval.

To connect the VIP Client Purchases panel to the shared Time Range Picker:

1. At the top of the dashboard click **Edit**.
2. In the VIP Client Purchases dashboard panel, click the **Edit Search** icon. The icon looks like a magnifying glass.
3. In the Edit Search dialog box, for **Time range** select **Shared Time Picker (BG_Purchases_Time_Range)**.
4. Click **Apply**.
5. In the Edit Dashboard window, click **Save** to save the changes to the dashboard.

The VIP Client Purchases panel is now connected to the Time range picker input on the dashboard.

When you change the time range on the dashboard, the panels that are connected to the shared Time Range Picker are updated. The searches that the panels are based on are run again to refresh the panels.

More dashboard actions

After you create a dashboard, use the buttons in the upper right corner to take actions on the dashboard, such as:

- Export the dashboard
- Convert the dashboard to HTML
- Edit the permissions to share the dashboard with other users

Next step

Congratulations! You have completed the Search Tutorial.

To learn more, see Additional Resources.

Additional resources

Additional resources

You can continue to use the tutorial data, run more searches, and create more dashboards.

The following sections provide additional information and links.

Splunk Community

The Splunk Community is amazing. Splunk Answers. User groups. Blogs. Find other users and splunkers to chat with on Slack.

Everything you need to connect with the Splunk Community is on the Community Portal.

Search resources

This tutorial was a brief introduction to navigating the search interface and using the search language. It walked you through running some basic searches and saving the results as a report and dashboard, but you can do much more with the Splunk software. For more details, see the following manuals:

- *Search Manual*: Explains how to search and use the Splunk Search Processing Language (SPL?). Look here for more thorough examples of writing Splunk searches to calculate statistics, evaluate fields, and report on search results.
- *Search Reference*: Provides a reference for users who are looking for a catalog of the search commands with complete syntax, descriptions, and examples for usage.

Splunk documentation

Splunk has a wide range of documentation, including tutorials, use cases, and manuals for administrators, developers, and users, as well as SDK and SPL command syntax documentation.

There are separate manuals for searches, dashboards and visualizations, reports, pivots, and alerts.

You will find all of the information on the Splunk Documentation site.

Quick References

Splunk Quick Reference Guide
: Contains information about fundamental concepts, features, and components in Splunk software. The guide also includes explanations and examples of common search commands and functions.

Dashboards Quick Reference Guide
: Provides an overview of the most common operations, definitions, and commands that you will use when you create dashboards and visualizations.

Splunk Enterprise system requirements

The Search Tutorial presents a snapshot of the Splunk Enterprise system requirements. For an explanation of the requirements, see System Requirements in the *Installation Manual*.

Accessing your data

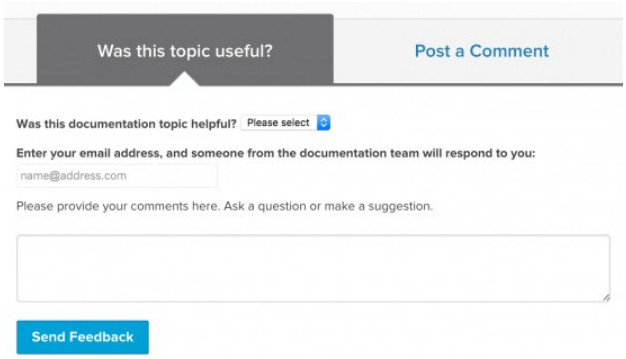
To learn more about the data you can index and types of data sources, see What data can I index? in the *Getting data In* manual.

Education

To learn more about Splunk features and how to use them, see the Splunk selection of Education videos and classes.

Send us feedback

At the bottom of every page of this tutorial, and all of the Splunk documentation, is a quick form that you can use to send us feedback.


Was this topic useful?
Post a Comment
Was this documentation topic helpful?
Please select
Enter your email address, and someone from the documentation team will respond to you:
name@address.com
Please provide your comments here. Ask a question or make a suggestion.
Send Feedback