



Splunk® Enterprise 8.2.0

搜索教程

生成时间: 2021 年 5 月 24 日, 14:42

Table of Contents

简介		3
关于本搜索教程		3
第 1 部分：入门		5
使用本教程的前提条件		5
安装 Splunk Enterprise		7
启动 Splunk Web		8
浏览 Splunk Web		10
第 2 部分：上载教程数据		14
请参阅上载数据		14
教程数据中包含哪些内容？		15
上载教程数据		15
第 3 部分：使用 Splunk 搜索应用		19
浏览搜索视图		19
指定时间范围		21
第 4 部分：搜索教程数据		25
基本搜索和搜索结果		25
使用字段搜索		28
使用搜索语言		33
使用子搜索		38
第 5 部分：用查找丰富事件		42
启用字段查找		42
通过字段查找进行搜索		49
第 6 部分：新建报表和图表		54
保存和共享您的报表		54
新建基本图表		58
新建一个叠加图表并浏览可视化选项		60
新建来自自定义图表的报表		64
从迷你图新建报表		66
第 7 部分：新建仪表板		68
关于仪表板		68
新建仪表板和面板		69
向仪表板添加更多面板		76
其他资源		84
其他资源		84

简介

关于本搜索教程

Splunk 搜索和报表应用程序（搜索应用）是使用 Splunk 软件进行搜索、保存报表，以及新建仪表板的主要界面。本搜索教程适用于使用 Splunk 平台和搜索应用的新用户。

通过本教程了解如何使用搜索应用。整个教程介绍了 Splunk Enterprise 和 Splunk Cloud 之间的区别。

您可能会发现，本教程中的屏幕截图与 Splunk 软件部署中的实际页面之间存在细微的差异。部分屏幕截图可能取自较旧版本的“搜索”应用，但是这些细微差异不会影响您成功读完本教程。

是否已经可以访问 Splunk 软件？

针对此教程，请使用免费试用版 Splunk 软件。

为什么？因为此教程使用一组特定数据，以确保搜索结果及您要了解的功能一致性。在本教程中，您将需要向 Splunk 平台上载教程特定的数据。您可能没有在生产、工作环境中上载数据的权限。此外，使用免费试用版软件可确保教程数据不会与您的工作数据混合。

免费试用版软件会在 30 天后变成免费版。如果您有免费版 Splunk 软件，则某些功能（如更改用户帐户菜单中的偏好）不可用。请参阅管理员手册中的“关于 Splunk Free”。

此手册中包含下载免费试用版 Splunk Enterprise 或 Splunk Cloud 的步骤。

本教程包含哪些内容？

您将了解到如何使用搜索应用向 Splunk 部署添加数据、搜索数据、将数据保存为报表和新建仪表板。如果您是搜索应用新用户，可以从此教程开始。

如何使用本教程

搜索教程中的每一部分都建立在前一部分基础上。例如，您在第 5 部分新建的搜索将用于第 7 部分中，以新建报表和图表，您不会跳过任何一部分，这一点非常重要。

- 第 1 部分：入门
- 第 2 部分：上载教程数据
- 第 3 部分：使用 Splunk 搜索应用
- 第 4 部分：搜索教程数据
- 第 5 部分：用查找丰富事件
- 第 6 部分：新建报表和图表
- 第 7 部分：新建仪表板

使用教程的 PDF 版本

您可以从 web 浏览器中的此在线教程中，将搜索字符串或正则表达式直接复制粘贴到搜索和报表应用中。

不要直接从电子版 PDF 文档中将搜索字符串或正则表达式复制并粘贴到搜索应用。从 PDF 复制搜索数据可能会导致搜索错误，因为 PDF 格式中包含隐藏字符。

另请参阅部分

本教程大部分主题末尾都有一个称为另请参阅部分。这些部分中包含与该主题介绍内容相关的 Splunk 文档的链接。

其他资源

请参阅本教程末尾的其他资源部分，了解关于下列对象的信息：

- Splunk 社区
- 快速参考信息链接
- Splunk 文档链接
- 如何提供反馈

后续步骤

要入门，继续参阅“使用本教程的前提条件”。

第 1 部分：入门

使用本教程的前提条件

您需要新建一个 Splunk.com 帐户、访问免费试用版 Splunk 软件，并下载教程数据文件。可能还有其他先决条件，具体取决于您使用的 Splunk 平台。

新建 Splunk.com 帐户

您需要一个 Splunk.com 帐户，以下载免费试用的 Splunk 软件。新建帐户是免费的。如果您还没有 Splunk.com 帐户，则需要新建一个。如果已有帐户，则需要登录该帐户。

1. 在单独的浏览器窗口中，前往 <https://www.splunk.com/>。
 - 在链接上使用 **CTRL+单击** 以打开新的浏览器选项卡中的网站。
 - 通过使用单独的浏览器选项卡，搜索教程说明不关闭，您就可以保留此选项卡。您可以在浏览器选项卡间来回切换。
 2. 在窗口的右上角，单击 Splunk 帐户图标 。
- 如果您已登录，您的姓名会显示在图标旁边。
- 要新建帐户，请单击 **注册** 并完成注册信息。
 - 要登录现有帐户，单击 **登录**。

选择一个平台

您可以通过 Splunk Cloud 或 Splunk Enterprise 的试用版本使用此教程。试用版本中的主要差别是许可证的长度。

Splunk Cloud

启动 Splunk Cloud 试用版后，您可以访问 Splunk Cloud 15 天。许可证试用版包括 Splunk Cloud 中的所有功能，可使用高级应用程序和加载项。您可以每天索引多达 5GB 数据。

15 天后，Splunk Cloud 试用版的使用权限过期。

Splunk Enterprise

当您首次下载 Splunk Enterprise 时，您将获得 60 天的 Splunk Enterprise Trial 许可证。许可证试用版包括 Splunk Enterprise 中的所有功能，可使用所有高级应用程序和加载项。您可以每天索引多达 500MB 数据。

60 天后，Enterprise 试用许可证转换为永久免费的许可证，一些功能将禁用，例如用户偏好、验证和告警。免费许可证还包括 500MB 的日常索引量，但没有到期时间。请参阅管理员手册中的“关于 Splunk Free”。

系统要求

确保您计算机满足所选平台的系统要求。

Splunk Cloud

必须有一个 Web 浏览器。Splunk Cloud 支持 Chrome、Firefox 和 Safari 浏览器的最新版本。

Splunk Enterprise

您可以在 Linux、Windows 和 Mac Os（仅限 10.14 和 10.15）中使用 Splunk Enterprise。对于本教程，您的计算机必须满足下表中所列的规格。

要求	最低支持的硬件容量
非 Windows 平台	双核 64 位 CPU，每个核心速率等于或大于 2Ghz，内存 4GB RAM
Windows 平台	双核 64 位 CPU，每个核心速率等于或大于 2Ghz，内存 4GB RAM
Web 浏览器	支持 Chrome、Firefox 和 Safari 浏览器的最新版本。

下载教程数据文件

本教程使用一个虚构的游戏商店案例，该商店称为 Buttercup Games，通过在线商店出售游戏和相关产品。

您必须下载几个数据文件以结合使用本教程。数据文件包含 web 访问日志文件、格式安全的日志文件、销售日志文件和 CSV 价格列表文件。

如果您使用 **Safari** 浏览器，请确保偏好 > 一般下的 Open "safe" files after downloading 选项未勾选。tutorialdata.zip 文件必须先压缩，然后才能成功上载。

1. 下载 tutorialdata.zip 文件。不要解压缩文件。
2. 下载 Prices.csv.zip 文件。此时不要解压缩文件。

访问试用版 Splunk 软件

针对此教程，请使用最新版软件。

如果您之前已下载 Splunk Enterprise Trial 软件，请再次下载试用软件。可以将 Splunk Enterprise Trial 许可证转换为免费许可证。Free 许可证有一些限制，您无法完成本教程所有部分。

1. 返回 Splunk 网站 (<https://www.splunk.com/>) 浏览器的选项卡。
2. 在窗口的右上角，单击 **Free Splunk**。
3. 选择您想要使用的平台，单击链接以下载试用软件。

Splunk Cloud

1. 确认您不是一个机器人。
2. 单击开始试用。
3. 出现一个确认页面，说明“您的 Splunk Cloud 试用版已准备就绪！”单击查看我的实例。

您也会收到一封电子邮件，其中包含 Splunk Cloud 试用版的 URL 和其他有用信息。

4. 接受服务条款。Splunk Cloud 应在浏览器窗口中打开。
5. 请参见后续步骤。

Splunk Enterprise

1. 识别想要配合教程使用的安装程序。

操作系统	针对此教程	可用安装程序
Windows	使用适合您的计算机的 MSI 文件图形安装程序。	2 种安装程序。适用于 64 位的 MSI 文件和适用于 32 位的 MSI 文件。
Linux	使用适合您的 Linux 分布的文件。	3 种安装程序。RPM 软件包、DEB 软件包和压缩 TAR (.tgz) 文件。
macOS	使用 DMG 软件包图形安装程序。 MacOS 支持已弃用。您只能在 10.4 或 10.5 版本中安装 Splunk Enterprise。	2 种安装程序。压缩 TAR (.tgz) 文件安装程序和 DMG 软件包。

2. 单击该安装程序旁边的立即下载。
3. 请参见后续步骤。

下一步

后续步骤取决于您使用的 Splunk 平台。

Splunk Cloud

Splunk Web 应自动启动。您收到的有关 Splunk Cloud 试用版的电子邮件包含可用于访问 Splunk Cloud 的用户名和密码。默认用户名是 sc_admin。

如果看到欢迎访问 Splunk Cloud 试用版窗口并邀请您将您的数据文件放入此处，请关闭该窗口。您将在第 2 部分中上载教程。现在请浏览 Splunk Web。

Splunk Enterprise

您必须安装 Splunk Enterprise。

另请参阅

- 《安装手册》中的“系统要求”
- 《管理员手册》中的“Splunk 许可证类型”

安装 Splunk Enterprise

这些步骤仅适用于 Splunk Enterprise。如果您使用的是 Splunk Cloud，请转至“浏览 Splunk Web”。

您可以在下列操作系统中安装 Splunk Enterprise。

- Linux 安装说明
- Windows 安装说明
- macOS 安装说明

对于其他安装程序或其他支持的操作系统，请参阅适用于这些平台的“安装分步说明”。安装完 Splunk Enterprise 之后，您可以继续浏览 Splunk Web。

Linux 安装说明

Splunk Enterprise 提供三种 Linux 安装程序选项：一个 RPM，一个 DEB，以及一个 .tgz 文件。

前提条件

您必需要有命令行界面（CLI）的访问权限。当您键入安装命令时，用您下载的 Splunk Enterprise 安装程序的文件名代替 `splunk_package_name`。

安装 Splunk Enterprise RPM

您可以将 Splunk Enterprise RPM 安装到默认目录 /opt/splunk 下或其他目录下。

1. 使用 CLI 安装 Splunk Enterprise。
 - 要安装到默认目录，键入 `rpm -i splunk_package_name.rpm`。
 - 要安装到其他目录，向安装命令添加 `--prefix` 标记。
例如，键入 `rpm -i --prefix=/opt/new_directory splunk_package_name.rpm`。
2. 前往启动 Splunk Web 的步骤。

安装 Splunk Enterprise DEB 软件包

- 您只能将 Splunk Enterprise DEB 安装到 /opt/splunk 目录。
- 此位置必须为常规目录，而不能是符号链接。
- 要安装软件包，您必须具有根用户的访问权限或具有 sudo 权限。
- 软件包不会新建环境变量来访问 Splunk Enterprise 安装目录。您必须自己设置这些变量。

如果需要将 Splunk Enterprise 安装到别处，或如果为 /opt/splunk 使用符号链接，则使用 tar 文件来安装软件。

1. 在 CLI 中，键入 `dpkg -i splunk_package_name.deb`。
2. 前往启动 Splunk Web 的步骤。

安装 Splunk Enterprise .tgz 文件

了解以下项目有助于确保使用解压的 TAR 文件成功安装：

- tar 的一些非 GNU 版本可能没有 `-c` 参数。在这种情况下，要安装到 /opt/splunk（无论是 cd 至 /opt），或在运行 tar 命令之前，将 tar 文件放入 /opt。这种方法适用于您的主机文件系统上的任何可访问目录。
 - Splunk Enterprise 不会新建 splunk 用户。如果希望 Splunk Enterprise 以特定用户身份运行，您必须在安装之前手动新建用户。
 - 确保磁盘分区拥有足够空间可容纳您计划保留索引的未压缩数据量。
1. 要在 Linux 系统上安装 Splunk Enterprise，使用 tar 命令展开 tar 文件到相应目录。默认安装目录是当前工作目录中的 splunk。

要安装到 /opt/splunk，请使用带 `-c` 参数的以下命令。

- ```
tar xvzf splunk_package_name.tgz -C /opt
```
2. 前往启动 Splunk Web 的步骤。

### Windows 安装说明

在这一教程中，您将使用默认安装设置安装 Splunk Enterprise，将以本地系统用户 admin 的身份运行软件。

1. 导航到安装程序所在的文件夹或目录。
2. 双击 `splunk.msi` 文件启动安装程序。
3. 在欢迎面板中，阅读许可协议并单击勾选此框以接受许可协议。
4. 单击下一步。
5. 显示终端窗口，提醒您指定管理员用户 ID 和密码以使用 Splunk 试用版本。

密码长度必须至少为 8 个字符。键入时光标不会移动。

记下用户 ID 和密码。您将使用这些凭据登录 Splunk Enterprise。

6. 单击下一步。
7. (可选) 系统将提示您在开始菜单上新建一个快捷方式。如果您想这么做，请单击新建开始菜单快捷方式。
8. 单击安装。
9. 在“安装完成”面板中，确认已选择使用 `Splunk 启动浏览器` 复选框。
10. 单击完成。
11. 安装完成，Splunk Enterprise 启动，Splunk Web 在浏览器窗口中启动。
12. 前往启动 Splunk Web 的步骤。

对于其他用户选项或要实施自定义安装，请参阅《安装手册》中的“在 Windows 上安装”的说明。

## macOS 安装说明

仅 10.14 和 10.15 版本支持 Splunk Enterprise。

1. 导航到安装程序所在的文件夹或目录。
2. 双击 `DMG` 文件。  
将打开包含 `splunk.pkg` 的 Finder 窗口。
3. 双击 `Install Splunk` 图标以启动安装程序。
4. 简介面板将列出版本和版权信息。单击继续。
5. 许可证面板列表显示软件许可协议。单击继续。
6. 您需要同意软件许可协议的条款。单击同意。
7. 在安装类型面板中，单击安装。这将在默认目录 `/Applications/splunk` 中安装 Splunk Enterprise。
8. 系统将提醒您键入用于登录到计算机的密码。
9. 当安装完成时，弹出的信息会通知您必须实施初始化。单击确定。
10. 显示终端窗口，提醒您指定管理员用户 ID 和密码以使用 Splunk 试用版本。

密码长度必须至少为 8 个字符。键入时光标不会移动。

记下用户 ID 和密码。您将使用这些凭据登录 Splunk Enterprise。

11. 弹出一个询问您想要做什么的窗口。单击启动并显示 `Splunk`。Splunk Enterprise 的登录页面在您的浏览器窗口中打开。
12. 关闭安装 `Splunk` 窗口。

安装程序在桌面上生成一个快捷方式，以便您可以随时从桌面启动 Splunk Enterprise。

13. 前往启动 Splunk Web 的步骤。

## 下一步

启动 Splunk Web

## 另请参阅

请参阅《安装手册》中的“在 Linux 上安装”。

## 启动 Splunk Web

这些步骤仅适用于 Splunk Enterprise。如果您使用的是 Splunk Cloud，请转至“浏览 Splunk Web”。

下载并安装完软件之后，您必须启动 Splunk Enterprise 和 Splunk Web。Splunk Web 是您使用 Web 浏览器访问的 Splunk Enterprise 的用户界面。

- 在 Linux 上启动 Splunk Enterprise
- 在 Windows 上启动 Splunk Enterprise
- 在 macOS 上启动 Splunk Enterprise

## 在 Linux 上启动 Splunk Enterprise

安装 Splunk Enterprise 后，使用 Splunk CLI 启动它。

### 前提条件

您需要了解如何访问 CLI。请参阅《管理员手册》中的“关于 CLI”。

### 步骤

1. 使用 Splunk Enterprise 命令行界面 (CLI) /code>，并导航到 bin 目录：

```
cd <Splunk_Enterprise_Installation_Directory>/bin
./splunk start
```

2. 提示您创建 Splunk Enterprise 管理员用户名。这是您登录 Splunk Enterprise 时使用的用户名，而不是您登录计算机或 splunk.com 时使用的用户名。您可以按 Enter 键使用默认的用户名 admin。

```
This appears to be your first time running this version of Splunk.
```

```
Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
```

```
Create credentials for the administrator account.
```

```
Characters do not appear on the screen when you type the password.
```

```
Please enter an administrator username:
```

3. 提示您为您刚刚新建的用户名新建密码。

```
Password must contain at least:
```

```
* 8 total printable ASCII character(s).
```

```
Please enter a new password:
```

4. 如果默认管理和 Splunk Web 端口已被使用（或者不可用），则提示 Splunk Enterprise 使用下一个可用端口。您可以接受该选项或指定一个要使用的端口。
5. 可选。您可以设置 SPLUNK\_HOME 环境变量到 Splunk Enterprise 安装目录。设置环境变量允许您稍后参考安装目录，而不必记住其确切位置：

```
export SPLUNK_HOME=<Splunk_Enterprise_Installation_Directory>
cd $SPLUNK_HOME/bin
```

6. 启动 Splunk Enterprise。

```
./splunk start
```

7. 接受 Splunk Enterprise 许可证。

在运行 start 命令之后，Splunk Enterprise 会显示许可证协议，并提示您先接受许可证再继续启动序列。

如果您在启动 Splunk Enterprise 时遇到问题，请参阅《安装手册》中的“第一次启动 Splunk Enterprise”。

8. 现在登录到 Splunk Web。

### 有用的 CLI 命令

如果您需要停止、重新启动或检查 Splunk Enterprise 服务器的状态，请使用以下 CLI 命令：

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

## 在 Windows 上启动 Splunk Enterprise

完成 Windows 安装后，Splunk Enterprise 会启动，同时还会在您的 Web 浏览器中打开 Splunk Web。

如果 Splunk Enterprise 未启动，您可以选择下列启动方式。

- 从开始菜单启动 Splunk Enterprise。
- 使用 Windows 服务管理器启动 Splunk Enterprise。
- 打开 cmd 窗口，转到 \Program Files\Splunk\bin 并键入 `splunk start`。

现在登录到 Splunk Web。

## 在 macOS 上启动 Splunk Enterprise

在 Mac OS 中，您可以从桌面启动 Splunk Enterprise。

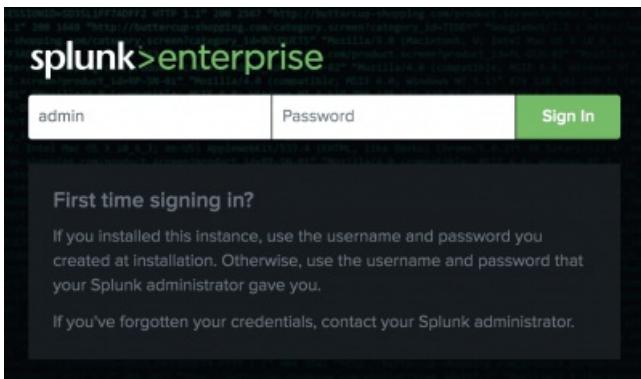
1. 双击桌面上的 **Splunk** 图标。
2. 第一次运行帮助应用程序时，它会通知您需要执行一个初始化。单击**确定**。Splunk Enterprise 初始化并设置许可证试用版。
3. 在 Splunk's Little Helper 窗口中选择**启动和显示 Splunk**。该选项会启动 Splunk Enterprise 并在您的 web 浏览器中打开 Splunk Web 页面。您还可以使用 Splunk's Little Helper 应用程序关闭 Splunk Enterprise。
4. 现在登录到 Splunk Web。

## 登录 Splunk Web

默认情况下，Splunk Web 在安装该 Web 的主机的端口 8000 上运行。如果在本地计算机上使用 Splunk Enterprise，则访问 Splunk Web 的 URL 是 <http://localhost:8000>。

当您首次启动 Splunk Enterprise 时，显示此登录屏幕。

1. 使用安装 Splunk Enterprise 时指定的用户名和密码登录。



2. 显示帮助我们改善 Splunk 软件窗口。阅读每个使用类型集合然后单击**确定**或**跳过**。

您看到的第一个页面是 Splunk Home。

## 下一步

您已下载教程数据文件并安装了 Splunk Enterprise。

继续“浏览 Splunk Web”。

## 浏览 Splunk Web

让我们来了解一下 Splunk 用户界面。

Splunk Web 是搜索、问题调查、报告结果和管理 Splunk 部署的主要界面。

### 关于 Splunk Home

Splunk Home 是 Splunk Web 中的初始页面。Splunk Home 是针对可从 Splunk 实例访问的数据和应用程序的交互门户。Splunk Home 页面主要包含以下部分：应用面板、浏览 Splunk 面板和 Splunk 栏。

#### Splunk Cloud

下图显示 Splunk Cloud 的 Splunk Home 页面：



## Splunk Enterprise

下图显示 Splunk Enterprise 的 Splunk Home 页面：



## 应用面板

**应用面板**列出您安装在 Splunk 实例中的应用程序。此列表仅显示您有权查看的应用。

首次打开 Splunk Web 时，您会在应用面板中看到**搜索和报表**。**搜索和报表**应用有时简称为**搜索应用**。如果计算机中安装了别的应用程序，它们也可能出现在应用面板中。

### 浏览 Splunk 面板

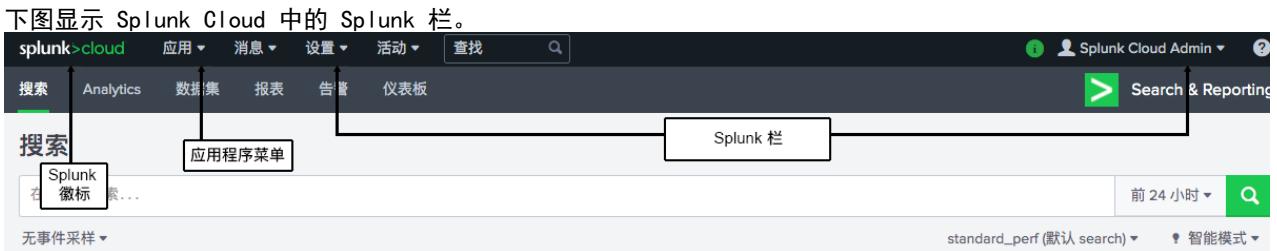
“**浏览 Splunk**”面板中包含帮您入门的页面链接。

### Splunk 栏

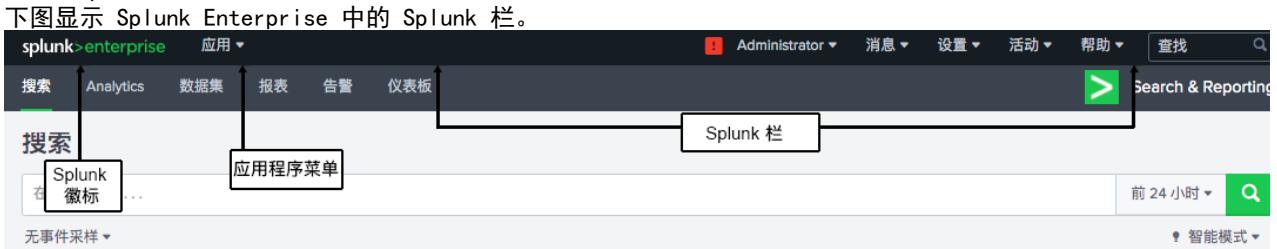
Splunk Web 中每个页面都会显示 Splunk 栏。您可以利用此栏来切换应用、配置 Splunk 部署、查看系统级消息以及监视搜索任务的进度。

- 在 Splunk 主页页面上，单击应用面板中的搜索和报表以打开搜索应用。当位于某应用中时，应用程序菜单在 Splunk 栏显示。您可以使用应用程序菜单在应用间切换。

#### Splunk Cloud



#### Splunk Enterprise



我们将详细浏览搜索应用。现在我们返回到 Splunk Home。

- 单击 Splunk 栅中的 Splunk 徽标。  
无论您位于应用中的哪个位置，单击 Splunk 徽标将始终返回 Splunk Home。

## 其他 Splunk 栅菜单

除了应用程序菜单，Splunk 栅有几个其他菜单。我们来浏览其中几个菜单看看。

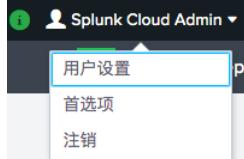
### 帐户菜单

使用帐户菜单编辑您的帐户设置，设置您的偏好，然后注销。

#### Splunk Cloud

“帐户”菜单显示 Splunk Cloud 管理员。

- 选择 Splunk Cloud 管理员 > 用户设置。

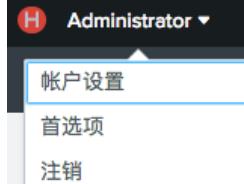


- 您可以在全名字段中输入您的姓名或昵称或保持原样。在本教程中，我们不更改其他设置。
- 单击保存。
- 单击 Splunk 徽标返回到 Splunk Home。

#### Splunk Enterprise

帐户菜单显示管理员。初始状态时它显示管理员，因为这是新安装的默认用户名。

- 选择管理员 > 帐户设置。



- 您可以在全名字段中输入您的姓名或昵称或保持原样。在本教程中，我们不会更改其他设置。
- 单击保存。
- 单击 Splunk 徽标返回到 Splunk Home。

## “消息”菜单

所有系统级错误消息都在消息菜单中列出。当您有要查看的新消息时，数字通知出现在消息菜单旁。通知显示您有的消息数量。



## 帮助

您获取 Splunk 软件帮助信息所使用的菜单依据您使用的 Splunk 平台而有所不同。

### Splunk Cloud

支持和服务菜单包含 Splunk Answers、文档主页页面、Splunk 支持和服务页面的一组链接。您也可以搜索在线文档。

### Splunk Enterprise

帮助菜单包含产品发行说明、教程、Splunk Answers、Splunk 支持和服务页面的一组链接。您也可以搜索在线文档。

## *Splunk* 栏中的其他菜单

您将在此教程的后面部分中了解到 *Splunk* 栏中其他菜单的相关信息。

## 下一步

搜索教程的第 1 部分到此结束。

您现在已经熟悉了 Splunk Web。继续第 2 部分：上载教程数据。

# 第 2 部分：上传教程数据

## 请参阅上传数据

将数据添加到 Splunk 部署后，数据将接受处理并转换为系列单独事件供您查看、搜索和分析。

### 哪种数据类型？

Splunk 平台接受任意类型的数据。尤其是所有 IT 流和历史数据。数据来源可以是事件日志、Web 日志、实时应用程序日志、网络源、系统指标、变更监视、消息队列、归档文件等等。

