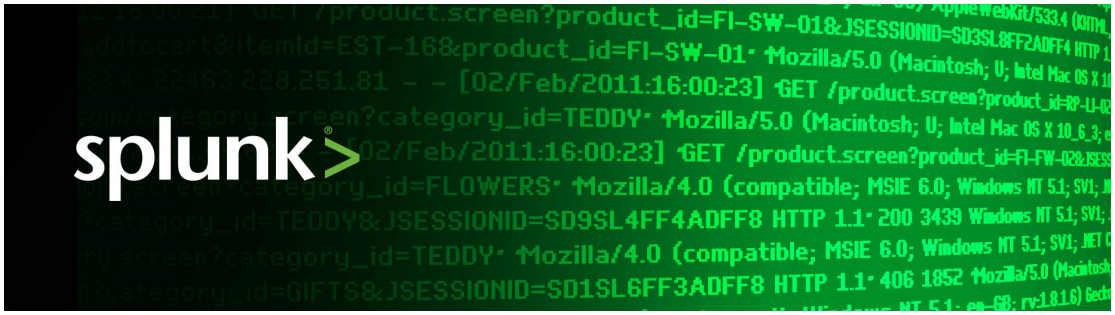


Splunk® Enterprise 6.5.0

数据模型和数据透视表教程

生成时间：2016 年 9 月 26 日下午 10:20

Table of Contents

简介

关于数据模型和数据透视表教程

本教程指导您如何将数据添加到 Splunk 部署、从本教程数据构建简单的数据模型，并根据这些数据模型创建新的数据透视表。

本教程的前提条件

本教程假设您有 Splunk 部署的使用权限。如果您正在使用 Splunk Enterprise，且安装和启动产品时需要指导说明，请参阅*《搜索教程》*中的以下主题。

- 在 Linux、Windows 或 Mac OS X 上安装 Splunk Enterprise
- 启动 Splunk Enterprise 和启动 Splunk Web

本教程包含哪些内容？

以下是您在本教程各个部分中可了解内容的明细。

- **简介**部分介绍完成本教程的前提条件和系统要求。同时还介绍了用于使用 Splunk Enterprise 和数据透视表的界面 - **Splunk Web**。
- **第 1 部分：将数据导入 Splunk Enterprise** 将介绍如何将教程数据添加到 Splunk Enterprise。本章包含可供下载的教程数据，即由虚构网上商店的 Web 服务器和 MySQL 日志组成的示例数据集。
- **第 2 部分：创建数据模型**将向您介绍如何创建新的数据模型、定义根数据集、编辑数据集字段并定义子字段。
- **第 3 部分：设计数据透视表报表**将介绍创建和保存数据透视表表格和图表。
- **第 4 部分：创建仪表板**将介绍创建新仪表板和将数据透视表添加到新的和现有仪表板。

使用教程 PDF

不要直接从 PDF 文档中将搜索或正则表达式复制并粘贴到 Splunk Web。在某些情况下，这样做会产生错误，因为 PDF 格式中包含隐藏字符。

使用本教程的前提条件

要开始本教程，您需要有 6.0 或以上版本 Splunk 部署的访问权限：Splunk Cloud 或 Splunk Enterprise。如果想要下载、安装并启动 Splunk Enterprise，本主题中包含系统要求和您需要了解的 Splunk 许可证事项。

如果您已经有 Splunk 部署的访问权限，请跳过本章并从第 1 部分开始：将数据导入 Splunk Enterprise。

系统要求

Splunk Enterprise 可在大部分计算平台上运行：Linux、UNIX、Windows 和 Mac OS。对于本教程，您需要一台满足表中所列规范的计算机或笔记本电脑。

平台	最低支持的硬件容量
非 Windows 平台	1x1.4 GHz CPU、1 GB RAM
Windows 平台	Pentium 4 或等同于 2Ghz、2GB RAM

安装 Splunk Enterprise 后，使用 Web 浏览器对其进行访问。Splunk Enterprise 6.0+ 支持最新版本的 Firefox、Chrome 和 Safari 浏览器。

以上是对 Splunk Enterprise 系统要求的简单介绍。请参阅《*安装*手册》中的“系统要求”主题。

下载 Splunk Enterprise 的最新版本

从 Splunk.com 下载页面下载 Splunk Enterprise 的最新版本。

如果您未登录到 Splunk.com，可单击下载软件包以转到注册表。如果您还没有 Splunk.com 帐户，请注册一个帐户。

本教程侧重介绍 Linux、Windows 和 Mac OS X。同时也将介绍操作系统特定功能之间的差异。

- **Splunk 针对 Linux 提供了三种安装选项：**RPM 下载（适用于 RedHat）、DEB 软件包（适用于

Debian Linux）和 tar 文件安装程序。对于本教程，您可以使用上述任何安装程序。
- **Splunk 提供了两种 Windows 安装程序：**MSI 文件和压缩的 zip 文件。本教程使用的是 MSI 文件图形安装程序。
- **Splunk 提供了两个 Mac OS X 安装程序**、一个 DMG 软件包和一个 tar 文件安装程序。本教程使用的是 DMG 软件包图形安装程序。

Splunk 许可证

Splunk 许可证用于限制 Splunk Enterprise 安装每天可以建立索引的数据量。Splunk Enterprise 使用 Enterprise 许可证或 Free 许可证运行。当您首次下载 Splunk Enterprise 时，您将获得一份为期 60 天的 Enterprise Trial 许可证。此 Trial 许可证允许服务器每天建立 500MB 的索引量以及所有 Enterprise 功能。请参阅*《管理员手册》*中有关“Splunk 许可证类型”的更多信息。

后续步骤

下一个主题介绍如何导航 Splunk Web 中的视图。

导航 Splunk Web

Splunk Web 是指 Splunk Enterprise 图形用户界面。本主题介绍如何在您需要完成此教程的 Splunk Web 过程中查找页面。

查找“Splunk 主页”

“Splunk 主页”是可从此 Splunk 实例访问的应用和数据的交互门户。

默认情况下，Splunk Home 是您登录后见到的第一个页面。如果不是，您的帐户可能配置为从另一个视图开启，如**搜索和报表**应用中的“搜索”或“数据透视表”。

您可以通过单击 Splunk 栏的 Splunk 徽标从任何其他视图返回到 Splunk 主页。

使用 Splunk 栏

Splunk Web 中每个页面的 Splunk 栏大体相同。当您在本教程中创建数据模型和数据透视表时，您将使用它在编辑器视图间切换。

应用

“应用”面板列出您有权查看的 Splunk 实例上安装的应用。从该列表中选择应用并打开它。如果您有多个应用，可以在工作区内对其执行拖放来进行重新排列。

您可在此面板上执行两个操作：

- 单击齿轮图标并管理安装在 Splunk 实例中的应用。
- 单击加号图标以浏览更多要安装的应用。

数据模型和**数据透视表**编辑器为**搜索和报表应用**的一部分。

浏览 Splunk Enterprise

浏览 Splunk Enterprise 面板上的选项可帮助您开始使用 Splunk Enterprise。单击此图标以打开“添加数据”视图、浏览新的应用、打开 Splunk Enterprise 文档或打开 Splunk Answers。

后续步骤

继续下一主题以将教程添加到 Splunk Enterprise 实例。

第 1 部分：将数据导入 Splunk Enterprise

将教程数据导入到 Splunk Enterprise

本主题将向您介绍下载教程数据集，并将其添加到 Splunk Enterprise。您可在几小时内完成本教程，但是，如果您要用几天的时间完成本教程，则需下载一个新的示例数据文件并添加。

下载示例数据文件

从以下位置下载并不解压缩教程数据文件：

http://docs.splunk.com/images/Tutorial/tutorialdata.zip

本教程数据文件每天都会更新并显示时间戳为过去 7 天的事件。

将示例数据添加到 Splunk Enterprise

1. 登录至 Splunk Enterprise。如果未进入“Splunk 主页”，请单击 Splunk 栏上的 Splunk 徽标以进入 Splunk 主页。
2. 在**浏览 Splunk Enterprise**下，单击**添加数据**。（**注意：**如果您的 Splunk 部署为自助式 Splunk Cloud 部署，请选择**设置**并单击**添加数据**。如果您的部署为托管式 Splunk Cloud 部署，则不会显示**添加数据**选项。这种情况下，您必须使用转发才能添加教程数据。）

添加数据视图显示添加数据的三个选项、通用数据类型列表和可用于扩展 Splunk Enterprise 功能以添加数据的加载项。

3. 在“您要如何添加数据？”下，单击**上载**。

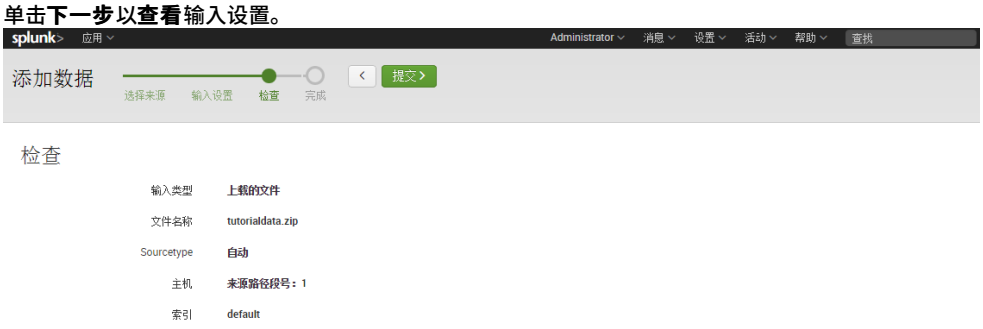
4. 在**选择来源**下，单击**选择文件**以浏览教程数据或将数据文件**拖放**到列出的框上。

因为教程数据文件为归档的数据文件，“添加数据”工作流中的下一步从**设置来源类型**更改为**输入设置**。

5. 单击**下一步**以继续到**输入设置**。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。

6. 使用路径名称的一部分修改主机设置，以分配主机名称：

7. 从菜单中选择**路径中的段**。
8. 键入 1 作为段编号。
9. 单击**下一步**以**查看**输入设置。



10. 单击**提交**。

11. 要确保数据添加成功，单击**开始搜索**。将打开“搜索”视图并运行教程数据来源的搜索。

后续步骤

本教程中的一些示例需要来自外部查找表的数据。将数据添加至 Splunk Enterprise 后，下一个主题将向您介绍如何添加查找表。

添加查找文件到 Splunk Enterprise

您将在本教程创建的数据模型和数据透视表需要来自外部查找文件的一些字段。本主题将介绍如何将所需的查找添加到 Splunk 部署，以及如何创建新查找定义。

字段查找使您能够参考位于外部 CSV 文件中、与您的事件数据匹配的字段。通过使用此匹配，您可以向每个事件添加更多有意义的信息和可搜索字段以丰富您的事件数据。

有关创建查找定义（以及上载 CSV 文件）的更多信息，请参阅“使用字段查找添加信息到您的事件”。

下载查找文件

下载并解压缩以下文件：

- http://docs.splunk.com/images/d/db/Prices.csv.zip

本文件将在 Buttercup Games 教程数据中存在字段的 `productId` 映射到产品名称和价格。

找到查找管理器

1. 在右上方的 Splunk 栏中，单击**设置**。
2. 在**知识**下方，单击*查找*。

将打开“查找”编辑器，您可以在其中创建新查找或编辑现有查找。

您可以通过单击表中的链接（**查找表文件**、**查找定义**和**自动查找**）来查看和编辑现有查找。

上载查找表文件

1. 在**查找表文件**“操作”下方的查找管理器中，单击**新增**。这将带您前往**新增**查找表文件视图，您可在此上载 CSV 文件以便在您的字段查找定义中使用。

