



Splunk® Enterprise 8.2.0

仪表板和可视化

生成时间: 2021 年 5 月 24 日, 14:44

Table of Contents

简介	4
入门	4
可视化入门	6
可视化参考	6
可视化的数据结构要求	7
事件列表	8
使用事件列表	8
表格可视化	10
表格可视化概述	10
生成表格	10
设置表格可视化的格式	11
表格列简单 XML	16
图表	23
图表概述	23
图表的数据	24
饼图	24
柱形图和条形图	26
折线和面积图	28
散点图	31
气泡图	32
图表的事件注释	33
图表显示问题	35
单值	38
概述	38
生成单值	38
自定义单值	39
仪表	42
使用仪表	42
地图	44
映射数据	44
生成分级统计地图	44
配置分级统计地图	46
使用 IP 地址生成分级统计地图	47
群集地图	48
教程：使用新的地理空间查找生成分级统计地图	51
教程概述	51
查找并下载 USDM 数据	51
上载并配置数据	52
下载加州各县的图形文件	53
新建地理空间查找	53
生成分级统计地图	54
(可选) 使用棚架视图可视化多个聚合函数	56
可视化的棚架布局	58
使用棚架布局拆分可视化	58
仪表板入门	64
仪表板概览	64
关于“仪表板编辑器”	65
在 Splunk Web 中构建和编辑仪表板	67
新建仪表板	67
使用仪表板面板	67
向仪表板添加面板	68
编辑仪表板	71
编辑可视化	73

新建和编辑表单	74
用简单 XML 新建仪表板	86
编辑简单 XML	86
搜索驱动仪表板和表单	87
仪表板和表单	97
仪表板示例	97
表单示例	106
使用第三方 XML 编辑器	112
钻取和仪表板交互	115
使用钻取构建仪表板交互性	115
链接到搜索	117
链接到仪表板	121
链接到 URL	126
管理当前仪表板中的标记值	129
仪表板中的标记用法	135
图表控制	150
管理和共享仪表板	155
配置仪表板权限	155
生成仪表板 PDF	156
复制和管理仪表板	159
简单 XML 引用	161
简单 XML 引用	161
图表配置参考	207
事件处理程序参考	218
标记参考	237
自定义简单 XML	238

简介

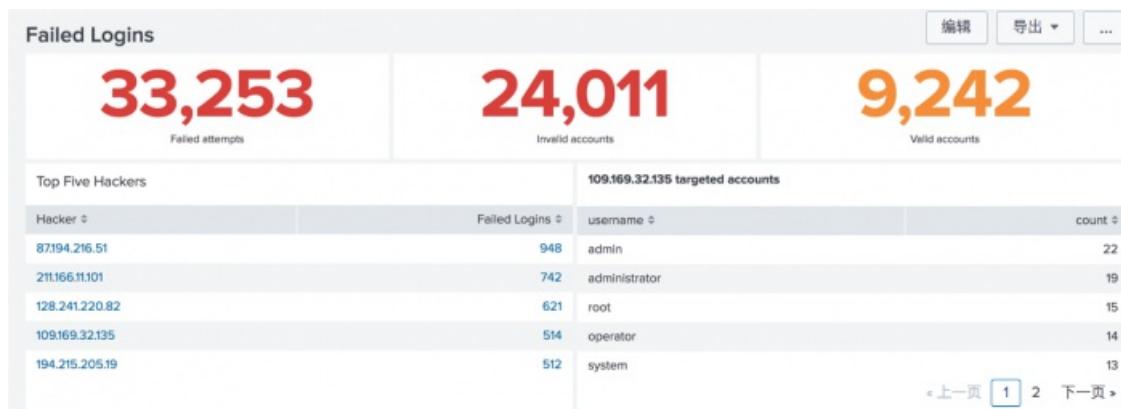
入门

了解如何分享有关数据可视化和仪表板的见解。

现在有两种不同的框架可用于创建可视化和仪表板。Splunk 经典仪表板和可视化框架使用简单 XML 作为源代码，用户界面受限。Splunk Dashboard Studio 框架使用 JSON 格式段落作为仪表板中对象和整个仪表板的源代码。用户界面或可视编辑器有很多格式选项。例如，您可以将可视化直接添加到仪表板并捕捉到搜索，称为数据源，不需要进入源编辑器或使用“搜索和报表”。要了解有关 Splunk Dashboard Studio 的更多信息，请参阅《*Splunk Dashboard Studio*》。

要查看比较两个框架之间主要功能可用性的表格，请参阅《*Splunk Dashboard Studio*》手册中的“比较经典 Splunk 仪表板（简单 XML）和 Splunk Dashboard Studio”。

要查看在创建经典仪表板和可视化时您将使用的最常用操作、定义和命令的简短简介的 PDF，请参阅“*Splunk 仪表板快速参考指南*”。



可视化和仪表板工作流

您有时可能需要生成新的可视化或编辑现有仪表板。仪表板和可视化的相关操作包括一个或多个以下任务。

选择可视化

- 选择一个可视化以显示特定数据见解。
- 要查找和比较可视化选项，请参阅“[可视化引用](#)”。

生成和配置可视化

- 编写一个搜索来生成可视化。确定此搜索以可正确呈现可视化的格式返回结果。请参阅“[可视化的数据结构要求](#)”大致了解数据格式。
- 经典仪表板和可视化中创建的可视化，可在“[搜索和报表](#)”中创建，并添加到仪表板或报表中。使用 Splunk Dashboard Studio 创建的可视化也可以在“[搜索和报表](#)”中创建，并添加到 Dashboard Studio 中预先存在或新建的仪表板中，或者可以在 Dashboard Studio 的可视编辑器中创建。
- 配置或更新可视化外观和行为。更改颜色模式、添加标题或调整其他可视化元素。请参阅“[可视化参考](#)”大致了解每个可视化类型的经典选项和详情链接。

构建和编辑仪表板

- 将可视化添加到经典 Splunk 仪表板框架或 Dashboard Studio 中的新建或现有仪表板中。
- 使用编辑用户界面调整仪表板组件。
- 通过添加用户输入将仪表板转换为表单。
- 要开始之前，请参阅“[仪表板概览](#)”和“[新建仪表板](#)”。要开始使用 Splunk Dashboard Studio，请参阅《*Splunk Dashboard Studio*》手册中的“[关于 Splunk Dashboard Studio 编辑器](#)”。

共享和管理仪表板

- 导出仪表板进行共享。要开始之前，请参阅“[生成仪表板 PDF](#)”。
- 管理仪表板的查看和编辑权限。有关详细信息，请参阅“[配置仪表板权限](#)”。
- 复制仪表板或在应用的主页面显示仪表板。要了解更多信息，请参阅“[复制和管理仪表板](#)”。

编辑简单 XML

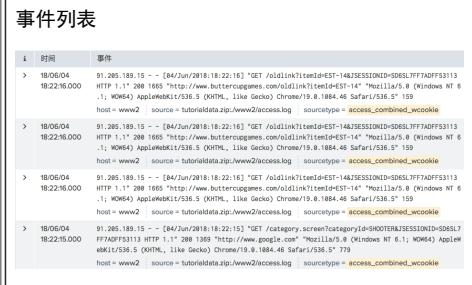
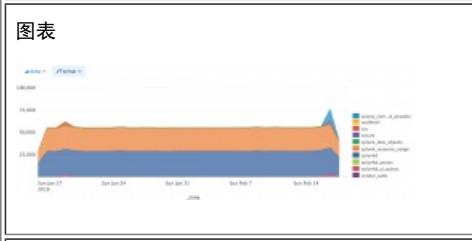
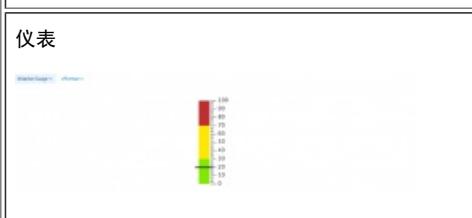
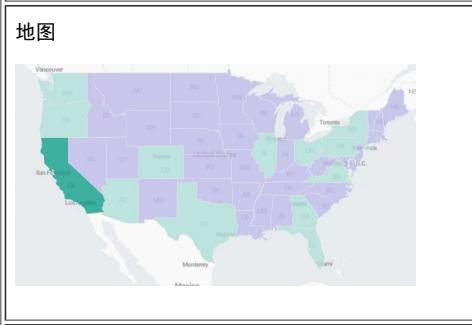
- 使用简单 XML 源代码来自定义仪表板内容和行为。有关概述信息，请参阅“关于编辑简单 XML”；有关详细信息，请参阅“简单 XML 引用”。

可视化入门

可视化参考

比较各选项并选择一个可视化来显示所需的数据见解。

要快速查看通用可视化的最基本概览和使用案例，注意您可以点击“开始”中的链接访问 Splunk 仪表板快速参考指南。

可视化	用法	更多信息请参阅
<p>事件列表</p> 	<p>显示搜索生成的事件。</p> <ul style="list-style-type: none">显示事件，但不进行额外处理。直接在仪表板中显示提取的字段和值。用户可单击事件字段或时间戳来打开更具体的搜索。	<p>使用事件列表</p>
<p>表格</p> 	<p>比较并聚合字段值。</p> <ul style="list-style-type: none">将一个或多个特定字段从搜索结果中隔离。为特定字段添加格式，以突出显示趋势或模式。	<p>表格可视化概述</p>
<p>图表</p> 	<p>可视化数据集中的一个或多个维度。</p> <p>使用以下一种图表类型，具体取决于您要可视化的维度（或字段）的数量。</p> <ul style="list-style-type: none">饼图面积图、折线图、柱形图、条形图气泡图和散点图	<p>图表概述</p>
<p>单值</p> 	<p>在上下文中显示聚合指标。</p> <ul style="list-style-type: none">实时跟踪近期更改或趋势。使用颜色来动态添加上下文。	<p>单值概述</p>
<p>仪表</p> 	<ul style="list-style-type: none">显示一个范围内的聚合指标。在指标逼近特定目标时对其进行跟踪。	<p>使用仪表</p>
<p>地图</p> 	<p>可视化带地理坐标的数据。</p> <ul style="list-style-type: none">使用分级统计地图显示和对比区域性趋势和密度。使用标记地图绘制地理数据。	<p>映射数据</p>

自定义可视化	<p>分析和代表唯一数据集。</p> <p>管理员必须安装自定义可视化应用，以便这些应用可为 Splunk 用户所用。</p>	<p>有关更多详细信息，请参阅“自定义可视化”。</p>
--------	---	------------------------------

可视化的数据结构要求

可视化需要特定格式或数据结构的搜索结果。编写查询以确保所生成结果的格式符合所构建可视化的需求。

本主题提供可视化数据结构的概述。要了解特定可视化的要求和如何以正确格式生成结果，请参阅以下主题之一。

事件列表

[使用事件列表](#)

表格可视化

[生成表格](#)

图表

[饼图](#)

[柱形图和条形图](#)

[折线和面积图](#)

[散点图](#)

[气泡图](#)

单值

[生成单值](#)

仪表

[使用仪表](#)

地图

[映射数据](#)

有关可视化选项的概述，请参阅本手册中的“[可视化参考](#)”。

数据和格式要求

根据您所新建的可视化，您可以使用特定搜索命令以正确格式生成结果。例如，许多可视化需要使用转换命令的搜索来呈现，如 stats、chart、timechart 或 geostats。

图表可对一个或多个数据系列或相关数据点进行可视化。取决于图表类型或复杂度，数据系列的数量和顺序可能有所不同。

单值和仪表可视化代表单个数字值。

映射结合查询和其他数据组件，包括带坐标或位置信息的数据、查找定义和地理标记文件。

使用统计表

在新建可视化时，可以在运行搜索后查看统计表，以确保所生成的结果字段均正确。统计表中列的数量和顺序代表搜索所生成的数据结构。

其他信息

查看特定可视化主题了解数据格式要求和查询建议。

关于可生成可视化的搜索命令，若想了解更多信息，请查看以下主题。

- [《搜索参考》中的“统计和图表函数”](#)
- [《搜索手册》中的“关于转换命令”](#)

事件列表

使用事件列表

在仪表板中添加一个事件列表，使用户可以访问某搜索生成的事件、字段和值。与图表或其他可视化不同的是，事件列表不会提取或处理搜索结果。

生成事件列表

事件列表中的内容取决于您所运行的搜索。没有其他额外数据格式要求。

前提条件

请参阅“配置选项”。

步骤

1. 在搜索页面中，运行一个搜索。
2. 选择事件选项卡以查看事件列表。
3. (可选) 选择另存为 > 仪表板面板，将事件列表添加到仪表板中。
4. (可选) 使用格式菜单或简单 XML 配置事件列表。

“配置”选项

使用格式菜单配置一个或多个如下所示的事件列表组件。您也可以使用简单 XML 对这些组件进行调整，并添加额外配置。

显示和格式选项

使用以下设置调整事件列表外观。

- 选择一个事件显示选项。
 - 列表(默认值)：分别显示每个事件的时间戳。
 - 原始：显示原始事件。
 - 表格：以表格形式显示事件。此格式与统计表可视化不同。
- 配置表格行编号、换行和最大行数

钻取

使用钻取编辑器和/或简单 XML 以启用和配置事件列表上的钻取。请参阅“将钻取用于仪表板交互”以了解有关启用和配置钻取的详细信息。

在简单 XML 中配置事件列表上的钻取时，您可以指定以下一项钻取设置以提供不同的分段选择选项。

钻取设置	用户可用的分段选项	示例
完全	选择一个主要段，或一个或多个连续的次要段。 第一个实例显示的是次要段选项。第二个实例显示的是主要段选项。	"GET /servicesNS/admin/simplexml/data/ui/viewstates?search=name%")" 200 1868 - - 8ms "GET /servicesNS/admin/simplexml/data/ui/viewstates?search=name%")" 200 1868 - - 8ms
内部	选择单个次要段。	"GET /servicesNS/admin/simplexml/data/ui/viewstates?search=name%")" 200 1868 - - 8ms
外部	选择一个完整的主要段。	"GET /servicesNS/admin/simplexml/data/ui/viewstates?search=name%")" 200 1868 - - 8ms
无	禁用钻取(默认)	

注意：如果事件的文本单独行较长，则处理事件分段是可能会导致浏览器性能问题。

有关更多信息，请参阅《知识管理器手册》中的“事件分段的类型”。

使用案例情景

管理员通过事件列表使用户可以访问最近的显著系统事件。要生成事件列表，管理员要运行以下搜索。

```
error OR failed OR severe OR ( sourcetype=access_* ( 404 OR 500 OR 503 ) )
```

管理员将事件列表添加至跟踪系统状态的仪表板中。仪表板用户单击列表中的事件字段或时间戳即可打开使用了所单击内容的搜索。

i	时间	事件
>	2/21/18 5:06:16.192	02-21-2018 17:06:16.192 +0000 ERROR FromProcessor - Error in 'from' command: Invalid argument: 'error' host = so1 source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
>	2/21/18 5:06:16.192	02-21-2018 17:06:16.192 +0000 ERROR FromProcessor - Error in 'from' command: Invalid argument: 'error' host = so1 source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
>	2/21/18 4:51:38.331	02-21-2018 16:51:38.331 +0000 WARN HttpListener - Socket error from 10.32.31.191 while accessing /en-US/statistics/@B73853057830FAE7E572FD0CF4B6938B3554E8A880F662E419C6A5159F9D0BDC/js/common.min.js: Broken pipe host = so1 source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
>	2/21/18 4:44:00.686	02-21-2018 16:44:00.686 +0000 ERROR IntrospectionGenerator:resource_usage - RU - Mount '/' () is not interesting, iostats will not be collected. host = so1 source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
>	2/21/18 4:43:58.383	02-21-2018 16:43:58.383 +0000 INFO WatchedFile - File too small to check seekcrc, probably truncated. Will re-read entire file='/opt/splunk/var/log/splunk/django_error.log'. host = so1 source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd

例如，单击某个事件中的来源值 `/opt/splunk/var/log/splunk/splunkd.log` 会在新窗口中打开以下搜索。

```
* source="/opt/splunk/var/log/splunk/splunkd.log"
```