一般来说，数据来源可分为以下三种类别。

| 数据来源         | 描述                                                                                              |
|--------------|-------------------------------------------------------------------------------------------------|
| 文件和目录        | 有很多您可能感兴趣的数据均来自文件和目录。                                                                           |
| 网络事件         | Splunk 软件可以为来自任何网络端口的远程数据以及来自远程设备的 SNMP 事件建立索引。                                                 |
| IT 操作        | 来自 IT 操作（如 Nagios、NetApp 和 Cisco）的数据。                                                           |
| Cloud 服务     | 来自 AWS 和 Kinesis 等 Cloud 服务的数据。                                                                 |
| 数据库服务        | 来自数据库（如 Oracle、MySQL 和 Microsoft SQL Server）的数据。                                                |
| 安全服务         | 来自安全服务（如 McAfee、Microsoft Active Directory 和 Symantec Endpoint Protection）的数据。                  |
| 可视化服务        | 来自可视化服务（如 VMWare 和 XenApp）的数据。                                                                  |
| 应用程序服务器      | 来自应用程序服务器（如 JMX & JMS、WebLogic 和 WebSphere）。                                                    |
| Windows 数据来源 | Windows 版本的 Splunk 软件接受多种的 Windows 特定输入，包括 Windows 事件日志、Windows 注册表、WMI、Active Directory 和性能监视。 |
| 其他数据来源       | Splunk 还支持其他输入源，例如，FIFO 队列、可通过 API 获取数据的脚本式输入以及其他远程数据接口。                                        |

有很多种数据类型，您都可以直接将数据添加到 Splunk 部署。很多常用数据源都会自动识别。

如果 Splunk 软件没有自动识别您想使用的数据，则您需要在添加数据前，提供数据的相关信息。

### 数据保存在哪里？

转换数据的过程称为编制索引。编制索引期间，将对传入数据进行处理，从而实现快速搜索和分析。处理的结果以事件的形式存储在索引中。

索引是数据的平面文件存储库。对于本教程，索引驻留在您访问您 Splunk 部署的计算机中。

事件在索引中以一组文件的形式存储，这些文件分为两类：

- 原始数据，即您添加到 Splunk 部署的数据。原始数据以压缩格式存储。
- 索引文件，包含指向原始数据的一些元数据文件。

这些文件位于一组按时间组织的目录（称为 **数据桶**）中。

默认情况下，所有数据都会存入单个、预配置的索引（名为 `main`）。当您将数据添加到 Splunk 实例时，可以创建索引存储数据。另外还有几个用于内部的其他索引。

### 下一步

现在，您已经熟悉了数据来源和索引，我们接下来了解一下您将使用的教程数据。

### 另请参阅

《数据导入》中的“使用应用导入数据”

《管理索引器和索引器群集》中的“关于管理索引”

# 教程数据中包含哪些内容？

教程数据文件每天都会更新并包含时间戳为过去 7 天的事件。教程数据包含虚拟在线商店 Buttercup Games 相关的多种类型信息。也许有人并不了解，Buttercup 是一匹小马，是 Splunk 的吉祥物。

信息包含来自邮件服务器和 web 帐户的 `access.log` 文件、`secure.log` 文件及 `vendor_sales.log` 文件。

## Access.log 文件数据

`Access.log` 文件中的原始数据数量庞大、难以读懂。每天都有这么多数据。这就是需要 Splunk 平台的原因。

```
175.44.24.82 - - [22/Feb/2021:18:44:40] "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; B0IE9;ENUS)" 307
142.233.200.21 - - [22/Feb/2021:19:20:13] "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 文件数据

`Secure.log` 文件中的原始数据如下所示：

```
Thu Mar 22 2021 00:15:06 mailsvl sshd[60445]: pam_unix(sshd:session): session opened for user mdubios by (uid=0)
Thu Mar 22 2021 00:15:06 mailsvl sshd[3759]: Failed password for djohnson from 194.8.74.23 port 3769 ssh2
Thu Mar 22 2021 00:15:08 mailsvl sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351
```

## Vendor\_sales.log 文件数据

`Vendor_sales.log` 文件中的原始数据如下所示：

```
[13/Apr/2021:18:23:07] VendorID=5037 Code=C AcctID=5317605039838520
[13/Apr/2021:18:23:22] VendorID=9108 Code=A AcctID=2194850084423218
[13/Apr/2021:18:23:49] VendorID=1285 Code=F AcctID=8560077531775179
[13/Apr/2021:18:23:59] VendorID=1153 Code=D AcctID=4433276107716482
```

## 下一步

现在我们上载教程数据至 Splunk 部署。

## 上载教程数据

本教程使用一组事先设计好的数据，以显示产品功能。使用教程数据可确保您的搜索结果与教程中的步骤一致。

### 前提条件

- 您的计算机必须已经有教程数据文件。
- `Tutorialdata.zip` 文件必须保持压缩状态，才能成功上载。有些浏览器会自动解压缩 ZIP 文件。请参阅“下载教程数据文件”了解更多信息。
- 本教程有助于您了解正在上载的数据类型。请参阅“教程数据中包含哪些内容？”。

## 使用添加数据向导

1. 如果显示欢迎窗口，关闭该窗口。
2. 单击设置 > 添加数据。



3. 单击窗口底部的上载。有其他选项用于添加数据，但是本教程中您将上载数据文件。

上载  
来自我的计算机的文件  
本地日志文件  
本地结构化文件（例如 CSV）  
添加数据教程

4. 在选择来源下，单击选择文件。

添加数据 <上一步 下一步>

选择来源

选择文件

将您的数据文件拖到这儿  
最大文件上载大小为500Mb

常见问题

- > Splunk 平台可索引何种类型的文件？
- > 来源是什么？
- > 如何在我的 Splunk 平台实例上获取远程数据？

5. 在您的下载目录中，选择 tutorialdata.zip 文件并单击打开。

因为您指定了一个压缩文件，Splunk 软件可识别该类型的数据来源。跳过“添加数据”向导中的设置来源类型步骤。当您要加载不属于压缩文件中的数据时，会要求您设置数据来源类型。

6. 单击下一步以继续到输入设置。

7. 在输入设置下，您可以覆盖关于“主机”、“来源类型”和“索引”的默认设置。

因为本教程使用 ZIP 文件，您将修改主机设置，通过使用 ZIP 文件中包含的文件的部分路径名称分配主机值。您指定的

设置取决于您使用的是 Splunk Cloud 还是 Splunk Enterprise 和您正在使用的操作系统。

#### Splunk Cloud

- 选择路径里的段。
- 段号处键入 1。

#### 适用于 Linux 或 Mac OS X 的 Splunk Enterprise

- 选择路径里的段。
- 段号处键入 1。



### 输入设置

可根据需要将此数据的其他输入参数设置如下：

#### 来源类型

来源类型是 Splunk 分配给所有传入数据的默认字段之一。它告诉 Splunk 您获取的数据类型，以便 Splunk 可智能地将数据格式化（在索引期间）。这也是将您的数据分类的一种方法，以便您可轻松搜索到它。

自动 选择 新建

#### 主机

当 Splunk 索引数据时，每个事件收到一个 "host" 值。主机值应为生成事件的计算机名称。您选择的输入类型决定了可用的配置选项。[了解更多信息](#)

- 常量值  
 路径的正则表达式  
 路径中的段

段号 ?

1

#### 索引

Splunk 在选定的索引中将传入数据存储为事件。如果您在定义数据的来源类型时有问题，则考虑使用 "sandbox" 索引作为目标。Sandbox 索引可以让您解决配置问题，而不会影响到生产索引。您始终可以稍后更改此设置。[了解更多信息](#)

索引 默认 创建新索引

#### 适用于 Windows 的 Splunk Enterprise

- 选择路径的正则表达式。
- 键入 \\(.\*)\\v 以便正则表达式从路径中提取主机值。

- 常量值  
 路径的正则表达式  
 路径中的段

正则表达式 ?

\.(.\*).v

#### 8. 请单击查看。以下屏幕出现后您可以查看输入设置。



9. 单击提交添加数据。



✓ 文件已成功上载。

配置您的输入，通过转到设置 > 数据输入



10. 要查看搜索应用中的数据，单击开始搜索。

您可能会看到一个屏幕，询问您是否想要浏览一下。您可以进行浏览或单击跳过。  
搜索应用会打开并自动运行教程数据来源的搜索。

source="tutorialdata.zip:\*

179,399 个事件 (2018/04 16:19:29.000 之前) 无事件采样

事件 (179,399) 模式 统计信息 可视化

| 时间                    | 事件                                                                                                                                                                                                                         |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 21/08/03 8:15:03.000  | =CU=PG=G06 "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.104.46 Safari/536.5" 101 host = www3   source = tutorialdata.zip:/www3/access.log   sourcetype = access_combined_wcookie |
| 21/08/02 18:24:02.000 | [02/Aug/2021:18:24:02] VendorID=5036 Code=B AcctID=6024298300471575 host = vendor_sales   source = tutorialdata.zip:/vendor_sales/vendor_sales.log   sourcetype = vendor_sales                                             |
| 21/08/02 18:23:46.000 | [02/Aug/2021:18:23:46] VendorID=7026 Code=C AcctID=8702194102896748 host = vendor_sales   source = tutorialdata.zip:/vendor_sales/vendor_sales.log   sourcetype = vendor_sales                                             |
| 21/08/02 18:23:31.000 | [02/Aug/2021:18:23:31] VendorID=1043 Code=B AcctID=206371890897951 host = vendor_sales   source = tutorialdata.zip:/vendor_sales/vendor_sales.log   sourcetype = vendor_sales                                              |

成功！结果证实了 tutorialdata.zip 文件中的数据已编制索引，同时事件已新建。

11. 单击 Splunk 徽标返回到 Splunk Home。

## 下一步

您已学习完此搜索教程的第 2 部分。

现在您已了解如何向 Splunk 平台添加数据。接下来您将开始了解如何搜索这些数据。继续第 3 部分：使用 Splunk 搜索应用。

# 第 3 部分：使用 Splunk 搜索应用

## 浏览搜索视图

在第 2 部分中，您已了解 Splunk 平台使用的数据类型，并已将教程数据上载到索引。在第 3 部分中，您将了解搜索应用。

### 查找 Splunk 搜索

1. 如果不在 Splunk Home 页面中，请单击 Splunk 栏上的 Splunk 徽标转到 Splunk Home。
2. 从 Splunk Home 上，在应用面板中单击搜索和报表。



搜索应用中的“搜索摘要”视图随即打开。

### 搜索摘要视图

搜索摘要视图显示与其他视图通用的元素，包括应用程序菜单、Splunk 栏、应用栏、搜索栏和时间范围挑选器；面板还包括特定于搜索摘要视图的一些元素，这些元素位于搜索栏下方：如何搜索面板及搜索历史面板。

Splunk Cloud 和 Splunk Enterprise 中的“搜索摘要”视图几乎相同。

下图显示了 Splunk Cloud 中的“搜索摘要”视图。

A screenshot of the Splunk Cloud Search Summary view. The interface includes a top navigation bar with 'splunk&gt;cloud' and '应用: Search &amp; Reporting' dropdowns, a user profile, and a search bar. Below the navigation is a dark header with tabs: '搜索' (Search), 'Analytics', '数据集' (Datasets), '报表' (Reports), '告警' (Alerts), and '仪表板' (Dashboards). A red circle labeled '3' is over the '仪表板' tab. A red circle labeled '1' is over the '搜索' tab. A red circle labeled '4' is over the search input field '在此输入搜索...'. A red circle labeled '2' is over the main search area. A red circle labeled '5' is over the time range selector '前 24 小时'. A red circle labeled '7' is over the 'standard\_perf (默认 search)' dropdown. A red circle labeled '6' is over the '如何搜索' (How to Search) section. A red circle labeled '8' is over the '搜索历史' (Search History) section.

| 数字 | 元素       | 描述                                                      |
|----|----------|---------------------------------------------------------|
| 1  | 应用程序菜单   | 在已安装的 Splunk 应用程序间进行切换。当前列出“搜索和报表”应用程序。此菜单位于 Splunk 栏中。 |
| 2  | Splunk 栏 | 编辑 Splunk 配置，查看系统级别的消息，获取产品使用帮助。                        |
| 3  | 应用栏      | 在当前应用程序中不同视图间进行导航。搜索和报表应用中的视图有：搜索、分析、数据集、报表、告警和仪表板。     |
| 4  | 搜索栏      | 指定搜索条件。                                                 |
| 5  | 时间范围挑选器  | 指定搜索时间周期，例如过去 30 分钟或昨天。默认时间范围为过去 24 小时。                 |
| 6  | 如何搜索     | 包含《搜索手册》和《搜索教程》的链接。                                     |

|   |                         |                                           |
|---|-------------------------|-------------------------------------------|
| 7 | 工作负荷管理（仅限 Splunk Cloud） | 指定要在哪个池中运行搜索或使用基于策略的池。这些策略在“工作负荷管理”应用中定义。 |
| 8 | 搜索历史                    | 可查看已运行搜索的列表。在您运行首次搜索后，即会显示搜索历史。           |

在 Splunk Enterprise 中，如何搜索中有一个附加选项，称为 **数据摘要**，显示已上载到 Splunk 实例且您有权查看的数据的摘要。还有一个名为 **使用表视图分析数据** 的选项，您可以在其中准备数据而无需使用搜索处理语言 (SPL)。

## 新搜索视图

运行搜索后，“新搜索”视图将打开。

此视图中的一些元素可能会很眼熟，例如应用栏、搜索栏和时间范围挑选器。搜索栏下还有时间线、字段边栏和事件视图。

Splunk Cloud 和 Splunk Enterprise 中的“新建搜索”视图几乎相同。

下图显示了 Splunk Cloud 中的“新搜索”视图。

| 数字 | 元素             | 描述                                                                                    |
|----|----------------|---------------------------------------------------------------------------------------|
| 1  | <b>应用栏</b>     | 在搜索和报表应用中的各个视图间导航：搜索、分析、数据集、报表、告警和仪表板。                                                |
| 2  | <b>搜索栏</b>     | 指定搜索条件。                                                                               |
| 3  | <b>时间范围挑选器</b> | 指定搜索的时间周期。                                                                            |
| 4  | <b>搜索操作按钮</b>  | 您可以执行的操作，包括使用搜索任务、共享、打印和导出搜索结果。                                                       |
| 5  | <b>搜索结果选项卡</b> | 您的搜索结果显示在哪个选项卡取决于您的搜索。一些搜索会生成一组事件，显示在事件选项卡中。另一些搜索会转换事件中的数据以生成搜索结果，这些数据显示在统计数据选项卡上。    |
| 6  | <b>搜索模式菜单</b>  | 使用搜索模式选择器来根据您的需求提供搜索体验。模式包括智能（默认值）、快速和详细。                                             |
| 7  | <b>时间线</b>     | 每个时间点上发生的事件数的虚拟表示。时间线中的高值或低值表示活动高峰或服务器停机。时间线选项位于时间线上方。您可以设置 timescale 格式、缩小或缩放至所选事件组。 |
| 8  | <b>字段边</b>     | 显示事件中发现的字段列表。字段分为已选字段和感兴趣的字段两组。                                                       |

| 栏        |                                                                       |
|----------|-----------------------------------------------------------------------|
| 9 事件查看器  | 显示匹配搜索的事件。默认情况下，最近的事件列在第一位。在每个事件中，匹配的搜索术语会突出显示。要更改事件视图，可使用列表、格式和每页选项。 |
| 10 保存为菜单 | 使用“另存为”菜单将您的搜索结果另存为报表、仪表板面板、告警或事件类型。                                  |

## 下一步

了解在搜索中指定时间范围的相关信息。

## 另请参阅

《搜索手册》中的“[查看搜索历史并与之交互](#)”  
 《数据导入》手册中的“[来源类型为何重要](#)”

## 指定时间范围

使用时间范围限制或筛选您的搜索条件是优化搜索的一种最简单高效的方式。

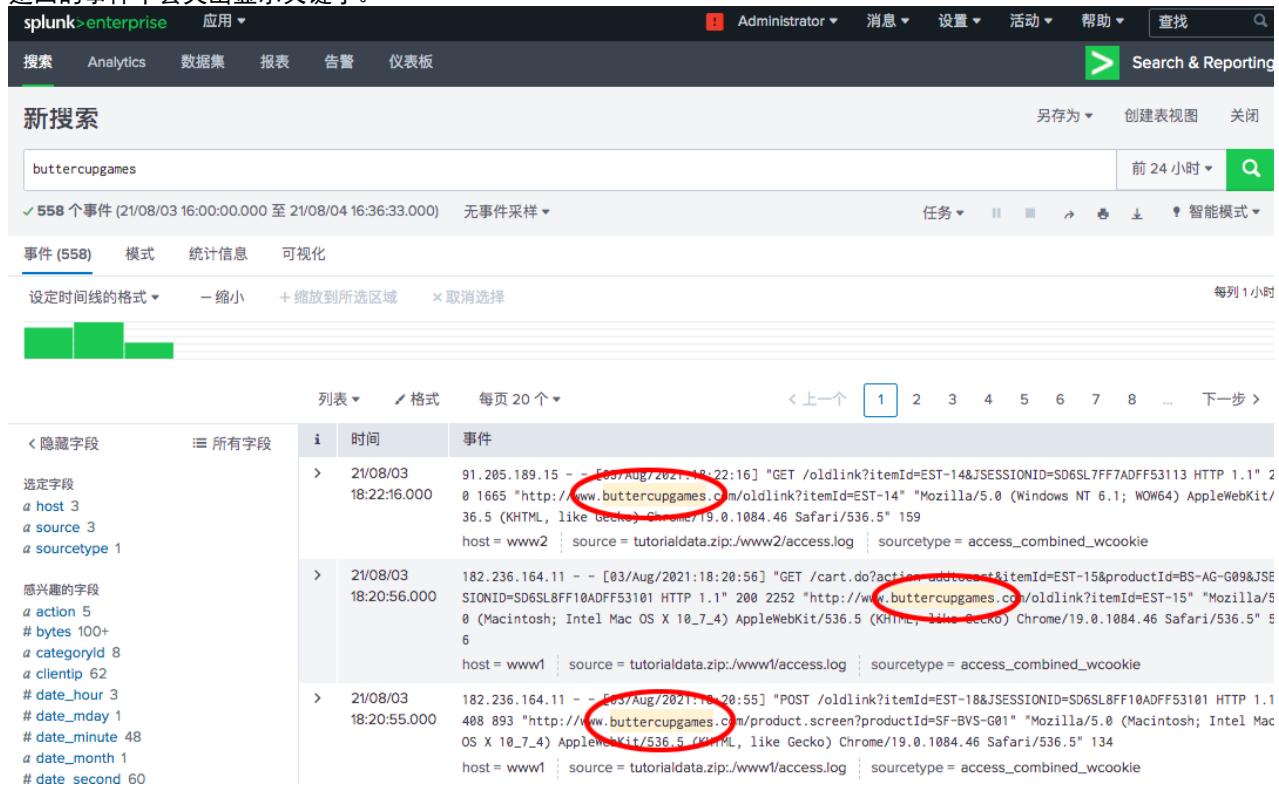
如果您知道问题发生的大致时间范围，您可以使用时间范围解决问题。将搜索时间范围缩小至问题发生的时间范围内即可。例如，要调查前一小时内发生的某事件，您可以选择默认时间范围过去 24 小时，但是最好选择过去 60 分钟。

我们来使用不同时间范围浏览一下 Buttercup Games 在线商店的数据。

1. 要开始新搜索，单击应用栏中的搜索。
2. 要在事件中搜索关键字，在搜索栏中键入 `buttercupgames` 并按 `Enter` 键。

`buttercupgames`

返回的事件中会突出显示关键字。



The screenshot shows the Splunk interface with a search bar containing "buttercupgames". The search results table displays 558 events from August 3rd, 2021, to August 4th, 2021. Three specific log entries are highlighted with red circles:

- First entry: 21/08/03 18:22:16.000 [03/Aug/2021:18:22:16] "GET /oldlink?itemId=EST-14&JSESSIONID=SD6SL7FF7ADFF53113 HTTP 1.1" 91.205.189.15 - - [03/Aug/2021:18:22:16] "GET /oldlink?itemId=EST-14" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 159 host = www2 | source = tutorialdata.zip://www2/access.log | sourcetype = access\_combined\_wcookie
- Second entry: 21/08/03 18:20:56.000 [03/Aug/2021:18:20:56] "GET /cart.do?action=addtocart&itemId=EST-15&productId=BS-AG-G09&JSESSIONID=SD6SL8F10ADFF53101 HTTP 1.1" 200 2252 "http://www.buttercupgames.com/oldlink?itemId=EST-15" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_7\_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 56 host = www1 | source = tutorialdata.zip://www1/access.log | sourcetype = access\_combined\_wcookie
- Third entry: 21/08/03 18:20:55.000 [03/Aug/2021:18:20:55] "POST /oldlink?itemId=EST-18&JSESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 408 893 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_7\_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 134 host = www1 | source = tutorialdata.zip://www1/access.log | sourcetype = access\_combined\_wcookie

请注意，返回的事件有数百个。

使用位于搜索栏右侧的时间范围挑选器在搜索中设置时间界限。默认时间范围为过去 24 小时。您可以将搜索限制为预设的时间范围之一，或使用自定义时间范围。

## 时间范围和教程数据

使用教程数据运行搜索之后，如果没有返回事件，可能是因为您下载 `tutorialdata.zip` 文件的时间已超过一天。下载 ZIP 文件时，会生成时间戳然后添加到数据中。

Buttercup Games 商店的教程数据包括七天的事件。事件的日期是基于您下载教程数据文件的日期。例如，如果您是今天下载文件，事件日期从上一周开始。如果今天是周三，事件的时间戳从上周三开始。昨天的事件是最后的事件。今天没有事件。使用今天或少于 24 个小时的任何时间搜索事件不会返回事件。

对于使用教程数据文件的所有搜索，您需要根据下载教程数据文件的时间调整搜索时间范围。如果您是 3 天前下载教程数据文件，则过去 3 天没有任何事件。可尝试不同的相对时间范围，例如上周或过去 7 天。

## 预设时间范围

时间范围挑选器有很多可供选择的预设时间范围。

1. 单击时间范围挑选器，查看时间范围选项列表。

预设选项包括实时、相对和其他时间范围。

- 实时搜索显示实时连续的事件视图。您可以指定检索事件的窗口。
- 历史搜索显示过去的事件。可以通过指定相对时间范围或指定特定日期和时间范围对搜索加以限制。

由于 Buttercup Games 在线商店的数据是历史数据快照，所以在本教程中，您将不会使用“实时”预设时间范围。



2. 在相对列表中的预设选项中，单击昨天。

返回的事件数量应较大。您已将时间范围由过去 24 小时改为昨天。

## 自定义时间范围

预设的时间范围对您的搜索不够准确时，请使用自定义时间范围。

### 指定相对时间范围

可使用相对选项指定自定义时间范围。

1. 打开时间范围挑选器。
2. 要运行一个时间范围为过去两天的搜索，选择相对时间范围选项。



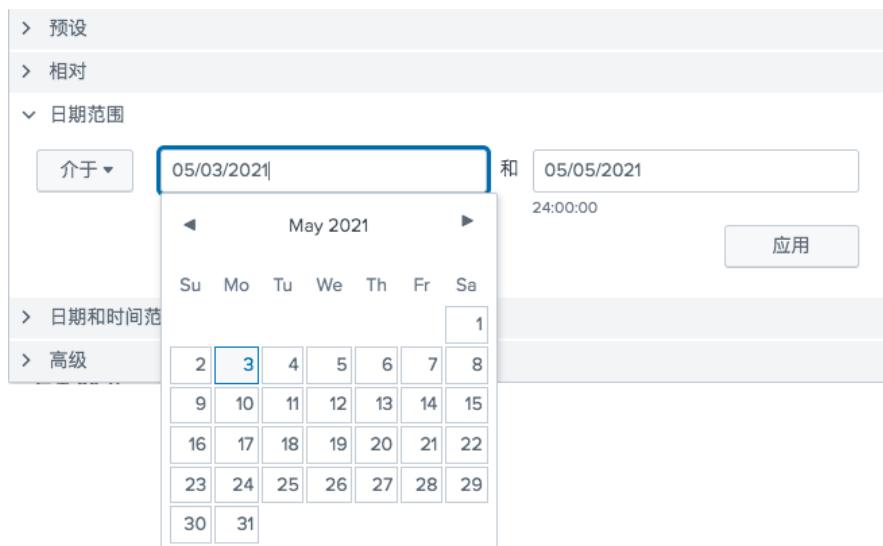
3. 为最早字段键入 2，从下拉列表中选择天前。
4. 对于最晚选项，默认为现在。选择今日的起始时间点。
5. 单击应用。  
单选按钮下方显示的时间戳根据您在相对时间范围列表中的选择进行调整。  
如之前所述，如果没有返回任何事件，请选择其他时间范围，例如 4 天前或 1 周前。

### 指定日期和时间范围

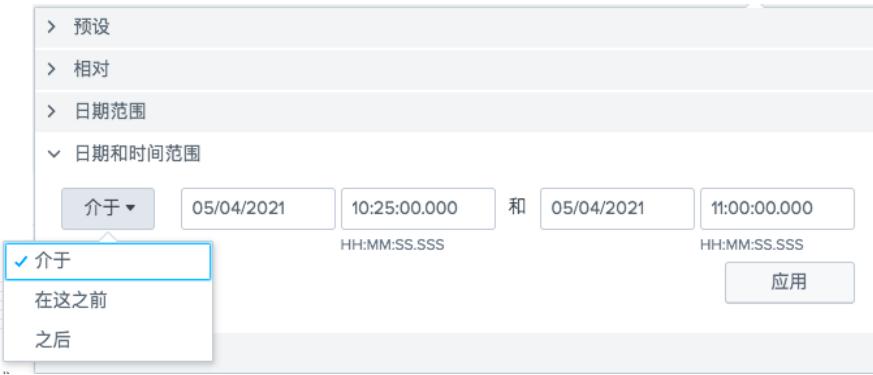
您还可以使用日期范围和日期和时间范围选项指定自定义时间范围。

- 使用介于指定事件发生时间必须介于的最早和最晚日期。
- 使用在此时间之前指定事件发生时间必须早于某日期。
- 使用自此时间起指定事件发生时间必须晚于某日期。

使用日期范围选项指定日期。下面的屏幕图像显示您可用于选择日期的日历。



想要指定日期和时间时可使用日期和时间范围选项。下面的屏幕图像显示“介于”、“之前”或“之后”选项。



例如，要解决发生于 2021 年 5 月 4 日 10:30 的问题，最早时间可指定为 2021 年 5 月 4 日 10:25:00.000，最晚时间可指定为 2021 年 5 月 4 日 11:00:00.000，以显示问题发生前后的事件。

## 下一步

搜索教程的第 3 部分到此结束。

您已浏览了搜索应用视图，并了解了指定搜索时间范围的重要性。继续第 4 部分：搜索教程数据。

## 另请参阅

[《搜索手册》中的“更改默认时间范围”](#)

# 第 4 部分：搜索教程数据

## 基本搜索和搜索结果

在本部分中，您将新建检索索引事件的搜索。

本教程数据针对 Buttercup Games 在线商店。商店出售游戏和其他相关产品，例如 T 恤。本教程主要搜索 Apache Web 访问日志并将访问日志与供应商销售日志进行关联。

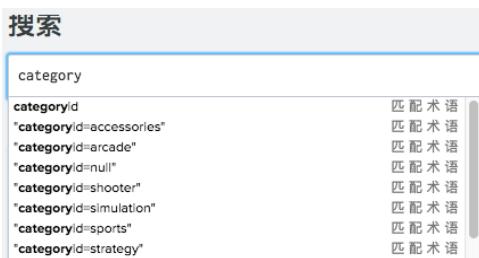
### 前提条件

完成第 2 部分上载教程数据中的步骤。

### 使用搜索助理

搜索助理是搜索应用中的一项功能，在您键入搜索条件时显示。搜索助理如同自动完成，但不仅限于此。

1. 单击应用栏中的**搜索启动新搜索**。
2. 在搜索栏中键入 **buttercup**。  
当您在搜索栏中键入几个字母时，搜索助理会将您的数据中与这些字母相匹配的术语列出来。
3. 单击应用栏中的**搜索启动新搜索**。
4. 在搜索栏中键入 **category**。您看到的术语是教程数据中的。



5. 从搜索助理列表中选择 "**categoryid=sports**"。
6. 按 **Enter**，或单击“搜索”栏右侧的**搜索图标**运行搜索。

| 时间                    | 事件                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 21/08/03 18:04:59.000 | 65.19.167.94 -- [03/Aug/2021:18:04:59] "GET /category.screen?categoryId=SPORTS&JSESSIONID=SD9SL4FF3ADFF53028 HTTP/1.1" 200 1155 "http://www.buttercupgames.com/product.screen?productId=CU-PG-G06" "Mozilla/5.0 (iPad; U; CPU OS 4_3_5 like Mac OS X; en-us) AppleWebKit/533.17.9 (KHTML, like Gecko) Version/5.0.2 Mobile/8L1 Safari/6533.18.5" 421<br>host = www2   source = tutorialdata.zip:/www2/access.log   sourcetype = access_combined_wcookie |
| 21/08/03 18:04:59.000 | 65.19.167.94 -- [03/Aug/2021:18:04:59] "GET /category.screen?categoryId=SPORTS&JSESSIONID=SD9SL4FF3ADFF53028 HTTP/1.1" 200 1155 "http://www.buttercupgames.com/product.screen?productId=CU-PG-G06" "Mozilla/5.0 (iPad; U; CPU OS 4_3_5 like Mac OS X; en-us) AppleWebKit/533.17.9 (KHTML, like Gecko) Version/5.0.2 Mobile/8L1 Safari/6533.18.5" 421<br>host = www2   source = tutorialdata.zip:/www2/access.log   sourcetype = access_combined_wcookie |

### 匹配搜索

搜索助理也会基于您近期所运行的搜索返回匹配的搜索。想要运行昨天或一周前的搜索时，匹配搜索列表就十分有用了。注销后搜索历史将保留。

您开始学习搜索语言后会发现搜索助理具有更多的用途。当您键入搜索命令时，搜索助理会显示命令信息。

### 从索引中检索事件

我们来试着找出 Buttercup Games 网站上发生的错误数量。

要检索提到错误或失败的事件，在搜索条件中键入关键字。如果您使用多个关键字，则必须指定布尔运算符，例如 AND、OR 和 NOT。

键入多个关键字时即暗含 AND 运算符。

例如，键入 `buttercupgames error` 与键入 `buttercupgames AND error` 意思相同。

1. 开始新搜索。
2. 更改时间范围为所有时间。
3. 要在提到 `buttercupgames` 的事件中搜索 `error`、`fail`、`failure`、`failed` 或 `severe` 等术语，运行下列搜索：

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

**提示：**您可以将本教程中的搜索直接复制粘贴到搜索栏中，而不必再键入搜索字符串。

4. 单击时间范围挑选器右侧的搜索图标以运行搜索。

注意：布尔运算符必须大写。星号 (\*) 字符用作通配符以匹配 `fail`、`failure`、`failed` 和 `failing` 等。

在求布尔表达式的值时，括号里的术语优先。NOT 子句先于 OR 子句进行评估。AND 子句的优先级最低。

此搜索检索到 427 个匹配事件。

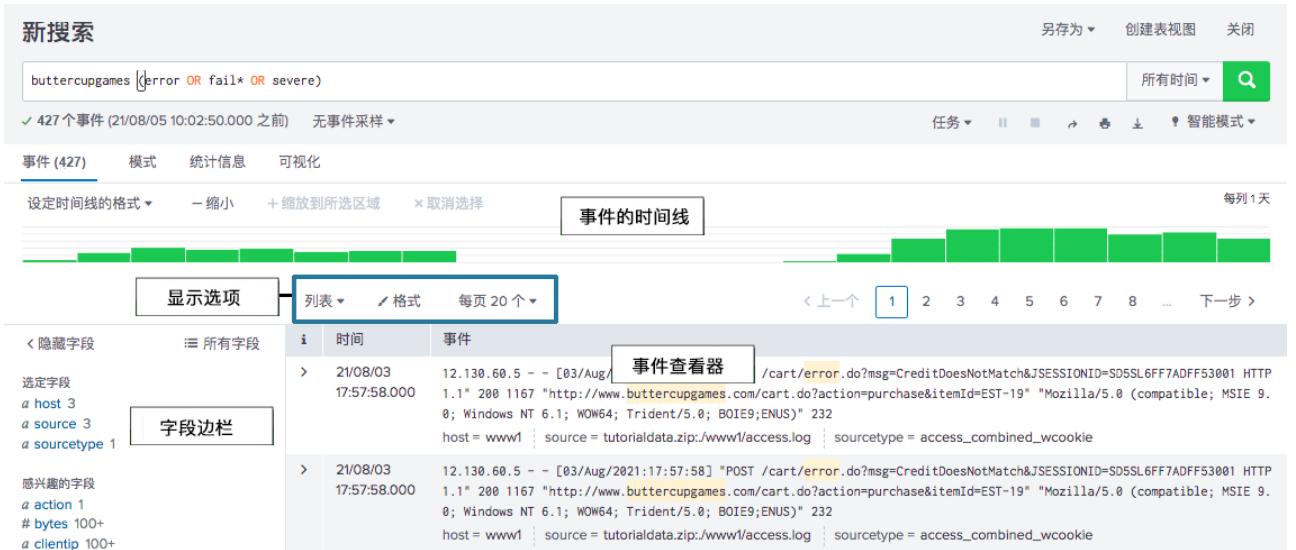
| 时间                    | 事件                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 21/08/03 17:57:58.000 | 12.130.60.5 - - [03/Aug/2021:17:57:58] "POST /cart/error.do?msg=CreditDoesNotMatch&JSESSIONID=SD5SL6FF7ADFF53001 HTTP/1.1" 200 1167 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-19" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 232<br>host = www1   source = tutorialdata.zip:/www1/access.log   sourcetype = access_combined_wcookie |
| 21/08/03 17:57:58.000 | 12.130.60.5 - - [03/Aug/2021:17:57:58] "POST /cart/error.do?msg=CreditDoesNotMatch&JSESSIONID=SD5SL6FF7ADFF53001 HTTP/1.1" 200 1167 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-19" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 232<br>host = www1   source = tutorialdata.zip:/www1/access.log   sourcetype = access_combined_wcookie |

## 理解搜索结果

搜索栏下方有四个选项卡：**事件**、**模式**、**统计**和**可视化**。

搜索结果将显示在哪个选项卡中取决于您使用的搜索命令类型。在本教程的前几部分中，您将用到**事件**选项卡。教程的后面章节中您将了解其他选项卡。

**事件**选项卡显示事件的时间线、显示选项、字段边栏和事件查看器。



默认情况下，事件会从最近期的开始排序，以列表形式显示。在每个事件中，匹配的搜索术语会突出显示。**列表**显示选项以三列显示事件信息。

| 柱形图      | 描述                                                                  |
|----------|---------------------------------------------------------------------|
| <i>i</i> | 使用事件信息列可展开或折叠事件信息的显示。默认情况下，显示为折叠状态。单击大于号 (>) 可展开显示。                 |
| 时间       | 事件的时间戳。为事件编制索引时，将提取事件的时间戳。如果事件不含时间戳，编制索引过程中将添加一个时间戳 - 编制事件索引的日期和时间。 |
| 事件       | 原始事件数据。每个事件下方都将显示字段边栏中的已选字段。                                        |

## 更改事件查看器的显示

### 1. 选择**列表**选项并单击表格。

显示内容改为显示事件信息列、时间戳列及已选字段各列。您将在本教程的后面部分中了解更多已选字段的相关信息。

### 2. 将显示改回**列表**。

## 事件的时间线

事件的时间线是每个时间点发生的事件数的直观展示。时间线随您的搜索结果更新时，存在条形群集或模式。每个条形的高度表示事件的计数。时间线中的高值或低值表示活动高峰或服务器停机。时间线突出显示事件的模式或事件活动中的高值或低值。时间线选项位于时间线上方。您可放大、缩小及更改时间线图表刻度。

## 字段边栏

添加数据到 Splunk 平台之后，即开始索引数据。作为索引流程的一部分，从数据提取信息，并形成格式为名称和值对，称为**字段**。您运行搜索时，搜索结果旁边的字段边栏中将列出所识别的字段。字段分为两类：

- **所选字段**在您的搜索结果中可见。默认情况下，显示主机、数据来源和来源类型。您可以选择要在您的事件中显示的其他字段。
- **感兴趣的字段**是从您的搜索结果的事件中提取的其他字段。

您可以隐藏字段边栏以最大化结果区域。

## 模式、统计和可视化

模式选项卡显示搜索返回的事件组中最常见模式的列表。每个模式都代表着拥有类似结构的事件。

当您使用诸如 `stats`、`top`、`chart` 等的转换命令运行搜索时，**统计**选项卡将填充。此选项卡中未显示 "Buttercupgames" 这一关键字搜索的结果，因为它不含任何转换命令。

使用转换命令的搜索还可填充**可视化**选项卡。**可视化**选项卡的结果区域包含一张图表和用来生成图表的统计表。

您将在本手册的后半部分了解转换命令、使用统计和可视化仪表板等详细信息。

## 下一步

了解使用字段搜索数据。

## 另请参阅

[《搜索手册》中的“使用搜索助理协助构建搜索”](#)

[《搜索手册》中的“通过模式选项卡识别事件模式”](#)

[《数据透视表手册》中的“数据透视表简介”](#)

## 使用字段搜索

要利用 Splunk 软件的高级搜索功能，您必须了解什么是字段以及如何使用字段。

### 什么是字段？

字段以多种形式存在于计算机数据中。通常，字段是一个值，在一行中拥有固定的分隔位置，也可能是一个名称和值对，每个字段名称有一个单个值。字段可为多值字段，即单一事件中的字段在在一个字段中可有多个值。

- 一些字段示例如下：针对访问 Web 服务器的 IP 地址的 `clientip`、针对事件时间戳的 `_time` 以及针对服务器域名的 `host`。
- 多值字段的一个较为常见的示例是电子邮件地址字段。虽然 `From` 字段只包含单一电子邮件地址，但 `To` 和 `Cc` 字段可能具有与其相关的一个或多个电子邮件地址。

字段是可搜索的名称和值对，可区分不同事件。不是所有事件都有相同字段和字段值。可利用字段编写更多定制的搜索以检索您所需的特定事件。

### 提取的字段

Splunk 软件在索引时间和搜索时间从事件数据中提取字段。

#### 索引时间

自 Splunk 软件接收新数据至数据写入索引的时间跨度。在索引时间内，数据将被分析为段和事件。将提取默认字段和时间戳并应用转换。

#### 搜索时间

始于搜索启动、止于搜索完成的时间周期。搜索时间周期内，将进行某些类型的事件处理，例如搜索时间字段提取、设置字段别名、来源类型重命名、事件类型匹配等。

数据建立索引时，将为每个事件提取默认字段和其他索引字段。

## 通过字段进行搜索

搜索字段时，使用语法 `field_name=field_value`。

- 字段名称区分大小写，但字段值不区分大小写。
- 可在字段值中使用通配符。
- 当字段值包含空格时，需要用引号。

尝试进行搜索。

- 单击应用栏中的搜索启动新搜索。请注意时间范围设置返回到默认的过去 24 小时。
- 要针对以 `access_` 开头的所有值搜索来源类型字段，运行下列搜索：