2. 要在“搜索”应用中保存您的查找表文件，将“目标”应用设置为搜索。
3. 在**上载查找文件**下方，浏览要上载的 CSV 文件 (prices.csv)。
4. 在**目标文件名**下方，将文件命名为 prices.csv。这是您在查找定义中用来参考该文件的名称。
5. 单击**保存**。这会将您的查找文件上载到“搜索”应用中，并返回到查找表文件列表。

注意：如果上传文件时出错，请确认您完成下载后已解压缩。

全局共享查找表文件

如果未共享查找文件，则当您定义查找时，不可以选择此查找文件。

1. 转到**查找表文件**列表。
2. 在 prices.csv 查找表**路径**的**共享**下方，单击**权限**。

   这将为 **prices.csv** 查找文件打开**权限**对话框。

3. 在**对象应显示于**下方，选择**所有应用**。

4. 单击**保存**。

现在，查找表应该共享为**全局**权限。

添加字段查找定义

1. 返回到查找管理器。
2. 在**查找定义**的**操作**下方，单击*新增*。这将带您前往**新增**查找定义视图，您可从中定义您的字段查找。

3. 将**目标应用**设置为**搜索**。
4. 将您的查找**命名**为 **prices_lookup**。

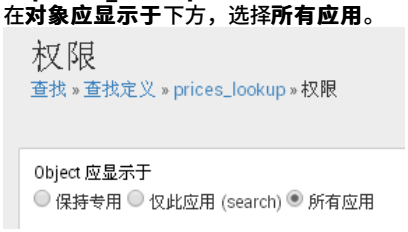
5. 在**类型**下方，选择**基于文件**。

   基于文件的查找从静态表中添加字段，通常是 CSV 文件。

6. 在**查找文件**下方，选择 *prices.csv*（您的查找表名称）。
7. 取消选定**配置基于时间的查找**和**高级选项**。
8. 单击**保存**。这会将 prices_lookup 定义为基于文件的查找。

与所有应用共享查找定义

1. 返回到**查找定义**列表。
2. 在 **prices_lookup** 的**共享**下，单击**权限**。这将打开 **prices.lookup** 的**权限**对话框。
3. 在**对象应显示于**下方，选择**所有应用**。



4. 单击**保存**。现在，prices_lookup 应该共享为**全局**权限。

后续步骤

继续到下一部分以了解数据模型并创建数据模型。

第 2 部分：构建数据模型

关于数据模型和数据模型数据集

本章中的主题将介绍如何使用"数据模型构建器"设计和构建教程数据的数据模型。

什么是数据模型？

数据模型是有关一个或多个数据集语义知识的分层结构搜索时间映射。它将编码构建这些数据集的各种专门搜索所需的域知识。简单地说，数据模型生成搜索。这些专门搜索反过来被用于为数据透视表用户生成报表。

要创建有效的数据模型，您必须了解您的数据源（无论来自日志文件、TCP/UDP 网络输入、接收自 API 的脚本式输入等）和数据语义（如何提取、相关和组织您数据中的各种字段）。本信息会影响您的数据模型架构。

数据模型可以从**提取**中获取各自的字段，这些提取定义于 Splunk Web 的**设置 > 字段 > 字段提取**页面中；或者，如果是 Splunk Enterprise， 则可以通过编辑 `props.conf` 和 `transforms.conf` 文件获取。但是，当定义数据模型时，您还可以通过基于正则表达式的字段提取、**查找**和 `eval` 表达式在搜索时获得其他字段。

在本教程中，您的数据源可以是 Web 访问和安全日志文件。大部分字段将自动提取。其他字段将使用查找文件添加并使用 eval 表达式计算。

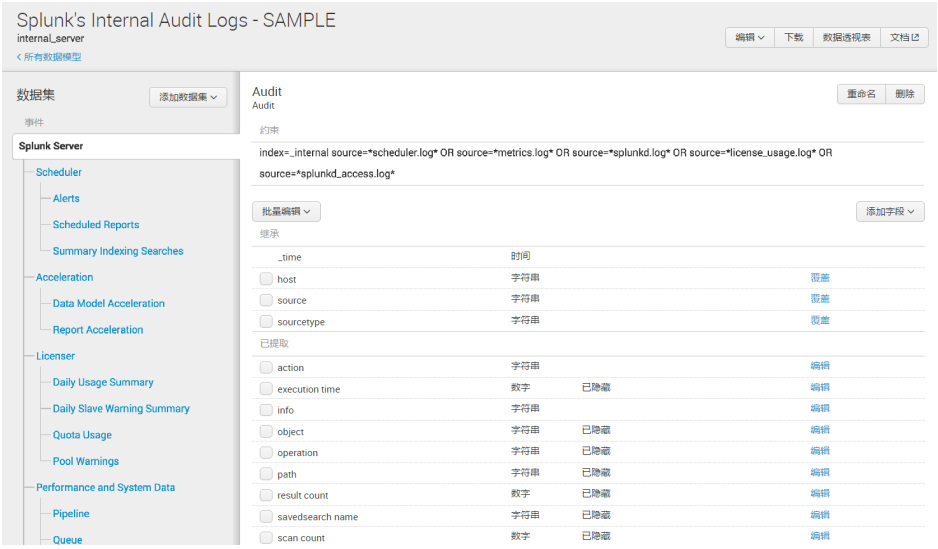
关于数据模型数据集

数据模型由一个或多个数据集组成。每个数据集以某种方式对应于您索引中的一组数据。数据集可分成四种类型：事件数据集、搜索数据集、交易数据集和子数据集。

可以使用父/子关系排列数据模型中的数据集。每个顶级或根数据集可以有多个子数据集，它们将继承父级的约束和字段，同时拥有自己的其他约束和字段。

注意：数据模型数据集是**知识对象**的一个类别。然而，数据模型数据集经常使用其他知识对象，如**提取的字段**、**已计算的字段**和**查找**，来定义它们代表的特定数据集。

这是通过数据模型构建器查看的数据示例。



本示例中，数据集层次结构位于左侧边栏。已选择 Splunk 服务器根事件数据集。Splunk 服务器数据集包含数据模型中的所有数据。所有为 Splunk 服务器对象（如计划程序、加速和许可证）分支的子数据集都包含该数据的不同子集。

数据模型构建器右侧为定义数据集的数据集约束及与该数据集相关的字段列表。本章的其他主题会向您介绍如何创建数据模型，以及如何使用数据模型构建器来定义其数据集层次结构和字段。

数据集约束

所有数据模型数据集均由成组的约束定义，这些约束会筛掉与对象无关的事件，帮助定义数据集代表的数据集。典型的约束看起来像类似搜索的第一部分，在添加管道和其他搜索命令之前。

约束由子数据集继承，以确保每个子数据集均代表其父数据集所代表数据的一个子集。之后，数据透视表用户即可使用这些子数据集，用已经预筛选掉无关数据的数据集来设计报表。

数据集字段

数据集字段分为五种：自动提取、Eval 表达式、查找、正则表达式和 Geo IP。

数据集字段是可以继承的。子数据集将自动拥有其父级的所有字段。您可以设计一个相对简单的数据模型，其中特定数据集树的所有必要字段都由根数据集定义，各子数据集之间以及与根数据集的差别仅在于它们各自的约束。

字段有多个用途。最明显的功能是提供了一组字段，方便数据透视表用户用于定义和生成数据透视表报表；用户拥有该组字段的使用权限，该组字段由用户进入数据透视表时选择的数据集决定。您可以添加字段到子数据集，为该子数据集覆盖的数据集所特定的数据透视表用户提供字段。

了解有关数据模型的更多信息

本主题介绍的信息仅限于您为教程数据构建数据模型所需知道的信息。有关更多信息，请参阅*《知识管理器手册》*中的“关于数据模型”和“设计数据模型数据集”。

后续步骤

继续下一主题，其中您将创建新数据模型。

创建新数据模型

本主题介绍如何基于教程数据创建新数据模型。数据模型在数据透视表内创建，同时您需要拥有“管理员”或“高级用户”角色才能创建数据模型。

允许角色创建数据模型

默认情况下，仅拥有“管理员”或“高级用户”角色的用户可以创建数据模型。对于其他用户，创建数据模型的能力与他

们的角色是否拥有对应用程序的“写入”访问权限相关。因为这是第一次安装，默认情况下您拥有管理员权限，同时应能够继续。

如果无法创建或编辑数据模型，则可能需要检查您的权限。有关更多信息，请参阅《知识管理器手册》中的“关于数据模型权限”。

导航到“数据模型”管理页面

1. 在 Splunk 栏，单击**设置**。

2. 在**知识**下，单击**数据模型**。

此时将进入**数据模型**管理页面。“数据模型”管理页面是数据模型的列表页面。如果您在此 Splunk Enterprise 实例中有现有数据模型，则此页面会将它们列出。使用此页面管理现有数据模型的权限、加速、复制和删除。通过右上角的**上载数据模型**和**新建数据模型**按钮，您还可使用此页面上载数据模型或创建新数据模型。

创建新数据模型

1. 在**数据模型**管理页面，单击**新数据模型**。这将打开**新数据模型**对话框。

2. 输入**标题**："Buttercup Games"，标题字段接受空格和任意字符。您在此输入的值是显示在数据模型列表页面上的值。
3. （可选）输入 **ID**："Tutorial"，如果您不更改 Id，它将自动读取为 "Buttercup_Games"。ID 必须是数据模型的唯一标识符。它不得包含空格或任何不是字母数字、下划线或连字符的任何字符（a-z、A-Z、0-9、_ 或 -）。同时不允许在两个字符之间使用空格。一旦定义数据模型 ID，您将无法更改它。
4. 在**应用**旁，从菜单中选择“搜索和报表”。
5. （可选）输入**描述**“启用数据分析和教程数据报表。”
6. 单击**创建**。该操作将打开 Buttercup Games **编辑数据集**页面。使用该页面可以：为新的数据模型创建数据集、定义数据集的约束和字段、以逻辑层次结构排列数据集，并管理这些数据集。

后续步骤

继续下一主题以添加根数据集到 Buttercup Games 数据模型。

定义数据模型的根数据集

在上一个主题，您创建了数据模型 "Buttercup Games"。

本主题将介绍如何为 Buttercup Games 购买活动添加根数据集。

编辑数据模型数据集

使用“编辑数据集”页面设计新的数据模型，或重新设计现有数据模型。在“编辑数据集”页面上，您可以为数据模型创建数据集、定义数据集的约束和字段，以逻辑层次结构排列数据集，并管理这些数据集。

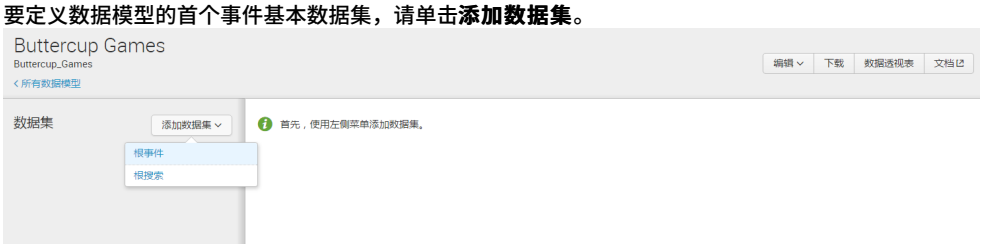
1. 从**数据模型**列表上，单击 **Buttercup Games**。该操作将打开 Buttercup Games 数据集编辑器视图。