表格可视化

表格可视化概述

表格有利于比较和聚合字段值。使用表格将整个数据集范围内的一个或多个指标的模式进行可视化。首先先用一个查询来生成一个表格，并利用格式突出显示值、添加上下文或新建可视化的侧重点。

Sales this month

Accessories and arcade game sales

categoryId	itemId	count
STRATEGY	EST-13	197 units
STRATEGY	EST-14	189 units
STRATEGY	EST-12	180 units
STRATEGY	EST-15	173 units
STRATEGY	EST-16	165 units
STRATEGY	EST-6	162 units
STRATEGY	EST-26	160 units
STRATEGY	EST-18	159 units
STRATEGY	EST-19	158 units
STRATEGY	EST-11	157 units
STRATEGY	EST-7	154 units
STRATEGY	EST-21	150 units
STRATEGY	EST-17	147 units
STRATEGY	EST-27	147 units
ARCADE	EST-16	115 units
ARCADE	EST-21	114 units
ARCADE	EST-13	109 units
ARCADE	EST-11	107 units
ARCADE	EST-19	104 units
ARCADE	EST-15	98 units

<上一个 1 2 3 4 5 6 7 8 9 ... 下一步>

新建表格可视化

了解如何生成和配置表格可视化。有关详细信息，请参阅下面的主题。

- 生成表格
- 设置表格可视化的格式
- 表格列简单 XML

生成表格

要生成表格，编写一个包含转换命令的搜索。从搜索页面运行搜索并选择统计选项卡以查看并设置表格格式。

您可以使用搜索中的 `table` 命令指定表格包含的字段或更改表格行的顺序。

搜索示例

• 转换搜索

此搜索使用 `chart` 转换命令。

```
index = _internal | chart avg(bytes) over sourcetype
```

此搜索会生成一个包含两列的表格。

事件 (282,982) 模式 [统计信息 \(12\)](#) 可视化

每页 20 个 格式 预览

sourcetype	avg(bytes)
first_install-too_small	
mongod	
scheduler	
splunk_archiver-too_small	
splunk_web_access	212415.976
splunk_web_service	
splunkd	67108864
splunkd_access	18524.06596767147
splunkd_conf	
splunkd_stderr	
splunkd_stdout	
splunkd_ui_access	1659.3662621167941

- 使用表格命令转换搜索

此搜索会生成包含 action、host 和 count 列的表格。

```
index = _internal | stats count by action, host
```

事件 (283,197) 模式 [统计信息 \(3\)](#) 可视化

每页 20 个 格式 预览

action	host	count
acquire_mutex	debianSplunk	98
base_initialize	debianSplunk	2
edit	debianSplunk	12

要改变出现在表格的列或更改列的顺序，请将 table 命令添加到此搜索。例如，添加 | table host count 以生成只包含 host 和 count 列的表格。

```
index = _internal | stats count by action, host | table host count
```

事件 (283,504) 模式 [统计信息 \(3\)](#) 可视化

每页 20 个 格式 预览

host	count
debianSplunk	98
debianSplunk	2
debianSplunk	12

表格迷你图

迷你图以结果集的形式显示数据模式或趋势。要生成表格迷你图，可在搜索中将 sparkline 功能与 stats 或 chart 结合使用。

迷你图宽度取决于默认的数据分箱。您可将数据分箱作为 sparkline 命令的一个参数来进行调整。

有关更多信息，请参阅《搜索手册》中的“为您的搜索结果添加迷你图”。

设置表格可视化的格式

使用格式菜单配置表格可视化。

添加摘要统计信息

使用格式菜单的摘要选项卡，将列总计和百分比包含在内。对于每个统计，表格底部会出现突出显示的摘要行。每个包含数字

值的列在其底部会显示行总计和/或百分比。

注意：摘要行的值反映的是整个搜索结果集的统计数据。对于结果超过一页的表格，摘要行的值不会仅适用于当前显示的页面。

摘要行和数据行的差异

表格中的数据行和摘要行之间存在一些行为和格式差异。

行为或格式	摘要行	数据行
静态突出显示颜色	是	否
行中的值可能会扭曲表格的颜色格式或数据叠加	否	是
列编号格式适用于行	是	是
钻取可用于行	否	是
包含在 PDF 或 CSV 报表中	否	是

总计数据行行为

静态摘要行适用于大部分的使用场景。如果在搜索中使用 `addcoltotals` SPL 命令生成总计数据行，则请注意以下表格行为影响。

- `addcoltotals` 行被视为表格中的数据行。
- 因为将这些行作为数据行进行处理，PDF 或 CSV 仪表板导出中将包含 `addcoltotals` 行。
- 如果表格包含 `addcoltotals` 数据行，则色标或数据叠加可能会有所扭曲。
- 表格不应同时包含 `addcoltotals` 数据行和列总计摘要行。如果您选择要包含总计摘要行，则应调整搜索以移除 `addcoltotals` 命令。

摘要行示例

以下示例显示将列总计和百分比行添加至表格中的使用场景。

总计摘要行

一个在线零售商的分析师在评估客户动作（如购买或数量变化）与产品类型之间的关系。此分析师也在比较不同客户动作的相对频率。

以下查询会生成一个表格，列出每个客户动作的产品类型计数。

```
... | chart count(itemId) over categoryId by action
```

分析师使用格式菜单将总计摘要行添加至表格中。

The screenshot shows a search results interface with a table. At the top, there are tabs for '事件 (118,596)' (Events), '模式' (Mode), '统计信息 (6)' (Statistics), and '可视化' (Visualization). Below these are filters: '每页 20 个' (20 per page), '格式' (Format), and '预览' (Preview). The table has columns: 'categoryId' (with a dropdown arrow), 'addtocart' (with a dropdown arrow), 'changequantity' (with a dropdown arrow), 'purchase' (with a dropdown arrow), 'remove' (with a dropdown arrow), and 'view' (with a dropdown arrow). The data rows are: ACCESSORIES (93, 43, 387, 43, 135), ARCADE (104, 51, 537, 57, 220), SIMULATION (54, 24, 273, 33, 110), SPORTS (24, 27, 148, 12, 65), STRATEGY (167, 87, 885, 92, 344), TEE (86, 25, 404, 39, 151), and a summary row (528, 257, 2634, 276, 1025). The 'remove' column shows significantly lower values than the other actions.

categoryId	addtocart	changequantity	purchase	remove	view
ACCESSORIES	93	43	387	43	135
ARCADE	104	51	537	57	220
SIMULATION	54	24	273	33	110
SPORTS	24	27	148	12	65
STRATEGY	167	87	885	92	344
TEE	86	25	404	39	151
	528	257	2634	276	1025

总计行列出每个客户动作的相应总计数。例如，结果集中有 2634 个购买事件，而产品删除事件只有 276 个。

百分比摘要行

分析师新建了一个表格，用于列出一个零售网站的购买活动。以下查询会比较不同产品类型的购买情况并生成结果。

```
... | chart count(itemId) over action by categoryId
```

通过格式菜单，分析师添加了一个百分比行至表格中。

事件 (118,596)		模式	统计信息 (1)	可视化				
每页 20 个		格式	预览					
action	ACCESSORIES	ARCADE	NULL	SHOOTER	SIMULATION	SPORTS	STRATEGY	TEE
purchase	387	537	2757	275	273	148	885	404
	6.8%	9.5%	48.7%	4.9%	4.8%	2.6%	15.6%	7.1%

此行列出了每个产品类型在所有购买中所占的百分比。例如，街机游戏占所有购买的 9.5%。

设置表格行的格式

每个表格行都可以分别设置格式以添加上下文或可视化侧重点。单击每列顶部的画笔图标以自定义颜色和数字格式。



事件 (118,596) 模式 统计信息 (5) 可视化

每页 20 个 格式 预览

action	NULL
addtocart	
changequantity	
purchase	
remove	
view	

注意：代表 `_time` 字段的列和迷你图列无法使用列表格设置功能。

列颜色

为表格列选择并配置以下一种颜色模式。

注意：列颜色格式设置会覆盖现有热图或高/低值数据叠加设置。

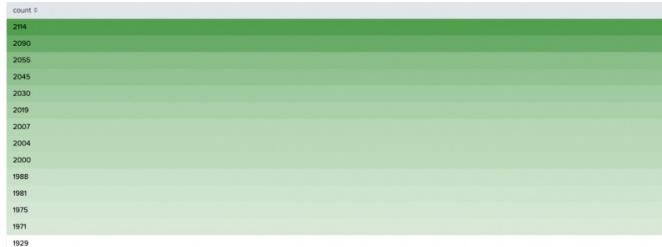
色标

在列单元格上使用序列或分散色标。您可以选择一个预设置的色标，也可以使用自定义配置，来管理色标中的颜色如何应用到列单元格中。

取决于搜索结果和数据分发，列颜色的渐变形式可能有所不同。具有相对相似值的列会显示大部分的颜色渐变。叠加值会限制渐变。

色标选项

色标类型	描述	示例
		本示例列使用的是序列色标。而且排序方式是将最大值显示在顶部。

序列	使用序列色标显示结果如何慢慢逼近列中的较高值。	
分散	分散色标可显示结果如何逼近较高值和较低值。	

配置自定义色标

您可以通过指定最小值、中间值和最大值的颜色来配置自定义颜色处理。使用以下其中一个选项来配置最小值、中间值和最大值在色标中的解读方式。

“配置”选项

选项	描述	使用案例示例
最高值和最低值	此选项会突出显示列中的最高值和最低值。	<ul style="list-style-type: none"> 显示销售数据集中购买最多的是哪个产品。 显示近期客户满意度调查结果向最高分和最低分分布的趋势。
数字	表示数字阈值。单元格颜色取决于值与这三个阈值的对齐情况。	<ul style="list-style-type: none"> 根据小、中和大花名册的尺寸显示部门课程注册情况。
百分比	根据结果值范围的百分比确定单元格颜色。	<ul style="list-style-type: none"> 显示学生期末考试的测试成绩。
百分位	根据结果值分布的百分位确定单元格颜色。	<ul style="list-style-type: none"> 比较客户满意度调查结果。

范围

根据值范围确定为本列的单元格套用相应的颜色。

使用范围分类比较单元格值。例如，使用红色、黄色和绿色范围颜色来表示低、中和高销售结果。



范围配置选项：

- 调整默认范围值和颜色设置。
- 添加或删除范围。

值

根据单元格值套用颜色。

使用自动的值颜色设置或定义自定义规则。自动值颜色设置会为列中的每个单元格套用一个颜色。值相同的单元格所显示的颜色也相同。

自定义规则有助于将您监控的特定值进行突出显示。例如，使用自定义规则将近期销售数据中三个新产品的数据进行突出显示。

itemid
EST-11
EST-12
EST-13
EST-14
EST-15
EST-16
EST-17
EST-18
EST-19
EST-21
EST-26
EST-27
EST-6
EST-7

数字格式

启用和调整每列的数字格式。数字格式设置面板包含以下选项。

- 启用或禁用数字格式。
- 设置小数精确度。
- 选择使用千分位分隔符。
- 指定测量单位以便为本列的值添加上下文。单位可放置于每个值的前面或后面。

配置表格属性

生成表格后，使用格式菜单配置一个或多个如下所示的表格组件。

- 在每个表格页面中显示的行数
- 换行
- 表格行编号显示

数据叠加

格式菜单还包含以下数据叠加选项。

热图

在表格中添加特定颜色的不同阴影，以在表格行上方显示值变量。

高值和低值

添加高值和低值颜色至表格，以突出显示最高和最低值。

仅在没有为表格添加列颜色格式的情况下使用数据叠加。列颜色格式会覆盖数据叠加配置。

钻取

默认情况下，将可视化保存到仪表板时禁用钻取。您可以使用钻取编辑器或 简单 XML 以启用和配置钻取选项。例如，使用钻取链接到用户在表格单元格中单击的值相关的 Splunk Answers 文章。请参阅“将钻取用于仪表板交互”以了解有关启用和配置钻取的详细信息。

简单 XML 钻取选项

在 简单 XML 中，您可以将钻取选项设为以下一个值。使用 `<drilldown>` 元素更改钻取行为。

选项	行为
----	----

单元格	默认情况下，使用所选单元格中的字段和值打开辅助搜索。
行	默认情况下，使用所选行中各单元格的字段和值打开辅助搜索。
无	禁用钻取。

表格列简单 XML

使用格式规则在简单 XML 中配置表格列。

指定用于管理列颜色格式设置的色标和颜色选项板规则。也可以使用数字格式规则来管理数字单元格值的外观。

将所有表格格式设置规则放在 `<table>` 仪表板元素中。

```
<table>
[...]
</table>
```

格式规则语法

要新建一个新格式规则，要指定格式规则类型和要应用此规则的列。使用以下语法：

```
<format type= [ "color" | "number" ] field=<column_name>>
  [...]
</format>
```

如果未指定字段，格式规则会应用于整个表格。

颜色格式规则

要添加列颜色，新建一个类型为“颜色”的格式规则，并指定要应用此规则的列的名称。

配置列颜色的第一步是指定色标类型。色标类型表示颜色应用到单元格中各值的方式。定义好色标之后，即可添加颜色选项板来指定该列要使用的颜色。

使用以下语法来指定颜色格式规则。

```
<format type="color" field=<column_name>>
  <scale type=<color_scale_type> [color scale option configurations] </scale>
  <colorPalette type=<color_palette_type> [color palette option configurations] </colorPalette>
</format>
```

色标类型和选项

category

根据类别将颜色套用到列中。您可以提供一个可选的类别列表来预先填充色标。如果结果中出现其他类别，则可将这些类别添加到指定类别之后。

选项和可接受的值	示例
(可选) 列出一个或多个类别字符串。	<pre><format type="color" field="server_status"> <scale type="category">online, offline </scale> </format></pre>

linear

将数值型数据映射到线性刻度。

选项和可接受的值	示例
无	<format type="color" field="purchases"> <scale type="linear"></scale> </format>

对数

将数值型数据映射到对数刻度。

选项和可接受的值	示例
无	<format type="color" field="performance"> <scale type="log"></scale> </format>

minMidMax

根据一个带最小值、中间值和最大值的范围来映射数值型数据。

为每个范围段指定类型和值。

minType 、 midType 、 maxType 选项	此类型的 minValue 、 midValue 、 maxValue 选项
数字 将值解释为离散数字。	任意有效的浮点数。
百分比 将值解释为数据值范围的百分比。	介于 0 和 100 之间的任意数字。
百分位 将值解释为数据分布的百分比。	介于 0 和 100 之间的任意数字。

默认类型和值

所有段类型都默认为 **number**。

所有百分比和百分位值的默认值如下。

- **minValue**: 使用数据中的最小值。
- **midValue**: 使用介于范围中最小值和最大值中间的值。
- **maxValue**: 使用数据中的最大值。

示例

```
<format type="color" field="field">
  <scale type="minMidMax" minType="number" minValue="2" midType="number" maxType="percent" maxValue="100"></scale>
</format>
```

sharedCategory

将此色标类型与 **sharedList** 选项板一起使用，为本列应用自动格式设置。

选项和可接受的值	示例
无。将此色标与 <code>sharedList</code> 选项板一起使用，如示例所示。	<pre><format type="color" field="sourcetype"> <scale type="sharedCategory"> </scale> <colorPalette type="sharedList"> </colorPalette> </format></pre>

threshold

为分箱数据指定一组有限的值阈值。

选项和可接受的值	示例
<p>以升序方式列出值。您可以使用任意有限数字，包含浮点值。</p> <p>所有小于第一个阈值的值都进入第一个箱中。所有大于或等于最后一个阈值的值都进入最后一个箱中。</p>	<pre><format type="color" field="purchase_count"> <scale type="threshold">0,30,70,100</scale> </format></pre>

颜色选项板的类型和选项

在定义了颜色格式规则并为其添加了色标之后，添加一个颜色选项板类型及其选项。颜色选项板决定色标将哪些颜色应用到列单元格中。

表达式

使用会为特定值返回某种颜色的逻辑表达式。

颜色字符串格式

使用以下任意一种格式。

- #FFF
- #FFFFFF
- 0xFFFF
- 0xFFFFFFFF
- rgb(255, 255, 255)
- rgba (255, 255, 255, 1)