```
sourcetype=access_*
```

此搜索表明您仅仅想要从您的 Web 访问日志检索事件，不想从他处检索。

此搜索在字段值中使用通配符（\*）`access_*` 来匹配任何 Apache web 访问来源类型。来源类型可能为 `access_common`、`access_combined` 或 `access_combined_wcookie`。

**新搜索**

sourcetype=access\_\*

1,948 个事件 (21/08/04 10:00:00.000 至 21/08/05 10:10:46.000) 无事件采样 ▾

任务 | 智能模式

事件 (1,948) 模式 统计信息 可视化

设定时间线的格式 | - 缩小 + 缩放到所选区域 × 取消选择 每列 1 小时

列表 格式 每页 20 个 ▾ 1 2 3 4 5 6 7 8 ... 下一步 >

| 所有字段                                                                                                                                              | i | 时间                       | 事件                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------|---|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 选定字段<br>a host 3<br>a source 3<br>a sourcetype 1                                                                                                  | > | 21/08/04<br>18:22:16.000 | 91.205.189.15 - - [04/Aug/2021:18:22:16] "GET /oldlink?itemId=EST-14&JSESSIONID=SD6SL7FF7ADFF53113 HTTP 1.1" 200 1665<br>"http://www.buttercupgames.com/oldlink?itemId=EST-14" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 159<br>host = www2   source = tutorialdata.zip:/www2/access.log   sourcetype = access_combined_wcookie                                                   |
| 感兴趣的字段<br>a action 5<br># bytes 100+<br>a categoryid 8<br>a clientip 100+<br># date_hour 9<br># date_mday 1<br># date_minute 59<br>a date_month 1 | > | 21/08/04<br>18:22:15.000 | 91.205.189.15 - - [04/Aug/2021:18:22:15] "GET /category.screen?categoryId=SHOOTER&JSESSIONID=SD6SL7FF7ADFF53113 HTTP 1.1" 200 1369<br>"http://www.google.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 779<br>host = www2   source = tutorialdata.zip:/www2/access.log   sourcetype = access_combined_wcookie                                                                    |
|                                                                                                                                                   | > | 21/08/04<br>18:20:56.000 | 182.236.164.11 - - [04/Aug/2021:18:20:56] "GET /cart.do?action=addtocart&itemId=EST-15&productId=BS-AG-G09&JSESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 200 2252<br>"http://www.buttercupgames.com/oldlink?itemId=EST-15" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 506<br>host = www1   source = tutorialdata.zip:/www1/access.log   sourcetype = access_combined_wcookie |

### 3. 在搜索结果中向下滚动事件列表。

如果您熟悉 Apache 日志的 access\_combined 格式，您可能会辨别出每个事件中的一些信息，例如：

- 用户访问网站的 IP 地址。
- 请求页面和引用页面的 URI 和 URL。
- 每个页面请求的 HTTP 状态代码。
- GET 或 POST 页面请求方法。

**新搜索**

sourcetype=access\_\*

1,948 个事件 (21/08/04 10:00:00.000 至 21/08/05 10:10:46.000) 无事件采样 ▾

任务 | 智能模式

事件 (1,948) 模式 统计信息 可视化

设定时间线的格式 | - 缩小 + 缩放到所选区域 × 取消选择 每列 1 小时

列表 格式 每页 20 个 ▾ 1 2 3 4 5 6 7 8 ... 下一步 >

| 所有字段                                                                                                                                              | i | 时间                       | 事件                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------|---|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 选定字段<br>a host 3<br>a source 3<br>a sourcetype 1                                                                                                  | > | 21/08/04<br>18:22:16.000 | 91.205.189.15 - - [04/Aug/2021:18:22:16] "GET /oldlink?itemId=EST-14&JSESSIONID=SD6SL7FF7ADFF53113 HTTP 1.1" 200 1665<br>"http://www.buttercupgames.com/oldlink?itemId=EST-14" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 159<br>host = www2   source = tutorialdata.zip:/www2/access.log   sourcetype = access_combined_wcookie                                                   |
| 感兴趣的字段<br>a action 5<br># bytes 100+<br>a categoryid 8<br>a clientip 100+<br># date_hour 9<br># date_mday 1<br># date_minute 59<br>a date_month 1 | > | 21/08/04<br>18:22:15.000 | 91.205.189.15 - - [04/Aug/2021:18:22:15] "GET /category.screen?categoryId=SHOOTER&JSESSIONID=SD6SL7FF7ADFF53113 HTTP 1.1" 200 1369<br>"http://www.google.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 779<br>host = www2   source = tutorialdata.zip:/www2/access.log   sourcetype = access_combined_wcookie                                                                    |
|                                                                                                                                                   | > | 21/08/04<br>18:20:56.000 | 182.236.164.11 - - [04/Aug/2021:18:20:56] "GET /cart.do?action=addtocart&itemId=EST-15&productId=BS-AG-G09&JSESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 200 2252<br>"http://www.buttercupgames.com/oldlink?itemId=EST-15" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 506<br>host = www1   source = tutorialdata.zip:/www1/access.log   sourcetype = access_combined_wcookie |

这些都是 Buttercup Games 网上商店的事件，您可能会在搜索结果中识别出其他信息和关键字，例如：Arcade、Simulation、productId、categoryId、purchase、addtocart 等等。

事件列表的左侧为字段边栏。当检索和搜索匹配的事件时，字段边栏更新已选字段和感兴趣的字段列表。这些是 Splunk 软件从您的数据中提取的字段。

The screenshot shows the Splunk search interface with a search bar at the top containing 'sourcetype=access\_\*'. Below it, a message says '1,948 个事件 (21/08/04 10:00:00.000 至 21/08/05 10:10:46.000) 无事件采样' and a search button. The main area has tabs for '事件 (1,948)', '模式', '统计信息', and '可视化'. A legend indicates event types: green for '正常' (Normal), yellow for '警告' (Warning), and red for '错误' (Error). The search results table has columns for '时间' (Time), '事件' (Event), and a third column. Two specific log entries are highlighted with red boxes:

```

|> 21/08/04 18:22:16.000 host = www2 | source = tutorialdata.zip://www2/access.log | sourcetype = access_combined_wcookie
|> 21/08/04 18:22:15.000 host = www2 | source = tutorialdata.zip://www2/access.log | sourcetype = access_combined_wcookie

```

首次运行搜索时，已选字段列表中显示默认字段：host、source 和 sourcetype。每个事件中都会显示这些默认字段。

感兴趣的字段是出现在至少 20% 的事件中的字段。

## 指定其他已选字段

您可以指定在已选字段列表中显示其他字段。向已选字段列表添加其他字段后，搜索结果中将显示该字段名称和字段值。

- 要向已选字段列表添加字段，单击字段边栏顶部的所有字段。

“选择字段”对话框显示您事件中的字段列表。值数量列显示事件中每个字段唯一值的数量。由于您的搜索条件指定来源类型，因此来源类型字段只有 1 个值。

### 选择字段

| 在过滤器内全选 |                                     | 取消全选        | 覆盖范围:1% 或以上 | 过滤器  | 提取新字段  |     |
|---------|-------------------------------------|-------------|-------------|------|--------|-----|
| i       | ✓                                   | 字段          |             | 值的数目 | 事件覆盖范围 | 类型  |
| >       | <input checked="" type="checkbox"/> | host        |             | 3    | 100%   | 字符串 |
| >       | <input checked="" type="checkbox"/> | source      |             | 3    | 100%   | 字符串 |
| >       | <input checked="" type="checkbox"/> | sourcetype  |             | 1    | 100%   | 字符串 |
| >       | <input type="checkbox"/>            | JSESSIONID  |             | >100 | 100%   | 字符串 |
| >       | <input type="checkbox"/>            | action      |             | 5    | 50.81% | 字符串 |
| >       | <input type="checkbox"/>            | bytes       |             | >100 | 100%   | 数字  |
| >       | <input type="checkbox"/>            | categoryId  |             | 8    | 43.09% | 字符串 |
| >       | <input type="checkbox"/>            | clientip    |             | >100 | 100%   | 字符串 |
| >       | <input type="checkbox"/>            | date_hour   |             | 6    | 100%   | 数字  |
| >       | <input type="checkbox"/>            | date_mday   |             | 1    | 100%   | 数字  |
| >       | <input type="checkbox"/>            | date_minute |             | 58   | 100%   | 数字  |
| >       | <input type="checkbox"/>            | date_month  |             | 1    | 100%   | 字符串 |
| >       | <input type="checkbox"/>            | date_second |             | 60   | 100%   | 数字  |
| >       | <input type="checkbox"/>            | date_wday   |             | 1    | 100%   | 字符串 |
| >       | <input type="checkbox"/>            | date_year   |             | 1    | 100%   | 数字  |
| >       | <input type="checkbox"/>            | date_zone   |             | 1    | 100%   | 字符串 |
| >       | <input type="checkbox"/>            | file        |             | 13   | 100%   | 字符串 |
| >       | <input type="checkbox"/>            | ident       |             | 1    | 100%   | 字符串 |

列表中含其他默认字段，来源类型特有的字段以及与 Buttercup Games 在线商店相关的字段。

- 除已选字段列表中自动显示的三个默认字段外，还有为数据建立索引时新建的其他默认字段。例如基于事件

- timestamp、以 date\_\* 开头的字段。标识含标点符号的数据的字段是 punct 字段。指定 Splunk 部署中数据位置的字段是 index 字段。
- 其他字段名适用于您搜索的 Web 访问日志。例如 clientip、method 和 status 字段。这些都不是默认字段。它们是在搜索时间提取的。
  - 其他提取字段和 Buttercup Games 网上商店相关。例如 action 和 categoryId 字段。
- 选择 action、categoryId 和 productId 字段，
  - 关闭选择字段对话框。

所选的三个字段出现在字段边栏中的已选字段下。如果所选字段存在于特定事件中，则它们将显示在搜索结果中的该事件下。每个事件可能不会有所有选定的字段，如下图所示。

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

- Search Bar:** sourcetype=access\_\*
- Results Summary:** 1,948 个事件 (21/08/04 10:00:00.000 至 21/08/05 10:10:46.000) 无事件采样 - 前 24 小时
- Event List:** A table showing search results. The first column is '时间' (Time), the second is '事件' (Event). Several rows are highlighted with red boxes, corresponding to the ones in the detailed view below.
- Selected Fields (Left Panel):** action 5, categoryId 8, host 3, productId 16, source 3, sourcetype 1
- Detailed View (Bottom Right):** A modal window for the 'action' field. It shows:
  - 5 值, 50.81% 的事件 (5 values, 50.81% of events)
  - 报表 (Report): 表格显示了值 (Value), 计数 (Count), 和 % (Percentage)。最高的是 purchase (30.85%)。
  - 时段上限值 (Time Range Limit Value): 具有此字段的事件 (Events with this field).
  - 罕见值 (Rare Values): 表格显示了值 (Value), 计数 (Count), 和 % (Percentage)。最高的是 purchase (30.85%).

## 标识字段值

字段边栏显示事件中每个字段唯一值的数量。这些数量与选择字段对话框中显示的数量相同。

- 在已选字段中，注意数字 5 紧邻 action 字段。
- 单击 action 字段。

| 值              | 计数  | %       |
|----------------|-----|---------|
| purchase       | 203 | 30.851% |
| addtocart      | 192 | 29.179% |
| view           | 163 | 24.772% |
| changequantity | 54  | 8.207%  |
| remove         | 46  | 6.991%  |

打开操作字段的字段摘要。

在这组搜索结果中，action 有五个值。超过 50% 的搜索结果中会出现 action 字段。

- 关闭操作字段摘要窗口。
- 查看您添加到已选字段的其他两个字段。categoryId 字段标识 Buttercup Games 在线商店出售的游戏和其他产品的种类。productId 字段包含每种产品的类别编号。
- 滚动查看事件列表。
- i 列包含事件信息，在 i 列中，单击事件旁边的箭头 (>)，展开事件信息。

| 时间                       | 事件                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 21/08/04<br>18:22:16.000 | 91.205.189.15 - - [04/Aug/2021:18:22:16] "GET /oldlink?itemId=EST-14&JSESSIONID=SD6SL7FF7ADFF53113 HTTP 1.1" 200 1665 "http://www.buttercupgames.com/oldlink?itemId=EST-14" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 159 host = www2   source = tutorialdata.zip:/www2/access.log   sourcetype = access_combined_wcookie |
| 21/08/04<br>18:22:15.000 | 91.205.189.15 - - [04/Aug/2021:18:22:15] "GET /category/screen?categoryId=SHOOTER&JSESSIONID=SD6SL7FF7ADFF53113 HTTP 1.1" 200 1369 "http://www.google.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 779                                                                                                                  |

事件操作

| 类型                                  | 字段          | 值                                 | 操作 |
|-------------------------------------|-------------|-----------------------------------|----|
| <input checked="" type="checkbox"/> | category_id | SHOOTER                           | ▼  |
| <input checked="" type="checkbox"/> | host        | www2                              | ▼  |
| <input checked="" type="checkbox"/> | source      | tutorialdata.zip:/www2/access.log | ▼  |
| <input checked="" type="checkbox"/> | sourcetype  | access_combined_wcookie           | ▼  |
| <input type="checkbox"/>            | JSESSIONID  | SD6SL7FF7ADFF53113                | ▼  |
| <input type="checkbox"/>            | bytes       | 1369                              | ▼  |
| <input type="checkbox"/>            | clientip    | 91.205.189.15                     | ▼  |
| <input type="checkbox"/>            | file        | category.screen                   | ▼  |

您可以使用此展开的面板查看特定事件中的所有字段，以及选择或取消选择单个事件各个字段。

## 运行有针对性的搜索

以下示例为使用字段的搜索。

### 搜索购买

从 Buttercup Games 商店中搜索成功的购买。

1. 开始新搜索。
2. 在时间范围挑选器中，从预设列表中选择昨天。
3. 运行以下搜索：

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

此搜索使用 HTTP 状态字段 status 指定成功的请求，并使用 action 字段仅搜索购买事件。

您也可以使用 status!=200 以相同的方式搜索失败的购买交易，这将查找 HTTP 状态代码不等于 200 的所有事件。

4. 将搜索的 status 部分改为 status!=200，重新运行搜索。

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

### 搜索错误

按数据来源不同，事件中设计的错误也不尽相同。要搜索错误，您必须指定这些不同的条件。

使用布尔运算符指定不同的错误条件，使用括号对搜索字符串的各部分进行分组。

1. 开始新搜索。
2. 更改时间范围为所有时间。
3. 运行以下搜索：