添加根数据集

数据模型通常由构建在根事件数据集上的数据集层次结构组成。每个根事件数据集代表一种约束（即筛掉与数据集无关事件的简单搜索）所定义的一组数据。更多有关根事件数据集和根搜索数据集的信息，请参阅“设计数据模型数据集”。

创建一个数据集，来追踪 Buttercup Games 网站上的购买请求。

1. 要定义数据模型的首个事件基本数据集，请单击**添加数据集**。



   您的首个根数据集可以是**根事件**或**根搜索**。
2. 选择**根事件**。该操作将带您前往**添加事件数据集**编辑器。

3. 输入数据集名称：**购买请求数据集名称**字段接受空格和任意字符。您将在“选择一个数据集”页面和其他列出数据模型数据集的地方看到这个名称。
4. 输入数据集 ID：**Purchase_Requests** 这应该会在您键入数据集名称的时候自动填充。如果希望更改，您可以编辑它。**数据集 ID** 必须为数据集的唯一标识符。它不得包含空格或任何不是字母数字、下划线或连字符的任何字符（a-z、A-Z、0-9、_ 或 -）。同时不允许在两个字符之间使用空格。数据集 ID 值一旦保存即无法编辑。
5. 输入下列搜索约束：`sourcetype=access_* action=purchase` 这将定义是购买事件的 Web 访问页面请求。为事件基本数据集提供**约束**后，您可以通过单击*预览*来测试您提供的约束是否返回了所需要的事件类型。

6. 单击**保存**。根据数据集的字段列表包括：主机、数据来源、来源类型和 _time。如果希望添加子数据集到客户端和服务器错误，您需要编辑字段列表以包括附加字段。

后续步骤

继续下一主题以添加更多字段到**购买请求**。

编辑字段列表

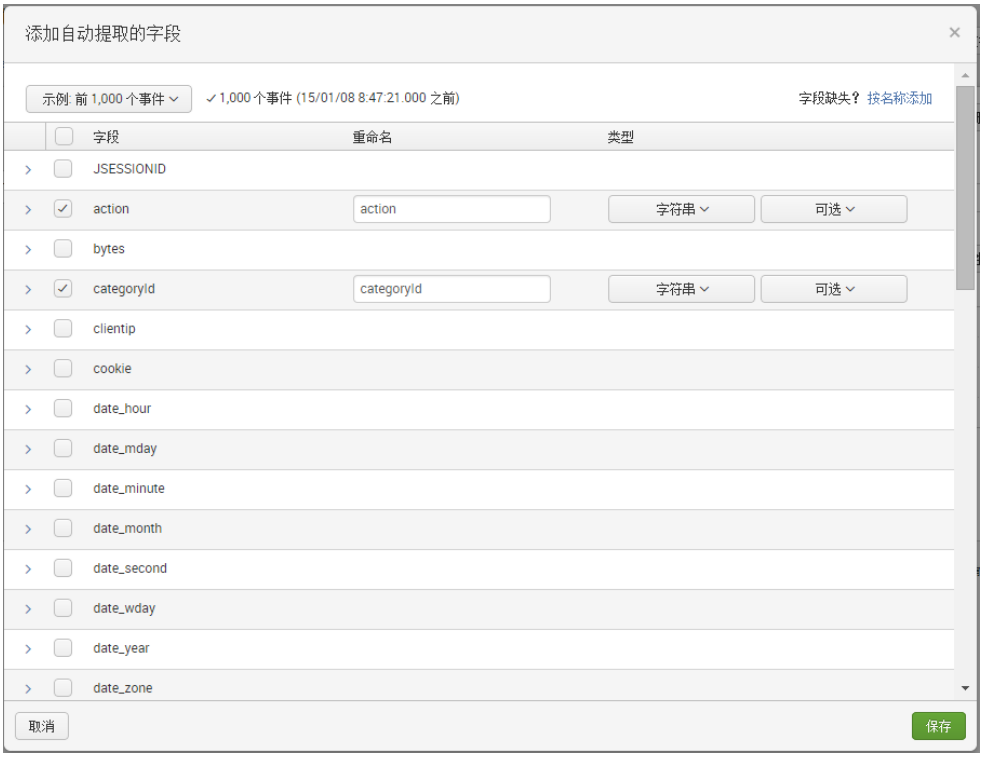
添加自动提取的字段

自动提取字段类型是一种可自动识别的提取字段（如默认字段或已建立索引的字段）或是您已通过**字段提取**页面在 Splunk Web 中定义好了的**搜索时间**字段提取；或者，如果您正在使用的是 Splunk Enterprise，则通过编辑 `props.conf` 和 `transforms.conf` 文件即可。

1. 在 Buttercup Games 数据集编辑器中单击**添加字段**。
2. 选择**自动提取**。

   将打开**添加自动提取的字段**窗口。

3. 滚动自动提取字段列表并选中 `action`、`categoryId`、`productId` 和 `status` 字段。



- 对于**类型**下的 `status` 字段，请确保数据类型为**数字**，您也可以将其保留为**可选**。
- 数据集字段可以为必填、可选、隐藏或隐藏和必填。
- “可选”意味着字段无需出现在数据集代表的所有事件中。该字段可能仅出现在部分数据集事件中。

4. 单击**保存**。

从查找表添加查找字段

创建查找字段需要至少一个定义于“查找”管理器中的**查找定义**。查找定义指示 Splunk 软件查找表所在的位置以及如何与它连接。一旦查找定义就位，Splunk 软件就可以把您选择的字段值和查找表中的字段值进行匹配，然后返回相应的字段/值组合，并以查找字段的方式把它们应用到您的数据集。

注意：编辑本数据模型数据集之前，必须先上传和定义字段查找。继续下一步之前请确认您已添加 prices.csv 查找表并定义 `price_lookup`。

从非自动的查找定义中添加查找字段。如果您定义自动查找，则字段已被添加到事件。这种情况下，字段可添加为“自动提取的字段”。

1. 返回至**购买请求**数据集的 **Buttercup Games** 数据集编辑器。
2. 单击**添加字段**并选择**查找**。

   该操作将打开**使用查找添加字段**页面。

3. 对于**查找表**，选择 **prices_lookup**。

   对于在 Buttercup Games 网站上销售的每个物品，prices_lookup 文件具有描述性产品名称和价格。您必须配置一个查找字段才能将这些字段添加到“购买请求”数据集。csv 查找表的标题值应如下所示：

   productId、product_name、price、sale_price、Code

   DB-SG-G01,Mediocre Kingdoms,24.99,19.99,A

4. 在**输入**下为**查找中的字段**选择 `productId` ，并在**数据集中的字段**内选择 `_raw`。

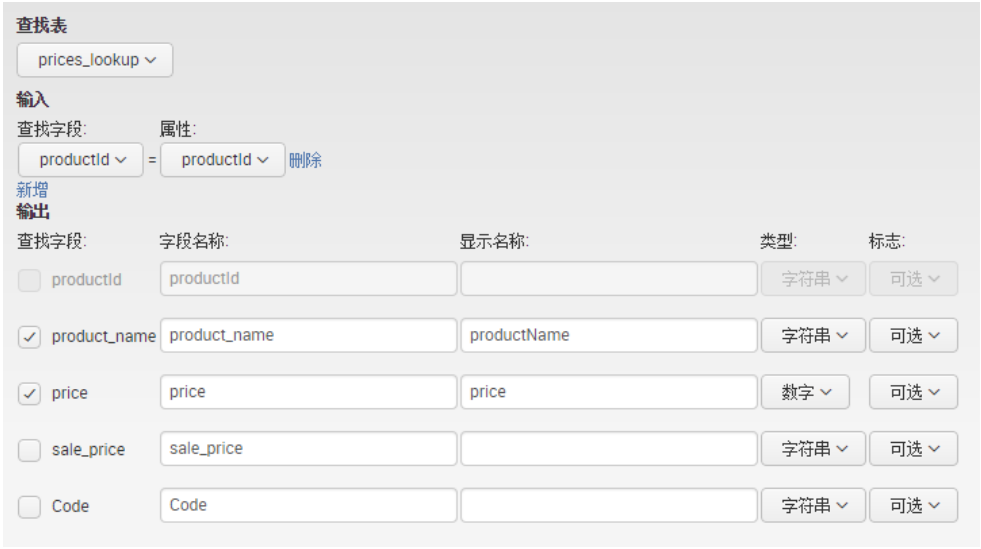
   查找中的字段是用于 csv 查找表的字段名称。数据集中的字段是用于事件数据的字段名称。

5. 在**输入**下，选择 **product_name** 和**价格**字段。

   从查找表标头行读取的输出字段在**字段名称**下列出。您可为每个字段键入**显示名称**。显示名称为用于您事件中字段的名称。

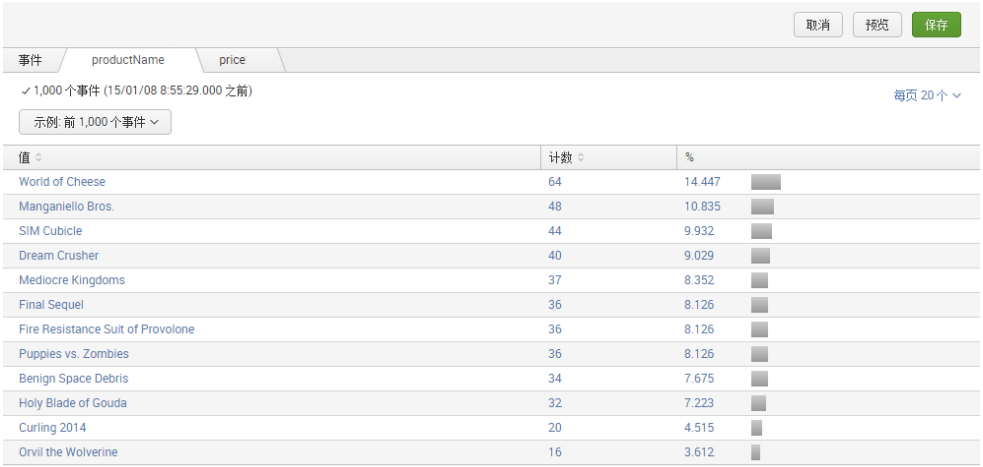
   因为 productId 是用于匹配事件和查找表的字段，您不可以更改其显示名称。

6. 对于 product_name，请键入**显示名称**“产品名称”。对于价格，请键入**显示名称**“价格”，并确保**类型**设置为**数字**。



7. 单击**预览**以查看您要添加的字段。

   使用制表符查看表格中的**事件**，或查看每个您在**输出**中选择的字段的值。例如，此屏幕截图显示产品名称的值。



值	计数	%
World of Cheese	64	14.447
Manganiello Bros.	48	10.835
SIM Cubicle	44	9.932
Dream Crusher	40	9.029
Mediocre Kingdoms	37	8.352
Final Sequel	36	8.126
Fire Resistance Suit of Provolone	36	8.126
Puppies vs. Zombies	36	8.126
Benign Space Debris	34	7.675
Holy Blade of Gouda	32	7.223
Curling 2014	20	4.515
Orvil the Wolverine	16	3.612

8. 单击**保存**。该操作将带您返回至您的数据集页面。

后续步骤

添加子数据集。

定义子数据集

子数据集继承属于其父数据集的所有约束和字段。定义新的子数据集时，为进一步限制该数据集，您需提供一个或多个附加约束。

为追踪 Buttercup Games 网站上的购买活动，您在上一个主题中添加了一个名为“购买请求”的根数据集。本主题将介绍添加子数据集的步骤，助您追踪成功和失败的购买活动。