示例

本表达式示例将颜色 #65A637 应用到值为 `splunkd` 的单元格中。对于其他值的单元格，则会使用颜色 #0000CC。

```
<colorPalette type="expression">if (value == "splunkd", "#65A637", "#0000CC")
</colorPalette>
```

list

为此选项板指定颜色字符串列表。

插入所列的颜色

添加布尔值 `interpolate` 指定是否插入与列表中所列颜色相邻的颜色。将 `interpolate` 设置为 "true" 可产生平滑的颜色渐变效果。

`interpolate` 默认为 `false`。

颜色字符串格式

使用以下任意一种格式。

- #FFF
- #FFFFFF
- 0xFFFF
- 0xFFFFFFFF
- rgb(255, 255, 255)

- `rgba (255, 255, 255, 1)`

示例

```
<colorPalette type="list" interpolate="true">[#65A637,#6DB7C6,#F7BC38,#F58F39,#D93F3C]
</colorPalette>
```

map

指定一个或多个单元格值与颜色字符串对之间的映射关系。

使用以下映射格式。

```
{ {<cell_value_string>} : {<color>} , {<cell_value_string>} : {<color>} }
```

颜色字符串格式

使用以下任意一种格式。

- `#FFF`
- `#FFFFFF`
- `0xFFFF`
- `0xFFFFFFFF`
- `rgb(255, 255, 255)`
- `rgba (255, 255, 255, 1)`

示例

```
<colorPalette type="map">{"online":#65A637, "offline":#6A5C9E}
</colorPalette>
```

minMidMax

指定在生成颜色渐变时要使用的最小和最大颜色值，或最小、中间和最大颜色值。渐变值会插入到指定的颜色中间。

为以下选项指定颜色。

- `minColor` (必填)
- `midColor` (可选)
- `maxColor` (必填)

颜色字符串格式

使用以下任意一种格式。

- `#FFF`
- `#FFFFFF`
- `0xFFFF`
- `0xFFFFFFFF`
- `rgb(255, 255, 255)`
- `rgba (255, 255, 255, 1)`

示例

```
<colorPalette type="minMidMax" minColor="#FFFFFF" maxColor="#65A637">
</colorPalette>
```

sharedList

将此选项板与 `sharedCategory` 色标一起使用，为本列应用自动格式设置。

示例

```

<format type="color" field="sourcetype">
    <scale type="sharedCategory"></scale>
    <colorPalette type="sharedList"></colorPalette>
</format>

```

数字格式规则

指定数字值的呈现方式。

使用以下语法来新建数字格式规则。

```

<format type="number" field="count">
    <option name="">[number_format_option_value]</option>
</format>

```

数字格式选项

名称	描述	可接受的值和默认值
precision	指定小数点后精确到几位。	使用介于 0 到 20 之间的数字。默认为 2。
useThousandSeparators	指定是否在每三个数字之间插入一个逗号或其他符号。所设置的符号取决于 Splunk 平台实例所使用的语言和所在区域。	布尔值。默认为 true。
unit	指定要放在值前面或值后面的单位标签。	使用任意字符串。为获得最佳效果，可使用缩写或其他简短的标签文本。
unitPosition	指定将 unit 标签放置在哪里。	[before after] 默认为 after。

数字格式示例

```

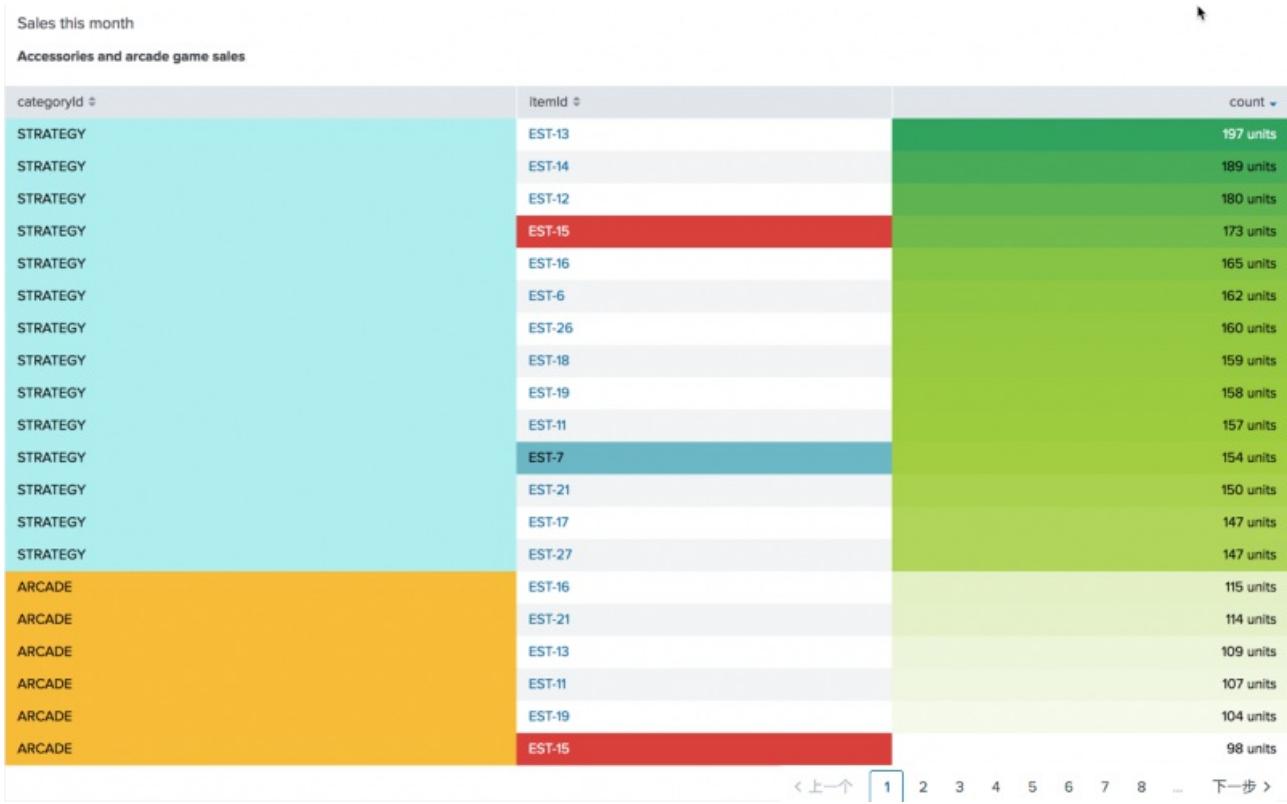
<table>
    <search>
        <query>index=_internal | head 10000 | stats count by sourcetype</query>
    </search>
    <format type="number" field="count">
        <option name="precision">3</option>
        <option name="useThousandSeparators">false</option>
        <option name="unit">MB</option>
        <option name="unitPosition">before</option>
    </format>
</table>

```

表格格式源代码示例

本表格示例将近期的销售业绩进行了可视化。

列代表产品类别和 ID 码，以及项目销售总计。格式规则有助于区分类别，突出显示特定项目，以及列出所有产品范围内的相对销售指标密度。



源代码包括色标、选项板和数字格式规则。

```

<dashboard>
  <label>Sales performance</label>
  <row>
    <panel>
      <title>Sales this month</title>
      <table>
        <title>Accessories and arcade game sales</title>
        <search>
          <query>source="tutorialdata (1).zip:/*" | stats count by categoryId, itemId | table categoryId itemId count</query>
          <earliest>0</earliest>
          <sampleRatio>1</sampleRatio>
        </search>
        <option name="count">20</option>
        <option name="dataOverlayMode">none</option>
        <option name="drilldown">cell</option>
        <option name="rowNumbers">false</option>
        <option name="wrap">true</option>
        <format type="color" field="itemId">
          <colorPalette type="map">{"EST-15":#D93F3C, "EST-7":#6DB7C6}</colorPalette>
        </format>
        <format type="color" field="categoryId">
          <colorPalette type="map">{"ACCESSORIES":#6DB7C6, "ARCADE":#F7BC38, "STRATEGY":#AFEEEE}</colorPalette>
        </format>
        <format type="color" field="count">
          <colorPalette type="minMidMax" maxColor="#31A35F" midColor="#A2CC3E" minColor="#FFFFFF"></colorPalette>
          <scale type="minMidMax" maxType="percentile" maxValue="100" midType="percentile" midValue="50" minType="percentile" minValue="0"></scale>
        </format>
        <format type="number" field="count">
          <option name="precision">0</option>
          <option name="unit">units</option>
        </format>
      </table>
    </panel>
  </row>
</dashboard>

```


图表

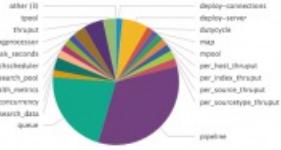
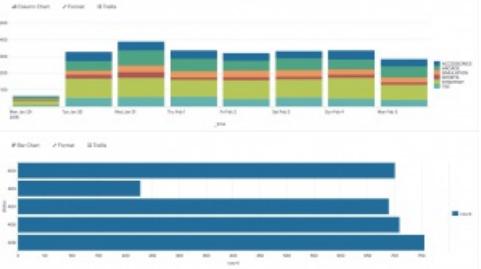
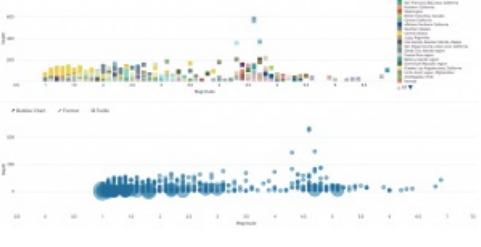
图表概述

选择一种图表类型来呈现一个结果集中的一或多个数据维度。了解图表如何将数据系列可视化。

要快速了解常用图表和通用图表使用命令，您可以点击“开始”中的链接查看 Splunk 仪表板快速参考指南。

选择图表

选择图表时可基于您要可视化的数据维度的数量。例如，使用饼图说明单个字段中多个值的组合方式。气泡图可用于说明单个数据集中多个字段之间的关系。

图表类型	描述
<p>饼图</p>  <p>显示单个维度。饼图扇区的大小代表一个字段的各个值的密度或频率。</p>	
<p>柱形图和条形图</p>  <p>代表数据集中的一或多个维度。这些图表用两个轴来绘制数据。每个轴代表一个结果字段。</p> <p>柱形图和条形图可用于对值和字段进行比较。</p>	
<p>折线图和面积图</p>  <p>折线图可呈现一段时间内值的变化情况。</p> <p>面积图呈现的是一段时间内聚合值的变化情况。</p>	
<p>散点图和气泡图</p>  <p>代表数据集中多个维度。这些图表用两个轴来绘制数据。数据点外观、尺寸和/或分布可表示额外模式或关系。</p>	

开始

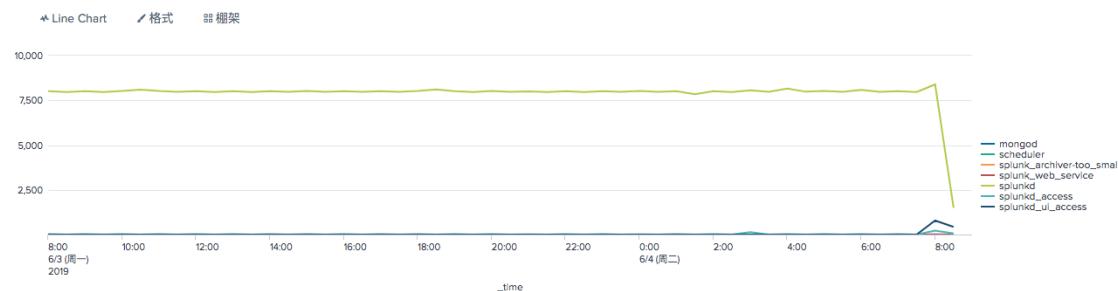
以下主题介绍如何构建和配置图表。

- 图表的数据
- 饼图
- 柱形图和条形图
- 折线和面积图
- 散点图
- 气泡图

图表的数据

不管要构建哪种图表，请从可生成一个或多个数据系列的转换搜索开始。

一个系列是指相关数据点的序列。可以在图表中绘制这些点。例如，折线图上的每一条线显示一个系列。



运行转换搜索时，选择统计选项卡。查看统计表以浏览生成的系列。在第一列后方，每个额外列代表一个系列。单个系列搜索生成两个列。多个系列搜索生成三个或三个以上列。

各种图表类型都进行了优化，以可视化一个或多个数据系列。

图表名称	针对单个系列进行了优化？	针对多个系列进行了优化？	注释
饼图	是	否	饼图只能呈现单个系列。
条形图	是	是	
柱形图	是	是	
折线图	是	是	折线图一般用于多个系列。
面积图	否	是	使用面积图呈现多个系列。
散点图	否	是	散点图最适用于两个数据系列。
气泡图	否	是	气泡图最适用于呈现三个数据系列。

饼图

饼图可显示整个数据集中，不同字段值的组合方式。饼图的每个扇区代表特定类别的相对重要性或相对数量。

数据格式设置

饼图代表单个数据系列。

在搜索中使用转换命令以生成单个系列。

例如，计算每个 source 字段类别的事件数。

```
... | stats count by source
```

在运行搜索后查看统计表，确保已生成单个系列。该表格应该包含两列。

示例搜索生成以下表格。

事件 (118,596)	模式	统计信息 (3)	可视化
source	每页 20 个	格式	预览
tutorialdata.zip:./www1/access.log			count 40884
tutorialdata.zip:./www2/access.log			38736
tutorialdata.zip:./www3/access.log			38976

表格第一列包含每个饼图扇区的标签。第二列包含对应于每个标签的数字值。数字值决定每个扇区的相对大小。

如果搜索生成的表格包含的列数超过两个，则额外的列将被忽略。

“配置”选项

格式菜单可用于配置以下饼图组件。

钻取

饼图的钻取功能使用户可以单击某个扇区，打开一个使用所单击的值的辅助搜索。您可在“仪表板编辑器”中启用或禁用钻取。请参阅“将钻取用于仪表板交互”以了解详细信息。

最小大小

设置最小百分比大小，以便在扇区超过 10 个时应用。低于最小百分比例的数据值将计入其他扇区。

新建饼图

前提条件

查看以下内容了解构建饼图的相关详细信息。

- 数据格式设置
- “配置”选项

步骤

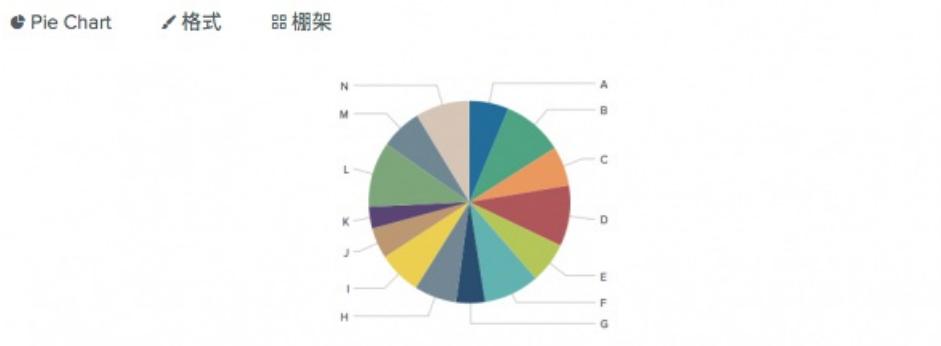
1. 编辑一个使用转换命令的搜索，以生成字段的值。
2. 运行该搜索。
3. 选择搜索栏下方的统计选项卡。此处的统计表应包含两列。
4. 选择可视化选项卡，然后用可视化挑选器选择饼状图可视化。
5. (可选) 使用格式菜单配置可视化。

示例

此搜索部分按 Code 字段值聚合事件。

```
... | stats count by Code
```

此搜索生成单个数据系列，代表 Code 字段的值。



此图表的最小大小配置为 5%。占总数据集 5% 以下的字段值将计入其他饼图扇区。

此搜索使用 `bytes` 和 `source` 字段生成单个系列。

```
index = _internal | chart avg(bytes) over source
```