```
(error OR fail* OR severe) OR (status=404 OR status=500 OR status=503)
```

4. 单击“已选字段”列表中的数据来源。

此搜索未指定来源类型。搜索将同时检索安全日志文件和 Web 访问日志文件中的事件。

### 搜索特定产品的销售情况

搜索昨天售出了多少模拟型游戏。

1. 更改时间范围为昨天。

如果您下载 `tutorialdata.zip` 文件的时间已超过一天，则不会显示时间戳为昨天的事件。这时，您需要将时间范围挑选器改为所有时间，运行先前的搜索。请观察搜索结果中的日期。使用时间范围挑选器中的日期范围选项指定结果中一个日期。

2. 运行以下搜索：

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

键入搜索时，搜索助理将显示以 "sourcetype" 开头的先前搜索列表。您可以选择之前运行的搜索，以搜索成功的购买行为，然后在该搜索末尾添加 `categoryId=simulation`。

返回的事件计数即为购买的模拟游戏的数量。

3. 查找 Buttercup Games 在线商店售出的每种产品的购买次数。

1. 将 `categoryId=simulation` 从搜索条件中移除，然后重新运行搜索。

2. 单击已选字段列表中的 `categoryId` 字段，定位唯一的 `categoryId` 值。

3. 单击 `categoryId` 名称，如 ACCESSORIES。`categoryId` 已添加到您的搜索，搜索再次自动运行。结果显示该产品的购买数量。

4. 关于上周每天的购买次数，可针对每个时间范围再次运行此搜索。

## 下一步

您可以使用所了解的字段相关知识利用 Splunk 搜索处理语言，以生成统计数据，并构建图表。

我们来了解如何使用搜索语言。

## 另请参阅

《知识管理器手册》中的

[关于字段](#)

[使用默认字段](#)

[当 Splunk® Enterprise 提取字段时](#)

## 使用搜索语言

到目前为止您运行的搜索从 Splunk 索引中检索事件。您被限定为询问那些只能通过返回的事件数回答的问题。

例如，您运行了下列搜索，以确定模拟游戏的售出数量：

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

要查找上周每天售出的数量，必须针对上周每天的数据再次运行此搜索。要了解哪些产品比其他产品更畅销，则需要分别针对八个 `categoryId` 值运行此搜索并比较获得的结果。

Splunk 开发了搜索处理语言 (SPL) 和 Splunk 软件结合使用。SPL 包括所有搜索命令及其函数、参数和子句。一种学习 SPL 语言的方法是使用搜索助理。

## 了解搜索助理

搜索助理有两种模式：紧凑和完整。默认模式是紧凑式。此模式在本教程的基本搜索和搜索结果主题中有所介绍。

本部分向您展示如何更改搜索助理设置。您将使用搜索助理以了解 SPL 并构建搜索。如果您有 Splunk Free 许可证，您无法更改搜索助理模式。请参阅“选择平台”了解 Splunk Trial 和 Splunk Free 许可证之间的区别。

您可以通过帐户菜单修改搜索助理模式：





将“搜索助理”模式更改为“完整”：

1. 在帐户菜单中，选择首选项。
2. 单击 SPL 编辑器。
3. 在搜索助理旁的一般上，单击完整。默认设置是“紧凑”。您可以看出模式中的深灰背景设置的模式。在完整模式下，当您在搜索栏中键入命令时会提供更多信息。
4. 单击应用。

利用完整模式的好处，使用 SPL 命令新建搜索。

1. 单击应用栏中的搜索启动新搜索。
2. 更改时间范围为所有时间。
3. 在搜索栏中键入字母 s。

搜索助理显示匹配搜索和匹配术语列表。此外，还简要介绍了如何执行搜索。

**搜索**

所有时间 搜索

自动打开

智能模式

如何搜索

步骤 1: 检索事件  
最简单的搜索返回与您在搜索栏中键入的术语匹配的事件:

术语: error login  
加引号的短语: "database error"  
布尔运算符: login NOT (error OR fail)  
通配符: fail\*  
字段值: status=404、status!=404 或 status>200

步骤 2: 使用搜索命令  
More advanced searches use commands to transform, filter, and report on the events you retrieved. Use the vertical bar |, or pipe character, to apply a command to the retrieved events.

4. 从匹配搜索列表中选择下列搜索，或在搜索栏中键入搜索。

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

5. **action=purchase** 之后，在搜索栏中键入管道符 ( | )。

管道符表示您将使用命令。管道左侧的搜索结果将用作管道右侧命令的输入。您可以通过搜索命令的系列或管道将某个命令的结果传递到另一个命令。

注意，搜索助理改为显示下一常用命令列表。

## 搜索

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

### 匹配搜索

```
sourcetype=access_* status=200...ame clientip AS "VIP ...
sourcetype=access_* status=200... values(productId) by...
sourcetype=access_* status=200... values(productId) by...
sourcetype=access_* status=200...urchase | top limit=1 ...
```

### 下一常用命令

```
timechart
chart
top
stats
dedup
fields
collect
multikv
regex
rex
```

### 如何搜索

✓ 自动打开

#### 使用搜索命令

更多高级搜索使用命令来转换、过滤以及报告检索的事件。

- 使用竖线或管道符将命令应用到检索的事件:

```
sourcetype=access_* error | top 20 uri
```

- 通过其他命令进一步限制或转换您的搜索结果:

```
sourcetype=access_* error | top 20 uri | search count>5
```

搜索助理将为您建议下一步使用的命令，并向您显示一些示例来帮助您构建搜索。

您希望搜索可以返回 Buttercup Games 在线商店最热卖的产品。

- 在下一常用命令下，选择 `top`。  
`top` 命令会附加到您的搜索字符串上。

## 搜索

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

### 匹配搜索

```
sourcetype=access_* status=200...ame clientip AS "VIP ...
sourcetype=access_* status=200... values(productId) by...
sourcetype=access_* status=200...urchase | top limit=1 ...
```

### 命令历史

```
... | top ESXHost
... | top user
... | top dest_ip
... | top dest_port
... | top limit=1 clientip
```

### 顶部

✓ 自动打开

帮助 [更多](#)

显示字段的最常见值。

### 示例

返回 "url" 字段的 20 个最常见值。

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

返回最高 URL 值。