添加一个子数据集

1. 在 **Buttercup Games** 数据集编辑器页面中单击**添加数据集**并选择**子项**。
   该操作将打开**添加子数据集**编辑器窗口。
2. 输入数据集名称：**成功购买**
3. 输入数据集 ID：**Successful_Purchases**
4. 在“继承自”下选择**购买请求**。这意味着本子数据集将继承来自父数据集**购买请求**的所有字段。
5. 输入**附加约束**：`status=200` 这意味着该数据集中的事件搜索在扩展后将如下所示：`sourcetype=access_* action=purchase status=200`
6. 单击**保存**。

添加第二个子数据集

1. 在 **Buttercup Games** 数据集编辑器页面中单击**添加数据集**并选择**子项**。
   该操作将打开**添加子数据集**编辑器窗口。
2. 输入数据集名称：**失败的购买活动**
3. 输入数据集 ID：**Failed_Purchases**
4. 在“继承自”下选择**购买请求**。这意味着本子数据集将继承来自父数据集**购买请求**的所有字段。
5. 输入**其他约束**：`status=40* OR status=50*` 这意味着该数据集中的事件搜索在扩展后将如下所示：`sourcetype=access_* action=purchase status=40* OR status=50*`
6. 单击**保存**。

后续步骤

现在，您创建了数据模型，可以生成数据透视表报表。继续下章以了解有关数据透视表的信息和如何创建数据透视表报表。

第 3 部分：设计数据透视表报表

关于数据透视表

“Splunk Enterprise 数据透视表”工具允许您使用显示选定“数据模型”不同方面的表格和数据可视化，快速设计报表。数据透视表允许您使用 UI 界面，而不是不得不使用搜索处理语言来生成这些报表。

数据透视表视图

有两种方式可以导航至“数据透视表”视图：

- 通过“数据集”页面
- 经由“设置”进入“数据模型”列表页面

前提条件

- 在创建并保存数据透视表中学习如何创建数据透视表。

步骤

出处	要做什么
数据集页面	1. 在“搜索和报表”应用中打开“数据集”列表页面。 2. 标识您想为其创建数据透视表的数据模型数据集。 3. 选择**数据透视表** 4. 单击**另存为...**将您所做的更改保存为报表或仪表板面板。
设置 > 数据模型	1. 选择**设置 > 数据模型** 2. 找到您想为其创建数据透视表的数据模型。如果创建成功，您应该会看到一个数据模型列表。 3. 在您想据其创建数据透视表的数据模型中选择数据集。 4. 单击**另存为...**将您所做的更改保存为报表或仪表板面板。

如果您在更小的浏览器窗口中查看数据透视表，则“搜索和报告”应用程序导航栏会隐藏起来。要使用导航栏，请单击右上角的菜单图标。导航栏随即向下滑动。

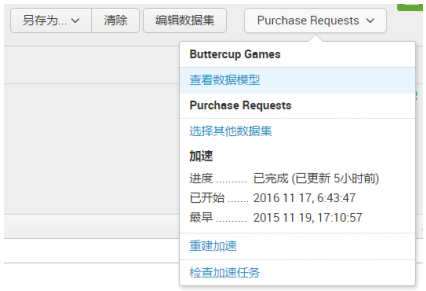
数据透视表的组件

以下展示了数据透视表的编辑器组件。

可视化类型：左侧竖线包含代表不同可视化类型的图标。选择不同的图标控制要显示的数据透视表构建器和报表界面。可视化类型是：统计表（默认）、柱形图、条形图、散点图、气泡图、面积图、折线图、饼图、单值显示、径向仪表、标记规和塞尺。

文档操作：上水平栏显示与文档相关的操作。这些操作包括：

- **另存为...：**将当前报表保存为新报表（**报表**）或仪表板面板（**仪表板面板**）。
- **清除：**将界面重置为初始状态，这将：删除保存的报表（如果适用）、把可视化类型更改为“统计表”，并用数据集计数的单个列值和所有时间的时间过滤器（如 _time 为适用字段）填充报表。
- **数据模型数据集：**此为最右边的按钮。按钮标签源自选定的数据模型数据集。例如，在屏幕截图中它为“购买请求”。使用此菜单可以导航回数据模型列表（**选择另一个数据模型**）、导航回数据模型数据集列表（**选择另一个数据集**）或编辑选定数据模型数据集（**编辑数据集**）。此外，您可以重新构建加速并检查加速任务。



任务操作：“暂停”和“停止”按钮控制“数据透视表”任务的进度。其他操作包括：**共享**、**导出**、**打印**和**在搜索中打开**。单击**在搜索中打开**将打开“搜索”视图，并运行当前搜索字符串。

了解更多信息

本主题简要介绍了您访问数据透视表界面需要了解的内容，本章其余部分介绍如何构建数据透视表。有关更多信息，请阅读《数据透视表手册》。

后续步骤

继续下一主题，其中您将使用数据透视表，从上一章创建的 **Buttercup Games** 数据模型构建报表。

创建并保存数据透视表

本主题向您介绍如何使用数据透视表创建和保存简单报表。本例将使用您在上一章中创建的数据模型数据集。如果您手中没有这些数据集，请参阅“创建新数据模型”。

这是一个非常简单的示例。在本教程的稍后主题，将显示更加复杂的示例。

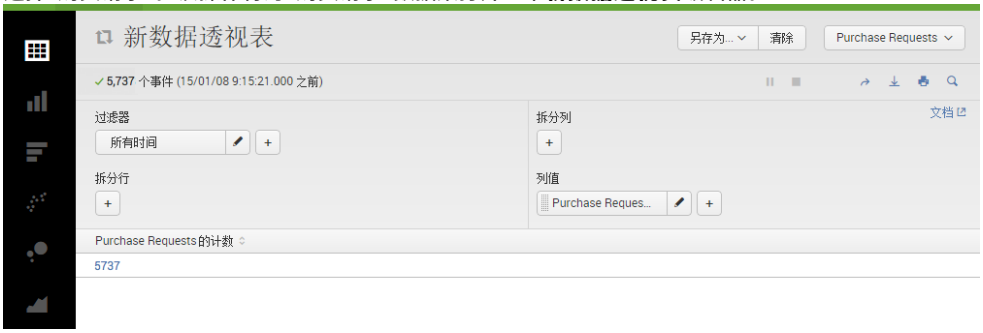
创建新数据透视表

当计划设置报表时，您首先需要选择代表广泛事件数据类别的数据模型进行处理。对于本教程，数据模型是"Buttercup Games"。

1. 选择**设置 > 数据模型。**
2. 在数据模型列表上，单击 **Buttercup Games**。该操作将带您前往**选择数据集**页面。

Buttercup Games 数据模型有一个根数据集，可以追踪源自该游戏网站的“购买请求”。“购买活动”数据集细分为“成功”和“失败”的购买活动。

3. 选择“购买请求”。该操作将为“购买请求”数据集打开一个**新数据透视表**编辑器。



默认情况下，“数据透视表编辑器”界面显示定义数据透视表表格的元素。这里有四个基本数据透视表元素类别：筛选、拆分行、拆分列和列值。首次为特定对象打开“数据透视表编辑器”时，将仅定义两个元素：

- 时间范围筛选元素（设置为“所有”时间）。
- 列值元素（设置为“<dataset_name> 计数”。

该元素为单个值，是数据集在整个时间期间内返回的事件总计数。在这种情况下，该计数是“购买请求的计数”。

4. 从可视化栏选择“单值显示”元素。
5. 在**标签下**的旁边键入**购买请求**。

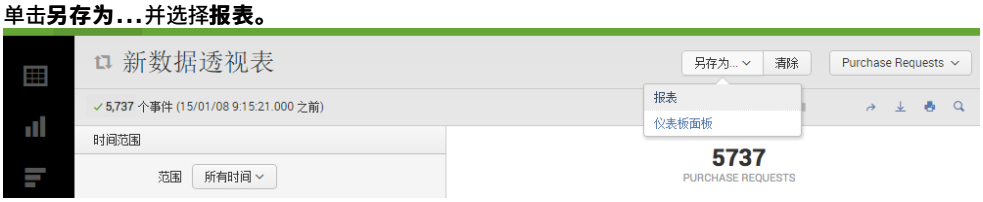
- 默认情况下，时间范围筛选元素被设置为“所有”事件。
- 单值可视化（单值、三个仪表类型）使用首列值元素获取其单值。这里，该字段为“购买请求计数”。
- 单值可视化不使用“拆分行”或“拆分列”元素。
- 您可以格式化数字的精度，并选择是否使用逗号。

将数据透视表保存为报表

在定义数据透视表后，您可以将其保存为报表或仪表板面板。在本示例中，您将单值显示另存为报表。我们将在稍后

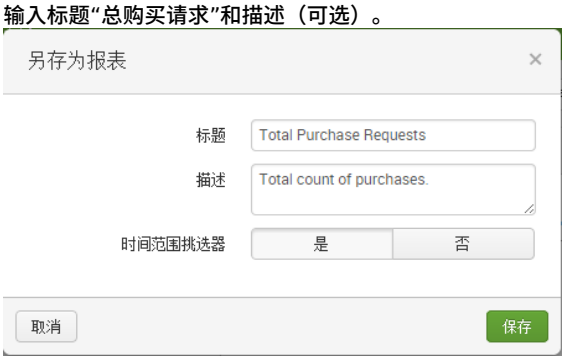
章节介绍仪表板和仪表板面板。

1. 单击**另存为...**并选择**报表。**

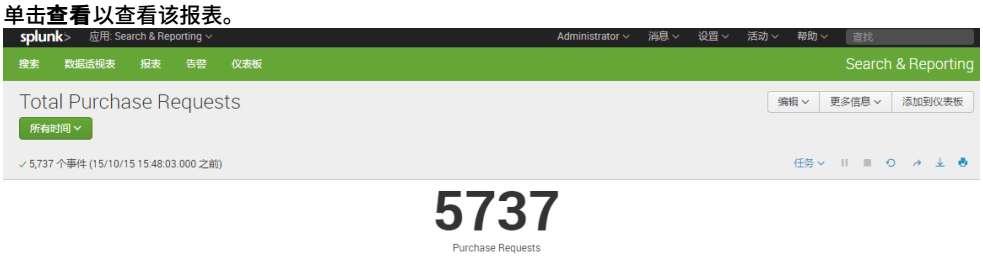


这将打开**另存为报表**对话框。

2. 输入标题“总购买请求”和描述（可选）。



3. 选择**是**以包含时间范围挑选器。（这应是默认值。）
4. 单击**保存**。在保存报表后，将显示窗口表示“您的报表已创建”。您可以继续编辑当前数据透视表，添加数据透视表到仪表板，更改保存的报表的其他设置或查看报表。
5. 单击**查看**以查看该报表。