此处 `source` 列提供饼图扇区标签。`avg(bytes)` 列提供每个扇区的相对大小，因为 `avg(bytes)` 总数的百分比由搜索返回。

柱形图和条形图

使用柱形图和条形图对比数据集间的字段值。

数据格式设置

柱形图和条形图可代表一个或多个数据系列。要确认搜索成功生成了一个或多个系列，单击统计选项卡。该表格应该包含至少两列。

如果表格结构并不具备有效的 X 轴或 Y 轴值，则搜索结果无法生成柱形图或条形图。例如，使用 `eval` 或 `fields` 命令可能会更改搜索结果结构。

统计表顺序和图表轴

柱形图和条形图以不同的方式处理统计表中的值。

柱形图从表格的第一列获取 X 轴值。表格的下一列提供 Y 轴值。

条形图从表格的第一列获取 Y 轴值。表格的下一列提供 X 轴值。

比如，使用 `timechart` 报表命令的任何搜索都将生成一个表格，其中 `_time` 是第一列。用此搜索生成的柱形图有一个名为 `_time` 的 X 轴。用此搜索生成的条形图有一个名为 `_time` 的 Y 轴。

单个和多个数据系列

柱形图和条形图可以可视化单个或多个数据系列。以下示例说明了如何生成这些系列。

单个系列

搜索对通过每种来源传输的字节平均数进行比较。在此搜索中，`over` 运算符表示 `source` 是表格的第一列。

```
... | chart avg(bytes) over source
```

此搜索生成以下表格。

事件 (118,596)	模式	统计信息 (3)	可视化
每页 20 个	格式	预览	
source	avg(bytes)		
tutorialdata.zip:./www1/access.log	2088.8132521279717		
tutorialdata.zip:./www2/access.log	2100.1112143742257		
tutorialdata.zip:./www3/access.log	2104.714285714286		

柱形图和条形图以不同的方式代表单个系列。

柱形图

`source` 值用于 X 轴。柱形图的 Y 轴是 `avg(bytes)`。

条形图

`avg(bytes)` 值用于 X 轴。条形图的 Y 轴代表 `source` 字段值。

多个数据系列

要生成多个数据系列，引入 `timechart` 命令将 `_time` 字段添加到搜索结果中。您也可以修改查询以引入 `split-by` 字段。

例如，通过将 `clientip` 添加为 `split-by` 字段来修改之前的单个系列搜索。

```
... | chart avg(bytes) over source by clientip
```

split-by 字段会生成多个数据系列。每个 clientip 就是一个数据系列，且对于每个 source 此系列都有自己的 avg(bytes) 值。

事件 (118,596) 模式 统计信息 (3) 可视化							
每页 20 个		格式		预览			
source	147.213.138.201	170.192.178.10	182.236.164.11	192.162.19.179	203.92.58.136	212.235.92.150	
tutorialdata.zip:./www1/access.log	2323.6451612983224	2284.0925925925926	2001.5348837209383	2317.9574468085107	2294.705882352941	2036.73	
tutorialdata.zip:./www2/access.log	2222.5882352941176	2182.2916666666665	2337.084210526316	2386.923076923077	2246.2272727272725	2484.014705882353	
tutorialdata.zip:./www3/access.log	2370.82	2304.245283018868	2474.1	2192.641975308642	2237.076923076923	2260.0095238095237	

要在条形或柱形图中显示多个系列，可使用格式菜单配置堆叠和多系列模式。

“配置”选项

使用格式菜单自定义一个或多个如下所示的柱形图和条形图组件。

- 图表标题
- 轴标题
- 最小和最大轴值
- 使用对数单位刻度。当轴值非常小或非常大时，此选项就非常有用。
- 指定是否要缩写 Y 轴数值。例如，如果您将此选项切换为打开，值 20,000 将缩写成 20K。在柱形图和条形图中只可以缩写 Y 轴的值。
- 图表图例位置和文本截断。
- 标签旋转

多系列选项

如果图表代表多个数据系列，您也可以配置以下选项。

多系列模式

比较多个系列中的趋势。启用此模式以便为每个系列显示各自的轴范围。

堆叠图表

使用堆叠图表查看特定字段值的更多详情。可以选择非堆叠、堆叠和 100% 堆叠条形图和柱形图。请参阅以下比较内容。

堆叠选项	柱形图或条形图外观	使用案例
非堆叠	不同系列的柱形图或条形图彼此相邻。	非堆叠图表适用于系列较少的情况。随着系列数的增加，图表可能越来越难懂。
堆叠	系列中的数据点显示为柱形图或条形图的段。柱形或条形的总值为段的总和。	使用堆叠的柱形图或条形图，以突出显示系列中数据点的相对数量、频率或重要性。请参阅下面的堆叠图表。
100%堆叠	每个条形或柱形划分为几个段，代表一个系列中每个数据值的分布百分比。	当每个柱形或条形中有重要的段大小变量，则使用 100% 堆叠以显示数据分布。

新建柱形图或条形图

前提条件

查看以下内容了解构建柱形图和条形图的相关详细信息。

- 数据格式设置
- “配置”选项

步骤

- 编写一个可生成一个或多个数据系列的搜索。
- 运行该搜索。
- 选择搜索栏下方的统计选项卡。此处的统计表应包含两列或更多列。
- 选择可视化选项卡，然后用可视化挑选器选择柱形图或条形图可视化。
- (可选) 使用格式菜单配置可视化。

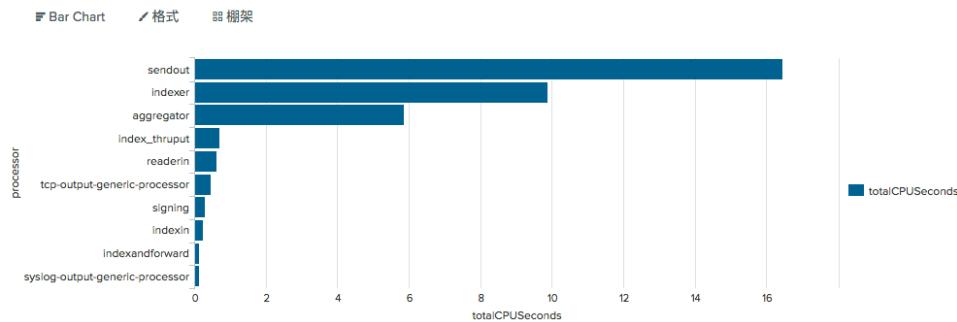
示例

条形图

此搜索计算每个处理器的 CPU 秒数总和。搜索同样按最大的十个总和数降序排列处理器。

```
index=_internal "group=pipeline" | stats sum(cpu_seconds) as totalCPUSeconds  
by processor | sort 10 totalCPUSeconds desc
```

搜索生成此条形图。

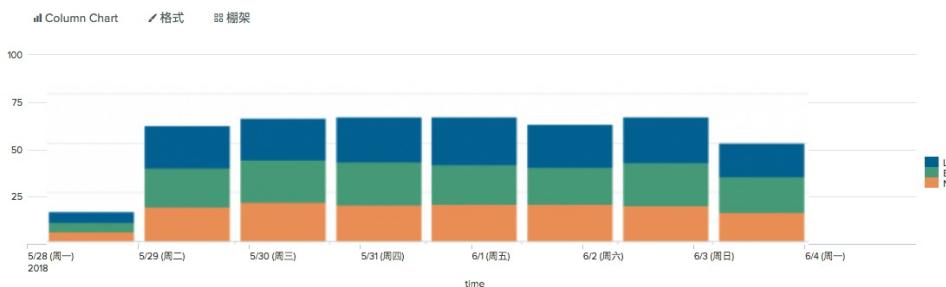


堆叠柱形图

此搜索部分根据随时间变化的代码值聚合事件。查询指定了要包含 `_time` 字段和 `Code` 字段的值。此查询为每个 `Code` 字段值生成一个系列。

```
... | timechart count by Code | fields _time L B N
```

堆叠柱形图显示不同时间点上每个代码的事件计数。您可以比较每个时间点上的 `L`、`B` 和 `N` 标记事件的数量。



折线和面积图

使用折线图和面积图来追踪随时间变化的数值趋势。您还可以使用折线图或面积图的 X 轴代表字段值，而不是时间。

数据格式设置

折线图可代表一个或多个数据系列。面积图代表多个数据系列。

如果搜索生成多个系列，图表中的每条线或面积会显示不同的颜色。

要确认搜索正确地生成了数据系列，单击搜索栏下方的统计选项卡。对于单个系列，统计表应包含至少两列；对于多个系列，则应包含三列或更多。

统计表顺序和图表轴

折线图和面积图从统计表的第一列获取 X 轴值。表格的下一列提供 Y 轴值。

比如，使用 `timechart` 报表命令的任何搜索都将生成一个表格，其中 `_time` 是第一列。用此搜索生成的折线图或面积图有一个名为 `_time` 的 X 轴。

如果表格结构并不具备有效的 X 轴或 Y 轴值，则搜索结果无法生成折线图或面积图。例如，使用 `eval` 或 `fields` 命令可能会更改搜索结果结构。

单个和多个数据系列

折线图或面积图一般用于代表多个系列。折线图也可用于单数据系列，但面积图不行。

单个系列

搜索对通过每种来源传输的字节平均数进行比较。在此搜索中，`over` 运算符表示 `source` 是表格的第一列。

```
... | chart avg(bytes) over source
```

此搜索生成以下表格。

事件 (7,929)	模式	统计信息 (3)	可视化
每页 20 个	格式	预览	
source ↴			avg(bytes) ↴
tutorialdata.zip:./www1/access.log			2056.4580233793836
tutorialdata.zip:./www2/access.log			2087.266439909297
tutorialdata.zip:./www3/access.log			2116.157317073171

在折线图中，`source` 值用于 X 轴。Y 轴代表 `avg(bytes)` 值。

多个数据系列

要生成多个数据系列，引入 `timechart` 命令将 `_time` 字段添加到搜索结果中。您也可以修改查询以引入 `split-by` 字段。

例如，通过将 `clientip` 添加为 `split-by` 字段来修改之前的单个系列搜索。

```
... | chart avg(bytes) over source by clientip
```

`split-by` 字段会生成多个数据系列。每个 `clientip` 就是一个数据系列，且对于每个 `source` 此系列都有自己的 `avg(bytes)` 值。

事件 (7,929)	模式	统计信息 (3)	可视化
每页 20 个	格式	预览	
source ↴	123.30.108.208 ↴	130.253.37.97 ↴	174.123.217.162 ↴
tutorialdata.zip:./www1/access.log	3257	2596.33333333333335	2592 3411.3333333333335
tutorialdata.zip:./www2/access.log	2608.75	3959	2535.5 2350.923076923077
tutorialdata.zip:./www3/access.log	2366.5	2549.5	2638 2563.875
			3547 1996.66666666666667
			1726.333333333333 3707
			3360.5 2252.75

“配置”选项

使用格式菜单配置一个或多个如下所示的折线图和面积图组件。

- 图表标题
- 轴标题
- Y 轴空值处理。选择以下各选项中的其中一项。
 - 将空的数据点显示为间隙。在此案例中，图表将显示任何断开的数据点的标记。
 - 将空数据点连接至零数据点。
 - 连接到下一个正数的数据点。
- 显示最小和最大 Y 轴值。
- 使用 Y 轴值的对数单位刻度。当 Y 轴值范围较广时，此选项显得非常有用。
- 指定是否要缩写 Y 轴数值。例如，如果您将此选项切换为打开，值 20,000 将缩写成 20K。在面积图和折线图中只可以缩写 Y 轴的值。
- 图表图例位置和标签截断。

多系列选项

如果图表代表多个数据系列，您也可以配置以下选项。

多系列模式

比较多个系列中的趋势。启用此模式以便为每个系列显示各自的轴范围。

堆叠面积图

当搜索生成多个数据系列，则可以使用堆叠面积图。堆叠无法用于折线图。

使用堆叠面积图可查看关于系列以及如何与整个数据集关联的详细信息。查看这里的比较表格，以选择堆叠选项。

堆叠选项	柱形图或条形图外观	使用案例
非堆叠	不同系列的区域在图表中的面积相等。	非堆叠图表适用于系列较少的情况。随着系列数的增加，图表可能越来越难懂。
堆叠	每个系列区域分开显示。	使用堆叠面积图，可突出显示系列的相对数量、频率或重要性。请参阅下面的堆叠图表。
100% 堆叠	此图表显示整个数据集中每个系列的分布百分比。	使用 100% 堆叠以侧重了解数据分布。

新建折线图或面积图

前提条件

查看以下内容了解构建柱形图和条形图的相关详细信息。

- 数据格式设置
- “配置”选项

步骤

1. 编写一个可生成多个数据系列的搜索。若要构建折线图，则可选择生成单个数据系列。
2. 运行该搜索。
3. 选择搜索栏下方的统计选项卡。此处的统计表应包含两列或更多列。
4. 选择可视化选项卡，然后用可视化挑选器选择折线图或面积图可视化。
5. （可选）使用格式菜单配置可视化。

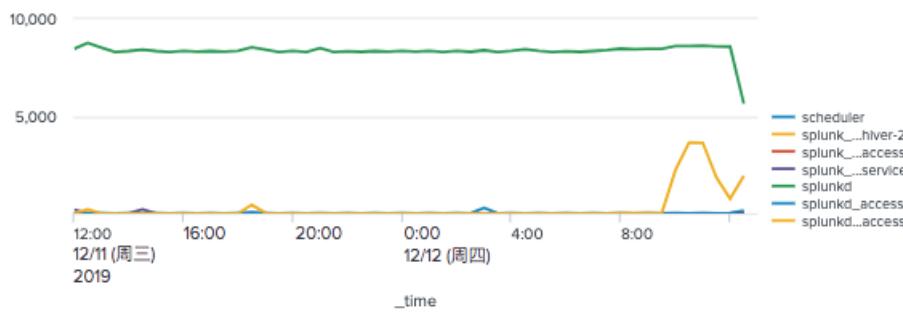
示例

折线图

此搜索追踪随时间变化的来源类型频率。

```
index=_internal | timechart count by sourcetype
```

搜索生成多个数据系列。折线图的每个系列以不同线条表示。

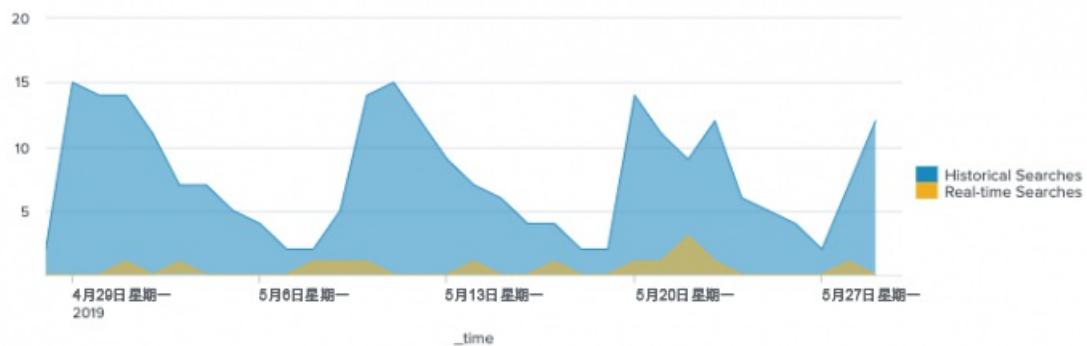


面积图

面积图中的阴影区域强调的是数量。此示例搜索追踪随时间变化的历史和实时搜索量。

```
index=_internal source=*_metrics.log group=search_concurrency "system total" NOT user=*
| timechart max(active_hist_searches) as "Historical Searches" max(active_realtime_searches) as "Real-time Searches"
```