```
... | top url
```

为每个"主机"返回最高"用户"值。

```
... | top user by host
```

- 在搜索栏中键入 `categoryId`。

下面的搜索即完整的搜索字符串。

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

- 管道符前的搜索条件 `sourcetype=access_* status=200 action=purchase` 从访问控制日志文件中定位成功（HTTP 状态为 200）及购买产品的事件。

- 管道符后的搜索条件 `top categoryId` 采纳定位的事件，为大多数常用值返回 `categoryId` 字段。

- 运行该搜索。  
`top` 命令的结果显示在统计选项卡内。

## 查看“统计”选项卡中的结果

`top` 命令是一个转换命令。转换命令将搜索结果转换为表。使用转换命令生成结果，继而利用这些结果新建可视化，如柱形图、折线图、面积图和饼图。您将在本教程后面的章节中进一步了解可视化。

由于转换命令以表的格式返回搜索结果，因此结果在统计选项卡中显示。

新搜索

sourcetype=access\_\* status=200 action=purchase | top categoryId

23,524 个事件 (21/08/05 10:28:22.000 之前) 无事件采样

任务 智能模式

事件 模式 统计信息 (7) 可视化

每页 20 个 格式 预览

| categoryId  | count | percent   |
|-------------|-------|-----------|
| STRATEGY    | 3614  | 30.367196 |
| ARCADE      | 2227  | 18.712713 |
| TEE         | 1662  | 13.965213 |
| ACCESSORIES | 1561  | 13.116545 |
| SIMULATION  | 1116  | 9.377363  |
| SHOOTER     | 1106  | 9.293337  |
| SPORTS      | 615   | 5.167633  |

在这一“成功购买”搜索中，找到七个不同的 category ID。列表按事件中 category ID 值的频率，按从高到低的顺序显示 category ID 值。

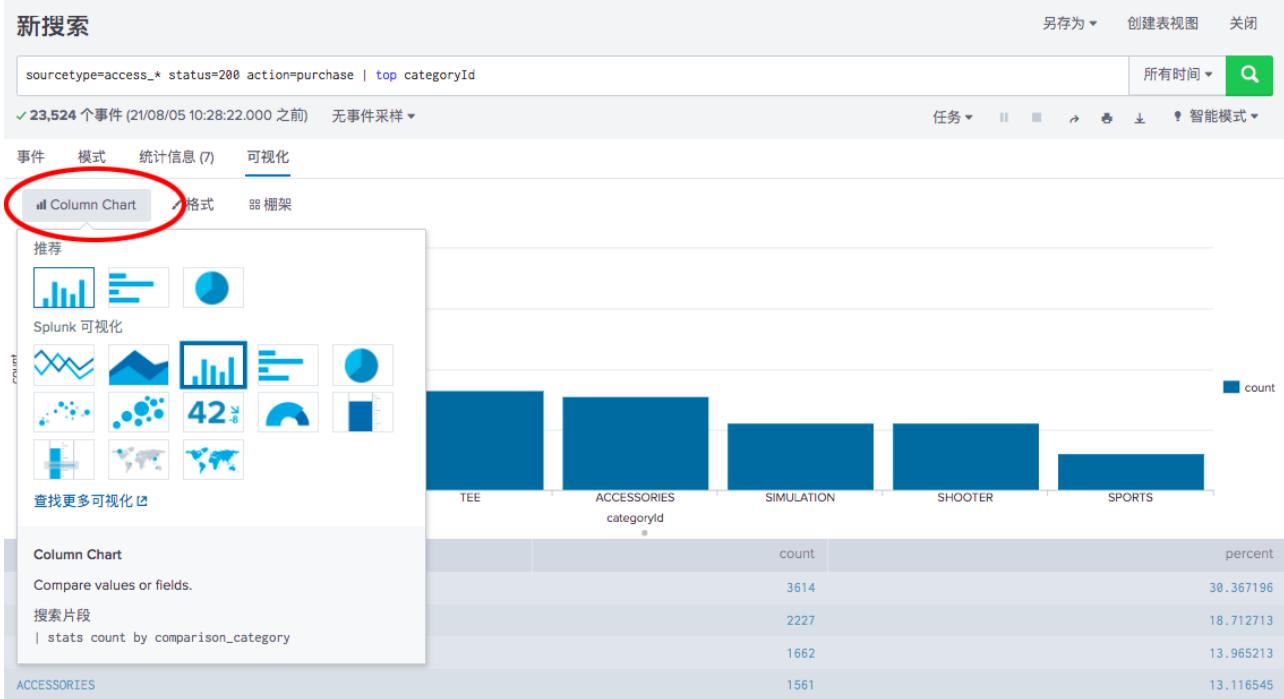
很多转换命令可以返回含有用的统计信息的其他字段。top 命令返回了两个新字段：count 和 percent。

- count 字段表示 categoryId 字段每个值在搜索结果中出现的次数。
- percent 字段表示计数 (count) 占总计数的大小。

## 查看和格式化“可视化”选项卡中的结果

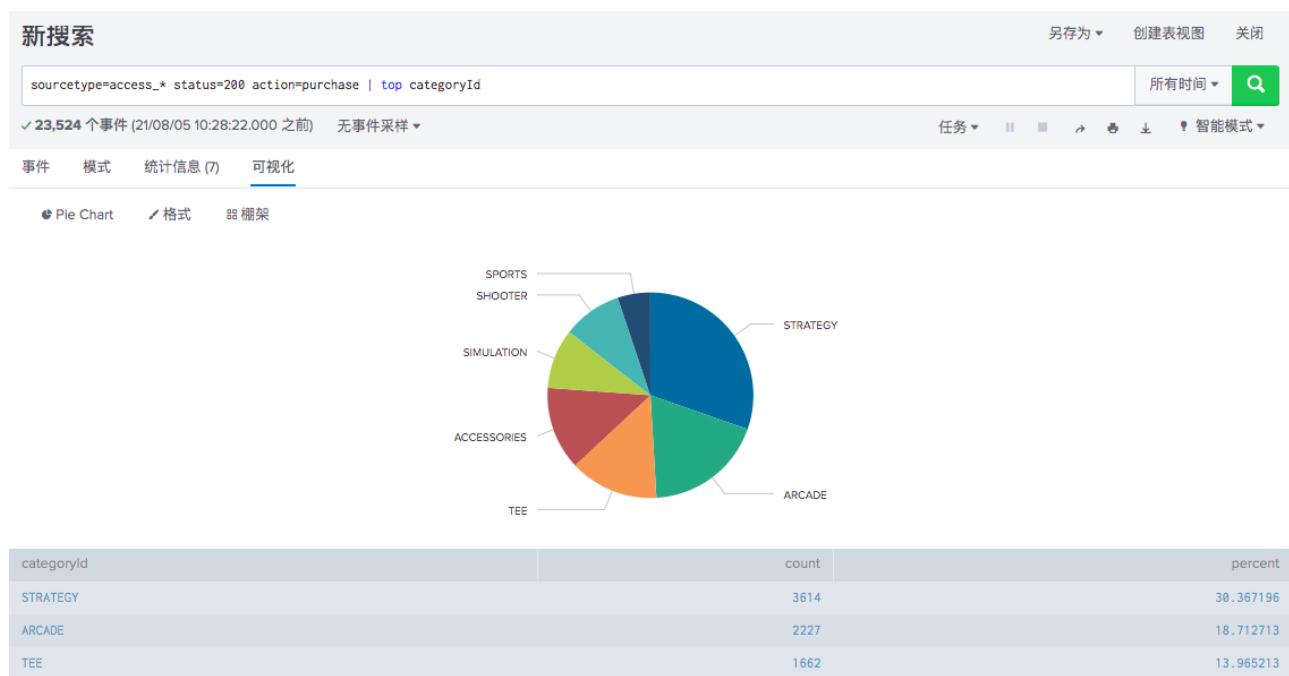
您也可在可视化选项卡中查看转换搜索的结果，此选项卡中也可设置图表类型格式。

1. 单击可视化选项卡。  
默认情况下，可视化选项卡打开时会显示一个柱形图。
2. 单击柱形图，打开可视化类型选择器。

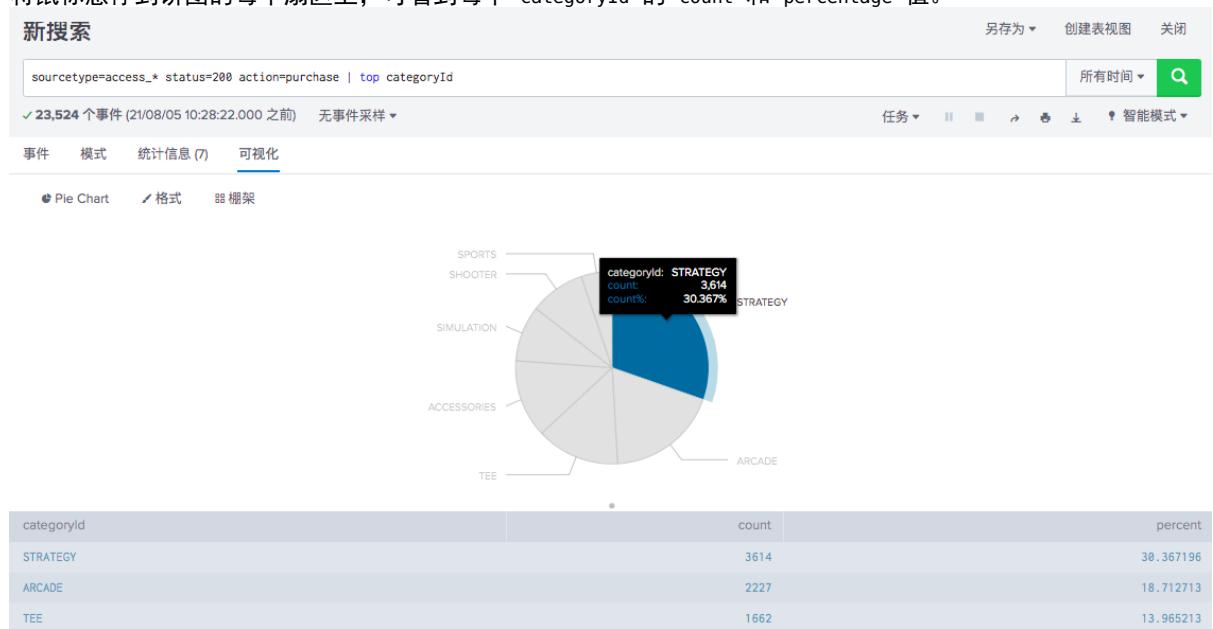


针对这组数据，建议您选择柱形图、条形图和饼图。

3. 选择饼图。  
现在，您的可视化如下饼图所示。

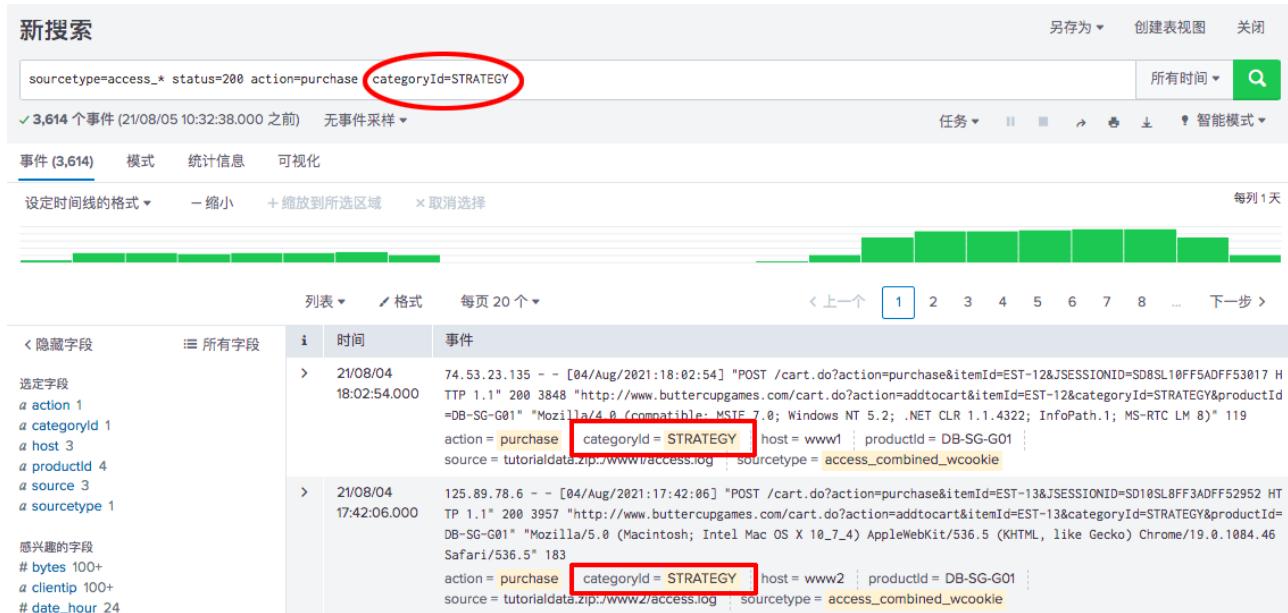


4. 将鼠标悬停到饼图的每个扇区上，可看到每个 categoryId 的 count 和 percentage 值。



5. 单击 STRATEGY 扇区。

categoryId=STRATEGY 添加到您的搜索字符串，替换 top 命令。搜索重新运行。



## 下一步

了解使用子搜索关联事件。

## 另请参阅

《搜索参考》中的 `top` 命令。

仪表板和可视化中的使用仪表板交互钻取

## 使用子搜索

此部分将介绍如何使用子搜索关联事件。

子搜索是用于缩小搜索事件集范围的搜索。子搜索的结果之后将用作主搜索或外部搜索中的一个参数。子搜索包括在方括号中，有一个主要搜索且将第一个进行评估。

我们来找找看 Buttercup Games 网上商店光顾频率最高的一位顾客，以及该顾客的购买情况。

下列示例显示子搜索的重要性。示例 1 显示不使用子搜索的情况下，如何查找最常光顾顾客。示例 2 显示使用子搜索的情况下，如何查找最常光顾顾客。

### 示例 1：不使用子搜索进行搜索

您想要找找看 Buttercup Games 网上商店光顾频率最高的一位顾客，以及该顾客的购买情况。使用 `top` 命令返回最常光顾顾客。

1. 开始新搜索。
2. 更改时间范围为所有时间。
3. 要查找访问在线商店次数最多的顾客，使用此搜索。

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

`limit=1` 参数指定返回 1 个值。`clientip` 参数指定要返回的字段

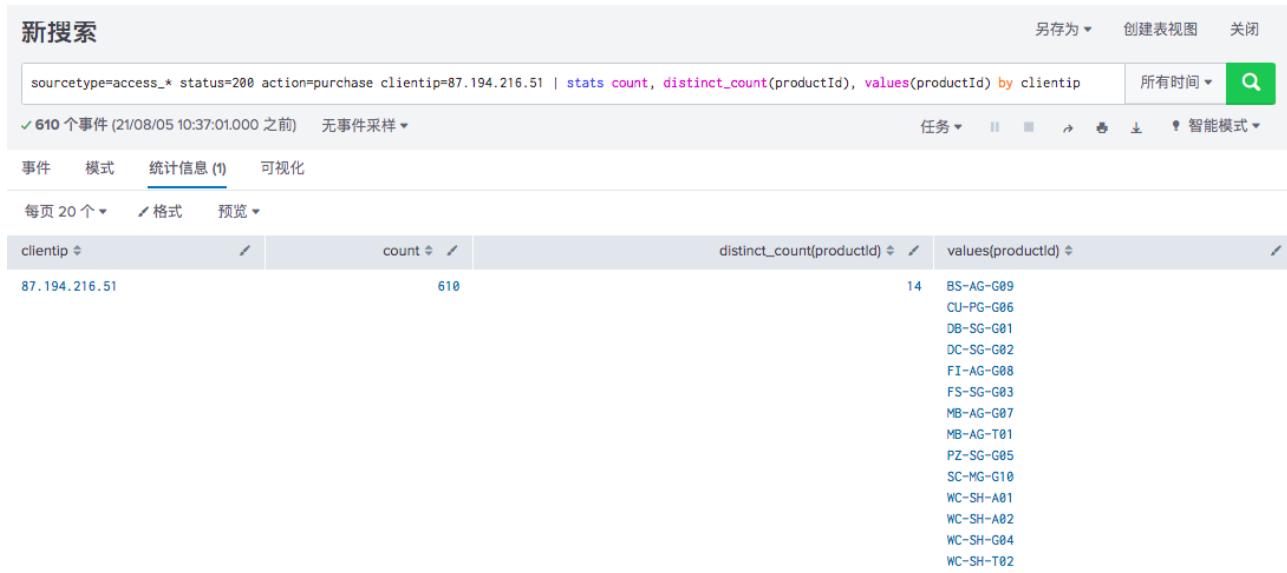


该搜索会返回一个 `clientip` 值 `87.194.216.51`，您将使用此值识别 VIP 客户。搜索还会返回计数和百分比。这些是使用 `top` 命令返回的默认字段。

- 现在，您需要运行另一个搜索，以确定此 VIP 客户购买了多少种不同产品。使用 `stats` 命令统计此 VIP 客户购买的数量。

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

本搜索将使用带有 `stats` 命令的几个统计函数。`distinct_count()` 函数的别名为 `dc()`。



此搜索使用了 `count()` 函数，以返回此 VIP 顾客的购买总数。`dc()` 函数即 `distinct_count` 函数。使用此函数可统计顾客购买的不同或每种产品的数量。`values` 函数用于将非重复产品 ID 作为多值字段。

此方法的缺点在于每次要构建此表格时您就必须运行两个搜索。买得最多的顾客不可能在任何时候都是同一人。

## 示例 2：使用子搜索进行搜索

让我们从第一个要求开始，识别单个 Buttercup Games 在线商店中最常光顾的顾客。

- 将下列搜索复制粘贴到搜索栏并运行此搜索。确保时间范围为所有时间。

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

此搜索会返回最常光顾的顾客的 `clientip` `clientip=87.194.216.51`。这里的搜索基本上与步骤 1 中的示例 1 相同。不同在于最后的管道命令 `| table clientip`，该命令在表中显示 `clientip` 信息。因为您只使用 `table` 命令指定 `clientip` 字段，所以这是唯一返回的字段。将 `top` 命令生成的计数和百分比字段从输出中弃用。

要知道顾客购买了什么东西，在相同的数据上运行搜索。您将提供最常光顾顾客搜索的结果，将此作为购买搜索的标准之一。

最常光顾的顾客搜索变成购买搜索的子搜索。购买搜索指的是外部或主要搜索。由于您在搜索相同的数据，外部搜索的开始和子搜索的开始相同。

子搜索用方括号 [ ] 括起，分析搜索条件时将首先处理子搜索。

2. 将下列搜索复制粘贴到搜索栏并运行此搜索。

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

由于 `top` 命令还返回 `count` 和 `percent` 字段，因此 `table` 命令用于只保留 `clientip` 值。

| clientip      | count | distinct_count(productId) | values(productId)                                                                                                                                                                  |
|---------------|-------|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 87.194.216.51 | 610   | 14                        | BS~AG~G09<br>CU~PG~G06<br>DB~SG~G01<br>DC~SG~G02<br>F1~AG~G08<br>FS~SG~G03<br>MB~AG~G07<br>MB~AG~T01<br>PZ~SG~G05<br>SC~MG~G10<br>WC~SH~A01<br>WC~SH~A02<br>WC~SH~G04<br>WC~SH~T02 |

这些结果应当与示例 1 中的两个搜索结果匹配，前提是您在同一时间范围内运行此搜索。如果您更改了时间范围，则可能会看到不同的结果，因为买得最多的顾客将有所不同。

此子搜索的性能取决于非重复 IP 地址匹配 `status=200` 和 `action=purchase` 的数量。如果有成千上万的非重复 IP 地址，则 `top` 命令必须在 `top 1` 返回之前追踪所有地址，这将影响性能。默认情况下，子搜索最多返回 10,000 个结果，运行时间最多 60 秒。在大型生产环境中，本例中的子搜索可能在完成之前已超时。最佳选择是重写查询，以限制子搜索必须处理的事件数量。或者，您可以增加最大结果数和最大运行时间参数。

### 让搜索语法更易于阅读

子搜索和长的复杂长搜索可能较难于读取。您可以将自动格式应用于搜索语法，使“搜索”栏中的搜索语法更易于阅读。使用以下键盘快捷键将自动格式应用于搜索。

- 对于 Linux 或 Windows 系统，用 `Ctrl + \`。
- 对于 Mac OSX，用 `Command + \`。您还可以使用 `Command + Shift + F`，这在很多非英语键盘上非常好用。

### 让搜索结果更易于理解

您可以通过对列进行重命名，使信息更容易理解。

| 柱形图               | Rename |
|-------------------|--------|
| count             | 购买总数   |
| dc(productId)     | 总产品    |
| values(productId) | 产品 ID  |
| clientip          | VIP 客户 |

通过对搜索中的字段使用 `AS` 操作符对列进行重命名。如果您想要使用的重命名包含空格，则必须用引号将新名括起。

3. 要对字段进行重命名，将下列搜索复制粘贴到搜索栏并运行此搜索。

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

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

- Search Bar:** The search bar contains the command: `sourcetype=access_* status=200 action=purchase [search sourcetype=access_* status=200 action=purchase | top limit=1 clientip | table clientip] | stats count AS "Total Purchased", distinct_count(productId) AS "Total Products", values(productId) AS "Product IDs" by clientip | rename clientip AS "VIP Customer"`. Several parts of this command are highlighted with red boxes: `stats count AS "Total Purchased"`, `distinct_count(productId) AS "Total Products"`, `values(productId) AS "Product IDs"`, and `clientip AS "VIP Customer"`.
- Results Table:** The results table shows the following data:

|               | Total Purchased | Total Products | Product IDs                                                                                                                                                                        | VIP Customer |  |
|---------------|-----------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|--|
| 87.194.216.51 | 610             | 14             | BS-AG-G09<br>CU-PG-G06<br>DB-SG-G01<br>DC-SG-G02<br>FI-AG-G08<br>FS-SG-G03<br>MB-AG-G07<br>MB-AG-T01<br>PZ-SG-G05<br>SC-MG-G10<br>WC-SH-A01<br>WC-SH-A02<br>WC-SH-G04<br>WC-SH-T02 |              |  |

4. 用此搜索试验。当您在不同的时间周期运行搜索时会发生什么？如果您希望找到销售量第一的产品和有多少人购买了该产品，又会如何？

## 下一步

搜索教程的第 4 部分到此结束。

您已经了解如何使用字段、Splunk 搜索语言以及子搜索来搜索数据。继续第 5 部分：用查找丰富事件。

## 另请参阅

- 《搜索手册》中的“关于子搜索”。
- 《搜索参考》中的 `top` 命令。
- 《搜索参考》中的 `stats` 命令。

# 第 5 部分：用查找丰富事件

## 启用字段查找

本教程数据中使用的事件包含带有产品代码和产品 ID 的字段。这些代码和 ID 不会告诉您太多有关产品的信息，如产品名称。能在报表和仪表板中显示实际产品名称对阅读这些报表或仪表板的人而言很有用。这就是需要查找文件的原因。

查找文件包含不经常改变的数据。这可能包括有关顾客、产品、员工、设备等信息。关于此教程，您将使用 CSV 查找文件，其中包括产品 ID、产品名称、常规价格、销售价格和产品代码。

启用字段查找共有五个关键步骤：

1. 上载查找文件
2. 与应用程序共享上载的文件
3. 新建查找定义
4. 与应用程序共享查找定义
5. 可选。自动定义查找

本教程的其余部分取决于您在此部分完成的步骤。  
如果您不配置字段查找，搜索不会生成正确的结果。

## 下载并解压缩教程查找文件

使用教程查找文件，您可以将 Buttercup Games 商店事件中的代码和 ID 与查找文件中的代码和 ID 匹配。该匹配称为字段查找。配置字段查找之后，您可以将查找文件中的任意字段添加到您的搜索中。查找文件有时称为查找表或查找表文件。

1. 下载 Prices.csv.zip 文件。
2. 解压缩 Prices.csv.zip 文件。ZIP 文件中只有一个 prices.csv 文件。

prices.csv 文件包含产品名称、价格和代码。例如：

| productId | product_name      | price | sale_price | 代码 |
|-----------|-------------------|-------|------------|----|
| 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  |

## 找到查找管理器

1. 在 Splunk 栏，单击设置。
2. 在知识部分，单击查找。

以下屏幕截图显示 Splunk Cloud 中的设置菜单。Splunk Enterprise 设置菜单有类似选项。



将打开“查找”管理器，您可以在其中创建新查找或编辑现有查找。

The screenshot shows the Splunk Search Manager interface. It has a header "查找" (Search) and a sub-header "创建和配置查找。" (Create and configure searches). Below this are three main sections: "查找表文件" (Search Tables), "查找定义" (Search Definitions), and "自动查找" (Auto Searches). Each section has a brief description and a "+ 新增" (Add New) button.

- 查找表文件**  
列出现有查找表或上载新文件。  
+ 新增
- 查找定义**  
编辑现有查找定义或定义新的基于文件的查找或外部查找。  
+ 新增
- 自动查找**  
编辑现有自动查找或将新查找配置为自动运行。  
+ 新增

您可以通过单击查找管理器中的链接查看和编辑现有查找。在本教程接下来的几个部分中，您将上载查找表文件、新建查找定义、新建自动查找。

## 上载查找表文件

要使用查找表文件，您必须将文件上传至 Splunk 平台。

1. 在查找管理器中，找到**查找表文件**并单击**新增**。  
您使用新增视图将想要上载的 CSV 文件作为查找表上载。

The screenshot shows the "New" search table file upload form. It includes fields for "目标应用" (Target Application) set to "search", "上载查找文件" (Upload Search File) with a "Choose file" button and "prices.csv" selected, and "目标文件名" (Target File Name) set to "prices.csv". A note below the file name field specifies naming conventions for gzip, CSV, and KMZ/KML files. At the bottom are "取消" (Cancel) and "保存" (Save) buttons.

2. **目标应用** 字段指定您要将查找表文件上传至的应用。要在搜索应用中上载文件，如果尚未选择文件，从列表中选择**搜索**。
3. 在上载查找文件下方，单击**选择文件**并浏览 `prices.csv` 文件。
4. 在**目标文件名**下，键入 `prices.csv`。  
这是您在新建查找定义时将使用的名称。
5. 单击**保存**。  
这会将您的查找文件上载到“搜索”应用中，并显示查找表文件列表。

如果 Splunk 软件不识别或无法上传文件，您可以进行下列操作。

- 检查文件是否为未解压缩。
- 如果有错误消息提示说文件没有换行，文件可能已被破坏。若文件上传前在 Microsoft Excel 中打开过，可能会出现这种情况。您应该删除 `Prices.csv.zip` 和 `prices.csv` 文件，然后重新下载 ZIP 文件并解压缩。

| 查找表文件                                                      |       |        |         |     |         |
|------------------------------------------------------------|-------|--------|---------|-----|---------|
| 新查找表文件                                                     |       |        |         |     |         |
| 已成功已保存了 prices.csv 中的“search”                              |       |        |         |     |         |
| 显示 5 个项目中的 1-5                                             |       |        |         |     |         |
| 应用                                                         | 所有者   | 共享     | 状态      | 操作  | 每页      |
| /opt/splunk/etc/apps/search/lookups/geo_attr_countries.csv | 无所有者  | search | 全局   权限 | 已启用 | 移动   删除 |
| /opt/splunk/etc/apps/search/lookups/geo_attr_us_states.csv | 无所有者  | search | 全局   权限 | 已启用 | 移动   删除 |
| /opt/splunk/etc/apps/search/lookups/geo_countries.kmz      | 无所有者  | search | 全局   权限 | 已启用 | 移动   删除 |
| /opt/splunk/etc/apps/search/lookups/geo_us_states.kmz      | 无所有者  | search | 全局   权限 | 已启用 | 移动   删除 |
| /opt/splunk/etc/users/admin/search/lookups/prices.csv      | admin | search | 专用   权限 | 已启用 | 移动   删除 |

另一个查找表文件和 Splunk 软件一并包含在列表中。

## 共享查找表文件

当您上载查找表文件时，默认共享设置为**专用**。要使用有其他应用程序或特定角色的文件时，您需要将权限更改为文件。本教程中，您将与所有应用程序共享查找表文件。

1. 在查找表文件列表中，找到路径列表最下方的 `prices.csv` 文件。
2. 注意在共享列中，`prices.csv` 已列为**专用**。
3. 要共享查找表文件，单击**权限**。
4. 在权限对话框中的 **Object** 应显示于下方，选择**所有应用**。



5. 单击**保存**。  
`Prices.csv` 查找表的共享设置已设为**全局**。

| 查找表文件                                                      |       |        |         |     |         |
|------------------------------------------------------------|-------|--------|---------|-----|---------|
| 新查找表文件                                                     |       |        |         |     |         |
| 已成功已保存了 prices.csv 中的“search”                              |       |        |         |     |         |
| 显示 5 个项目中的 1-5                                             |       |        |         |     |         |
| 应用                                                         | 所有者   | 共享     | 状态      | 操作  | 每页      |
| /opt/splunk/etc/apps/search/lookups/geo_attr_countries.csv | 无所有者  | search | 全局   权限 | 已启用 | 移动   删除 |
| /opt/splunk/etc/apps/search/lookups/geo_attr_us_states.csv | 无所有者  | search | 全局   权限 | 已启用 | 移动   删除 |
| /opt/splunk/etc/apps/search/lookups/geo_countries.kmz      | 无所有者  | search | 全局   权限 | 已启用 | 移动   删除 |
| /opt/splunk/etc/apps/search/lookups/geo_us_states.kmz      | 无所有者  | search | 全局   权限 | 已启用 | 移动   删除 |
| /opt/splunk/etc/users/admin/search/lookups/prices.csv      | admin | search | 全局   权限 | 已启用 | 移动   删除 |

## 添加字段查找定义

查找表文件与一个应用程序共享还远远不够。您必须定义查找表文件中的信息，以及该信息与事件中字段的联系。这被称为**查找定义**。

1. 在查找表文件对话框中，选择痕迹中的**查找**，以返回到查找管理器。

**查找表文件**

显示 5 个项目中的 1-5

App Search & Reporting (sea) 所有者 任何 在应用中可见 过滤器 搜索 25 每页

| 路径                                                         | 所有者   | App    | 共享      | 状态  | 操作      |
|------------------------------------------------------------|-------|--------|---------|-----|---------|
| /opt/splunk/etc/apps/search/lookups/geo_attr_countries.csv | 无所有者  | search | 全局   权限 | 已启用 | 移动   删除 |
| /opt/splunk/etc/apps/search/lookups/geo_attr_us_states.csv | 无所有者  | search | 全局   权限 | 已启用 | 移动   删除 |
| /opt/splunk/etc/apps/search/lookups/geo_countries.kmz      | 无所有者  | search | 全局   权限 | 已启用 | 移动   删除 |
| /opt/splunk/etc/apps/search/lookups/geo_us_states.kmz      | 无所有者  | search | 全局   权限 | 已启用 | 移动   删除 |
| /opt/splunk/etc/apps/search/lookups/prices.csv             | admin | search | 全局   权限 | 已启用 | 移动   删除 |

2. 在查找定义中，单击新增。
- 随即打开“新增查找定义”页面，您可以在此页面中定义字段查找。
3. 对于目标应用设置，确保已设为搜索以为搜索应用添加查找定义。
4. 为名称键入 `prices_lookup`。
5. 为类型选择基于文件。
6. 基于文件的查找通常是静态表，例如 CSV 文件。
- 对于查找文件，选择 `prices.csv`，即您新建的查找表文件的名称。

**新增**

查找 > 查找定义 > 新增

|                                                                     |               |
|---------------------------------------------------------------------|---------------|
| 目标应用                                                                | search        |
| Name *                                                              | prices_lookup |
| 类型                                                                  | 基于文件          |
| 查找文件 *                                                              | prices.csv    |
| 创建和管理查找表文件。                                                         |               |
| <input type="checkbox"/> 配置基于时间的查找<br><input type="checkbox"/> 高级选项 |               |
| <a href="#">取消</a> <a href="#">保存</a>                               |               |

7. 不要勾选配置基于时间的查找和高级选项的复选框。
8. 单击保存。`Prices_lookup` 现已定义为基于文件的查找。

| 查找定义                             |          |                                                           |                        |       |        |         |          | <a href="#">新查找定义</a>                                        |
|----------------------------------|----------|-----------------------------------------------------------|------------------------|-------|--------|---------|----------|--------------------------------------------------------------|
| <a href="#">查找</a> > 查找定义        |          |                                                           |                        |       |        |         |          |                                                              |
| 已成功已保存了 prices_lookup 中的“search” |          |                                                           |                        |       |        |         |          |                                                              |
| 显示 6 个项目中的 1-6                   |          |                                                           |                        |       |        |         |          |                                                              |
| 名称                               | 类型       | 支持的字段                                                     | 查找文件                   | 所有者   | 应用     | 共享      | 状态       | 操作                                                           |
| dnslookup                        | external | clienthost,clientip                                       |                        | 无所有者  | system | 全局   权限 | 已启用   禁用 | <a href="#">复制</a>                                           |
| geo_attr_countries               | file     | country,region_wb,region_un,subregion,continent,iso2,iso3 | geo_attr_countries.csv | 无所有者  | search | 全局   权限 | 已启用   禁用 | <a href="#">复制</a>                                           |
| geo_attr_us_states               | file     | state_name,state_fips,state_code                          | geo_attr_us_states.csv | 无所有者  | search | 全局   权限 | 已启用   禁用 | <a href="#">复制</a>                                           |
| geo_countries                    | geo      | None                                                      | geo_countries.kmz      | 无所有者  | search | 全局   权限 | 已启用   禁用 | <a href="#">复制</a>                                           |
| geo_us_states                    | geo      | None                                                      | geo_us_states.kmz      | 无所有者  | search | 全局   权限 | 已启用   禁用 | <a href="#">复制</a>                                           |
| prices_lookup                    | file     | productId,product_name,price,sale_price,Code              | prices.csv             | admin | search | 专用   权限 | 已启用   禁用 | <a href="#">复制</a>   <a href="#">移动</a>   <a href="#">删除</a> |

注意“查找定义”页面中支持的字段列。Splunk 软件自动将 CSV 查找表文件中的第一行解释为查找表的字段名称或列标题。

## 与所有应用共享查找定义

您已新建查找定义，现在需要指定想要在哪个应用中使用查找表。

1. 在查找定义列表中，为 prices\_lookup 单击权限。
2. 在权限对话框中的 Object 应显示于下方，选择所有应用。



3. 单击保存。

在查找定义页面中，prices\_lookup 现已拥有全局权限。

您可以使用此字段查找从查找表文件向事件添加信息。通过在搜索中指定 lookup 命令以使用字段查找。或者可设置自动运行字段查找。

## 自动查找

如果您希望向事件应用字段查找，可以将查找设置为自动运行，而无需使用搜索中的 lookup 命令。

1. 在查找表文件对话框中，选择痕迹中的查找，以返回到查找管理器。
2. 在查找管理器中，单击自动查找的新增。

这将带您前往新增自动查找视图，您可在此配置查找以自动运行。

## 新增

查找 > 自动查找 > 新增

目标应用: search  
Name \*: autolookup\_prices  
查找表 \*: prices\_lookup  
应用到: sourcetype  
已命名 \*: access\_combined\_wcookie  
查找输入字段:  =  删除  
+ 添加另一个字段  
查找输出字段:  =  删除  
+ 添加另一个字段  
 重写字段值  
取消 保存

3. 对于目标应用设置，确保已设为搜索以为搜索应用添加自动查找。
4. 为名称键入 `autolookup_prices`。
5. 对于查找表，选择 `prices_lookup`。  
其他选项是随附产品的查找表文件。
6. 应用到的值 `sourcetype` 已选。为已命名键入 `access_combined_wcookie`。

目标应用: search  
Name \*: autolookup\_prices  
查找表 \*: prices\_lookup  
应用到: sourcetype  
已命名 \*: access\_combined\_wcookie

7. 在两个文本框中为查找输入字段键入 `productId`。

查找输入字段是查找表和事件共有的字段。查找输入字段用于关联或链接在事件中有字段的查找表文件中的字段。

- 第一个文本框指定查找表文件中的字段名称。
- 第二个文本框指定事件中的字段名称。

查找表文件有一列 `productId`，其中列出了与事件中 `productId` 字段值匹配的值。

目标应用

Name \*

查找表 \*

应用到

查找输入字段  =  删除

+ 添加另一个字段

8. **查找输出字段**指定要添加到事件数据中的查找表文件中的字段名称。您可以指定不同名称。

查找表文件有多个字段。您将指定要出现在事件中查找表中的两个字段。

1. 在第一个文本框中，键入 `product_name`。这是 `prices.csv` 文件中包含针对每个 `productId` 描述性名称的字段。
2. 在第二个文本框，在等号后面键入 `productName`。这是将在您事件中显示的字段（产品的描述性名称）的名称。
3. 单击 **添加另一个字段**，以在第一个字段后添加另一字段。
4. 在第一个文本框中键入 `price`。这是 `prices.csv` 文件中的字段，该文件中列出了每个 `productId` 的价格。我们为事件中显示的字段使用同一名称。在第二个文本框内键入 `price`。

目标应用

Name \*

查找表 \*

应用到

查找输入字段  =  删除

+ 添加另一个字段

查找输出字段  =  删除

=  删除

+ 添加另一个字段

重写字段值

取消 保存

9. 保持**覆盖字段值**未选中状态。

10. **单击保存**。

显示自动查找视图，列表中显示您配置的查找 `autolookup_prices`。全名是 `access_combined_wcookie : LOOKUP-autolookup_prices`。

自动查找

查找 > 自动查找

已成功已保存了 autolookup\_prices 中的"search"

显示 1 个项目中的 1-1

应用 Search & Reporting (s... 所有者 任何 在应用中可见 过滤器

名称 : 查找 : 所有者 : 应用 : 共享 :

access\_combined\_wcookie : LOOKUP-autolookup\_prices

prices\_lookup productId AS productId OUTPUTNEW price AS price  
product\_name AS productName

所有者: admin 应用: search 共享: 专用 | 权限

## 与所有应用共享自动查找

您已新建自动查找，现在需要指定想要在哪个应用中使用查找表。

1. 在自动查找列表中，对于 `access_combined_wcookie : LOOKUP-autolookup_prices`，单击权限。
2. 在权限对话框中的 `Object` 应显示于下方，选择所有应用。
3. 单击保存。  
在自动查找页面，查找权限现设为全局。

## 下一步

您已设置搜索应用自动从您的查找表定义中检索信息。

现在您可以使用这些查找定义进行搜索。

## 通过字段查找进行搜索

现在您已定义 `prices_lookup`，可在搜索结果中看到该查找中的字段。

### 在您的搜索结果中显示查找字段

由于 `prices_lookup` 是一个自动查找，查找表中的字段将自动显示在搜索结果中。

1. 从自动查找窗口中单击 Splunk 栏中的应用菜单。
2. 单击搜索和报表以返回搜索应用。
3. 更改时间范围为所有时间。
4. 运行下列搜索以定位所有 web 访问活动。

`sourcetype=access_*`

5. 在字段边栏中，滚动查看感兴趣的字段列表，并找出 `price` 字段。  
这一字段已从您新建的自动查找添加到您的事件中。
6. 单击价格以打开该字段的摘要对话框。



摘要对话框包含许多有关价格字段的信息。例如：超过 50% 的事件中出现价格字段。有您可以访问的一组内置报表。已列出几个聚合计算，如平均、最小和标准偏差。与每个价格所出现于的事件数量和百分比。

7. 在已选的旁边，单击是。这将价格字段从字段边栏中的感兴趣的字段列表移到所选字段列表。
8. 关闭对话框。
9. 在字段边栏中，滚动查看感兴趣的字段列表，并找出 productName 字段。
10. 单击 productName 以打开该字段的摘要对话框。
11. 在已选的旁边，单击是。
12. 关闭对话框。

已选字段列表和搜索结果中都列出了 price 和 productName 字段。

注意，不是所有事件都显示 price 和 productName 字段。

| 隐藏字段                                                                                                                                                                                                       | 所有字段 | i | 时间                         | 事件                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 选定字段                                                                                                                                                                                                       |      |   | > 21/08/04<br>18:22:16.000 | 91.205.189.15 - - [04/Aug/2021:18:22:16] "GET /oldlink?itemId=EST-14&JSESSIONID=SD6SL7FF7ADFF53113 HTTP 1.1" 200 1665 "http://www.buttercupgames.com/oldlink?itemId=EST-14" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 159 host = www2   source = tutorialdata.zip:/www2/access.log   sourcetype = access_combined_wcookie                                                                                                                                              |
| # price 9<br># productid 16<br># productName 16                                                                                                                                                            |      |   | > 21/08/04<br>18:22:15.000 | 91.205.189.15 - - [04/Aug/2021:18:22:15] "GET /category.screen?categoryId=SHOOTER&JSESSIONID=SD6SL7FF7ADFF53113 HTTP 1.1" 200 1369 "http://www.google.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 779 categoryId = SHOOTER   host = www2   source = tutorialdata.zip:/www2/access.log   sourcetype = access_combined_wcookie                                                                                                                                        |
| 感兴趣的字段                                                                                                                                                                                                     |      |   | > 21/08/04<br>18:20:56.000 | 182.236.164.11 - - [04/Aug/2021:18:20:56] "GET /cart.do?action=addtocart&itemId=EST-15&productId=BS-AG-G09&JSESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 200 2252 "http://www.buttercupgames.com/oldlink?itemId=EST-15" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 506 action = addtocart   host = www1   price = 24.99 productId = BS-AG-G09 productName = Benign Space Debris source = tutorialdata.zip:/www1/access.log   sourcetype = access_combined_wcookie |
| # bytes 100+<br># clientip 100+<br># date_hour 24<br># date_mday 18<br># date_minute 60<br># date_month 2<br># date_second 60<br># date_wday 7<br># date_year 1<br># date_zone 1<br># file 14<br># ident 1 |      |   | > 21/08/04<br>18:20:55.000 | 182.236.164.11 - - [04/Aug/2021:18:20:55] "POST /oldlink?itemId=EST-18&JSESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 408 893 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 134 host = www1   price = 26.99 productId = SF-BVS-G01 productName = Grand Theft Scooter source = tutorialdata.zip:/www1/access.log   sourcetype = access_combined_wcookie                                            |

## 使用新查找字段搜索

当您设置自动查找时，即指定索引事件中的 productId 字段对应于 prices.csv 文件中的 productId 字段。

当您运行搜索时，Splunk 软件使用此对应关系来检索或查找来自 prices.csv 文件的数据。

这使您能够指定搜索条件中的 productName 和 price 字段。索引字段中不包含产品名称和价格信息。此信息位于查找文件 prices.csv 中。

## 示例：显示产品名称和价格

您可以使用 stats 命令显示 Buttercup Games 产品名称及相应价格列表，输出按产品列出价格的表格。搜索还会使用 AS 关键词和 rename 命令。

## 1. 使用所有时间时间范围内运行以下搜索。

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

The screenshot shows a search interface with the following details:

- Search Query:** sourcetype=access\_\* |stats values(price) AS Price BY productName |rename productName AS "Product Name"
- Results Count:** 177,907 个事件 (21/08/05 13:07:42.000 之前)
- Time Range:** 所有时间
- Table Headers:** Product Name, Price
- Table Data:** A list of products and their prices, such as Benign Space Debris (24.99), Curling 2014 (19.99), Dream Crusher (39.99), Final Sequel (24.99), Fire Resistance Suit of Provolone (3.99), Grand Theft Scooter (26.99), Holy Blade of Gouda (5.99), Manganiello Bros. (39.99), Manganiello Bros. Tee (9.99), Mediocre Kingdoms (24.99), Orvil the Wolverine (39.99), Pony Run (49.99), Puppies vs. Zombies (4.99), SIM Cubicle (19.99), World of Cheese (24.99), and World of Cheese Tee (9.99).

## 示例：显示 VIP 客户的购买情况

本教程有关于搜索的第 4 部分中，您已新建返回 VIP 客户已购买产品的产品 ID 的以下搜索。

```
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"
```

该搜索的结果显示在以下图像中。

**新搜索**

另存为 ▾ 创建表视图 关闭

```
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"
```

所有时间 ▾  Q

✓ 610 个事件 (21/08/05 13:09:04.000 之前) 无事件采样 ▾

任务 ▾ || ■ ▶ ⏪ ⏩ ⏴ ⏵ 智能模式 ▾

事件 模式 统计信息 (1) 可视化

每页 20 个 ▾  格式 预览 ▾

| VIP Customer  | Total Purchased | Total Products | Product IDs                                                                                                                                                                        |
|---------------|-----------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 87.194.216.51 | 610             | 14             | BS-AG-G09<br>CU-PG-G06<br>DB-SG-G01<br>DC-SG-G02<br>FI-AG-G08<br>FS-SG-G03<br>MB-AG-G07<br>MB-AG-T01<br>PZ-SG-G05<br>SC-MG-G10<br>WC-SH-A01<br>WC-SH-A02<br>WC-SH-G04<br>WC-SH-T02 |

这些事件返回产品 ID，因为那是您事件中关于产品的唯一数据。但是现在您已定义了自动查找，可以返回实际产品名称。

1. 确保时间范围设为所有时间。
2. 使用相同的搜索，将值 (`productId`) 改为值 (`productName`)。
3. 运行该搜索。

```
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"
```

结果像之前的搜索一样显示 VIP 顾客的购买。但是，此结果更有意义，因为显示的是查找表中的产品名称，而不是隐晦的产品 ID。

**新搜索**

另存为 ▾ 创建表视图 关闭

```
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"
```

所有时间 ▾  Q

✓ 610 个事件 (21/08/05 13:10:08.000 之前) 无事件采样 ▾

任务 ▾ || ■ ▶ ⏪ ⏩ ⏴ ⏵ 智能模式 ▾

事件 模式 统计信息 (1) 可视化

每页 20 个 ▾  格式 预览 ▾

| VIP Customer  | Total Purchased | Total Products | Product Names                                                                                                                                                                                                                                                                                              |
|---------------|-----------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 87.194.216.51 | 610             | 14             | Benign Space Debris<br>Curling 2014<br>Dream Crusher<br>Final Sequel<br>Fire Resistance Suit of Provolone<br>Holy Blade of Gouda<br>Manganiello Bros.<br>Manganiello Bros. Tee<br>Mediocre Kingdoms<br>Orvil the Wolverine<br>Puppies vs. Zombies<br>SIM Cubicle<br>World of Cheese<br>World of Cheese Tee |

## 下一步

搜索教程的第 5 部分到此结束。

您已经了解了如果在搜索中使用字段查找。在您运行更多的搜索时，您可能需要保存它们，或将其共享给其他人。继续第 6 部分：新建报表和图表。

## 另请参阅

《知识管理员手册》中的“关于查找”

# 第 6 部分：新建报表和图表

## 保存和共享您的报表

在本教程的前几部分中，您学习了使用 Splunk 软件进行搜索的基础，如何使用子搜索以及如何从查找表添加字段。第 6 部分将介绍如果保存和共享您的搜索，详细了解搜索示例。

本教程的其余部分取决于您在“启用字段查找”部分完成的步骤。  
如果您不配置字段查找，搜索不会生成正确的结果。

### 将搜索保存为报表

保存搜索即会新建报表。新建报表后，可通过报表进行更多操作。

1. 选择时间范围过去 7 天并运行以下搜索。  
这是您在通过字段查找进行搜索部分中运行的相同搜索。