查看保存的报表

从数据透视表创建的报表将始终保存在当前应用和所有人命名空间下。

1. 单击应用导航栏的**报表**以查看所有已保存报表的列表。

2. 使用 **i** 列中的箭头查看有关**购买总次数请求**报表的信息。

3. 单击报表名称以查看该报表。

后续步骤

在本主题中，您使用数据透视表创建和保存了报表。继续下一主题以创建更多数据透视表可视化。

创建数据透视表表格

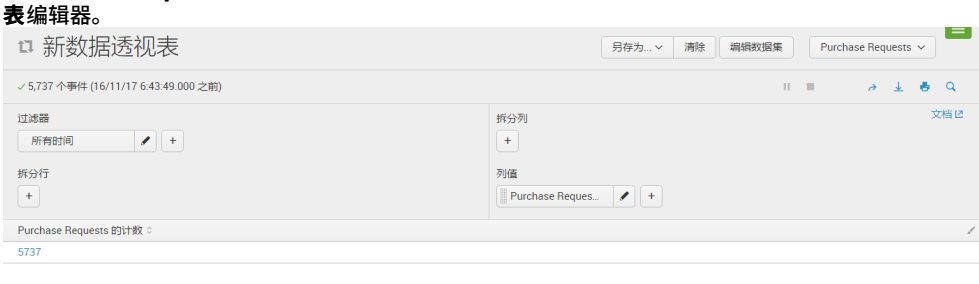
在之前的主题中，您使用数据透视表查找购买请求总数，并保存单值显示为报表。本主题中，您将使用数据透视表可视化编辑器为 Buttercup Games“成功的购买活动”数据集创建一个数据透视表表格。

“成功的购买活动”数据集中的字段针对从 Buttercup Games 网站上购买到的产品。包括自动提取的字段（categoryId 和 productId）及查找字段（价格和 product_name）。

Buttercup Games 网上商店提供数百种各种类别的产品，同时您希望知道有关过去一周购买的物品的详细信息。您可以创建数据透视表报表，该报表按产品名称分解为购买事件总数，同时可快速看到哪些产品在这一周期内的销量最高。

定义新数据透视表

1. 选择**设置 > 数据模型**
2. 选择 **Buttercup Games** 数据模型并选择**成功的购买活动**子数据集。将打开**成功购买**的**新建数据透视表**编辑器。



添加数据透视表元素

您可以添加来自每个数据透视表元素类别的多个元素以定义您的数据透视表表格。在确定表格应提供的信息过程中，可以轻松添加、定义和删除数据透视表元素。

- **要添加数据透视表元素：**单击 + 图标。该操作将打开元素对话框，您可以在其中选择字段，然后定义元素使用该字段的方式。
- **要检查或编辑元素：**单击元素上的“铅笔”图标。这将打开元素对话框。
- **要重新排序和转换数据透视表元素：**在数据透视表元素类别中拖放某个元素可以将其重新排序。在元素类别之间拖放以转换它们。
- **要从数据透视表编辑器删除数据透视表元素：**打开其元素对话框并单击**删除**按钮，或向上或向下拖动元素，直到它变成红色并放下。

在**筛选器**下，当构建数据透视表时，时间筛选始终显示；您无法删除它。它定义了数据透视表返回结果的时间范围。它的用法与整个 Splunk Web 使用的时间范围菜单完全相同。有关更多信息请参阅《搜索手册》中的“选择要应用于搜索的时间范围”。

更改时间范围筛选

目前，您的数据透视表表格显示单值，**所有时间**的“成功购买”的总计数。

将**时间筛选**更改为查看不同时间范围的“成功购买”。

1. 在“过滤器”下，单击**所有时间**旁边的“铅笔”打开时间范围挑选器。

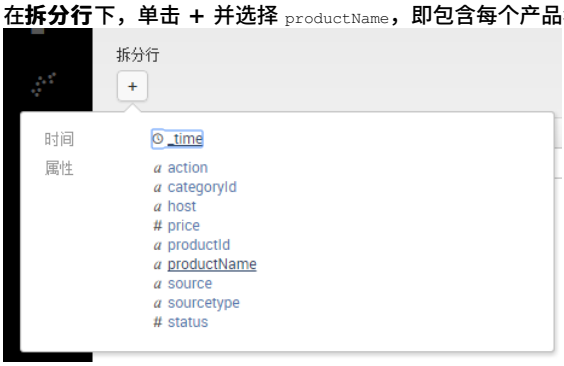
2. 在**预设**和**相对**下，单击“最后 7 天”。

（如果这不显示任何事件，您可以选择“所有时间”并继续。）

添加拆分行元素

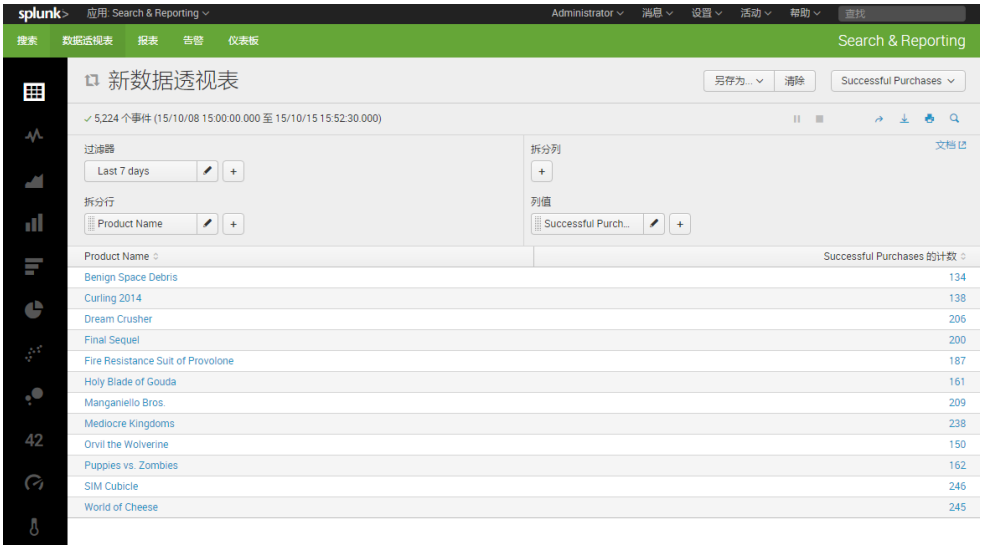
添加数据透视表元素以按名称查看每个产品的“成功购买计数”：

1. 在**拆分行**下，单击 **+** 并选择 `productName`，即包含每个产品名称的查找字段，基于 `productId`。



这将打开允许您设置字段格式的对话框。

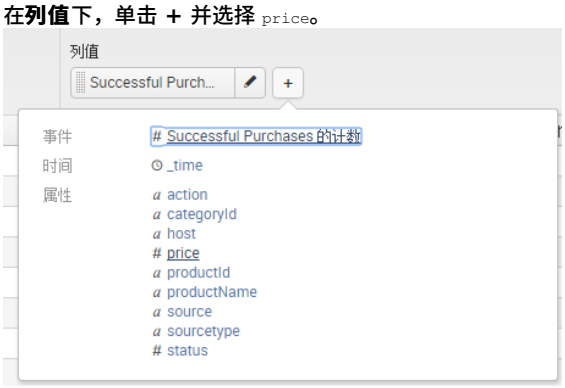
2. 重命名字段**产品名称**并单击**添加到表格**。



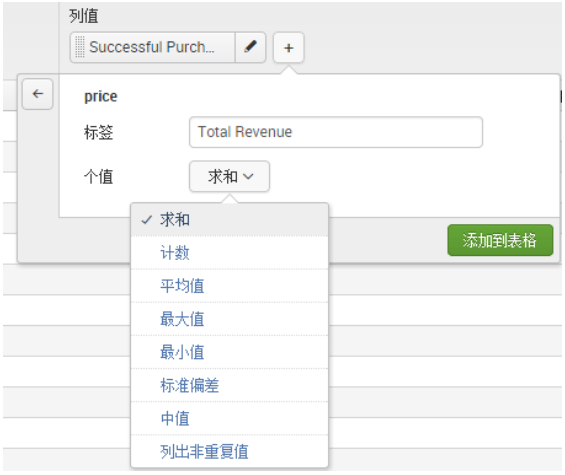
添加列值元素

添加**列值**以查看成功购买的每个产品所赚取的总额：

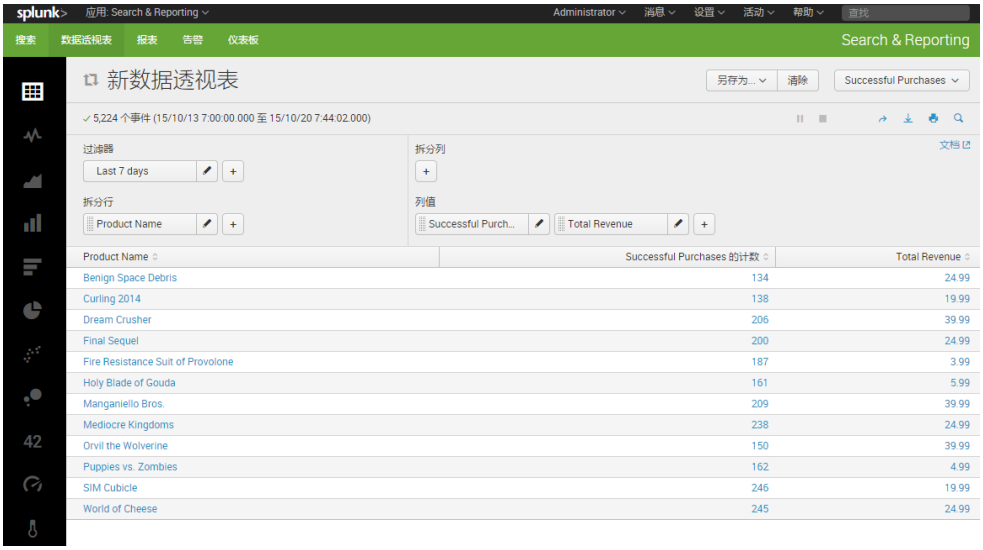
1. 在**列值**下，单击 **+** 并选择 `price`。



2. 在对话框中，设置字段的格式：



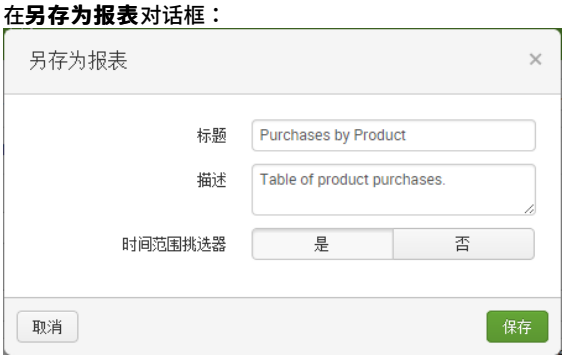
3. 输入标签**总收入**。
4. 选择值**求和**。这将创建名为**总收入**的字段，它是产品的每个成功购买的价格的总和。（如果您要在此表格中查看每个个别产品的成本，则将 `price` 值添加为另一个“拆分行”。）
5. 单击**添加到表格**。