此搜索生成两个数据系列。每个系列在图表中显示为不同的阴影区域。

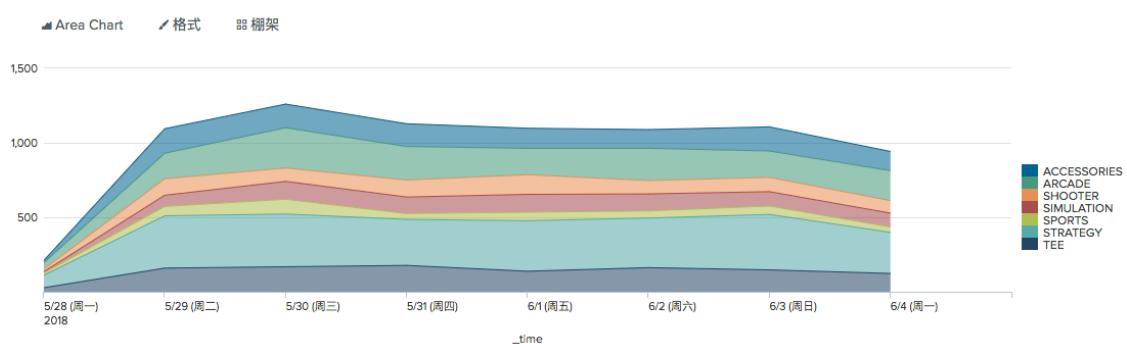


堆叠面积图

此搜索追踪随时间变化不同系列的吞吐量。以下示例使用搜索教程数据文件。要了解有关将此数据导入到您的 Splunk 实例中的更多信息，请参阅《搜索教程》中的“上载教程数据”。

```
sourcetype=access_* status=200 action=purchase categoryId!=NULL | timechart count(categoryId) by categoryId
```

搜索生成多个系列。每个系列显示为堆叠图表的颜色区域。可以通过堆叠比较不同系列的总和。



散点图

使用散点图显示离散数据点之间的关系。数据点分布可说明两个维度的趋势或关系。

数据格式设置

散点图最适用于两个数据系列。使用转换命令聚合值。可以使用带以下语法的 `table` 命令来管理结果字段排序。

```
... | table <marker_name_field><x-axis_field><y-axis_field>
```

在运行搜索后查看统计选项卡，确保统计表包含三列。必要时，也可以使用 `table` 命令更改各列的顺序。

“配置”选项

使用格式菜单配置一个或多个如下所示的散点图组件。

- 轴标题
- 图例位置和截断
- 轴刻度和间隔值
- 轴最小和最大值
- 缩写 Y 轴和 X 轴数值

新建散点图

前提条件

查看以下内容了解构建柱形图和条形图的相关详细信息。

- 数据格式设置
- “配置”选项

步骤

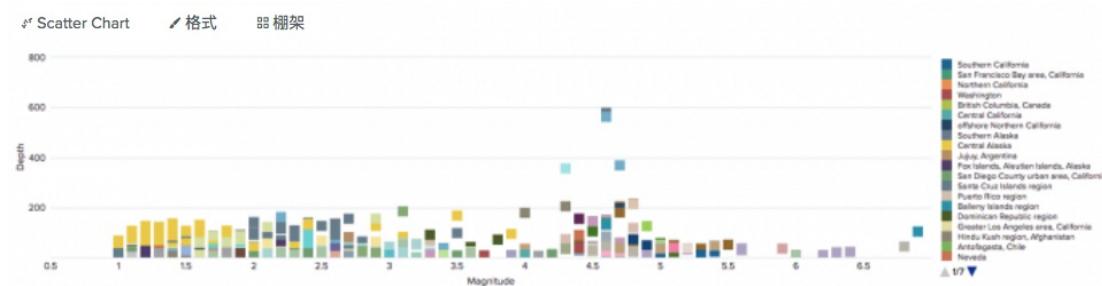
1. 编写一个可生成两个数据系列的搜索。
2. 运行该搜索。
3. 选择搜索栏下方的统计选项卡。此处的统计表应包含三列。
4. 选择可视化选项卡，然后用可视化挑选器选择散点图可视化。
5. (可选) 使用格式菜单配置可视化。

示例

一个分析师新建了一个散点图来跟踪近期地震的位置、震级和深度。

此搜索会生成一个三列的统计表。第一列显示地震位置值。第二列代表地震的震级值，在 X 轴中绘制。第三列代表地震的深度值，画在 Y 轴上。

```
source="earthquake.csv" | table Region Magnitude Depth
```



使用简单的 XML 以构建更复杂的散点图。有关更多信息，请参阅“图表配置参考”中的“面积图、条形图、柱形图、折线图和散点图”和“散点图特定属性条目”。

气泡图

使用气泡图可以以三维形式查看多个系列数据。气泡位置代表数据系列的两个维度。气泡大小代表第三个维度。

数据格式设置

要新建气泡图，请从生成多个数据系列的搜索开始。用以下语法生成此系列。

```
<pre> ... | <stats_command><y-axis_field><x-axis_field><bubble_size_field>
```

查询中的单个 group-by 字段会生成一个可视化，其中所有的气泡颜色都相同。要想通过 stats 命令获取系列颜色，可使用两个 group-by 字段。这样就能为这两个字段的每个唯一组合生成气泡。第二个字段的数值决定系列颜色。

“配置”选项

气泡图配置包含以下选项。可以使用格式菜单调整这些设置。

- 最小和最大气泡标记大小
- 轴标题
- X 轴标签旋转和截断
- 轴刻度、间隔、最小和最大值
- 缩写 Y 轴和 X 轴数值

新建气泡图

前提条件

查看以下内容了解构建柱形图和条形图的相关详细信息。

- 数据格式设置
- “配置”选项

步骤

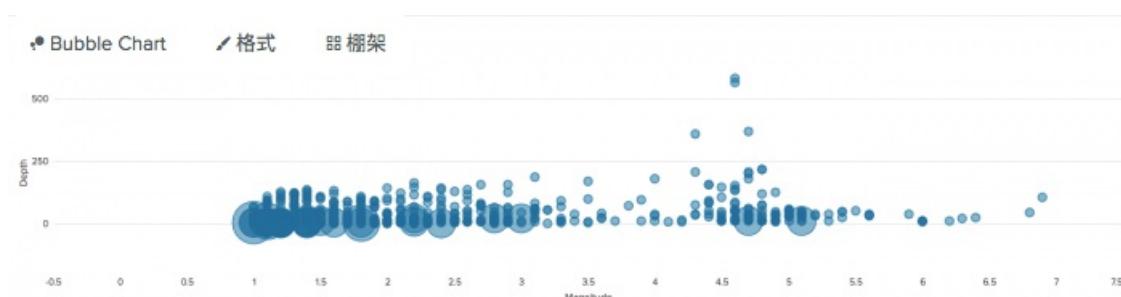
1. 编写一个可生成三个数据系列的搜索。
2. 运行该搜索。
3. 选择搜索栏下方的统计选项卡。此处的统计表应包含四列。
4. 选择可视化选项卡，然后用可视化挑选器选择气泡图可视化。
5. (可选) 使用格式菜单配置可视化。

示例

此搜索根据位置聚合地震事件。它将根据每个地震位置生成代表震级、深度和次数的数据系列。

```
source="earthquakes.csv" | stats count by place, mag, depth
```

此搜索生成气泡图，其中 X 轴和 Y 轴代表震级和深度。气泡图大小表示特定位置的相对计数值。



图表的事件注释

事件注释使您可以将上下文添加到时间图表返回的趋势。例如：如果有显示上周网站登录错误的图表，您可以添加标记服务器在该阶段故障时间的事件注释。如果大部分登录错误是在服务器故障期间发生的，则可以断定这两个事件是相关的。以这种方式使用事件注释，使您可以关联离散数据集。

以彩色标记显示事件注释，这样当您将鼠标悬停在注释上时，会显示标签中的时间戳信息和自定义描述。

只有折线图、柱形图和面积图支持事件注释。

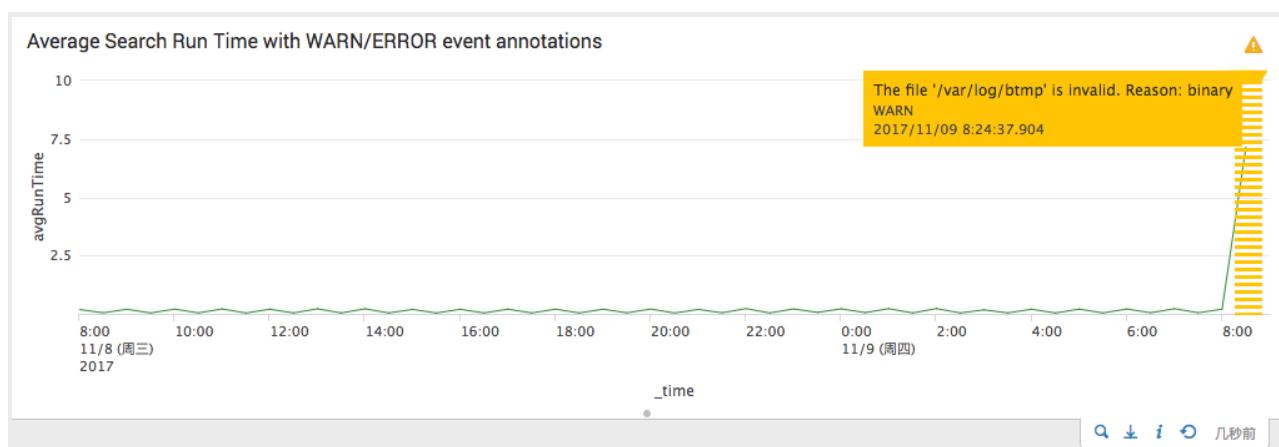
如果您在编辑搜索面板中设置自动刷新延迟，您必须在 XML 中为事件注释搜索手动添加相同的刷新时间。例如，如果您在 UI 中设置延迟，会与主要搜索的面板来源选项卡中的 30 秒延迟代码相似。

```
<refresh>30s</refresh>
```

```
<refreshType>delay</refreshType>
```

要确保事件注释也以相同的计划刷新，请向运行事件注释的辅助搜索添加相同的代码行。

下图是包括事件注释的仪表板面板示例。面板显示描述平均搜索运行时间（叠加从带有 "WARN" 和 "ERROR" 通知的内部日志辅助搜索中获取的事件注释）的图表。黄色标签显示 "WARN" 事件注释的自定义消息。



新建事件注释

使用 Simple XML 通过仪表板编辑器新建事件注释。事件注释搜索来自日志和查找的数据或来源于您手动添加的数据来源。如果您不了解使用 Simple XML 编辑仪表板，请参阅“[编辑 Simple XML](#)”。

要将事件注释添加到图表，请使用后跟搜索要注释的事件数据的 `search type= "annotation"` 命令和查询的时间范围。例如：以下是上述仪表板的 Simple XML。

```
<dashboard>
  <label>Search Analysis</label>
  <description>Search metrics correlated with user activity and log events</description>
  <row>
    <panel>
      <title>Average Search Run Time with WARN/ERROR event annotations</title>
      <chart>
        <search>
          <query>index=_audit action=search result_count="*" | timechart avg(total_run_time) as avgRunTime</query>
          <earliest>-24h@h</earliest>
          <latest>now</latest>
        </search>

        <!-- Secondary search that drives the annotations -->
        <search type="annotation">
          <query>index=_internal (log_level="WARN" OR log_level="ERROR")</query>
          | eval annotation_label = message
          | eval annotation_category = log_level</query>
          <earliest>-24h@h</earliest>
          <latest>now</latest>
        </search>

        <!-- Customize the event annotation colors based on category name -->
        <option name="charting.annotation.categoryColors">{"ERROR": "#ff3300", "WARN": "#ffcc00"}</option>

        <option name="charting.chart">line</option>
        <option name="charting.drilldown">none</option>
        <option name="charting.legend.placement">none</option>
        <option name="charting.lineWidth">1</option>
        <option name="charting.seriesColors">[#339933]</option>
        <option name="height">287</option>
      </chart>
    </panel>
  </row>
</dashboard>
```

注释搜索字段

使用以下字段定义事件注释搜索。

字段名称	类型	必填	描述
_time	epoch 时间	是	事件的时间戳。
annotation_label	字符串	否	显示在注释标签中的消息。
annotation_category	字符串	否	使用此字段按照类型对注释事件进行分组。
annotation_color	字符串	否	使用此字段为注释事件分配颜色。必须使用十六进制代码指定颜色，例如 <code><option name="charting.annotation.categoryColors">{"ERROR": "#ff3300", "WARN": "#ffcc00"}</option></code> 。

如果您使用此字段指定事件注释的颜色，它将覆盖图表配置属性 `charting.annotation.categoryColors`。如果您已指定搜索中的字段 `annotation_category`，您可以使用 `charting.annotation.categoryColors` 属性而非 `annotation_color` 以将颜色分配给返回类别标签和标记。

有关此属性的详情信息，请参阅“图表配置参考”中的 `charting.annotation.categoryColors`。

图表显示问题

本主题介绍了使用图表可视化中的显示问题。

使用非转换命令搜索

使用不包含转换命令的搜索无法呈现图表，如以下选项。

```
chart  
timechart  
stats  
eval
```

有关更多信息，请参阅《[搜索手册](#)》中的“关于转换命令和搜索”。

时间图表

您只能使用 `timechart` 命令绘制基于时间的数据，这会生成基于 `_time` 的输出。如果您尝试使用任何其他转换搜索命令来绘制基于时间的系列，或重命名 `_time` 值，图表会将时间戳数据当作一系列字符串来处理。

数据截断

为避免浏览器性能受影响，Splunk 软件会限制单个图表中呈现的数据量。如果搜索结果超出限制，消息会与图表一起出现，表示数据已截断。

根据 Splunk 实例类型和仪表板编辑权限，您可以使用配置设置和 Simple XML 更改默认呈现行为。

有编辑权限的用户可以修改仪表板中单个图表的 Simple XML 数据截断设置。

Splunk Enterprise 管理员还可以添加或编辑 `visualizations.conf` 和 `web.conf` 的本地副本以配置 Splunk 部署中图表的截断设置。

使用以下表格比较配置选项。

呈现限制类型	在	设置	默认	配置位置
数据点总计	仪表板中的一个图表	<code>charting.chart.resultTruncationLimit</code>	50000	简单 XML
每个系列的数据点	仪表板中的一个图表	<code>charting.data.count</code>	10000	简单 XML
每个系列的数据点	一个图表类型	<code>data_sources.primary.params.count</code> 替换 <code>web.conf</code> 中的弃用 <code>jschart_results_limit</code> 设置。 设置为数值时，会覆盖此类图表中的 <code>charting.data.count Simple XML</code> 设置。	1000	<code>visualizations.conf</code>
数据点总计	所有浏览器中的所有图表	<code>jschart_truncation_limit</code>	无默认值。指定总数据点数以覆盖单个浏览器设置。	<code>web.conf</code>
数据点总计	单个浏览器中的图表	以下设置中的一个或更多。 <ul style="list-style-type: none">• <code>jschart_truncation_limit.chrome</code>• <code>jschart_truncation_limit.safari</code>• <code>jschart_truncation_limit.firefox</code>• <code>jschart_truncation_limit.ie11</code>	50000	<code>web.conf</code>
数据系列	所有图表	<code>jschart_series_limit</code>	100	<code>web.conf</code>

简单 XML 数据截断选项

您可以使用简单 XML 在单个图表中调整数据截断。

一个图表的数据点限值

您可通过编辑特定图表的简单 XML，配置该图表中可绘制的最大点数。对于 `<chart>` 元素，编辑 `charting.chart.resultTruncationLimit` 属性，如“图表配置参考”中的“面积图、条形图、柱形图、折线图和散点图”中所述。

一个图表中的每个系列数据点限值

您可以限制图表中每个系列可呈现的搜索结果数据点数。编辑 `charting.data.count` 简单 XML 设置，以覆盖数据系列的默认值 10000。

配置文件数据截断设置

Splunk Enterprise 管理员可以添加或编辑 `$SPLUNK_HOME$/etc/system/local/web.conf` 或 `$SPLUNK_HOME$/etc/system/local/visualizations.conf` 中的截断设置。

一个或多个浏览器中所有图表的数据点限值

`web.conf` 配置文件指定不同浏览器图表中可绘制的最大点数。所有浏览器中数据点数的限值为 50000。

您可以覆盖单个浏览器设置或添加 `jschart_truncation_limit` 设置（位于 `$SPLUNK_HOME$/etc/system/local/web.conf`）以定义所有浏览器的限值。`jschart_truncation_limit` 可覆盖任意单个浏览器设置。