```
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"
```

如果您的搜索没有返回结果，请增加搜索时间范围。例如，可以基于时间范围过去 30 天或所有时间运行此搜索。

2. 在搜索栏上方，单击另存为，并选择报表。

The screenshot shows a search results page for a search titled "VIP Customer". The search bar contains the complex query provided above. The results table has three columns: "VIP Customer", "Total Purchased", and "Product Names". There are 378 events from July 29 to August 5, 2014. The "Product Names" column lists 14 items, which are: Benign Space Debris, Curling 2014, Dream Crusher, Final Sequel, Fire Resistance Suit of Provolone, Holy Blade of Gouda, Manganiello Bros., Manganiello Bros. Tee, Mediocre Kingdoms, Orvil the Wolverine, Puppies vs. Zombies, SIM Cubicle, World of Cheese, and World of Cheese Tee.

| VIP Customer  | Total Purchased | Product Names                                                                                                                                                                                                                                                                                                 |
|---------------|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 87.194.216.51 | 378             | 14 Benign Space Debris<br>Curling 2014<br>Dream Crusher<br>Final Sequel<br>Fire Resistance Suit of Provolone<br>Holy Blade of Gouda<br>Manganiello Bros.<br>Manganiello Bros. Tee<br>Mediocre Kingdoms<br>Orvil the Wolverine<br>Puppies vs. Zombies<br>SIM Cubicle<br>World of Cheese<br>World of Cheese Tee |

3. 在“另存为报表”对话框中，为标题键入 VIP Customer。
4. 为描述键入 Buttercup Games most frequent shopper。

## 另存为报表

标题: VIP Customer  
描述: Buttercup Games most frequent shopper  
内容: 统计表  
时间范围挑选器: 是  
取消 保存

### 5. 为时间范围挑选器单击是。

在报表中包含时间范围挑选器后，您可以选择以不同时间范围运行报表。

### 6. 单击保存。

随即将打开一个确认对话框，确认报表已新建：在此对话框中，您可以执行下列操作。

- 继续编辑。优化搜索和报表格式。
- 添加到仪表板。允许您将报表添加到一个新的或已有的仪表板中。
- 查看。查看报表。

### 7. 单击查看。

您指定的标题和描述显示在报表顶部。时间范围挑选器也在报表顶部。如果您为搜索指定一些其他时间范围，该时间范围会出现在报表中。

VIP Customer  
Buttercup Games most frequent shopper  
前 7 天  
378 个事件 (21/07/29 13:00:00.000 至 21/08/05 13:11:30.000)  
1 result 每页 20 个  
时间范围挑选器

| VIP Customer  | Total Purchased | Total Products | Product Names                                                                                             |
|---------------|-----------------|----------------|-----------------------------------------------------------------------------------------------------------|
| 87.194.216.51 | 378             | 14             | Benign Space Debris<br>Curling 2014<br>Dream Crusher<br>Final Sequel<br>Fire Resistance Suit of Provolone |

## 查看和编辑报表

您可以查看和编辑已保存的报表。可从报表中直接编辑报表。

### 1. 单击 VIP 客户报表中的编辑。

您可以在搜索视图中打开报表，或编辑报表描述、权限、计划和加速。您也可以从本菜单中复制、嵌入和删除本报表。

VIP Customer  
Buttercup Games most frequent shopper  
前 7 天  
378 个事件 (21/07/29 13:00:00.000 至 21/08/05 13:11:30.000)  
1 result 每页 20 个  
时间范围挑选器

| VIP Customer  | Total Purchased | Total Products | Product Names                                                                                             |
|---------------|-----------------|----------------|-----------------------------------------------------------------------------------------------------------|
| 87.194.216.51 | 378             | 14             | Benign Space Debris<br>Curling 2014<br>Dream Crusher<br>Final Sequel<br>Fire Resistance Suit of Provolone |

### 2. 单击更多信息可查看报表相关信息。

在更多信息菜单中，您可以查看并编辑报表的不同属性，包括其计划、加速、权限和嵌入。

新建者 ..... 由 [搜索](#) 新建。  
应用 ..... search  
计划 ..... 未计划。 [编辑](#)  
操作 ..... 0 操作  
加速 ..... 已禁用。 [编辑](#)  
权限 ..... 专用。由 admin 拥有。 [编辑](#)  
已修改 ..... 2021/08/05 13:13:28  
嵌入 ..... 已禁用。 [编辑](#)

### 3. 查看时间范围挑选器，它位于窗口左上角。

时间范围挑选器允许您更改时间段来运行此搜索。例如，您可以选择“预设时间范围”或“定义自定义时间范围”，使用时间范围挑选器来为 VIP 客户运行本周、过去 60 分钟或过去 24 小时的搜索。

**VIP Customer**  
Buttercup Games most frequent shopper

所有时间 ▾

预设

| 实时        | 相对    | 其他       |
|-----------|-------|----------|
| 30 秒窗口    | 今天    | 前 15 分钟  |
| 1分钟窗口     | 一周迄今  | 前 60 分钟  |
| 5分钟窗口     | 工作周迄今 | 过去 4 小时  |
| 30 分钟窗口   | 一个月迄今 | 过去 24 小时 |
| 1小时窗口     | 年度迄今  | 过去 7 天   |
| 所有时间 (实时) | 昨天    | 过去 30 天  |
|           | 前一周   |          |
|           | 前一工作周 |          |
|           | 上月    |          |
|           | 上一年   |          |

> 相对  
> 实时  
> 日期范围  
> 日期和时间范围  
> 高级

Product Names ▾

- Benign Space Debris
- Curling 2014
- Dream Crusher
- Final Sequel
- Fire Resistance Suit of Provolone
- Holy Blade of Gouda
- Manganiello Bros.
- Manganiello Bros. Tee
- Mediocre Kingdoms
- Orvil the Wolverine
- Puppies vs. Zombies
- SIM Cubicle
- World of Cheese
- World of Cheese Tee

## 查找和共享报表

您可以使用应用栏访问报表。

### 1. 单击报表打开报表页面并查看报表列表。

搜索 Analytics 数据集 报表 告警 仪表板 > Search & Reporting

**报表**

报表基于单个搜索且可能包括可视化、统计信息和/或事件。单击名称可查看报表。在数据透视表或搜索中打开报表，以优化参数或进一步浏览数据。

| 所有                                | 您的        | 此应用的    | 过滤器    |        |    |
|-----------------------------------|-----------|---------|--------|--------|----|
| 7 报表                              |           |         |        |        |    |
| <i>标题</i>                         | 操作        | 下一次计划时间 | 所有者    | 应用     | 共享 |
| > Errors in the last 24 hours     | 在搜索中打开 编辑 | 无       | nobody | search | 应用 |
| > Errors in the last hour         | 在搜索中打开 编辑 | 无       | nobody | search | 应用 |
| > License Usage Data Cube         | 在搜索中打开 编辑 | 无       | nobody | search | 应用 |
| > Messages by minute last 3 hours | 在搜索中打开 编辑 | 无       | nobody | search | 应用 |
| > Orphaned scheduled searches     | 在搜索中打开 编辑 | 无       | nobody | search | 应用 |
| > Splunk errors last 24 hours     | 在搜索中打开 编辑 | 无       | nobody | search | 应用 |
| > VIP Customer                    | 在搜索中打开 编辑 | 无       | admin  | search | 专用 |

在保存报表时，共享即设置为专用，只有您可以查看和编辑报表。通过更改报表权限，可以允许其他应用查看或编辑，或者查看并编辑报表。

### 2. 在 VIP 客户报表的操作下，单击编辑。

3. 选择编辑权限。



4. 在“编辑权限”对话框中，将为...显示设置为应用。  
显示内容展开，显示更多设置。  
5. 为每个人勾选读取下的复选框。  
这一操作会为可访问此应用的每个人提供查看报表的权限。

编辑权限

报表 VIP Customer

所有者 admin

应用 search

显示

以.....身份运行

[了解更多信息](#)

|                    | 读取                                  | 写入                       |
|--------------------|-------------------------------------|--------------------------|
| 每个人                | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| admin              | <input type="checkbox"/>            | <input type="checkbox"/> |
| can_delete         | <input type="checkbox"/>            | <input type="checkbox"/> |
| power              | <input type="checkbox"/>            | <input type="checkbox"/> |
| securegateway      | <input type="checkbox"/>            | <input type="checkbox"/> |
| splunk-system-role | <input type="checkbox"/>            | <input type="checkbox"/> |
| user               | <input type="checkbox"/>            | <input type="checkbox"/> |

6. 单击保存。  
报表页面显示。VIP 客户报表的共享设置现在为应用，而不是专用。

搜索 Analytics 数据集 报表 告警 仪表板

Search & Reporting

## 报表

报表基于单个搜索且可能包括可视化、统计信息和/或事件。单击名称可查看报表。在数据透视表或搜索中打开报表，以优化参数或进一步浏览数据。

| 所有       | 您的                              | 此应用的      | 过滤器 | 搜索               |
|----------|---------------------------------|-----------|-----|------------------|
| <b>i</b> | <b>标题</b>                       |           |     |                  |
| >        | Errors in the last 24 hours     | 在搜索中打开 编辑 | 无   | nobody search 应用 |
| >        | Errors in the last hour         | 在搜索中打开 编辑 | 无   | nobody search 应用 |
| >        | License Usage Data Cube         | 在搜索中打开 编辑 | 无   | nobody search 应用 |
| >        | Messages by minute last 3 hours | 在搜索中打开 编辑 | 无   | nobody search 应用 |
| >        | Orphaned scheduled searches     | 在搜索中打开 编辑 | 无   | nobody search 应用 |
| >        | Splunk errors last 24 hours     | 在搜索中打开 编辑 | 无   | nobody search 应用 |
| >        | VIP Customer                    | 在搜索中打开 编辑 | 无   | admin search 应用  |

## 下一步

我们来浏览一些其他搜索示例，尝试使用图表可视化及将搜索保存为报表，从新建基本图表开始。

## 另请参阅

《报表手册》中的

关于报表  
加速报表

## 新建基本图表

在此示例中，您通过计算客户在线上商城网站所采取的操作的相关信息比较用户操作的计数。

- 查看每种产品的次数
- 将每种产品添加至购物车的次数
- 购买每种产品的次数

### 前提条件

这些示例需要“启用字段查找”部分的 productName 字段。您必须先完成所有这些步骤，然后再继续了解本部分。如果您不配置字段查找，搜索不会生成正确的结果。

### 步骤

1. 开始新搜索。
2. 时间范围设为所有时间。
3. 运行以下搜索：

```
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"
```

本搜索运用 chart 命令来计算 action=purchase 和 action=addtocart 的事件数。搜索随后使用 rename 命令重命名结果中显示的字段。

chart 命令是一个转换命令。搜索结果显示在统计信息选项卡内。

**新搜索**

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"

154,315 个事件 (21/08/05 13:32:57:000 之前) 无事件采样 ▾

另存为 ▾ 创建表视图 关闭

所有时间 ▾

任务 ▾

事件 模式 统计信息 (14) 可视化

每页 20 个 ▾ 格式 预览 ▾

| Product Name                      | Views | Adds to Cart | Purchases |
|-----------------------------------|-------|--------------|-----------|
| Benign Space Debris               | 5834  | 1225         | 605       |
| Curling 2014                      | 6004  | 1184         | 615       |
| Dream Crusher                     | 8756  | 1890         | 926       |
| Final Sequel                      | 7823  | 1804         | 891       |
| Fire Resistance Suit of Provolone | 8458  | 1794         | 846       |
| Holy Blade of Gouda               | 7160  | 1533         | 715       |
| Manganiello Bros.                 | 8134  | 1796         | 953       |
| Manganiello Bros. Tee             | 8673  | 1866         | 938       |
| Mediocre Kingdoms                 | 10002 | 2154         | 1068      |
| Orvil the Wolverine               | 6539  | 1411         | 669       |
| Puppies vs. Zombies               | 6658  | 1338         | 729       |
| SIM Cubicle                       | 10198 | 2176         | 1116      |
| World of Cheese                   | 10323 | 2291         | 1106      |
| World of Cheese Tee               | 6639  | 1377         | 724       |

4. 单击可视化选项卡。搜索结果以饼图形式显示。
5. 将显示形式更改为柱形图。



## 下一步

新建一个叠加图表并浏览可视化选项

## 另请参阅

《搜索参考》中的 chart 命令  
《搜索参考》中的重命名命令  
《搜索手册》中的“转换命令”

## 新建一个叠加图表并浏览可视化选项

在此示例中，您新建将两个数据系列叠加为行，三个数据系列叠加为列的图表。叠加图将在以一种图表显示“操作”，如添加到购物车和购买，以另一种图表显示转化率，如购买视图。

您将使用 stats 命令以对用户操作进行计数。eval 命令用于计算这些操作的转换率。例如，查看产品的人将产品添加到购物车的频率。

这一示例使用来自此教程“启用字段查找”部分中的 productName 字段。  
如果您不配置字段查找，本部分中的搜索不会生成正确的结果。

让我们从运行搜索和以图表形式查看结果开始。

1. 开始新搜索。
2. 更改时间范围为所有时间。
3. 运行以下搜索：

```
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"
```

eval 命令用于定义两个新字段。这些字段包含转换率。

- 查看购买比字段计算查看产品的客户的数量与购买产品的客户的数量比。计算结果返回一个百分比。
- cartToPurchases 字段计算将产品添加至购物车的客户数量与购买产品的客户的数量比。计算结果返回一个百分比。

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

```
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 results table displays 154,315 events from August 5, 2011, at 13:35:04.000. The table has six columns: Product Name, Views, Adds To Cart, Purchases, viewsToPurchases, and cartToPurchases. The table lists various products with their respective statistics.

| Product Name                      | Views | Adds To Cart | Purchases | viewsToPurchases   | cartToPurchases    |
|-----------------------------------|-------|--------------|-----------|--------------------|--------------------|
| Benign Space Debris               | 5834  | 1225         | 605       | 10.3702434007542   | 49.38775510204081  |
| Curling 2014                      | 6004  | 1184         | 615       | 10.243171219187207 | 51.942567567567565 |
| Dream Crusher                     | 8756  | 1890         | 926       | 10.57560529922339  | 48.99470899470899  |
| Final Sequel                      | 7823  | 1804         | 891       | 11.389492522050364 | 49.390243902439025 |
| Fire Resistance Suit of Provolone | 8458  | 1794         | 846       | 10.002364625206905 | 47.15719063545151  |
| Holy Blade of Gouda               | 7160  | 1533         | 715       | 9.986033519553072  | 46.64057403783431  |
| Manganiello Bros.                 | 8134  | 1796         | 953       | 11.716252766166708 | 53.062360801781736 |
| Manganiello Bros. Tee             | 8673  | 1866         | 938       | 10.815173527037935 | 50.26795284038011  |
| Mediocre Kingdoms                 | 10002 | 2154         | 1068      | 10.677864427114576 | 49.58217270194986  |
| Orvil the Wolverine               | 6539  | 1411         | 669       | 10.230922159351582 | 47.41318214032601  |
| Puppies vs. Zombies               | 6658  | 1338         | 729       | 10.949234004205467 | 54.48430493273543  |
| SIM Cubicle                       | 10198 | 2176         | 1116      | 10.943322220043147 | 51.28676470588235  |
| World of Cheese                   | 10323 | 2291         | 1106      | 10.713939746197811 | 48.275862068965516 |

4. 单击可视化选项卡。

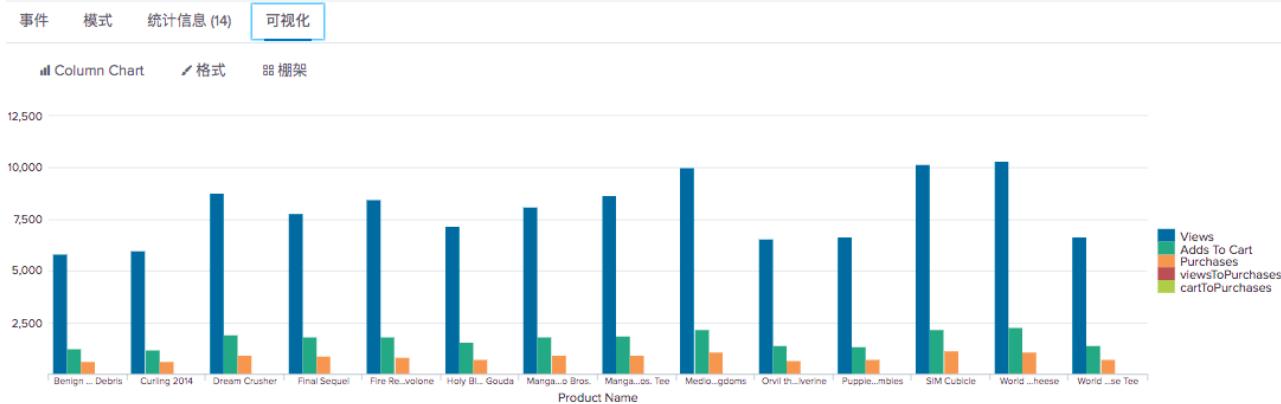
这是“新建基本图表”部分中的同一图表，还有两个其他数据系列，viewsToPurchases 和 cartToPurchases。

新搜索

```
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"
```

154,315 个事件 (21/08/05 13:35:04.000 之前) 无事件采样 ▾

另存为 ▾ 创建表视图 关闭 所有时段 ▾   搜索



接下来的几个步骤将重新组织图表可视化的格式，已将转换比例的两个数据系列覆盖到操作的三个数据系列之上。

## 设置 X 轴标签格式

注意 X 轴上的标签被截断。因为产品太多导致标签被截断加大读取困难。让我们来解决这个问题。

1. 单击格式和 X 轴。
2. 如果是标签旋转，选择第二个选项，即 -45 度。

事件 模式 统计信息 (14) 可视化

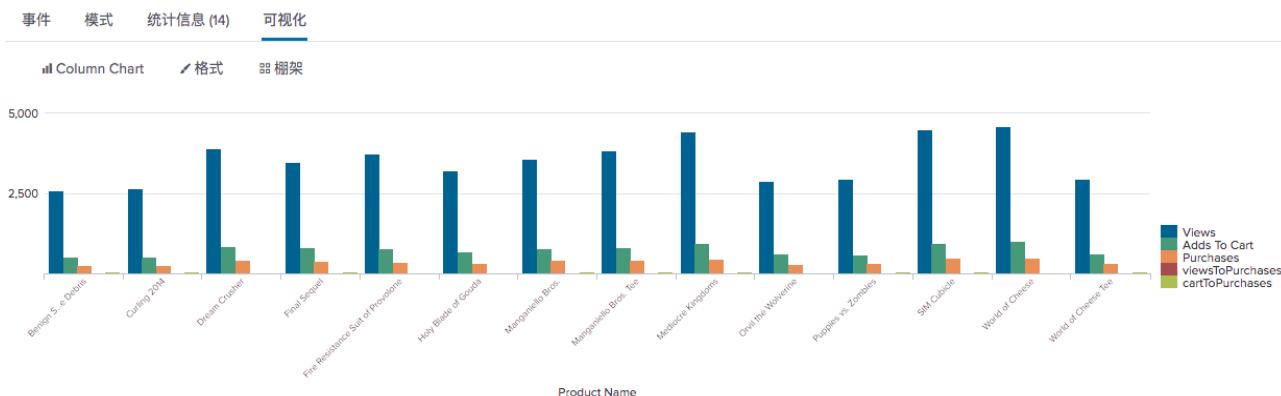
Column Chart 格式 框架

常规 X轴 Y轴 图例

标题：默认  
X轴：45° abc  
Y轴：  
标签旋转：abc  
标签截断：是 否

3. 关闭格式对话框。

注意 X 轴上标签的变化。



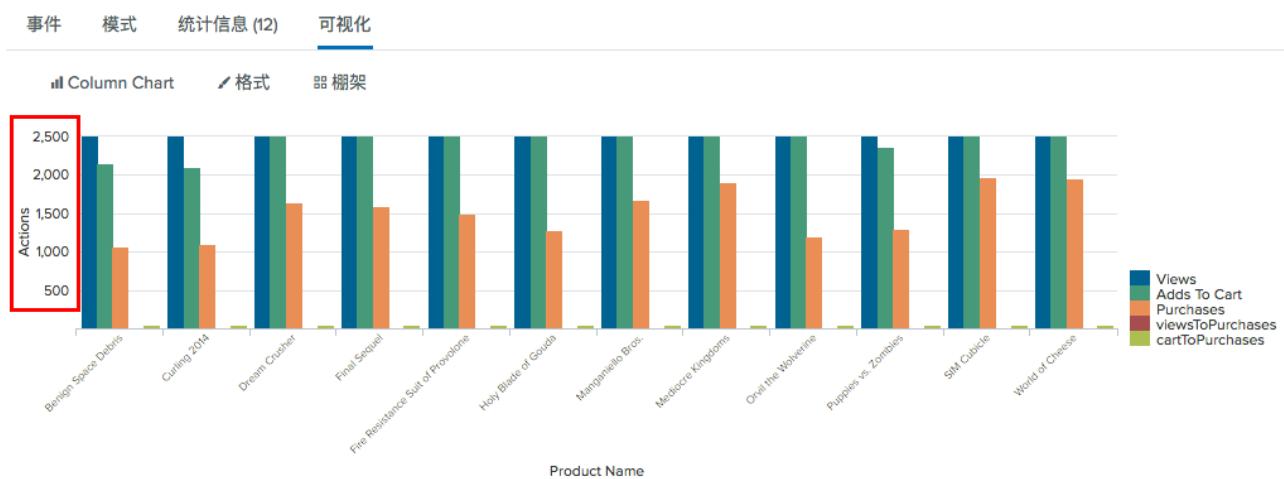
## 设置 Y 轴值格式并添加标题

注意 Y 轴上的数字，数字范围从 1000 到 3000，且没有可以识别该轴追踪内容的标题。把图表做的更加易读，

1. 单击格式和 Y 轴。  
我们要添加标题并在 Y 轴指定其他数字间隔。
2. 为标题选择自定义并键入 **Actions**。
3. 为间隔键入 **500**。
4. 为最大值键入 **2500**。



5. 关闭格式对话框。注意 Y 轴上的标签和值变化。



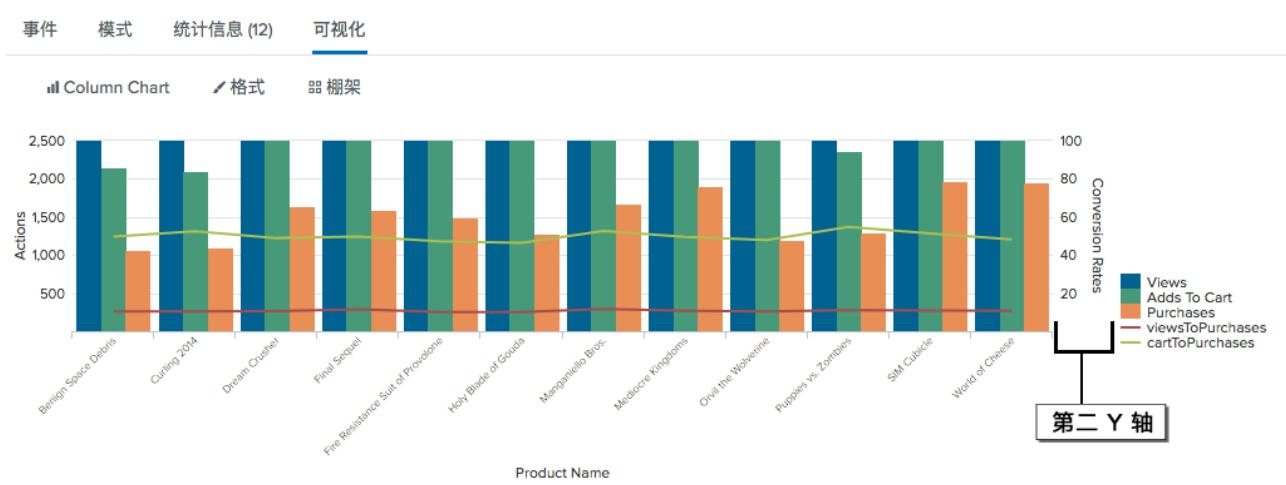
## 设置第二个 Y 轴格式

查看图例。它显示代表操作的部分列，如“查看和购买”，和部分代表转换率的列，如 `viewstoPurchases`。操作是特定字段中值的计数。转换率是百分比。这两种类型的信息应该单独显示。

1. 要解决这个问题，请单击格式和图表覆盖。  
要将操作与转换率分离，您可以将一组值叠加于另一组值上。在此示例中，您会将转换率作为行叠加到操作上，操作将保留为列。
2. 要想进行叠加，单击框内部。开始并选择 `viewstoPurchase`。在此单击框内，选择 `cartToPurchase`。这区分了您想要叠加到柱形图的两个系列。
3. 对于显示为轴，单击开。
4. 为标题选择自定义



5. 键入 **Conversion Rates**。
6. 对于刻度，单击线性。
7. 为间隔键入 **20**。为最大值键入 **100**。
8. 关闭格式对话框。注意，转换率目前在图表中显示为行。

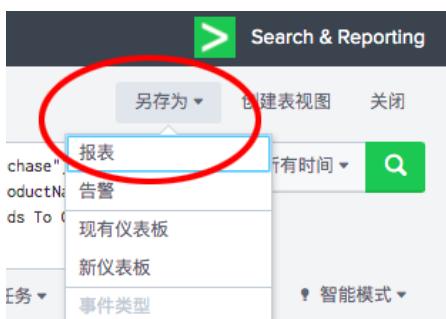


图表右侧的轴称为第二个 Y 轴。折线系列标签和值已在轴上显示。

## 将修订图表另存为报表

您已对图标做出很大更改以增加其可读性。现在该将图表另存为报表。

1. 单击另存为，然后选择报表。



2. 在将报表另存为对话框中，为标题键入 **Comparison of Actions and Conversion Rates by Product**。
3. 为描述键入 **The number of times a product is viewed, added to cart, and purchased and the rates of purchases from these actions.**
4. 单击保存
5. 在确认对话框中，单击查看。



## 下一步

新建来自自定义图表的报表

## 另请参阅

《搜索参考》中的 stats 命令

《搜索参考》中的 eval 命令

《仪表板和可视化》中的图表概览

## 新建来自自定义图表的报表

在此示例中，您新建了一份报表，该报表列出一段时间内所购买产品的图表。此示例使用 timechart 命令和图表选项以新建和自定义图表。

这一示例使用来自此教程“启用字段查找”部分中的 productName 字段。  
如果您不配置字段查找，本部分中的搜索不会生成正确的结果。

1. 开始新搜索。
2. 更改时间范围为所有时间。
3. 运行以下搜索：

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

此搜索使用 count() 函数来为拥有 action=purchase 字段的事件计数。

搜索还使用 usenull 和 useother 参数以确保 timechart 命令对有 productName 值的事件计数，productName 空值的事件不包含在内。

统计信息选项卡显示下表。

新搜索

sourcetype=access\_\* | timechart count(eval(action="purchase")) by productName usenull=f useother=f