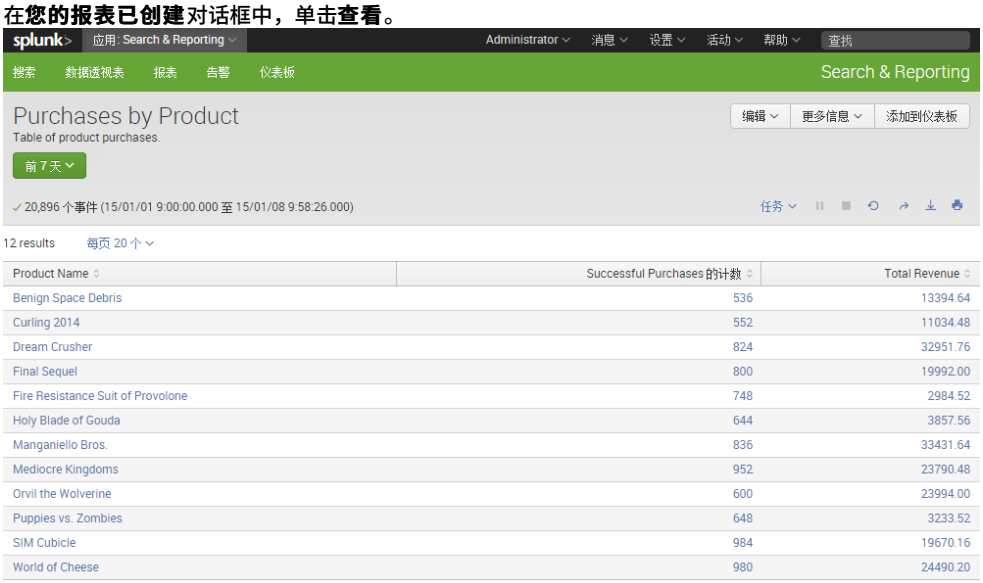
保存数据透视表表格

另存“数据透视表”表格为名为**按产品购买**的报表。

1. 单击**另存为**，然后选择**报表**。
2. 在**另存为报表**对话框：



3. 输入**标题**“按产品分类购买活动”。
4. （可选）添加**描述**“产品购买活动表格”。
5. 包含一个**时间范围挑选器**。
6. 单击**保存**。
7. 在**您的报表已创建**对话框中，单击**查看**。



后续步骤

继续下一主题以创建一些简单的数据透视表可视化。

创建数据透视表图表

在上一个主题，您使用“数据透视表”可视化编辑器来构建表格。本主题中，您将使用相同的数据集创建图表可视化。

定义新数据透视表

有两种方式可以导航至“数据透视表”视图：

- 通过“数据集”页面
- 经由“设置”进入“数据模型”列表页面

前提条件

- 在创建并保存数据透视表中学习如何创建数据透视表。

步骤

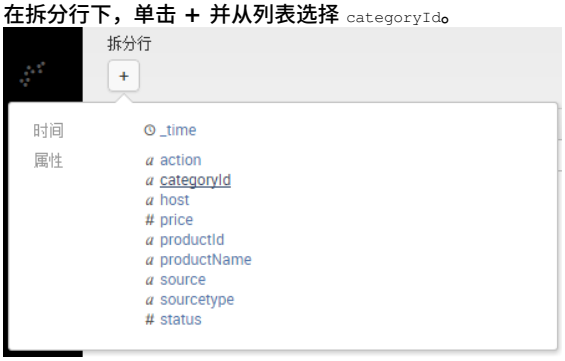
从哪里开始	要做什么
数据集页面	1. 在“搜索和报表”应用中打开“数据集”列表页面 2. 选择成功的购买活动子对象 3. 选择**数据透视表**
设置 > 数据模型	1. 选择**设置 > 数据模型** 2. 选择 Buttercup Games 数据模型 3. 选择成功的购买活动子数据集 4. 选择**数据透视表**

添加数据透视表元素

在上一个主题，我们介绍了按产品 ID 和名称购买。现在，让我们按类别报告成功购买计数。

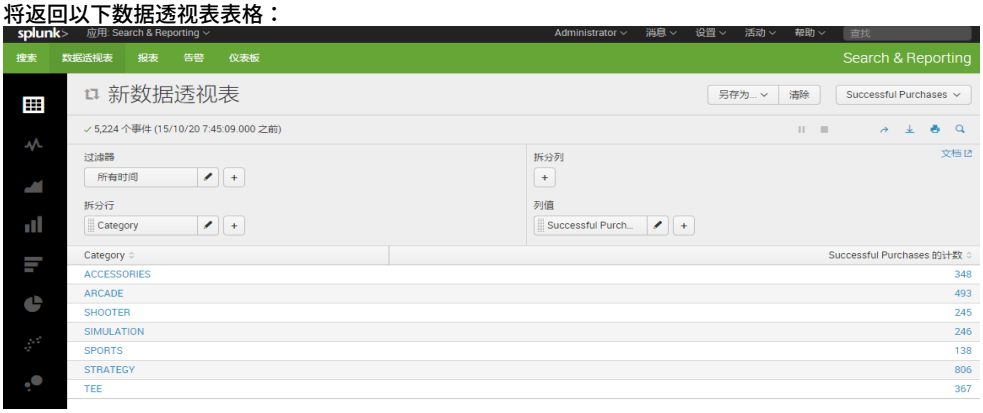
为字段 `categoryId` 添加**拆分行**。

1. 在拆分行下，单击 + 并从列表选择 `categoryId`。



2. 输入标签**类别**并单击**添加到表格**。

将返回以下数据透视表表格：

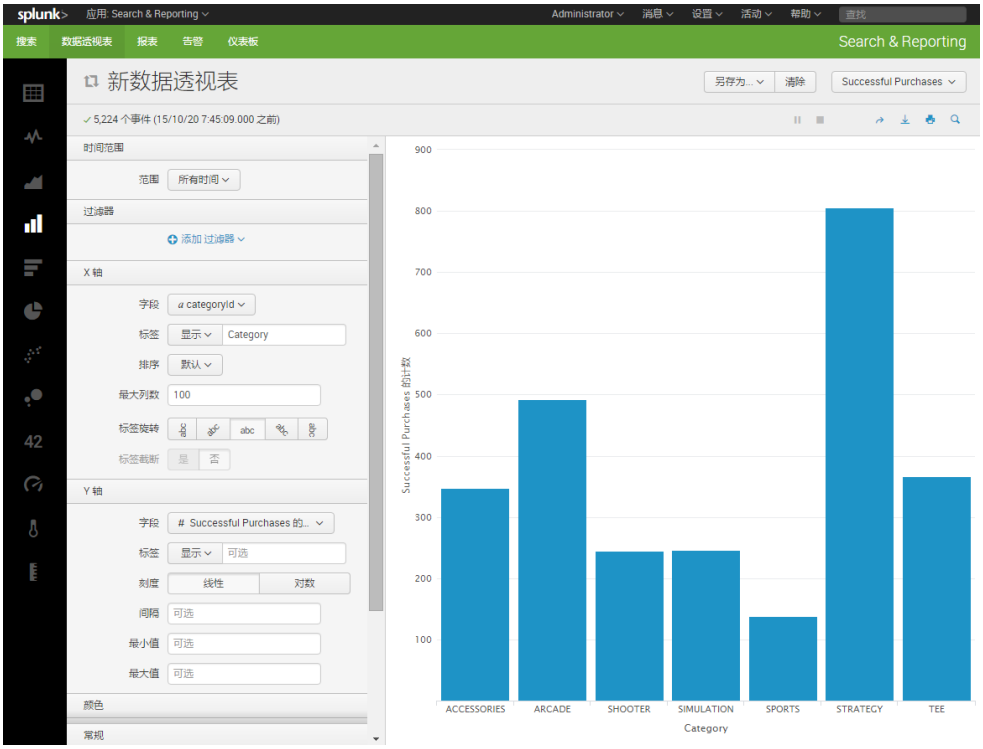


更改可视化类型

1. 单击可视化栏的**柱形图**图标。

柱形图的**新建数据透视表**编辑器显示。

- 柱形图使用数据透视表表格定义中的首个拆分行提供 **X-轴**值。在这种情况下，该**拆分行**是**类别**。
- 柱形图使用数据透视表表格定义中的首个列值提供 **Y 轴**值。这里，**列值**是**成功购买计数**。

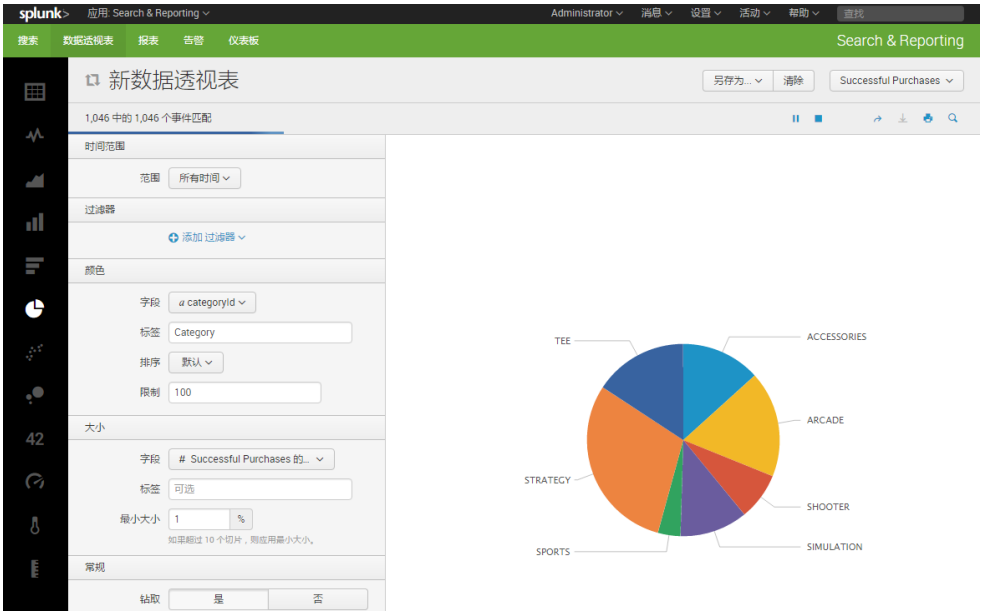


该数据还可以可视化为饼图。

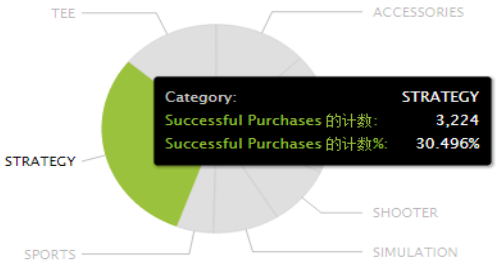
2. 单击可视化栏的**饼图**图标：

柱形图的**新建数据透视表**编辑器显示。

- 饼图使用来自首个**拆分行**元素（类别）的值确定其扇形的数量和颜色。
- 饼图使用首**列值**元素（成功购买计数）确定其扇形的相对大小。



将鼠标悬停在饼图的扇形上以查看指标：类别、成功购买计数和成功购买总计数百分比。



后续步骤

在本章中，您创建了三个数据透视表并将其中两个保存为报表。最后一个数据透视表图表，您将其保存为仪表板面板。继续下一章节以阅读有关仪表板的信息。

第 4 部分：创建仪表板

关于仪表板

Splunk Enterprise 可以帮助您以交互方式轻松地构建并编辑**仪表板**，而无需编写一行 XML 代码。

- **将您刚才创建的数据透视表添加到新的或现有仪表板：**创建您喜欢的数据透视表可视化后，可以使用“创建仪表板面板”功能直接开始创建仪表板。它会引导您基于搜索来创建仪表板面板，并将其添加到新的或现有的仪表板。在完成之后，您仍然处于“数据透视表”视图中。
- **使用“仪表板编辑器”来创建仪表板，并使用仪表板面板来填充它们：**您还可以使用“仪表板编辑器”来编辑现有仪表板。如果您具有一组数据透视表报表，并希望在此基础上快速创建一组仪表板面板，则这种仪表板创建方法非常有用。

更改仪表板权限

您可以从“仪表板编辑器”指定仪表板的访问权限。但是，您的用户角色（以及为该角色定义的功能）可能限制您可以定义的访问权限类型。

如果您的用户角色为*管理员*（具有默认的功能集），则您可以创建专用、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。