注意： `charting.chart.resultTruncationLimit` 简单 XML 选项会覆盖单个图表中的限值。

所有图表的数据系列限值

您可以限制图表可以呈现的数据系列数。添加或编辑 `jschart_series_limit` 值（位于 `$SPLUNK_HOME$/etc/system/local/web.conf` 中）以覆盖数据系列的默认值 100。

如果搜索结果超出此限值，图表将只显示此限值规定的系列数。警告消息出现以显示图表正在显示截断搜索结果。例如，如果 `jschart_series_limit` 为 40 而搜索返回 50 个数据系列，那么一个图表只会呈现前 40 个系列。

一个图表类型中每个系列的数据点限制

限制以特定图表呈现每个系列的搜索结果数据点的数量。编辑 `visualizations.conf` 中的 `data_sources.primary.params.count` 设置以覆盖 1000 个结果行的默认值。

例如：您可以设置饼状图中每个系列的数据点限制。在 `$SPLUNK_HOME$/etc/system/local/visualizations.conf` 中编辑 [pie] 图表类型段落：

```
[pie]
data_sources.primary.params.count = 10
```

自最新的软件版本开始，弃用所有图表的每个系列设置的 `web.conf jschart_results_limit` 数据点。改用 `data_sources.primary.params.count`。

数据系列和数据点限值优先顺序

如为单个图表，如果 `jschart_series_limit` 和 `charting.data.count` 简单 XML 选项相乘表示一个大于 `web.conf` 中 `jschart_truncation_limit` 的数，则将减少每个系列的数据点以符合 `jschart_truncation_limit` 设置。

比如，`jschart_series_limit` 可能为 10，图表中的 `charting.data.count` 限值为 100。这两个设置值相乘表示图表的总数据点限值为 1000。如果 `js_chart_truncation_limit` 为 800，那么减少每个系列的数据点以符合 800 这个总数据点限值。

要覆盖所有图表中的 `js_chart_truncation` 限值，您可以使用 `charting.chart.resultTruncationLimit` 简单 XML 选项更改单个图表的限值。

关于编辑配置文件

有关结合使用 `web.conf` 和 `visualizations.conf` 配置文件的更多信息，请参阅《管理员手册》中的以下主题。

- 如何编辑配置文件
- `web.conf` 规范文件
- `visualizations.conf` 规范文件

类别限制

当根据类别来绘制数据时，Splunk 软件对图表显示的标签有所限制。这种限制对于水平轴（X 轴）和垂直轴（Y 轴）不一样。
X 轴的每个标签必须至少有 20 像素可用。Y 轴必须至少有 15 像素可用。如果需要的像素不可用，则标签不能显示。
您可放大 X 轴来查看被类别限制隐藏的标签。请参阅“平移和缩放图表控制”，以获得详细信息。

单值

概述

使用单值可视化显示一个指标及其上下文。单值可视化为返回离散数字的搜索显示结果和上下文。

此单值可以是特定事件的一个计数或其他聚合。例如，以下可视化显示一个热门柠檬汁摊位的销售额。



标题、单位符号和范围颜色的效果进行了加强。数值右边的趋势标记和下面的迷你图显示数据随时间变化的方式。

若要使用单值可视化，请参阅以下主题。

- 生成单值
- 自定义单值

生成单值

了解如何编写查询以生成单值可视化。

使用 `timechart` 命令新建时间系列图和使用 `stats` 命令聚合数据的查询最适用于单值可视化的工作。

使用时间图表以生成单个值

此搜索和可视化在 Splunk 部署中使用 `timechart` 追踪日常错误。

```
index=_internal source="*splunkd.log" log_level="error" | timechart count
```



要访问迷你图和趋势标记，搜索必须包含 `timechart` 命令，这是非常重要的。使用 `timechart` 意味着时间系列数据将对迷你图和趋势标记处理可用。

如果使用 `stats` 命令作为完整 `timechart` 查询的一部分，则可视化不会包含迷你图或趋势标记。

使用 `stats` 以生成单个值

如果您使用 `stats` 命令以生成单个值，则可视化显示不带趋势标记或迷你图的聚合数值。例如，此查询和可视化使用 `stats` 记录给定一周的所有错误。

```
index = _internal source = "*splunkd.log" log_level = "error" | stats count
```



单个值的查询和时间范围

设置能最好地驱动您所期望的单值查询是很重要的。

- 搜索单个值以避免在可视化中出现意外的结果。在“仪表板编辑器”中可选择单个值可视化，即使搜索会返回多个值。在这种情况下，单个值可视化使用结果表第一个单元格中的值。

- 时间范围挑选器和查询命令协同工作，以生成单值可视化的结果。在可视化中使用 stats 显示时间范围内结果的聚合总数的查询。使用 timechart 生成可视化以显示该范围内的最新结果的查询。

有关 stats 命令的详细信息，请参阅《搜索参考》中的 stats。

有关 timechart 命令的详细信息，请参阅《搜索参考》中的 timechart。

可生成迷你图和趋势标记的查询

默认情况下，迷你图一般出现在通过 timechart 命令生成的单值的下面。它显示您在搜索中指定的时间范围内指标的增减。

此可视化为过去一周数据的搜索显示结果。使用时间范围挑选器以选择本周意味着迷你图反映的是过去七天里数据的变化。



此可视化为过去一天数据的相同搜索显示结果。使用时间范围挑选器以选择今天意味着迷你图反映的是过去 24 小时里数据的变化。



趋势标记一般出现在通过 timechart 命令生成单值的右边。它显示的是在自定义时间范围内最新的数据行为。趋势标记由一个数字和一个箭头组成，以代表数据中最近发生的变化。

趋势箭头可能会根据数据行为指向上或下，也可能直接指向旁边表示没有任何变化。默认情况下，趋势标记值评估结果中两个最新数值的差异。您可以在格式菜单的“常规”设置面板中更改趋势时间窗口，也可以通过调整 timechart 的 span 参数来更改。如果您使用格式菜单中的比较字段，则它会覆盖您在搜索字符串中指定的 span 命令。例如：

```
index=_internal source="*splunkd.log" log_level="error" | timechart count
```

自定义单值

了解如何配置单值可视化组件。

值范围和颜色

颜色可在单值可视化中强调范围值或趋势。在“格式”菜单中，您可以选择是否使用颜色。如果您选择使用颜色，您可以选择

根据数值还是趋势使用颜色。

注意：对于使用 stats 聚合结果的查询，只能通过数值选项使用颜色。

您还可以调整颜色模式，以更改颜色在前景还是背景中显示。



根据您选择的颜色模式，对按照数值使用 timechart 生成的单值进行着色，以表示迷你图和趋势标记呈现的是黑色（前景颜色）还是白色（背景颜色）。

按照数值着色

按照数值着色适用于使用 stats 或 timechart 生成单值可视化。按照数值着色意味着可视化中的单个数字值根据搜索生成的数值和数值对应的范围而更改颜色。比如，如果您将数值范围 30–50 映射到黄色，则单值 35 显示的就是黄色。

您可以为查询调整数值范围，以更改不同的结果可视化的方式。在默认情况下，对于按照数值着色的功能，有五种范围和颜色。您可以添加或移除范围、为每个范围修改数值，以及使用“格式”菜单更改与每个范围相关的颜色。

比如，此 timechart 生成的单个数值可视化表示按照数值着色，并且具有所选的背景颜色模式。



按照趋势着色

按照趋势着色适用于使用包含 timechart 命令的查询而生成的单值。按照趋势着色表示此可视化中的迷你图和趋势标记更改颜色以显示数据中的变化。默认情况下，如果更改值是正数，则迷你图和趋势标记显示绿色，而负数则显示红色。当结果显示无更改，则趋势颜色为黑色。

比如，此可视化表示按照趋势着色，并且具有所选的前景颜色模式。



您可以在“格式”菜单中为趋势颜色进行相反设置。您还可以为可视化指定不同的趋势时间窗口。

现有单个值可视化中的 rangemap 设置迁移

现有的单个值可视化可以使用带有 rangemap 命令的查询来配置范围和颜色。

默认情况下，单值可视化具有此颜色范围的映射配置。

- low: 绿色
- guarded: 蓝色
- elevated: 黄色
- high: 橙色
- severe: 红色

警告：由于 rangemap 命令的支持有所限制，因此不建议建立新单值可视化。当前使用 rangemap 查询将生成单值，但是 UI 配置覆盖基于查询的设置。

对于现有的单个值可视化，建议将 rangemap 命令设置从查询中迁移出来。通过格式菜单颜色面板中等效的范围和颜色设置替代基于查询的设置。

标题和单位

使用“格式”菜单的“常规”选项面板以添加单个值可视化的标题。您可以在“数字格式”面板中指定一个测量单位及其位置。例如，您可以在反映美国销售额的数值前面添加 \$ 或在追踪数据转换的数值后面添加 MB。

注意：如果您从较早版本的 Splunk 软件中迁移，且您的可视化包含“之前”和“之后”标签，则“格式”菜单显示使用“单位”和“标题”字段更新标签和单位文本的提示。

标题

标题为单值可视化添加描述性上下文。要添加标题选择“格式”菜单常规面板。在此使用标题文本字段输入描述。标题显示在单值下方。

单位

单位可以显示单值的标准测量。要添加单位至可视化，请选择“格式”菜单中**数字格式**面板并编辑“单位”字段。您可以选择单位显示在数值前面还是后面。单位文本的字符数量建议为五个或以下。若文本更长，可使用标题。

数字格式设置

如果您正在使用的是一个较大的单个值或者需要较高精确度的数值，则您可以更改可视化的数字格式。在“格式”菜单的“数字格式”面板中，您可以选择千分位或十进制的不同精确度。

钻取

默认情况下，钻取对单值可视化禁用。有关启用和配置钻取的更多信息，请参阅“将钻取用于仪表板交互”。

仪表

使用仪表

使用径向仪表、塞尺和标记规以映射范围相关的数值。仪表可视化提供指标状态和范围信息，您可以快速进行解释。发生时您可以使用实时搜索来生成追踪数值波动的仪表。

数据格式设置

要生成仪表，使用可返回单个数字值的搜索。例如，使用一个搜索，使其返回在特定时间范围或实时窗口内出现的、带特定字段值的事件的事件计数。如果您使用的是实时搜索，则范围标记会移动以显示指标随时间的变化情况。

仪表类型

所有仪表类别都能可视化单个聚合指标。

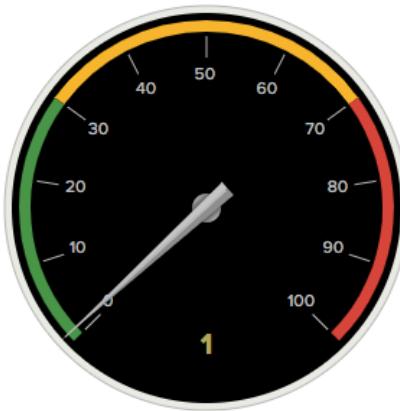
例如，此搜索聚合错误日志事件。

```
index=_internal source="*splunkd.log" log_level="error" | stats count as errors
```

此搜索可生成任意一种可用的仪表类型。

径向仪表

Radial Gauge 格式 棚架

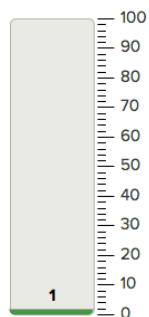


径向仪表包含一个四舍五入的数值刻度和指针，以在刻度中显示当前值。当前值也是在仪表的底部显示。您可以配置径向仪表，以便为刻度中的每个数值范围使用特定的颜色。

如果搜索生成配置的最小和最大范围以外的当前值，则仪表指针在数值刻度下端和上端之间来回摆动。

塞尺

Filler Gauge 格式 棚架

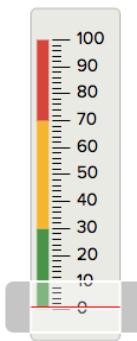


塞尺包含一个数值刻度容器，可以随着当前值的变化填满和清空。填充级别显示当前值在数值刻度的位置。

当前值也是在仪表的填充部分显示。当数值低于最小值时，容器显示为空。而当数值高于最大值时，显示为已满。

标记规

Marker Gauge 格式 柜架



标记规显示数值范围和颜色，其中标记会通过移动来显示当前值。

如果搜索生成的当前值在配置的最小和最大范围以外，则标记在数值刻度下端和上端之间来回摆动。

“配置”选项

使用格式菜单配置仪表类型和颜色范围。

颜色范围

使用格式 > 颜色范围面板选择手动或自动颜色范围配置。默认前三个范围为绿色、黄色和红色。

如果查询包含针对范围配置的 `gauge` 命令，则将颜色范围的处理方式设置为自动。

如果查询包含 `gauge`，则格式菜单中的范围配置会覆盖查询中的 `gauge` 命令设置。

新建仪表可视化

前提条件

查看以下内容了解构建柱形图和条形图的相关详细信息。

- 数据格式设置
- 仪表类型
- “配置”选项

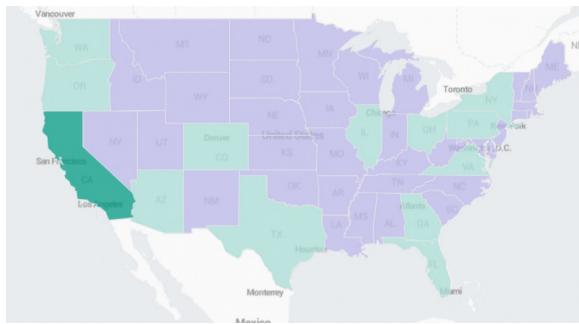
步骤

1. 编写一个可生成单个聚合值的搜索。
2. 运行该搜索。
3. 选择可视化选项卡，然后用可视化挑选器选择径向仪表、塞尺或标记规。
4. (可选) 使用格式菜单配置可视化。

地图

映射数据

可视化包含地理信息的数据有若干选项。



Choropleth 地图使用阴影效果显示相对指标，如预定义地理区域的人口或选举结果。例如，此图像显示的是美国地图。两种颜色的州的阴影都深浅不同。一种颜色代表特定指标的较低值。此颜色中最深的阴影代表最低的数值。另一种颜色代表相同指标的较高值。此颜色中最深的阴影代表最高的数值。当数值逐渐趋向此范围的中间值时，阴影都会有所暗淡。

您也可以新建带地理数据的其他可视化，如群集地图或图表。

入门

通过以下主题了解有关新建分级统计地图和其他地理可视化的信息。

- 生成分级统计地图
- 配置分级统计地图
- 群集地图

另请参阅

要了解地理空间查找的相关信息，请参阅《知识管理器手册》中的“配置地理空间查找”。

生成分级统计地图

地理可视化根据位置聚合事件。位置名称可能已包含在事件中。您还可以使用搜索从每个事件中已标记的经度和纬度来生成位置。

Choropleth 地图具有特定的数据和组件要求。搜索使用这些数据和组件来生成分级统计地图。

使用地图组件和地理数据

运行搜索前，请查看以下组件和数据详细信息。

建立地理可视化的组件

要求使用这些组件新建地理可视化。

组件	描述	可用选项
带地理坐标的数据	地理可视化从包含每个事件的位置信息的数据开始。此数据可能来自多个来源，包括传感器或转发的数据来源。	或者： <ul style="list-style-type: none">带有已标记的经度和纬度坐标的数据。与查找中位置名称相匹配的数据。具有可以使用 <code>iplocation</code> 命令生成 <code>lat</code> 和 <code>lon</code> 字段的 IP 地址字段的数据。更多信息，请参见“使用 IP 地址生成分级统计地图”。
查找表格文件	查找文件定义区域边界，如美国州与州之间的边界。 从搜索和报表主页选择设置 > 查找 > 查找表文件以查看可用文件。	或者： <ul style="list-style-type: none">美国 <code>geo_us_states</code>，以及世界各国 <code>geo_countries</code> 内置文件。其他地方已上传的 KMZ 或 KML 文件。将文件上传至查找表文件管理器页面。

地理空间查找	<p>地理空间查找匹配的是查找表文件中的区域定义坐标。</p> <p>从主页选择设置 > 查找 > 查找定义以查看可用查找定义。</p>	<p>或者：</p> <ul style="list-style-type: none"> 美国和世界各国的内置查找。 新建地理空间查找。有关更多信息，请参阅《知识管理器手册》中的“配置地理空间查找”。
--------	--	---