177,907 个事件 (21/08/05 13:41:48.000 之前) 无事件采样

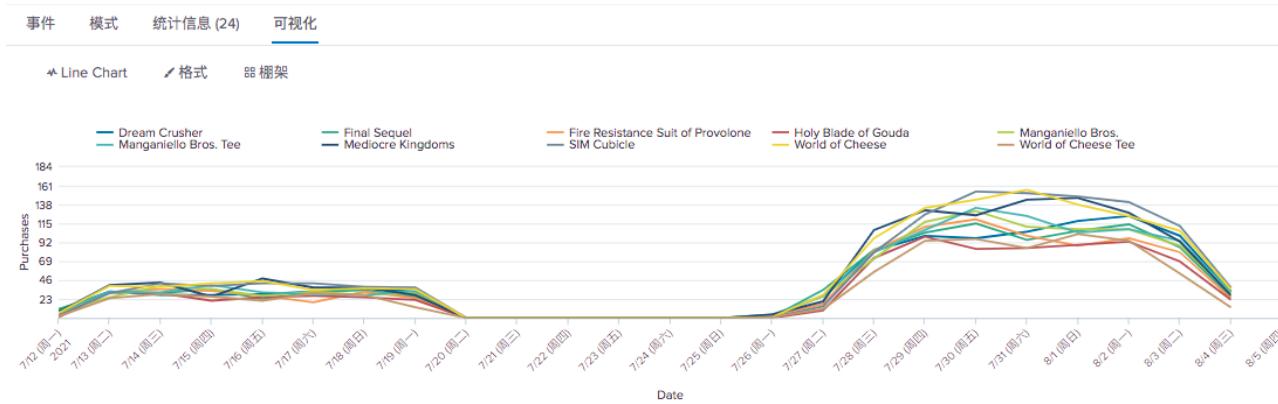
任务 智能模式

事件 模式 统计信息 (24) 可视化

每页 20 个 格式 预览 < 上一个 1 2 下一步 >

| _time      | Dream Crusher | Final Sequel | Fire Resistance Suit of Provolone | Holy Blade of Gouda | Manganillo Bros. | Manganillo Bros. Tee | Mediocre Kingdoms | SIM Cubicle | World of Cheese | World of Cheese Tee |
|------------|---------------|--------------|-----------------------------------|---------------------|------------------|----------------------|-------------------|-------------|-----------------|---------------------|
| 2021/07/12 | 9             | 11           | 4                                 | 1                   | 7                | 7                    | 7                 | 3           | 6               | 2                   |
| 2021/07/13 | 32            | 31           | 31                                | 31                  | 25               | 32                   | 40                | 30          | 39              | 24                  |
| 2021/07/14 | 28            | 30           | 35                                | 30                  | 39               | 31                   | 43                | 42          | 38              | 29                  |
| 2021/07/15 | 28            | 35           | 33                                | 21                  | 35               | 40                   | 26                | 39          | 42              | 26                  |
| 2021/07/16 | 29            | 23           | 27                                | 25                  | 27               | 31                   | 48                | 42          | 45              | 21                  |
| 2021/07/17 | 32            | 31           | 19                                | 27                  | 32               | 29                   | 37                | 42          | 34              | 30                  |
| 2021/07/18 | 36            | 34           | 32                                | 25                  | 28               | 28                   | 37                | 38          | 36              | 28                  |
| 2021/07/19 | 32            | 26           | 24                                | 22                  | 30               | 33                   | 28                | 37          | 35              | 13                  |

4. 单击可视化选项卡。
5. 将图表类型修改为折线图。
6. 使用格式下拉列表设置 X 轴、Y 轴和图例格式以产生以下图表。



此表列出了图表的变化。

| 图表变化     | 设置或值   |
|----------|--------|
| 图表类型     | 折线图    |
| X 轴自定义标题 | 日期     |
| X 轴标签    | -45 度角 |
| Y 轴自定义标题 | 购买     |
| Y 轴间隔    | 10     |
| 图例位置     | Top    |

7. 单击另存为，然后选择报表。
  1. 在将报表另存为对话框中，为标题键入 Product Purchases over Time。
  2. 为描述键入The number of purchases for each product。
  3. 为内容选择第一选项折线图和统计表。
  4. 为时间范围挑选器保留默认设置是。
8. 单击保存。
9. 在确认对话框中，单击查看以查看报表。



## 下一步

从迷你图新建报表

## 另请参阅

《搜索参考》中的 `timechart` 命令  
《仪表板和可视化》中的图表概览  
《报表手册》中的关于报表

## 从迷你图新建报表

在此示例中，您新建随时间变化显示购买数量趋势的报表。这一示例使用迷你图。迷你图是在搜索结果表内部显示的内联图表，它专门显示有关每行主键的随时间变化趋势。

对于使用 `stats` 和 `chart` 命令的搜索，您可以在结果表中添加迷你图。

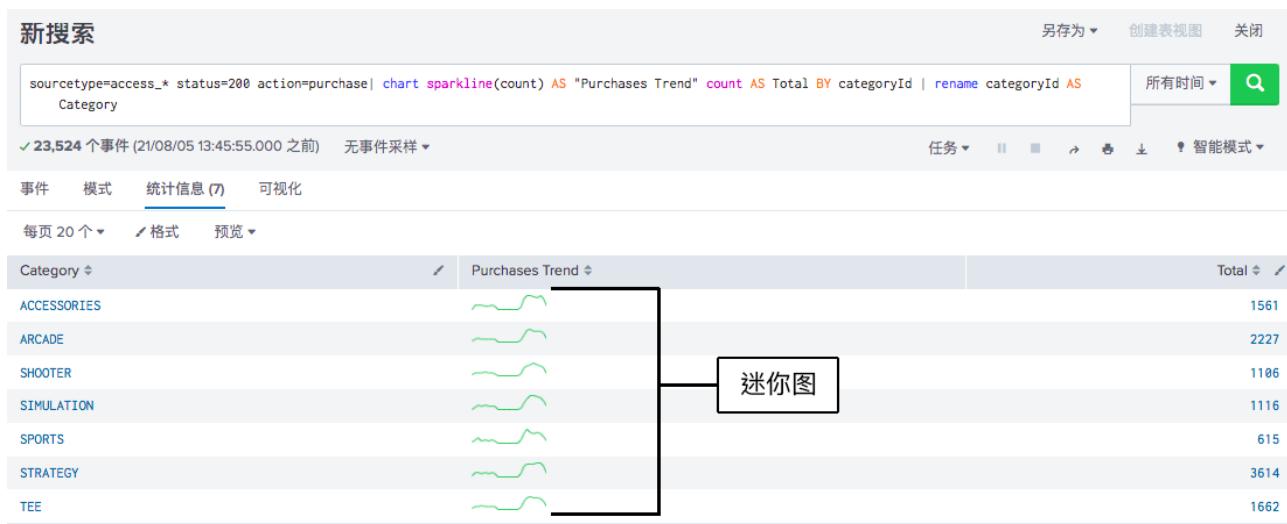
这一示例使用来自此教程“启用字段查找”部分中的 `productName` 字段。  
如果您不配置字段查找，本部分中的搜索不会生成正确的结果。

1. 开始新搜索。
2. 时间范围设为所有时间。
3. 运行以下搜索：

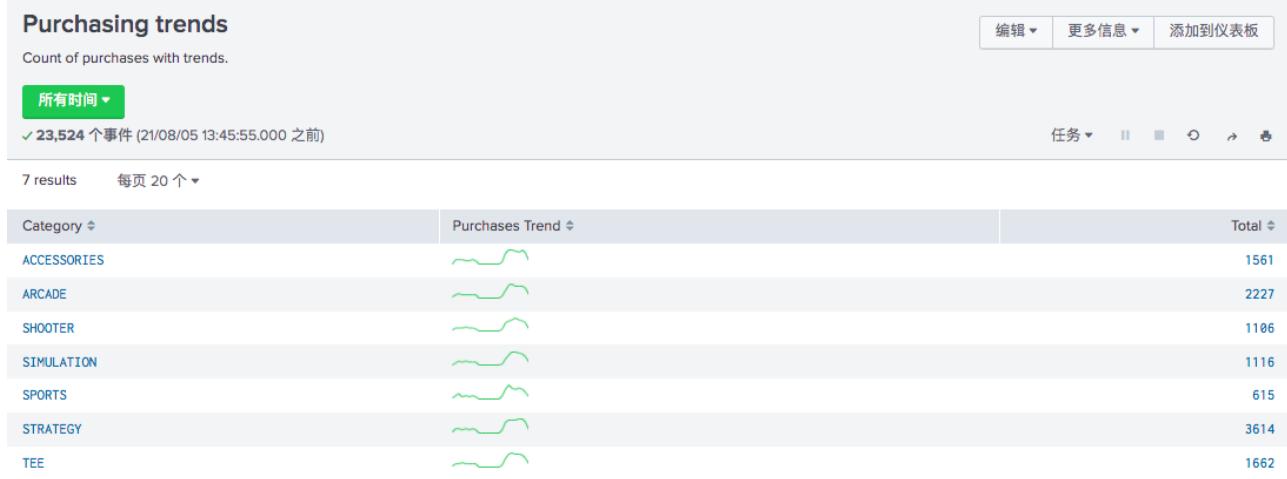
```
sourcetype=access_* status=200 action=purchase| chart sparkline(count) AS "Purchases Trend" count AS Total BY categoryId | rename categoryId AS Category
```

本搜索使用 `chart` 命令，通过运用 `action="purchase"` 来计算购买数量。搜索通过使用 `categoryId` 指定每种产品的购买。不同之处在于购买计数现在是 `sparkline()` 函数的参数。

当您使用 `AS` 关键词重命名列时，多于一个单词的名称需要用引号。这一搜索中引号用在购买趋势名称上，而不是用在类别名称上。



4. 单击另存为，然后选择报表。
5. 在将报表另存为对话框中，为标题键入 Purchasing trends。
6. 为描述键入Count of purchases with trends。
7. 单击保存。
8. 在确认对话框中，单击查看。您的报表应该如下方所示。



## 下一步

搜索教程的第 6 部分到此结束。

到目前为止，您已将保存的搜索另存为报表。继续第 7 部分：新建仪表板，了解如何将搜索和报表另存为仪表板面板。

## 另请参阅

[《搜索参考》中的 chart 命令](#)

[《搜索手册》中的“为您的搜索结果添加迷你图”](#)

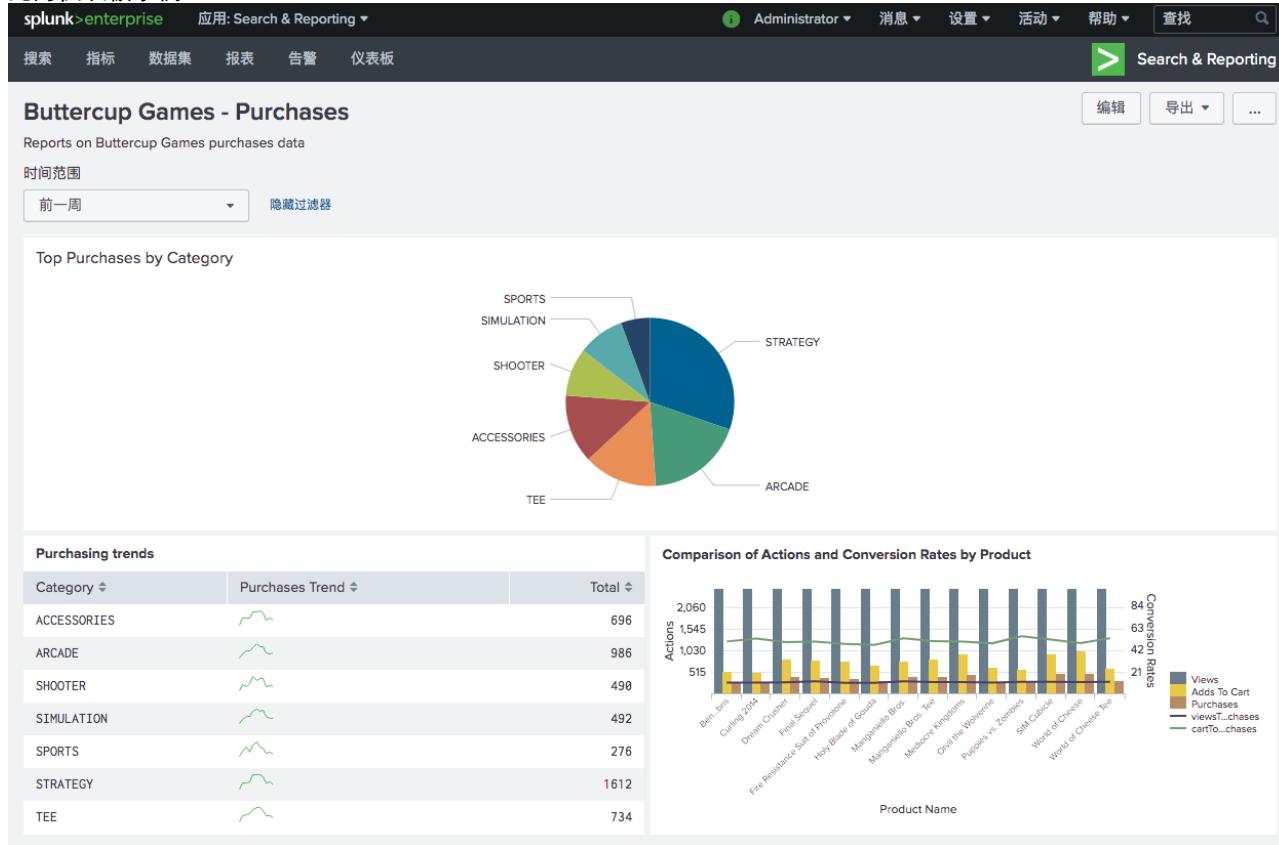
# 第 7 部分：新建仪表板

## 关于仪表板

仪表板是由面板组成的视图。面板可能包含搜索框、字段、图表、表格、列表等模块。仪表板面板通常连接报表。

在新建一个搜索可视化或报表后，您可以将其添加到一个新的或已有的仪表板中。您也可以使用仪表板编辑器新建和编辑仪表板。当您有一组已保存报表，想要快速将其加入一个仪表板时，仪表板编辑器很有用。

此为仪表板示例。



## 更改仪表板权限

您可以通过“仪表板编辑器”获得仪表板的访问权限。但是，您的用户角色以及为该角色定义的功能可能会限制您可以定义的访问权限类型。

如果您的 Splunk 用户角色为管理员（具有默认的功能集），则您可以新建专用、在特定应用中可见，或在所有应用中可见的仪表板。您也可以为其他 Splunk 用户角色（例如，用户、管理员和具有特定功能的其他角色）提供访问权限。

## 更改仪表板面板可视化

在您使用“仪表板编辑器”新建面板之后，使用“可视化编辑器”来更改面板中的可视化类型，并指定该可视化的显示方式和行为。

## 编辑仪表板的 XML 配置

您可以通过编辑仪表板的 XML 配置，来编辑仪表板中的面板。这样便可以使用“仪表板编辑器”中不具备的功能。例如，编辑 XML 配置以更改仪表板的名称，或者为表格指定自定义行数。

## 下一步

我们可以新建仪表板和仪表板面板（基于搜索和报表）。

## 另请参阅

《仪表板和可视化》中：

仪表板快速参考指南  
可视化参考  
可视化的数据结构要求

在《管理员手册》中：

管理知识对象权限

## 新建仪表板和面板

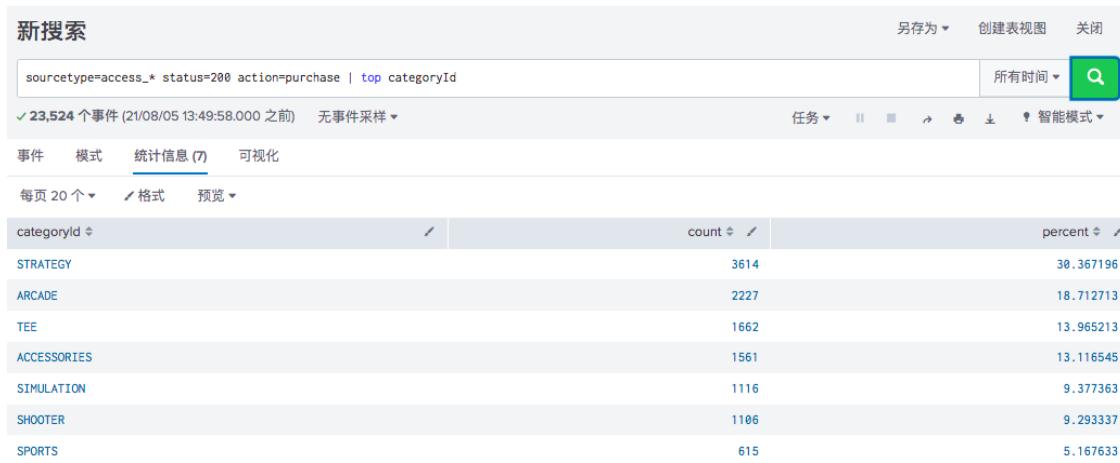
本主题介绍如何将搜索另存为仪表板面板以及如何将输入元素添加到仪表板。

### 将搜索另存为仪表板面板

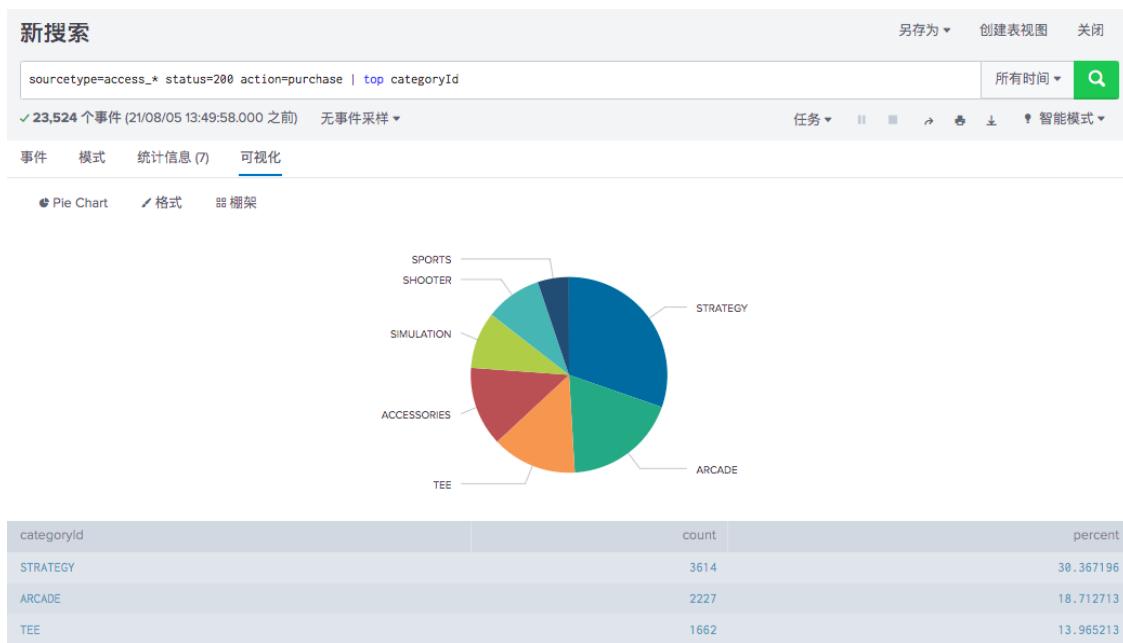
1. 开始新搜索。
2. 更改时间范围为上周。
3. 运行以下搜索：

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

此搜索会针对成功 (status=200) 购买次数，从网络服务器访问日志文件返回事件。top 命令会自动返回各产品的购买计数且每种产品的百分比是总购买量。



4. 单击可视化选项卡。显示的是折线图。
5. 将折线图改为饼图。



6. 单击另存为，并选择仪表板面板。
7. 定义一个新的仪表板和仪表板面板。
  1. 对于仪表板，单击新建。
  2. 为仪表板标题键入 **Buttercup Games - Purchases**。  
仪表板 ID 字段显示 **buttercup\_games\_purchases**。
  3. 为仪表板描述键入 **Reports on Buttercup Games purchases data**。
  4. 为仪表板权限保留默认设置专用。
  5. 为面板标题键入 **Top Purchases by Category**。
  6. 为面板内容保留饼图设置。

将面板保存到新仪表板

仪表板标题  buttercup\_games\_purchases 编辑 ID

描述

权限 启用专用

您要如何构建仪表板?

典型仪表板  
 传统的 Splunk 仪表板构建器

Dashboard Studio 新  
 一个新的构建器，用于创建视觉效果丰富、可自定义的仪表板

---

面板标题

可视化类型 Pie Chart 统计表

> 高级面板设置

取消
保存到仪表板

8. 单击保存。
9. 在确认对话框中，单击查看仪表板。



您已拥有具有一个报表面板的仪表板。要添加更多的报表面板，可运行新的搜索并将它们保存到此仪表板，或向此仪表板添加已保存的报表。在下一部分中，您会向此仪表板添加更多面板。

现在，我们花点时间来详细了解一下这个仪表板面板。

## 查看和编辑仪表板面板

有一个独立视图，您可以通过此独立视图查看您有权访问的仪表板。通过此视图，您可以新建仪表板、更改仪表板和仪表板面板。

1. 单击应用栏中的仪表板查看仪表板视图。

可能会看到一个弹出对话框，询问是否想要浏览仪表板。如果选择浏览，浏览结束时可以选择自己尝试使用仪表板。此选项显示仪表板视图。

除了您新建的 **Buttercup Games - Purchases** 仪表板以外，列表中还有几个内置仪表板。

| 操作 | 所有者    | 应用                    | 共享 | 类型      |
|----|--------|-----------------------|----|---------|
| 编辑 | admin  | search                | 专用 | Classic |
| 编辑 | nobody | splunk_secure_gate... | 全局 | Classic |
| 编辑 | nobody | search                | 应用 | Classic |
| 编辑 | nobody | search                | 应用 | Classic |
| 编辑 | nobody | search                | 应用 | Classic |
| 编辑 | nobody | splunk_secure_gate... | 全局 | Classic |
| 编辑 | nobody | splunk_secure_gate... | 全局 | Classic |
| 编辑 | nobody | splunk_secure_gate... | 全局 | Classic |
| 编辑 | nobody | splunk_secure_gate... | 全局 | Classic |

2. 为 **Buttercup Games - Purchases** 仪表板单击 **i** 列中的箭头符号 (>) 以展开仪表板信息。

您可以看到此仪表板与之相关的应用的相关信息（无论仪表板是否已计划）以及仪表板权限。

## 仪表板

[新建新仪表板](#)

仪表板包含搜索、可视化和用于捕获并显示现有数据的输入控制。

最新资源

|                                                              |                                                                                |                                                          |
|--------------------------------------------------------------|--------------------------------------------------------------------------------|----------------------------------------------------------|
| ☆ Dashboard Studio 示例<br>仪表板和可视化浏览示例。 <a href="#">访问示例中心</a> | □ Dashboard Studio 介绍<br>了解如何通过 Dashboard Studio 构建仪表板。 <a href="#">了解更多信息</a> | □ 典型仪表板介绍<br>了解如何构建传统的简单 XML 仪表板。 <a href="#">了解更多信息</a> |
|--------------------------------------------------------------|--------------------------------------------------------------------------------|----------------------------------------------------------|

9 仪表板

| 标题                                                 | 操作 | 所有者    | 应用                    | 共享 | 类型      |
|----------------------------------------------------|----|--------|-----------------------|----|---------|
| Buttercup Games - Purchases                        | 编辑 | admin  | search                | 专用 | Classic |
| Reports on Buttercup Games purchases data          |    |        |                       |    |         |
| 应用 ..... search                                    |    |        |                       |    |         |
| 计划 ..... 未计划. 编辑                                   |    |        |                       |    |         |
| 权限 ..... 专用。由 admin 拥有。 编辑                         |    |        |                       |    |         |
| 已修改 ..... 2021/08/05 13:53:11                      |    |        |                       |    |         |
| > End-to-End Websocket Test                        | 编辑 | nobody | splunk_secure_gate... | 全局 | Classic |
| > Integrity Check of Installed Files               | 编辑 | nobody | search                | 应用 | Classic |
| > Job Details Dashboard                            | 编辑 | nobody | search                | 应用 | Classic |
| > Orphaned Scheduled Searches, Reports, and Alerts | 编辑 | nobody | search                | 应用 | Classic |
| > Request Tracing                                  | 编辑 | nobody | splunk_secure_gate... | 全局 | Classic |
| > Secure Gateway Status Dashboard                  | 编辑 | nobody | splunk_secure_gate... | 全局 | Classic |
| > Single Value Test                                | 编辑 | nobody | splunk_secure_gate... | 全局 | Classic |
| > Subscription Tracing                             | 编辑 | nobody | splunk_secure_gate... | 全局 | Classic |

## 向仪表板添加控制

您可以向仪表板面板添加输入控制，例如时间范围挑选器。

- 在仪表板列表中，单击 **Buttercup Games - Purchases**，以显示仪表板。
- 单击编辑。

**Buttercup Games - Purchases**

Reports on Buttercup Games purchases data

Top Purchases by Category

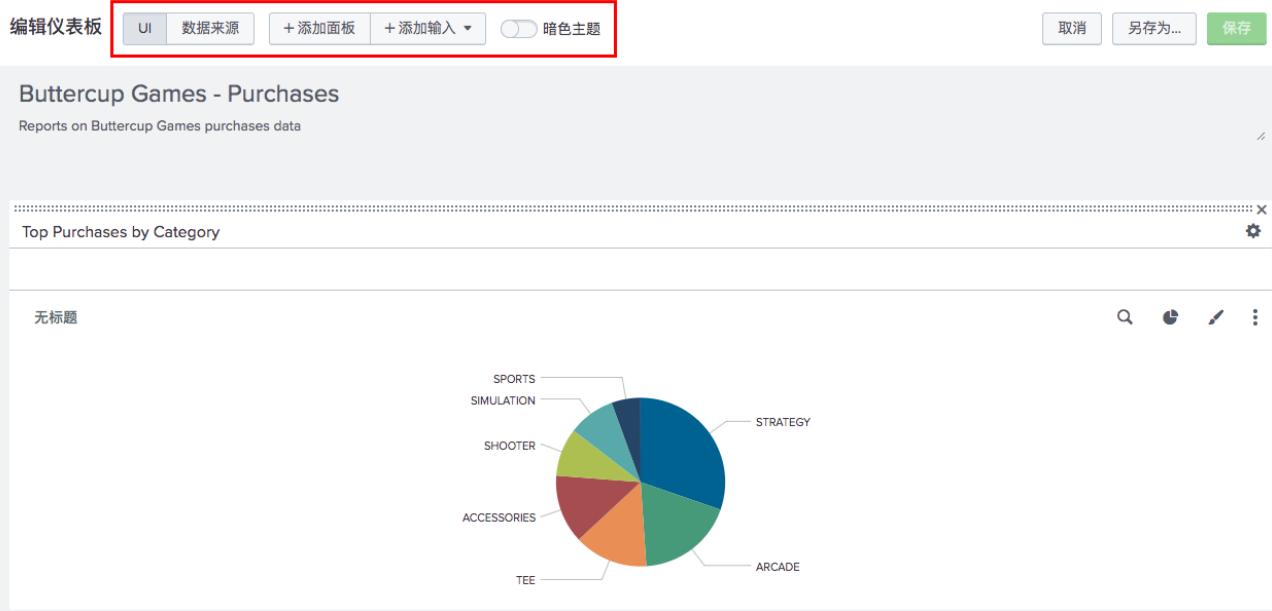
| Category    | Approximate Proportion |
|-------------|------------------------|
| STRATEGY    | ~35%                   |
| ARCADE      | ~25%                   |
| ACCESSORIES | ~10%                   |
| TEE         | ~8%                    |
| SIMULATION  | ~5%                    |
| SHOOTER     | ~5%                    |
| SPORTS      | ~2%                    |

编辑   导出 ...