更多有关为仪表板和其他知识对象设置权限的信息，请参阅《管理员手册》中的“管理知识对象权限”。

更改仪表板面板可视化

在您使用“仪表板编辑器”创建面板之后，使用“可视化编辑器”来更改在面板中显示的可视化类型，并确定该可视化的

显示方式和行为。“可视化编辑器”只允许您从其数据结构要求与为面板指定的搜索相匹配的可视化类型中选择。

- 如需要概览各种可视化类型及其格式/显示选项，请参阅《仪表板和可视化手册》中的“可视化参考”主题。
- 更多有关可视化类型所需数据结构的信息，请参阅《仪表板和可视化手册》中的“可视化数据结构要求”。

编辑仪表板的 XML 配置

虽然不要求您使用 XML 来构建仪表板，但是通过编辑仪表板的 XML 配置可以编辑仪表板面板。它提供了在“仪表板编辑器”中不具备的功能编辑方式。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。

如果您用“仪表板编辑器”创建仪表板，且想了解更多有关编辑此类仪表板 XML 的信息，请参阅《仪表板和可视化手册》中的“仪表板示例”。

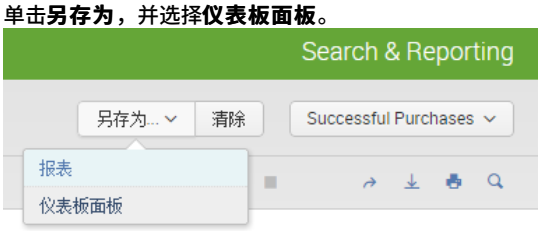
添加数据透视表到仪表板

本主题将继续第 3 部分介绍的内容：设计数据透视表报表。您上次创建的数据透视表是饼图。如果还未创建该图表，您可以返回上一主题完成。现在，您将保存该可视化到新仪表板面板，然后添加所有之前的数据透视表报表到同一仪表板。

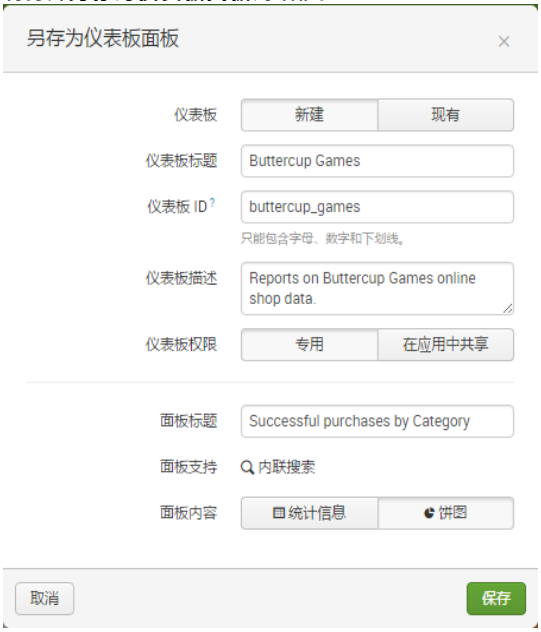
将数据透视表另存为仪表板面板

您刚刚创建了饼图，现在让我们将它保存到仪表板面板。

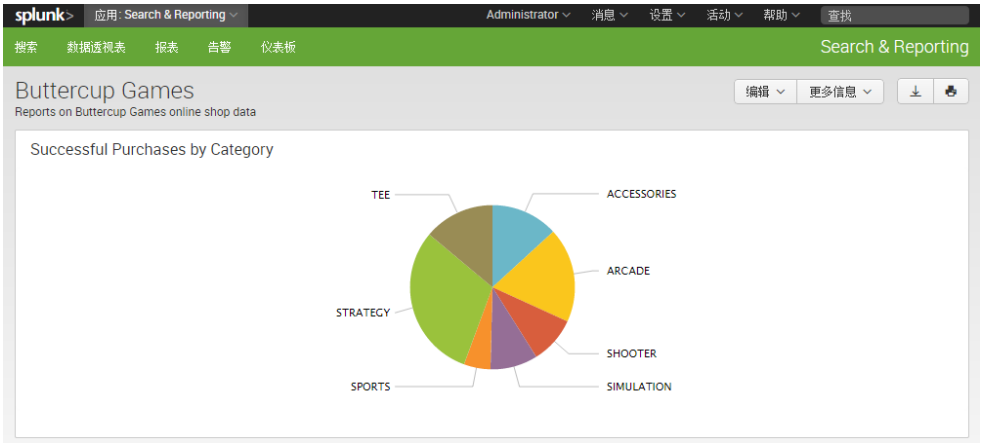
1. 单击**另存为**，并选择**仪表板面板**。



将打开**另存为仪表板面板**对话框。



2. 定义用于保存面板的新仪表板：
   - 对于**仪表板**，单击**新建**。
   - 输入**仪表板标题：**Buttercup Games。**仪表板 ID** 将使用 Buttercup_games 更新
   - （可选）添加**仪表板描述：**报告 Buttercup Games 网上商店数据。
3. 定义仪表板面板：
   - 输入**面板标题：**按类别的成功购买
   - 保留**面板支持**为内联搜索。
   - 对于**面板内容**，单击**饼图**。
4. 单击**保存**。仪表板已成功创建。
5. 要继续，单击**查看仪表板**。



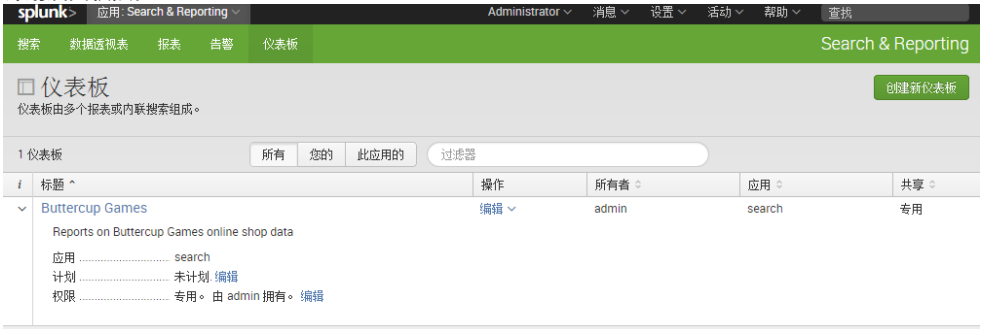
查看和编辑仪表板面板

保存仪表板之后，可以通过单击应用导航栏中的**仪表板**对其进行访问。

1. 单击应用导航栏中的**仪表板**。这将带您前往**仪表板**列表页面。

您可以**创建新仪表板**和编辑现有仪表板。您会看到刚刚创建的 **Buttercup Games** 仪表板。

2. 在 **i** 栏下，单击 **Buttercup Games** 旁的箭头以查看有关仪表板的更多信息：所处的应用上下文、是否已计划及其权限。



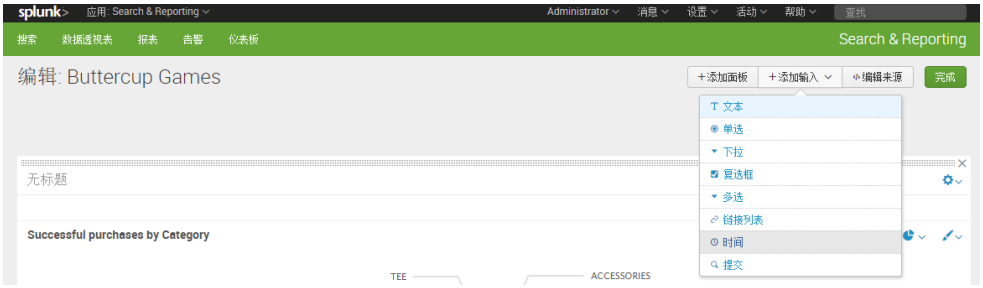
该信息中还提供了可编辑仪表板"计划"和"权限"的快速链接。要查看仪表板，单击仪表板的**标题**或选择**操作**下的**编辑**选项。**注意：**如果您单击查看仪表板，同时无法查看它（或它显示空白），检查您是否拥有对数据模型的读取访问权限。为此，转到**管理数据模型**视图，并编辑 **Buttercup Games** 数据模型的权限以在应用中共享。

将输入添加到仪表板

1. 在**仪表板**列表中，单击 **Buttercup Games** 返回到仪表板。
2. 单击**编辑**并选择**编辑面板**。**编辑：Buttercup Games** 视图打开。

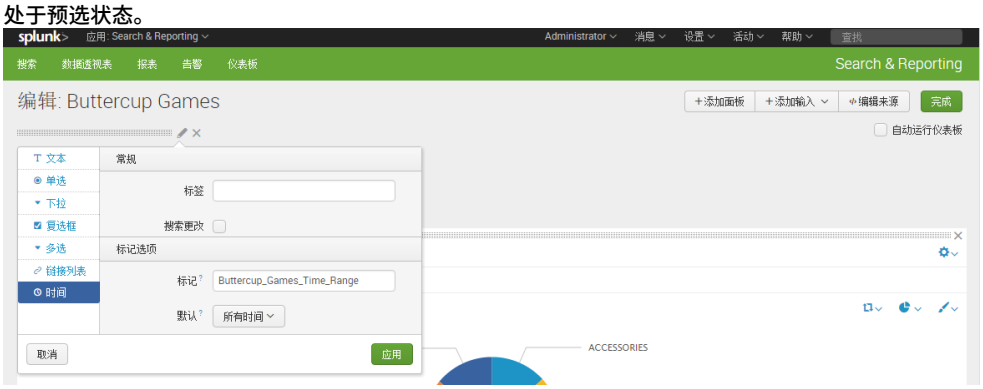
在此视图中，您具有编辑按钮：**添加输入**、**添加面板**并**编辑来源**。