使用规范化的数据

当数据规范化时，Choropleth 地图工作状态最佳。规范化对数据进行调整，以便更为精确地反映您所可视化的指标。例如，分级统计地图能够比较两个人口不同的城市之间的销售业绩。使用规范化以生成此地图，意味着单独的人口差异无法决定地图上城市之间销售状况的比较。

测试自定义查找文件

如果您正在使用自定义查找表文件和地理空间查找，您可以在新建分级统计地图前使用 `inputlookup` 命令以确保该文件和查找运行正常。

有关更多信息，请参阅《知识管理器手册》中的“配置地理空间查找”。

显示地图上的所有特征（不考虑数据范围）

如果数据集不包含可分级统计地图中每个特征的聚合值，您可以使用 `geom` 命令 `allFeatures` 参数以在呈现时显示地图上的所有形状。

有关更多信息，请参阅《搜索参考》中的 `geom`。

新建搜索

您需要搜索坐标数据、转换搜索和地理空间查找来构建分级统计地图或其他地理可视化。以下步骤说明如何新建分级统计地图搜索。或者，您也可以使用这些步骤来生成地理数据的其他可视化。

前提条件

确保已获得用于构建地理可视化的正确数据和组件。请参阅“数据和组件要求”。

步骤

建立搜索后，运行搜索的每个部分以确保其功能正常。根据您正在建立的可视化和现有的组件，有些步骤是可选的。

1. 指示一个事件数据来源。

```
source=my_data.csv |
```

从已标记的地理坐标或位置名称字段的事件数据来源开始。例如，在罗列公司零售位置的 `.csv` 文件中有一个记录。此文件包含每个记录的经度和纬度坐标。

```
Store Number,Name,Facility ID,Products,Services,Country,Latitude,Longitude
12345,Buttermilk Tea Shop,54321,"Tea, Cake",Wi-Fi,US,43.031873,-71.073203
```

2.（可选）添加查找。

```
lookup geo_us_states longitude as Longitude, latitude as Latitude |
```

如果事件数据已经包括位置名称或 `featureId` 字段，则您可以跳过此步骤。

此查找使用地理坐标为事件生成 `featureId` 和 `featureCollection` 字段。`featureId` 是地理特征的名称，其中包含一组特定的地理坐标，如州或城市名。在默认情况下，`featureCollection` 是查找定义名称。

添加查找和运行搜索之后，请查看可用的所选字段或感兴趣的字段以确保 `featureId` 已罗列。否则，查找不会从地理坐标生成 `featureId`。字段区分大小写。

3. 使用转换命令。

```
stats count by featureId |
```

使用查找的地理输出字段 `featureId` 以聚合数据。如果您不需要查找，请通过已存在于事件数据中的位置名称字段来聚合。

4.（可选）选择并配置可视化。

您也可以使用此搜索来生成地理数据的非地图可视化。如果您并非要构建分级统计地图，则搜索完成。使用可视化挑选器选择可视化类型。使用格式菜单以进行配置。

5. (可选) 使用 geom 完成分级统计地图搜索。

如果正在建立分级统计地图, 请添加 geom 命令并传入 featureCollection 参数的查找名称。

根据事件是否包含 featureId 字段, 选择如下选项之一。

事件包含	后续步骤	示例
featureId 字段	1. 使用这些字段所属的查找。 2. 指示字段 geom 应当解释哪些事件为 featureIdField。	geom geo_us_states featureIdField="State"
位置名称, 无 featureId 字段。这可能是因为您之前跳过查找。	1. 使用包含位置名称的查找。例如, 如果事件使用美国的州名, 则使用 geo_us_states。	geom geo_us_states

有关分级统计地图查询的更多信息和高级选项, 请参阅《搜索参考》中的 geom。

示例搜索

在前述步骤中汇编的完整搜索应该是这样的。

```
source=my_data_source.csv | lookup geo_us_states longitude as Longitude, latitude as Latitude | stats count by featureId | geom geo_us_states
```

配置分级统计地图

要查看或更改分级统计地图配置, 请选择格式菜单和下列设置面板之一。

常规

调整常规设置, 包括初始地理坐标和通过滚轮进行缩放。您还可以选择隐藏地图图例。

颜色

颜色模式和数据箱设置决定分级统计地图使用颜色可视化数据的方式。选择颜色模式并在颜色面板中配置数据箱。

颜色模式

颜色模式	说明和用例	示例
分类	通过类别值列出颜色区域。例如, 您可以按照州来追踪热卖产品的销售情况。如果多个州具有相同的热卖产品, 则他们共享一种颜色。	
序列	单个色调从浅到深的颜色区域。此模式帮助您找到指标非常高的区域。	
分散	用两种不同颜色, 按由浅到深的程度标记各个区域。此模式显示指标特别高或低的区域。当区域指标逐渐趋向此范围的中间值时, 阴影都会有所暗淡。	

数据箱

已聚合的数据值将分为一组数据箱。每个数据箱对应一个特定的数值范围并且具有独特的颜色或阴影。您可以针对所选颜色模式调整数据箱数量和数据箱颜色分配。

地图右边的分级统计地图图例显示的是数据箱及其颜色和数值范围。

形状

对应分级统计地图上一个区域的形状。例如，美国的分级统计地图中的每个州都是一个形状。您可以调整形状不透明度和边框。

平铺

平铺代表地图背景特征，如海洋。显示或隐藏平铺。

使用 IP 地址生成分级统计地图

`iplocation` 命令通常是在通过具有相关 IP 地址的事件中生成地图的最简单方法。如果事件中有 IP 地址数据，您可以使用 `iplocation` 查找其在第三方数据库中的位置信息，并在搜索结果中生成位置字段。

根据数据中可用的 IP 地址信息，`iplocation` 可以在事件中生成位置字段，包括 `City`、`Country`、`Region`、`latitude` 和 `longitude`。通过将可选的 `allfields` 参数设为 `true`，您还可以添加 `Continent`、`MetroCode`（仅限美国）和 `Timezone` 字段。

使用 IP 地址进行地理定位对于确定近似位置而不是精确地址非常有用。您的 Splunk 平台实例包括一个 `GeoLite2-City.mmdb` 数据库文件的副本，该文件提供列出的 IP 地址的城市级位置信息。

如果您想要更精确地映射数据，则需要使用比 IP 地址更详细的位置信息的数据，并使用所需的地理边界配置地理空间查找。请参阅《知识管理器手册》中的“配置地理空间查找”了解更多。

前提条件

- 具有相关 IP 地址的数据，如 Web 访问日志。本主题中的示例使用来自 [搜索教程](#) 中的 `sourcetype=access_combined_wcookie` 数据。要按示例操作，下载 `tutorialdata.zip` 文件并查看“[上载教程数据](#)”获取上载说明。
- 执行字段提取以在必要时隔离 IP 地址。请参阅《[知识管理器手册](#)》中的“[使用字段提取器构建字段提取](#)”。
- 熟悉地理空间可视化。请参阅“[生成分级统计地图](#)”了解分级统计地图的更多信息。
- 确定您希望在分级统计地图中为边界使用什么地理空间查找文件。要使用查找而不是 Splunk 软件随附的 `us_states` 和 `world_countries`，请参阅《[知识管理器手册](#)》中的“[在 Splunk Web 中定义地理空间查找](#)”。

将地理信息添加到您的数据中

您可以使用 `iplocation` 命令，从第三方数据库检索数据中与 IP 地址相关的地理信息。

1. 导航到搜索和报表应用的搜索视图。
2. 在搜索栏中输入以下内容以改进搜索，使其将包含 IP 地址的事件包含在内。

```
source="tutorialdata.zip" sourcetype=access_combined_wcookie clientip=*
```

3. 将以下内容添加到搜索，以使用 `iplocation` 命令，IP 地址字段名称作为参数。

```
| iplocation clientip
```

4. 验证新位置字段是否已添加到事件旁边的“感兴趣的字段”列。
在教程数据中，`City`、`Country`、`Region`、`lat` 和 `lon` 字段被添加到事件中。

生成分级统计地图

现在已经添加了地理信息字段，您可以使用 `stats` 和 `geom` 命令创建分级统计地图可视化。

1. 在上一项任务中开始的搜索基础上，使用转换命令聚合数据，以便在地理特性集合中每个特性都有一行，您希望通过这一行来映射数据。

```
| stats count by Country
```

2. 将以下内容添加到搜索以使用 `geom` 命令将地理边界添加到表格中的各行。

```
| geom geo_countries allFeatures=True featureIdField=Country
```

3. 使用完整搜索生成地图

```
| stats count by Country| geom geo_countries allFeatures=True featureIdField=Country
```

下表解释了搜索中包含的两个参数的用途：

参数	用途
<code>allFeatures=true</code>	确保 <code>featureCollection</code> 中的所有功能都显示在地图上，即使聚合数据没有针对集合中的每个功能的值。
<code>featureIdField</code>	如果字段名称不是 “ <code>featureIdField</code> ”，提供映射到地理空间查找中功能的字段名称。

4. 运行该搜索。

5. 选择可视化选项卡，然后从可视化选项中选择分级统计地图。如果您想要映射的功能是数值型的，那么分级统计可视化将生成带有相应阴影的数据箱。如果是类别，可视化将为每个类别分配颜色。

6. 根据需要调整分级统计地图的设置。

- 如果功能的颜色没有如您所期望的那样，那么值可能过于集中在特定的数据箱中而无法正确显示。尝试调整基本搜索以消除离群值。

- 请参见“生成和配置分级统计地图”获取如何配置分级统计地图的更多信息。

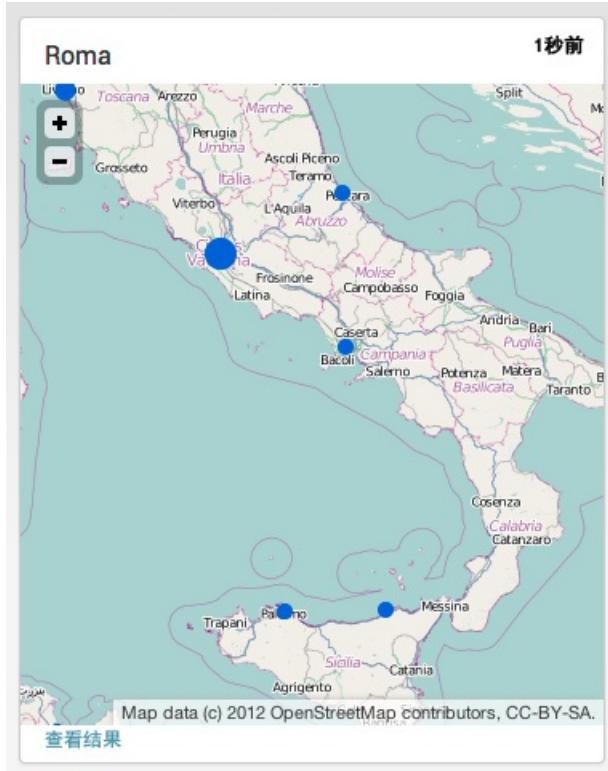
7. (可选) 将您的地图保存到报表或仪表板。

已完成的分级统计地图中的阴影表示链接到地图上各国家的客户端 IP 地址的数量：



群集地图

使用群集地图可视化在地图上绘制聚合值。



数据格式设置

若要生成群集地图，可使用 `geostats` 命令。`geostats` 命令生成的事件包含标记的纬度和经度坐标。它类似于 `stats` 命令，但为缩放级别和映射单元格提供了选项。

有关更多信息，请参阅《搜索参考》中的 `geostats`。

“配置”选项

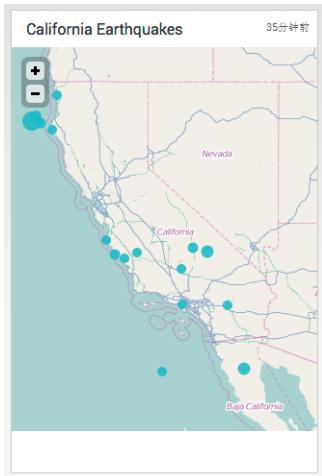
格式菜单可用于调整以下群集地图组件。

- 平铺外观和来源
- 群集标记外观
- 通过滚轮进行缩放的行为

示例

下面的搜索生成了一幅地图，显示在过去 30 天内加利福尼亚震级大于 3 的地震。

```
index=main mag>3 | geostats latfield=latitude longfield=longitude count
```



当用户单击表示地震数据的群集时，搜索将启动使用该群集纬度和经度边界的详细搜索。

```
index=main mag>3 | search latitude>=36.21094 latitude<36.56250 longitude>=-122.34375 longitude<-121.64062
```

教程：使用新的地理空间查找生成分级统计地图

教程概述

分级统计地图可视化按位置聚合的数据。

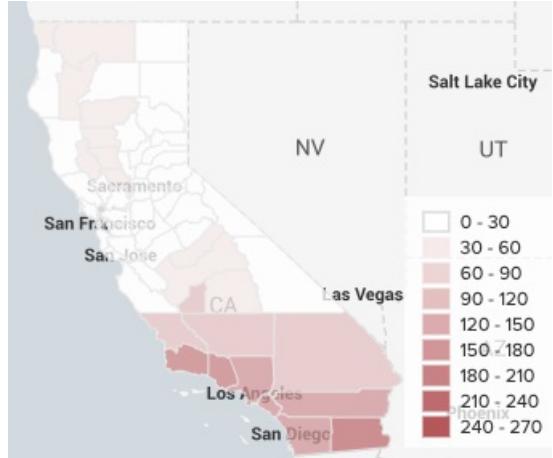
要创建可可视化值的分级统计地图，您需要一个地理特性集合，提供与数据粒度级别相同的地理边界。例如，如果您想要按州映射美国人口，可以使用 Splunk 搜索创建一个统计表，其中每个州的人口作为一行，并使用 geo_us_states 查找在地图上呈现各州的几何形状。要按县映射人口，您可能需要创建更精细的表格（其中美国每个县作为一行）和一个新的地理空间查找（提供美国所有县的边界）。要了解地理空间查找的更多信息，请参阅《知识管理器手册》中的“在 Splunk Web 中定义地理空间查找”。

目标

在本教程中，您将了解如何执行以下操作：

- 查找来自美国干旱监控局的公共数据文件和适当粒度级别的地理空间边界文件并上传到 Splunk 平台实例中。
- 除了 Splunk 软件包含的 geo_us_states 和 geo_countries 查找外，使用查找文件创建新的地理空间查找。
- 生成分级统计地图，说明 2018 年加利福尼亚州的干旱严重程度。

您完成的分级统计地图如下图所示：



前提条件

确保您已运行 Splunk 平台实例。相关信息，请参阅以下链接：

- Splunk Enterprise
- Splunk Cloud
- Splunk Cloud 免费试用版

步骤

1. 查找并下载 USDM 数据
2. 上载并配置数据
3. 下载加州各县的图形文件
4. 新建地理空间查找
5. 生成分级统计地图
6. （可选）使用棚架视图可视化多个聚合函数

查找并下载 USDM 数据

本教程使用来自美国干旱监控局 (USDM) 的加利福尼亚干旱数据，USDM 是由内布拉斯加大学林肯分校美国国家抗旱中心、美国农业部和美国海洋及大气管理局联合制作的一项服务。USDM 监测全国范围内的干旱严重程度，并每周发布干旱严重程度指标，指标等级分为 0 到 4 级，从“异常干旱”到“极其干旱”。本教程使用 2018 年加利福尼亚州县级干旱程度数据。请参见 USDM 网站的“什么是美国干旱监控局？”查看干旱严重程度范围和可用数据类型的详细信息。

下载干旱监测局数据集

按照这些步骤从网站下载合适的数据。或者，直接下载 `us_drought_monitor.csv.zip` 文件。

1. 导航到 USDM 网站的数据 > 数据下载 > 全面的统计数据。
2. 输入以下信息：

数据下载页面中的字段	值	注释
开始日期	2018/1/1	您将映射 2018 年干旱严重程度。
结束日期	2018/12/31	
空间范围	县	您选择的空间范围决定了数据的空间粒度，这需要与您在下一步下载的地理空间查找文件的粒度匹配。
统计数据类别	百分比区域	
统计数据类型	分类	这确保各干旱严重程度类别中的值是离散的，而不是累积的，这样您可以计算干旱严重程度索引的加权和。
位置	美国大陆 (CONUS)	本教程重点是加利福尼亚的映射干旱数据，因此，我们不需要下载美国大陆以外的数据。

3. 单击提交。
- 文件下载到您的计算机。
4. 打开文件确保其下载正确并重命名为 `us_drought_monitor.csv`.