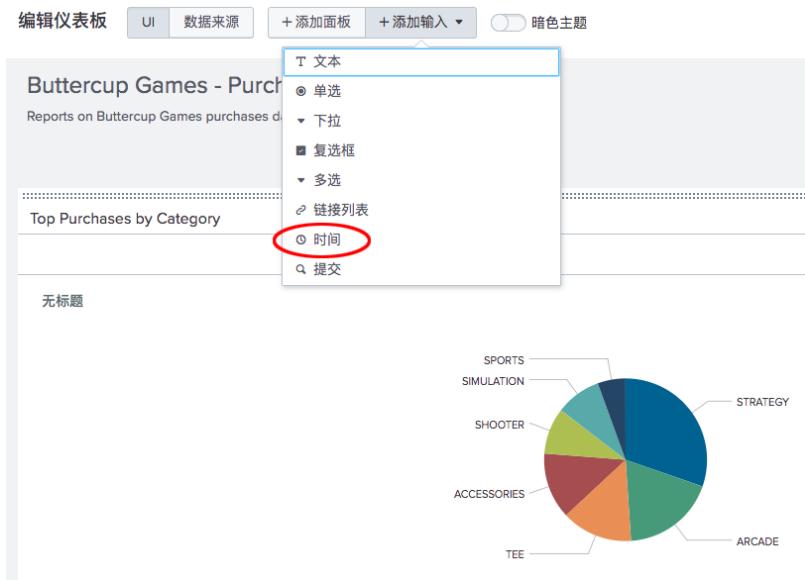
您可以使用 UI 或数据源来编辑仪表板。您可以通过 UI 选项添加面板和输入至仪表板中。

- 您可使用添加面板选项新建面板、将报表添加为面板、或复制现有仪表板。
- 您可使用添加输入选项从控制列表中选择一项添加到仪表板中，包括文本、复选框和时间范围挑选器。
- 您可使用深色主体选项更改仪表板的背景显示。要启用主题更改，您必须保存并刷新仪表板。

您可以通过数据源选项直接为面板编辑 XML 源。本教程不包含直接编辑数据源的相关内容。



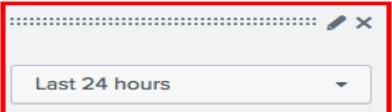
3. 单击添加输入并选择时间。



仪表板中显示时间范围挑选器输入控制。

### Buttercup Games - Purchases

Reports on Buttercup Games purchases data



Last 24 hours

#### Top Purchases by Category

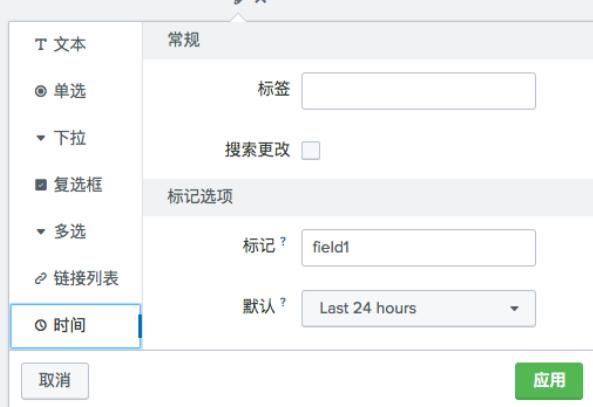
无标题



- 单击时间范围挑选器的编辑输入图标。图标看起来像支铅笔。这将打开一组输入控件。时间输入类型已选定。

### Buttercup Games - Purchases

Reports on Buttercup Games purchases data



常规

标签

搜索更改

标记选项

标记 ?

默认 ?

取消 应用

- 为标签键入 **Time range**。
- 为标记，将默认标记名称替换为 **field1**。键入 **BG\_Purchases\_Time\_Range**。

添加至仪表板的空间具有标识符，标识符名称为**输入标记**。本步骤为时间范围挑选器重新定义输入标记的名称。输入标记的默认名称为 **field1**、**field2**、**field3** 等。向仪表板添加控件时可更改输入标记。为标记命名有助于更方便地了解您正在使用哪个输入。在此示例中，您正在使用包含简短版仪表板标题的标记名称。

- 对于默认，将默认时间范围更改为上周。
- 单击应用。

您添加至仪表板的输入控件独立于仪表板面板。如果希望面板中的图表在您更改时间范围时刷新，需要将仪表板面板连接到时间范围挑选器输入控件。

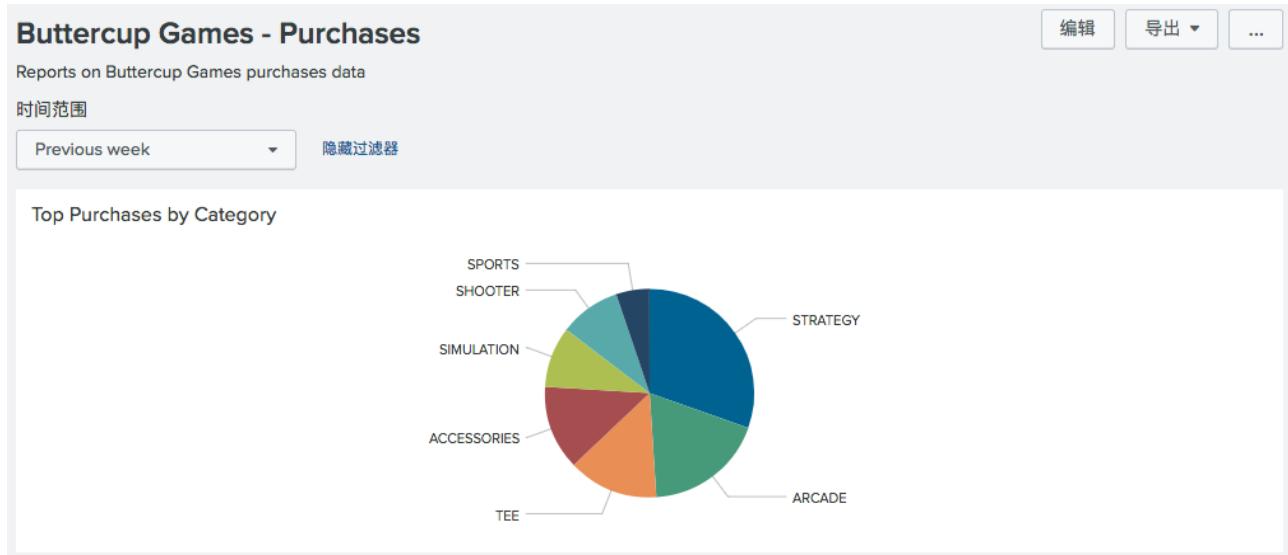
- 在仪表板面板中，单击编辑搜索图标。此图标形似一个放大镜。



6. 在编辑搜索对话框中，时间范围的默认选择是使用时间挑选器。单击以查看选项。您想要选择共享时间挑选器(BG\_Purchases\_Time\_Range)。



7. 单击应用。  
8. 在编辑仪表板窗口中，单击保存以保存对仪表板所做的修改。  
面板此时已连接仪表板中的时间范围挑选器输入控件。此时间范围挑选器称为共享的时间挑选器。支持面板的内联搜索现在使用在共享的时间挑选器中指定的时间范围。



您可以使仪表板包含多种面板，连接到共享的时间范围挑选器的面板、显示特定时间范围（在面板所基于的搜索中指定的时间范围）内数据的面板。

在下一部分中，您将了解将其他面板连接到共享时间挑选器的更多相关内容。

## 下一步

了解向仪表板添加更多面板的信息。

## 另请参阅

[仪表板和可视化中的“关于仪表板编辑器”](#)。

## 向仪表板添加更多面板

在本教程之前的章节中，您已运行过搜索并将它们另存为报表。在本部分中，您会将已保存的报表添加到现有的仪表板。您还要根据即席搜索添加更多面板。

### 将已保存的报表添加到仪表板

#### 前提条件

确保您有 **Buttercup Games - Purchases** 仪表板。这是本教程前面的“新建仪表板和面板”部分中新建和编辑的仪表板。在继续本部分之前，您必须创建该仪表板。

#### 步骤

1. 要显示仪表板列表，单击应用栏中的仪表板并选择 **Buttercup Games - Purchases** 仪表板。

仪表板

仪表板包含搜索、可视化和用于捕获并显示现有数据的输入控制。

最新资源

| 操作 | 所有者    | 应用                    | 共享 | 类型      |
|----|--------|-----------------------|----|---------|
| 编辑 | admin  | search                | 专用 | Classic |
| 编辑 | nobody | splunk_secure_gate... | 全局 | Classic |
| 编辑 | nobody | search                | 应用 | Classic |
| 编辑 | nobody | search                | 应用 | Classic |
| 编辑 | nobody | search                | 应用 | Classic |
| 编辑 | nobody | splunk_secure_gate... | 全局 | Classic |
| 编辑 | nobody | splunk_secure_gate... | 全局 | Classic |
| 编辑 | nobody | splunk_secure_gate... | 全局 | Classic |
| 编辑 | nobody | splunk_secure_gate... | 全局 | Classic |

2. 在操作列中，单击编辑并选择编辑面板。编辑仪表板页面会打开。
3. 单击添加面板。

Buttercup Games - Purchases

Reports on Buttercup Games purchases data

时间范围

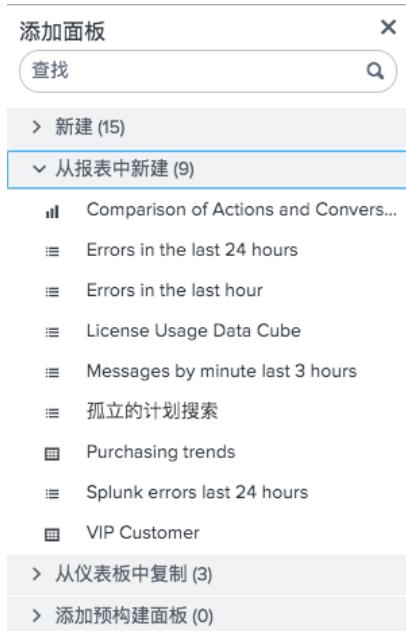
前一周

Top Purchases by Category

无标题

SPORTS  
SIMULATION  
SHOOTER  
STRATEGY

4. 要从现有报表中添加新面板，单击从报表新建。此列表展开以显示您已新建、保存和内置的报表。



## 5. 选择购买趋势。

在“添加面板”边栏旁，显示预览边栏。预览包括报表、报表所依据的搜索和报表本身的预览。这是您新建的迷你图图表报表。

| Category    | Purchases Trend | Total |
|-------------|-----------------|-------|
| ACCESSORIES |                 | 1561  |
| ARCADE      |                 | 2227  |
| SHOOTER     |                 | 1106  |
| SIMULATION  |                 | 1116  |
| SPORTS      |                 | 615   |
| STRATEGY    |                 | 3614  |
| TEE         |                 | 1662  |

## 6. 单击添加到仪表板。

新面板会显示在仪表板底部。

## 7. 从“添加面板”边栏菜单选择报表产品操作和转换率的对比并将其添加到仪表板。

添加面板

查找

> 新建 (15)

从报表中新建 (10)

**Comparison of Actions and Conver...**

- Errors in the last 24 hours
- Errors in the last hour
- License Usage Data Cube
- Messages by minute last 3 hours
- 孤立的计划搜索
- Product Purchases over Time
- Purchasing trends
- Splunk errors last 24 hours
- VIP Customer

显示更多

> 从仪表板中复制 (7)

> 添加预构建面板 (0)

预览

添加到仪表板

新建者 ..... 由 搜索 新建。

应用 ..... search

计划 ..... 未计划。

操作 ..... 0 操作

加速 ..... 已禁用。

权限 ..... 专用。由 admin 拥有。

已修改 ..... 2021/08/05 13:40:03

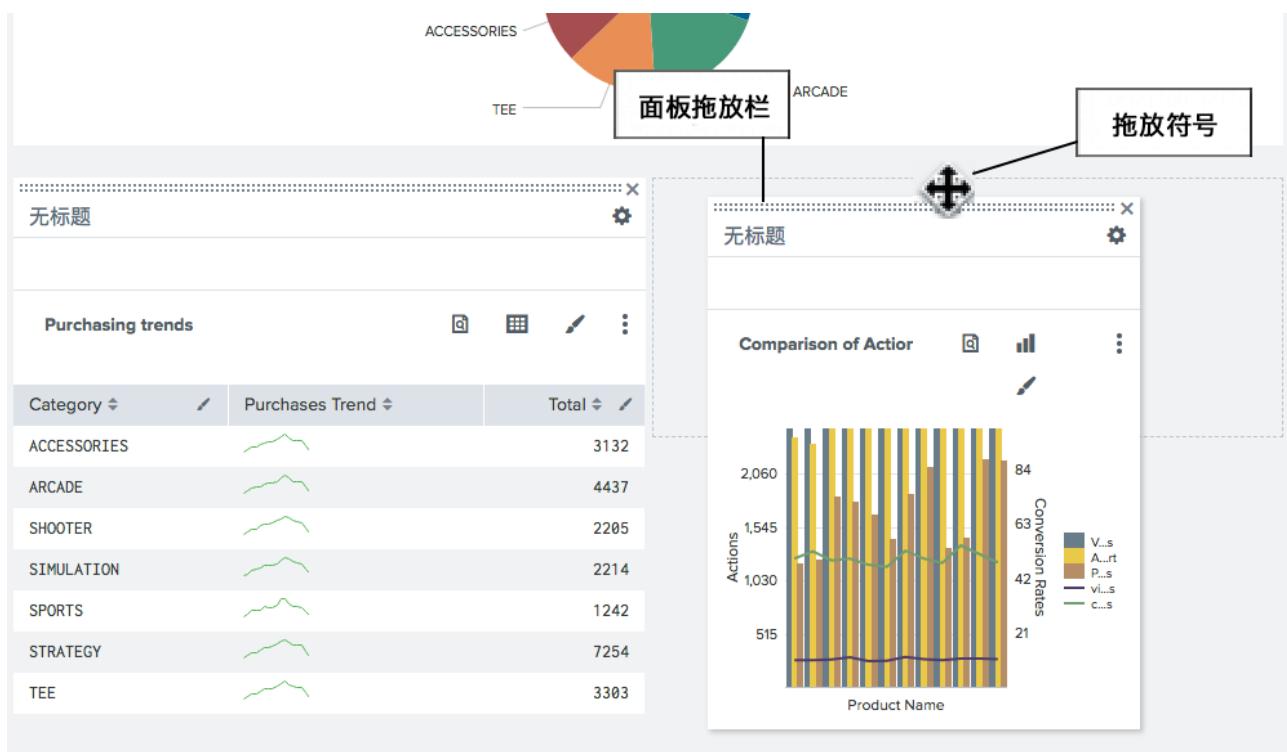
嵌入 ..... 已禁用。

搜索字符串

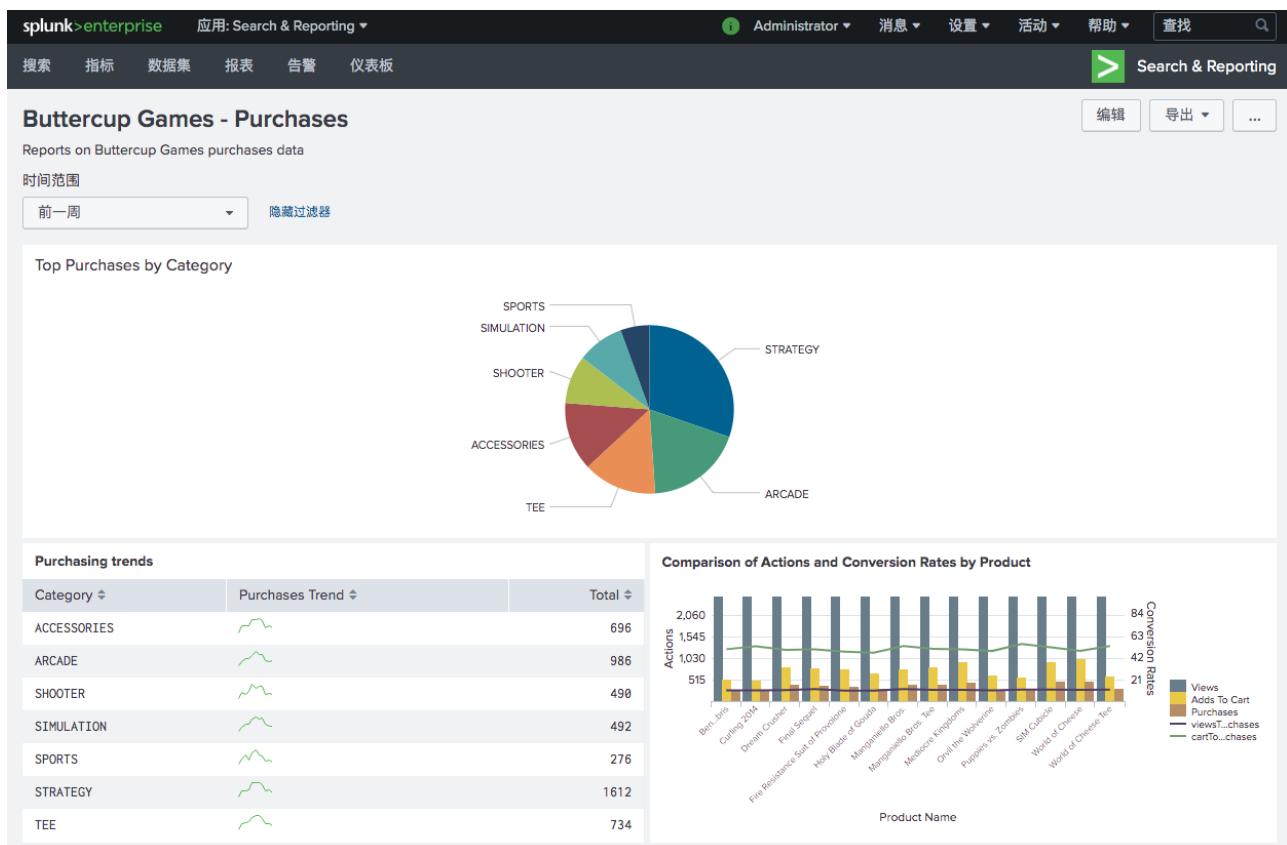
```
sourcetype=access_* status=200 | stats count AS views
count(eval(action="addtocart")) AS addtocart
count(eval(action="purchase")) AS purchases by productName | eval
viewsToPurchases=(purchases/views)*100 | eval cartToPurchases=
(purchases/addtocart)*100 | table productName views addtocart
purchases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

| Product Name | Views | Add...art | Pur...ses | car...ses |
|--------------|-------|-----------|-----------|-----------|
| Product A    | 2200  | 1800      | 900       | 55        |
| Product B    | 2100  | 1900      | 950       | 58        |
| Product C    | 2000  | 1700      | 850       | 52        |
| Product D    | 1900  | 1600      | 800       | 48        |
| Product E    | 1800  | 1500      | 750       | 45        |
| Product F    | 1700  | 1400      | 700       | 42        |
| Product G    | 1600  | 1300      | 650       | 40        |
| Product H    | 1500  | 1200      | 600       | 38        |
| Product I    | 1400  | 1100      | 550       | 35        |
| Product J    | 1300  | 1000      | 500       | 32        |
| Product K    | 1200  | 900       | 450       | 30        |
| Product L    | 1100  | 800       | 400       | 28        |
| Product M    | 1000  | 700       | 350       | 25        |
| Product N    | 900   | 600       | 300       | 22        |
| Product O    | 800   | 500       | 250       | 20        |

8. 关闭添加面板边栏。
9. 重新安排仪表板上的面板。  
使用面板顶部的面板拖放栏拖放面板。拖动面板时，拖放栏上显示四向箭头符号。



10. 在编辑仪表板窗口中，单击保存以保存对仪表板所做的修改。  
您完成的仪表板外观应如下图所示。



## 将搜索结果添加到现有的仪表板

您可将即席搜索的结果另存为现有仪表板中的面板。

### 前提条件

这一示例需要来自此教程“启用字段查找”部分中的 `productName` 字段。您必须先完成所有这些步骤，然后再继续了解本部分。如果您不配置字段查找，本部分中的搜索不会生成正确的结果。

让我们用该查找运行以下搜索。

1. 单击应用栏中的搜索启动新搜索。
2. 确保时间范围设为所有时间。
3. 运行以下搜索确定 VIP 客户和客户购买的产品。

```
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"
```

下图显示的是搜索结果。

| VIP Customer  | Total Purchased | Total Products | Product Names                                                                                                                                                                                                                                                                                            |
|---------------|-----------------|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 87.194.216.51 | 618             | 14             | Benign Space Debris<br>Curling 2014<br>Dream Crusher<br>Final Sequel<br>Fire Resistance Suit of Provolone<br>Holy Blade of Gouda<br>Manganelli Bros.<br>Manganelli Bros. Tee<br>Mediocre Kingdoms<br>Orvil the Wolverine<br>Puppies vs. Zombies<br>SIM Cubicle<br>World of Cheese<br>World of Cheese Tee |

4. 单击另存为，然后选择仪表板面板。
5. 要选择仪表板，请单击现有然后选择 Buttercup Games - 购买商品。
6. 键入 VIP 客户购买商品作为面板名称。
7. 单击保存。
8. 单击查看仪表板。
9. 单击编辑。
10. 在仪表板编辑器中，将 VIP 客户购买商品面板拖到按类别列出最热卖商品饼状图旁边。
11. 单击保存。

您的仪表板外观应如下图所示。

## Buttercup Games - Purchases

编辑

导出 ▾

...

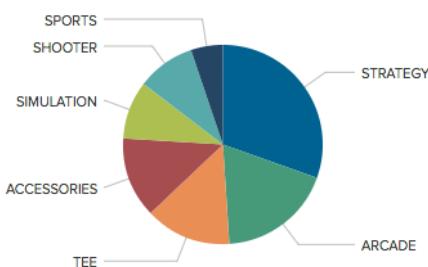
Reports on Buttercup Games purchases data

时间范围

Previous week ▾

隐藏过滤器

### Top Purchases by Category



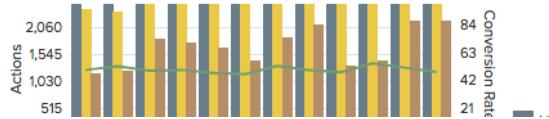
### VIP Client Purchases

| VIP Customer  | Total Purchased | Total Products | Product Names                                                                                                                                                                                                                                                 |
|---------------|-----------------|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 87.194.216.51 | 1206            | 14             | Benign Space Debris<br>Curling 2014<br>Dream Crusher<br>Final Sequel<br>Fire Resistance Suit of<br>Provolone<br>Holy Blade of Gouda<br>Manganiello Bros.<br>Mediocre Kingdoms<br>Orvil the Wolverine<br>Puppies vs. Zombies<br>SIM Cubicle<br>World of Cheese |

### Purchasing trends

| Category    | Purchases Trend | Total |
|-------------|-----------------|-------|
| ACCESSORIES |                 | 3132  |
| ARCADE      |                 | 4437  |

### Comparison of Actions and Conversion Rates by Product



## 将面板连接到共享的时间范围挑选器

您想要添加到仪表板的面板类型决定了您是否可以将面板连接到共享的时间范围挑选器中。

**Buttercup Games - Purchases** 仪表板现在包含在以下表格中列出的面板。

| 面板名称        | 面板来源 |
|-------------|------|
| 按类别的热卖购买    | 临时搜索 |
| 购买趋势        | 报表   |
| VIP 客户购买    | 临时搜索 |
| 产品操作和转换率的对比 | 报表   |

如果是基于临时搜索的面板，您可以将面板连接到共享的“时间范围挑选器”。如果面板是报表，您无法将它连接到共享的时间范围挑选器。可将报表计划为在设定的时间间隔运行。

要将 VIP 客户端购买面板连接到共享时间范围挑选器：

1. 在仪表板的顶部单击编辑。
2. 在 VIP 客户购买仪表板面板中，单击编辑搜索图标。此图标形似一个放大镜。
3. 在编辑搜索对话框中，为时间范围选择共享的时间挑选器 (`BG_Purchases_Time_Range`)。
4. 单击应用。
5. 在编辑仪表板窗口中，单击保存以保存对仪表板所做的修改。

VIP 客户购买面板现连接到仪表板上的时间范围挑选器输入。

在您更改仪表板中的时间范围之后，连接到共享“时间范围挑选器”的面板会更新。会重新运行面板所依据的搜索以刷新面板。

## 更多仪表板操作

在您新建仪表板之后，使用右上角的按钮进行仪表板操作，诸如：

- 导出仪表板
- 编辑权限以将仪表板共享给其他用户

## 下一步

恭喜！您已学习完此搜索教程。

要了解更多信息，请参阅“额外资源”。

# 其他资源

## 其他资源

您可以继续使用教程数据，运行更多搜索并新建更多仪表板。

以下部分提供了其他信息和链接。

### Splunk 社区

Splunk 社区很棒，有很多非常活跃的成员，他们都支持新用户。您可以在 Splunk Answers 上搜索解决方案或提问、通过聊天小组联系乐于助人且风趣的 Splunk 爱好者，或者在您附近的“用户组”中与您当地的用户会面。社区门户有您需要发现如何通过 Splunk 社区取得成功的一切内容。

### 搜索资源

本教程对搜索界面导航和搜索语言使用进行了简单介绍。它引导您运行了一些基本搜索并将结果另存为报表和仪表板，但您可以通过 Splunk 软件完成更多的操作。有关更多详细信息，请参阅以下手册：

- **《搜索手册》**：说明了如何搜索和使用 Splunk 搜索处理语言 (SPL™)。可以在此处找到有关编写 Splunk 搜索来计算统计信息、评估字段以及报告搜索结果的更全面的示例。
- **搜索参考**：为需要以目录方式查看搜索命令以及完整语法、描述和用法示例的用户提供了一个参考。

有关创建表格视图的信息，请参阅《知识管理器手册》中的“管理表数据集”。

### 仪表板和可视化

关于创建仪表板的信息，请参阅“仪表板和可视化”

要构建自定义仪表板和可视化，请参阅 Splunk Dashboard Studio 文档。

### Splunk 文档

Splunk 文档类型多样，包括教程、使用案例、管理员、开发人员和用户手册以及 SDK 和 SPL 命令语法文档。

搜索、仪表板和可视化、报表、指标和告警都有各自的手册。甚至还有一本提供给继承 Splunk 部署人员的手册。

您可以在 Splunk 文档站点中找到所有信息。

### 快速参考

#### Splunk 快速参考指南

包含有关 Splunk 软件中重要概念、功能和组件的信息。这一指南还包括常用搜索命令和函数的解释和示例。

#### 仪表板快速参考指南

提供当您新建仪表板和可视化时将使用的最常用操作、定义和命令的概览。

#### 命令快速参考

以字母顺序列出的所有 SPL 命令，带简要说明，并提供通往命令文档的链接。

### Splunk Enterprise 系统要求

搜索教程是对 Splunk Enterprise 系统要求的简单介绍。有关要求的解释说明，请参阅《安装手册》中的“系统要求”。

### 访问数据

要了解有关数据类型的更多信息，您可以添加并使用应用为数据建立索引，请参阅数据导入手册中的“数据导入入门”。

### 教育

要了解更多 Splunk 功能和使用方法，请参阅 Splunk 教学视频和课程系列。

### 提供反馈

此教程及所有 Splunk 文档每页底部都有一个快速表格，您可以使用此表格向我们提供反馈。

## Was this topic useful?

Was this documentation topic helpful?

Enter your email address, and someone from the documentation team will respond to you:

Send me a copy of this feedback

Please provide your comments here. Ask a question or make a suggestion.