3. 单击**添加输入**并选择**时间**。

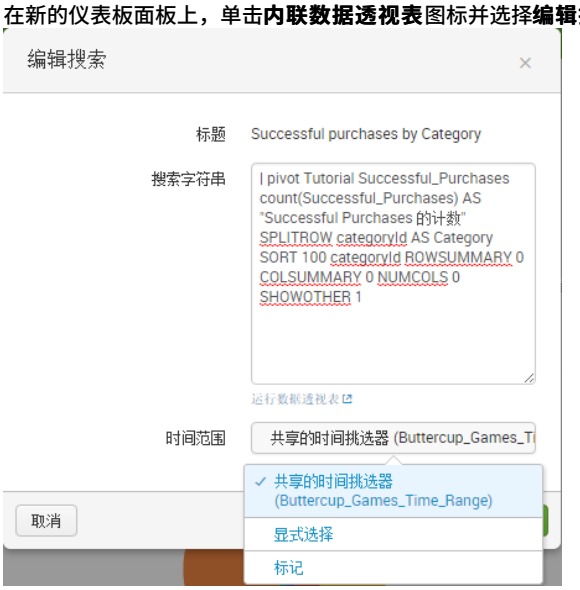


这会将共享的时间范围挑选器的输入添加到仪表板编辑器。

4. 单击用于时间范围挑选器的**编辑输入**图标。它看起来像一支铅笔。这将打开一组输入控件。**时间**输入类型应该处于预选状态。



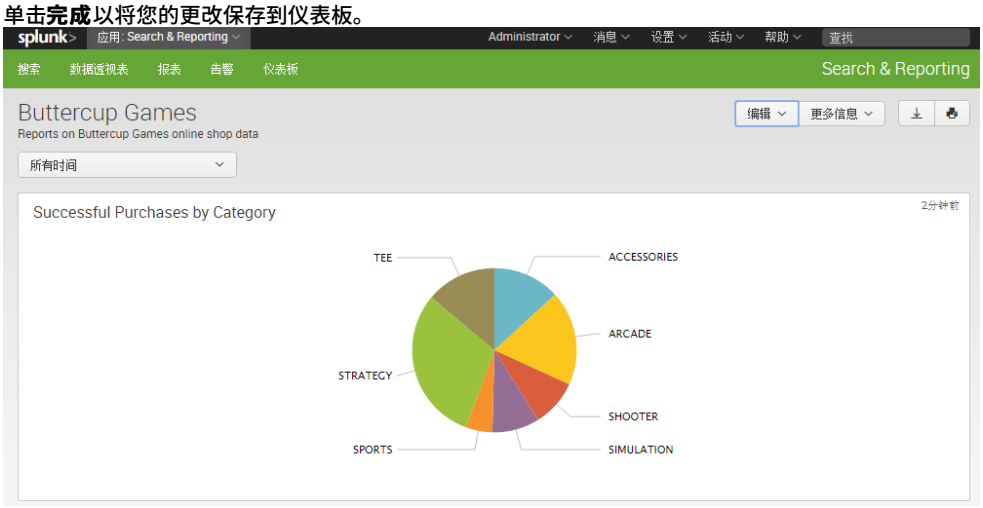
5. 将**令牌**值更改为 **Buttercup_Games_Time_Range** 并单击**应用**。本可选步骤为时间范围挑选器重新定义输入令牌的名称。由于输入令牌的默认名称不太具备描述性（field1、field2、field3 等等），当您在仪表板上有多个输入时您可能希望这样做。这有助于更方便地了解您正在使用哪个输入。您还可以通过更改**默认**值有选择地更改挑选器的默认时间范围。现在默认是**所有时间**。在接下来的两步中，将您的仪表板面板连接到该时间范围挑选器。
6. 在新的仪表板面板上，单击**内联数据透视表**图标并选择**编辑搜索字符串**。这将打开**编辑搜索**对话框。



7. 单击**时间跨度范围**并选择**共享的时间挑选器 (Buttercup_Games_Time_Range)**。
8. 单击**保存**。面板现在连接到共享的时间范围挑选器的输入。操纵面板的内联搜索现在使用为共享的时间范围挑

选器所选择的时间范围。当您添加面板到该仪表板时，重复步骤 6 至 8 来将新的面板连接到共享的时间范围挑选器的输入。您的仪表板必须提供使用共享时间范围挑选器的混合面板，以及为固定时间范围显示数据的面板。

9. 单击**完成**以将您的更改保存到仪表板。



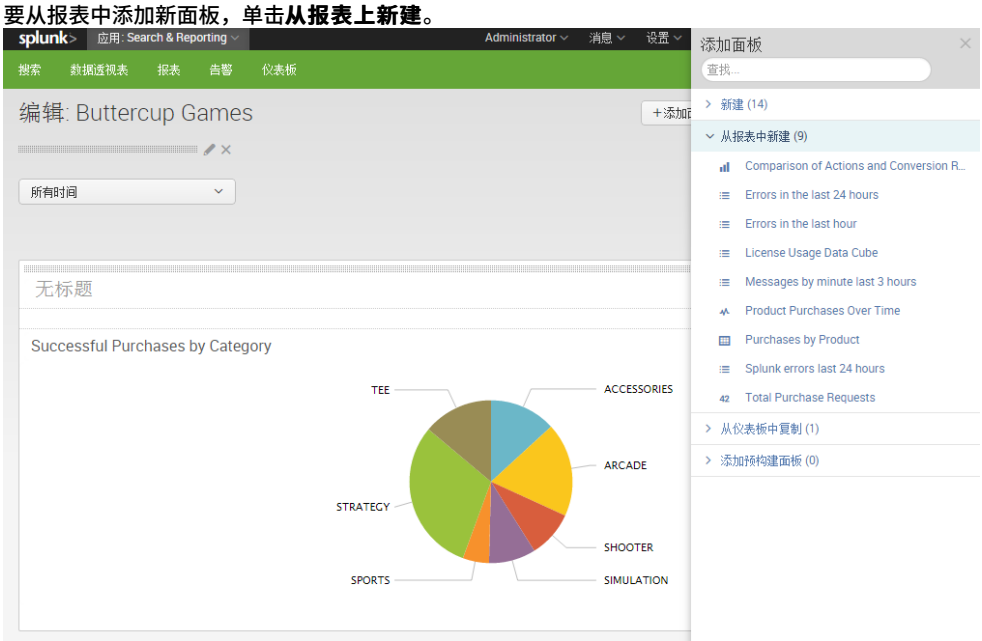
将已保存的报表添加到仪表板

使用您在早期创建的已保存报表中的一个来添加其他面板。

1. 在 **Buttercup Games** 仪表板，单击**编辑**并选择**编辑面板**。
2. 在**编辑：Buttercup Games** 视图中，单击**添加面板**。

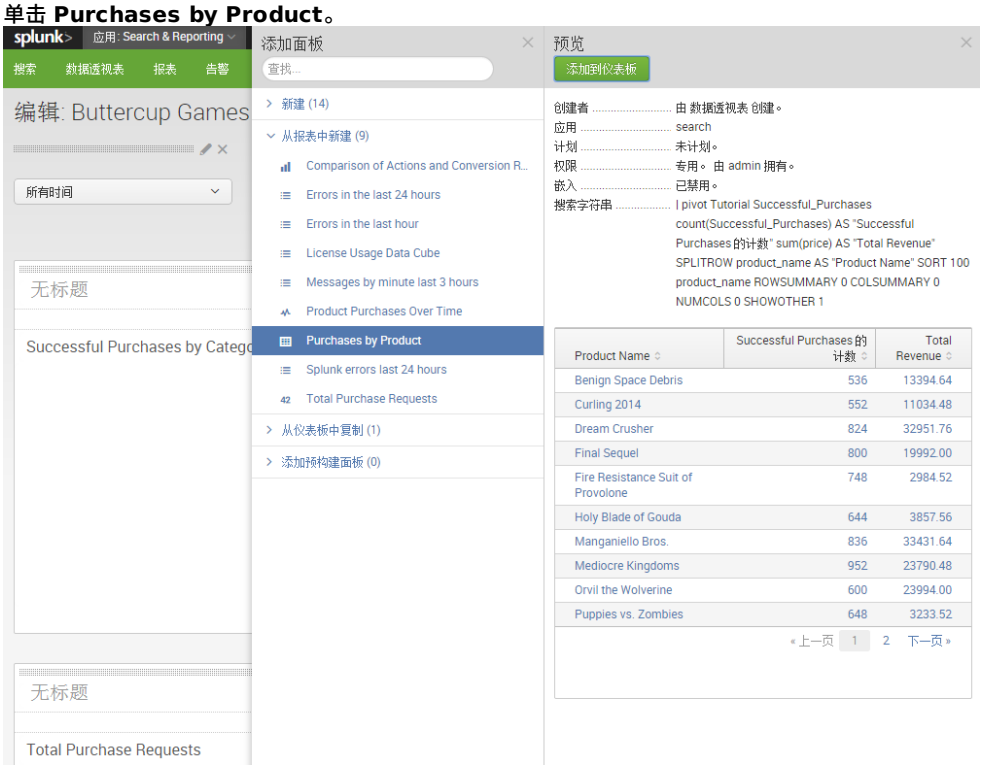
添加面板边栏菜单幻灯片打开。

3. 要从报表中添加新面板，单击**从报表上新建**。



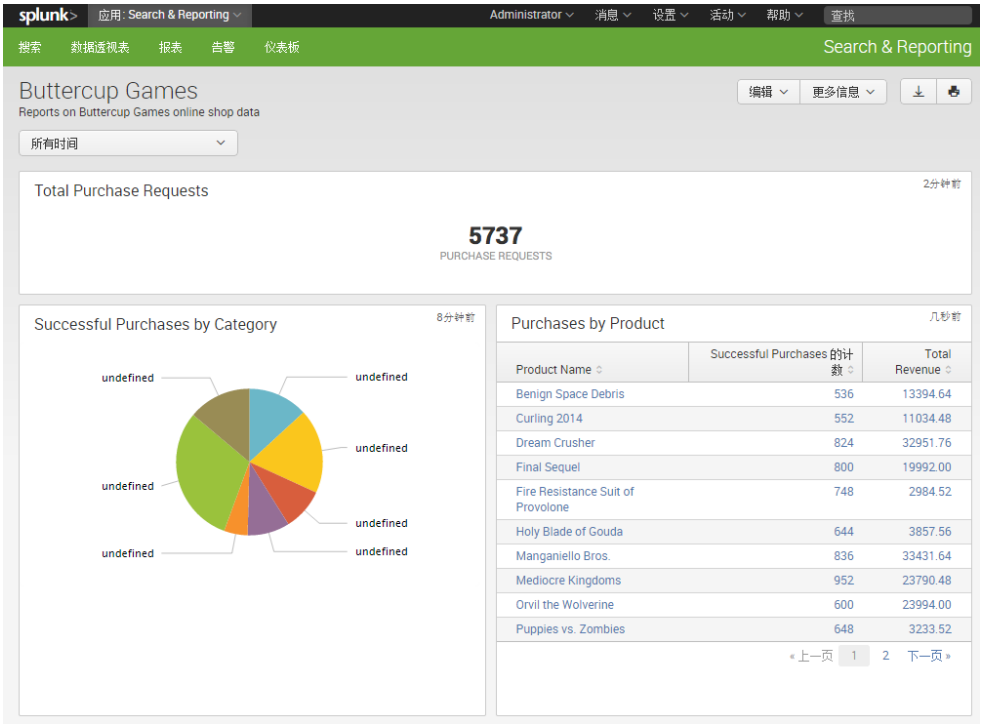
4. 单击**购买总次数请求**。此幻灯片将打开预览面板，显示保存的报表相关信息。

5. 单击**添加到仪表板**。新面板放置到仪表板编辑器。您可通过单击任何地方以关闭**添加面板**边栏菜单或选择另一个报表以添加到仪表板。在关闭**添加面板**边栏菜单前，添加第二个报表。
6. 单击 **Purchases by Product**。



7. 单击**添加到仪表板**。
8. 关闭边栏菜单。在仪表板编辑器视图中，拖放此面板，以在仪表板上对其进行重新排列。**注意：**如果您想要新面板使用共享的时间范围挑选器输入，请重复步骤 6 到 8 从“添加输入至仪表板”过程开始，以将他们连接到输入。

9. 单击**完成**。您的仪表板外观应如下所示：



后续步骤

这将完成数据模型和数据透视表教程。继续到下一章节，阅读您接下来可以做什么。

后续步骤

更多数据模型和数据透视表资源

本教程简要介绍了构建数据模型，然后使用它们创建数据透视表可视化和报表。有关更多详细信息，请参阅以下手册：

- **知识管理器手册：**包含介绍如何使用“数据模型编辑器”设计和构建数据模型的部分。
- **数据透视表手册：**介绍如何使用“数据透视表编辑器”为事件数据生成表格、图表和可视化。

我们鼓励您研究教程数据，运行更多搜索并创建更多仪表板！

要了解有关 Splunk 搜索处理语言的更多信息，请参阅《搜索教程》。

要了解有关 Splunk Enterprise 的更多功能及其使用方法，请参阅教育视频和课程部分。