下一步

下载加州各县的图形文件

上载并配置数据

使用 Splunk Web 界面将干旱监控数据上载到 Splunk 平台实例。

前提条件

- 查找并下载 USDM 数据

步骤

按照以下步骤将干旱监控数据上载到 Splunk 平台实例：

1. 解压缩 `us_drought_monitor.csv.zip` 文件。
2. 单击设置 > 添加数据。
3. 单击从我的计算机上载文件。
4. 单击选择文件，然后从文件中选择 `us_drought_monitor.csv`。
5. 单击打开 > 下一步。
6. 确保来源类型设置为 csv 且各字段命名正确。
7. 根据捕获日期配置时间戳。在此文件中，此信息位于名为 `MapDate` 的字段中。
 1. 单击时间戳。
 2. 选择提取 > 高级。
 3. 在时间戳字段框中输入 `MapDate`。
 4. 在时间戳格式下，输入 `strptime()` 字符串 `%Y%m%d` 允许索引器读取格式正确的日期。请参见《数据导入》手册中的“配置时间戳识别”获取关于 `strptime()` 字符串的更多信息。
8. (可选) 将此配置另存为新输入类型。
 1. 单击另存为保存此输入类型。
 2. 在名称字段中输入 `drought_csv`。
 3. 单击保存。
9. 单击下一步。确保输入设置正确。
10. 单击查看，然后单击提交上载文件。
11. 单击开始搜索查看数据。

下一步

下载加州各县的图形文件

下载加州各县的图形文件

要在 Splunk Web 中生成分级统计地图，您需要一个地理特性集合文件，也称为 `shapefile` 或锁眼标记语言/锁眼标记压缩 (`KML/KMZ`) 文件，该文件提供与数据空间粒度匹配的地理边界。本教程使用加利福尼亚州的县级干旱数据，因此需要一个将加利福尼亚州划分为县的特性集合。您可以从加拿大政府 California Open Data Portal 下载此文件。

大多数美国、城市和州级政府网站都有地理空间信息系统 (GIS) 数据门户，您可以从这些门户下载地理参考地图。其他提供有用地理参考地图的网站包括美国人口普查局地图边界文件网站和美国地质调查局国家地图数据下载网站。

前提条件

- 查找并下载 USDM 数据
- 上载并配置数据

步骤

按照这些步骤下载合适的地理特征集合。或者，直接下载 `ca_counties.kmz.zip` 文件。

1. 导航到加利福尼亚 Open Data Portal 的数据集页面。
2. 从以下两种方法中选择其中一种，查找加利福尼亚县边界的 `.kmz` 文件：
 1. 在搜索栏中输入 California Counties。
 2. 使用以下选择缩小搜索范围：
3. 选择标题为 California Counties 的文件并下载 `.kmz` 文件。
4. 将下载的文件重命名为 `ca_counties.kmz`。

数据集搜索页面中的字段	值
主题	经济和人口统计资料
格式	kml

下一步

新建地理空间查找

新建地理空间查找

使用地理特征集合文件在 Splunk Web 中创建新的地理空间查找。关于地理空间查找的更多信息，请参阅《知识管理器手册》中的“在 Splunk Web 中定义地理空间查找”。

前提条件

- 查找并下载 USDM 数据
- 上载并配置数据
- 下载加州各县的图形文件

上载查找文件

按照以下步骤在 Splunk Web 中上载地理空间特征集合文件：

1. 解压缩上一步中下载的 `ca_counties.kmz.zip` 文件。
2. 导航到设置 > 查找。
3. 在查找表格文件中，单击 + 新增。
4. 确保目标应用设置设为搜索。
5. 在上载查找文件下，单击选择文件然后选择 `ca_counties.kmz`。
6. 在目标文件名下，输入 `ca_counties.kmz`。

配置地理空间查找

按照以下步骤在 Splunk Web 中配置新的地理空间查找：

1. 单击设置 > 查找，单击查找定义下的 + 新增。
2. 确保目标应用设置设为搜索。
3. 在名称下，输入 `ca_county_lookup`。

4. 在类型下，选择地理空间。
5. 在查找文件下，选择您刚刚上载的 `ca_counties.kmz` 文件。
6. 将特征 ID 元素留空，因为此文件包括 `.kml` 文件中默认 `Placemark/name` 下的县名称。有关地理空间查找中的 XML 路径表达式的更多信息，请参阅《知识管理器手册》中的“特征 ID 元素字段”。
7. 单击保存。
8. (可选) 测试您的地理空间查找文件。

1. 在“搜索和报表”应用搜索栏中，运行以下搜索：

```
| inputlookup ca_county_lookup
```

如果没有显示结果，尝试扩大搜索的时间范围。

2. 验证 `featureId` 字段每个县有一行且 `geom` 字段包含多边形和坐标。您的搜索结果表应如下所示：

计数	featureCollection	featureId	geom
0	ca_county_lookup	Alameda	{"type": "MultiPolygon", "coordinates": [[[[-122.31109619140625, 37.8634033203125], [-122.31109619140625, 37.8634033203125]]]]}}
0	ca_county_lookup	Alpine	{"type": "MultiPolygon", "coordinates": [[[[-119.93537902832031, 38.8084831237793], [-119.93537902832031, 38.8084831237793]]]]}}
0	ca_county_lookup	Butte	{"type": "MultiPolygon", "coordinates": [[[[-121.63543701171875, 40.000885009765625], [-121.63543701171875, 40.000885009765625]]]]}}
0	ca_county_lookup	Calaveras	"type": "MultiPolygon", "coordinates": [[[[-120.21088409423828, 38.500003814697266], [-120.21088409423828, 38.500003814697266]]]]}}

3. 选择可视化选项卡，将可视化类型设为分级统计地图。
4. 单击 + 按钮或双击地图放大至加利福尼亚，验证县多边形显示正确。

下一步

生成分级统计地图

生成分级统计地图

要创建分级统计地图，请在用于在地图上绘制地理空间边界的地理特性集合中聚合数据，以创建每个特性或多边形一行的表格。地图上每个多边形的颜色底纹表示聚合值。

前提条件

- 查找并下载 USDM 数据
- 上载并配置数据
- 下载加州各县的图形文件
- 新建地理空间查找

创建分级统计统计数据表

使用 Splunk 搜索处理语言 (SPL) 创建包含多边形名称相应的聚合的表格。在此情况下，我们正在按县映射加利福尼亚，这样您需要一个表格，每个县对应一行。

1. 导航到“搜索和报表”应用。
2. 将以下内容输入搜索栏以将年份限制到 2018 年，州限制为加利福尼亚州，这样您的表格只会包含您想要映射的数据。

```
source="us_drought_monitor.csv" State = CA date_year=2018
```

3. 将以下内容添加到搜索以将“县”一词从“县”字段中删除，这样该字段与查找中的 `featureId` 字段匹配。

```
| rex field=County "(?<County>.+)" County"
```

4. 添加以下内容以计算聚合干旱评分，从而将四个干旱严重程度类别合成一个可以映射的值。请参见 USDM 网站的“干旱严重级别和覆盖索引”页面查看关于此聚合值的更多信息。

```
| eval droughtscore = D1 + D2*2 + D3*3 + D4*4
```

5. 添加以下内容聚合每周干旱评分，以生成一个表格，每个县对应一行。

```
| stats avg(droughtscore) as "2018 Drought Score" by County
```

使用 `avg()` 计算数据平均值有助于规范化数据，收紧颜色数据箱传播的范围。使用 `sum()` 或 `max()` 聚合数据可能会扩大传播范围，这样数据箱宽度会变大，生成一个信息较少的地图。

6. 将以下内容添加到搜索以使用 `geom` 命令将地理空间查找文件中的多边形和相应的县行关联起来。

```
| geom ca_county_lookup featureIdField=County
```

将整个搜索放在一起，如下所示（此搜索最终会需要一个索引和一个“所有时间”的时间范围）：

```
source="us_drought_monitor.csv" State = CA date_year=2018 | rex field=County "(?<County>.+) County" | eval droughtscore = D1 + D2*2 + D3*3 + D4*4 | stats avg(droughtscore) as "2018 Drought Score" by County | geom ca_county_lookup featureIdField=County
```

结果显示在“统计”选项卡中，包括如下内容：

- “县”列，用作 `featureId`。在分级统计地图中，各多边形被称为一个特性，其唯一值是 `featureId`。
- “2018 干旱评分”列，也就是分级统计地图中阴影部分的值。
- `featureCollection` 列，表示 `geom` 命令检索多边形边界的地理特性集合。
- `geom` 列，包含地理多边形坐标。

统计数据表如下所示：

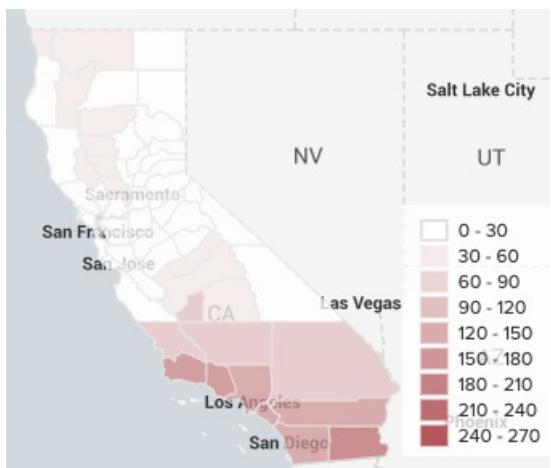
县	2018 干旱评分	featureCollection	geom
Alameda	16.037	ca_county_lookup	{"type": "MultiPolygon", "coordinates": [[[[-122.31109619140625, 37.8634033203125], [-122.31109619140625, 37.8634033203125]]]]}
Alpine	0	ca_county_lookup	{"type": "MultiPolygon", "coordinates": [[[[-119.93537902832031, 38.8084831237793], [-119.93537902832031, 38.8084831237793]]]]}
Butte	23.843	ca_county_lookup	{"type": "MultiPolygon", "coordinates": [[[[-121.63543701171875, 40.000885009765625], [-121.63543701171875, 40.000885009765625]]]]}
Calaveras	3.614	ca_county_lookup	{"type": "MultiPolygon", "coordinates": [[[[-120.21088409423828, 38.500003814697266], [-120.21088409423828, 38.500003814697266]]]]}

生成并配置您的分级统计地图

按照以下步骤将您的表格转换为信息分级统计地图：

1. 选择搜索栏下方的可视化选项卡。
2. 确保将可视化类型设为分级统计地图。如果没有，选择当前可视化类型的名称，然后选择“推荐”下方的分级统计地图。
3. 通过点击+按钮或双击地图放大到加利福尼亚查看您的地图。
4. （可选）增加数据箱的数量以创建更多信息可视化。
 1. 单击格式>颜色。
 2. 在数据箱数量下，选择较高的数字，如8或者9。使用更多的数据箱可以增加表示干旱评分值组的阴影的数量，并反映出具与县之间更细微的差异。
5. （可选）要为下次运行搜索保留缩放设置，选择“常规”下方的填充当前地图设置。
6. 将您的地图保存到仪表板。
 1. 选择另存为>仪表板面板。
 2. 在仪表板下，选择新建。
 3. 在仪表板标题下，输入CA Drought Monitor。
 4. 在面板标题下，输入Drought score by county。
 5. 在面板内容下，选择Choropleth Map。
 6. 单击保存。

完成后是以下分级统计地图，说明了2018年加利福尼亚州各县的干旱严重程度。



要进一步放大并查看加利福尼亚的特定分区，选择平铺 > 从预设置配置填充 > 打开街道地图将背景层更改为更详细的地图。

下一步

(可选) 使用棚架视图可视化多个聚合函数

(可选) 使用棚架视图可视化多个聚合函数

有时在相同的地图区域上显示多个阴影值是有用的。如果您想要调用多个聚合函数创建分级统计表格，使用棚架视图并排比较这些函数。

前提条件

- 查找并下载 USDM 数据
- 上载并配置数据
- 下载加州各县的图形文件
- 新建地理空间查找
- 生成分级统计地图

步骤

1. 当您在构建生成分级统计表格的搜索时，调用 stats 命令中的多个函数。在此示例中，我们比较干旱评分均值、最大值和最小值：

```
source="us_drought_monitor.csv" State = CA date_year=2018 | rex field=County "(?<County>.+)" County" | eval droughtscore=D1 + D2*2 + D3*3 + D4*4 | stats avg(droughtscore) as "Average 2018 Drought Score" max(droughtscore) as "Max 2018 Drought Score" min(droughtscore) as "Min 2018 Drought Score" by County
```

2. 将以下内容添加到搜索以使用 SPL 搜索中的 geom 命令将相应的地理空间多边形添加到表格中：

```
| geom ca_county_lookup featureIdField=County
```

3. 运行该搜索。

4. 在可视化选项卡中，注意：因为您提供了多个要映射的聚合值，所以没有显示有阴影的功能。选择棚架布局解决这个问题。

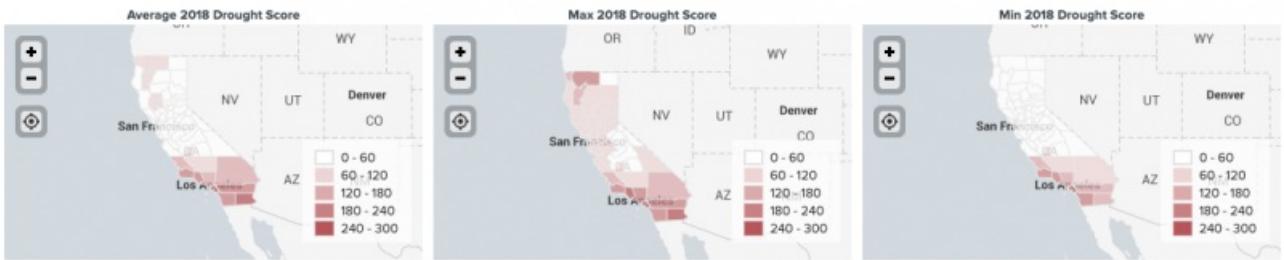
5. 勾选标记为使用棚架布局的复选框。

6. 在拆分依据下，选择聚合 (3)。

7. 滚动和缩放到每个地图上的加利福尼亚，比较三种不同的值的阴影模式。

8. 将棚架地图保存到仪表板。

棚架地图提供三个聚合值并排的可视化，以提供 2018 年加利福尼亚的干旱条件完整图片：



可视化的棚架布局

使用棚架布局拆分可视化

您可以使用棚架布局按字段或聚合拆分搜索结果，对每个字段值单独进行可视化。

这是一个应用了棚架布局的单值可视化。按产品类别值拆分客户购买结果。用户可以了解不同产品类型的购买指标的差异。



使用案例

使用棚架布局以使给定数据维度的值差异更显著。

突出显示离群值

棚架布局可使离群字段值更醒目。

例如，仪表板用户可能想要在网络中跨多个服务器追踪状态。使用棚架布局的单值可视化可以同时显示多个服务器的状态。有异常状态值的服务器会更显著。

比较特定指标的趋势

您可以拆分搜索结果，这样直观地比较不同的字段值会更容易。

例如，您可以将棚架布局应用于条形图，显示不同产品类型的最近客户活动。您可以通过拆分客户行为字段，浏览不同产品类型的购买频率变化。

使用一个搜索监视多个资源

如果您想要在不新建和运行多个搜索或生成多个可视化的情况下监视多个资源，使用棚架布局会有用。您可以使用一个搜索为某一类或一组中的各资源生成指标，然后拆分您正在追踪的字段上的可视化。

棚架布局的数据格式设置

您可以使用棚架布局拆分字段的搜索结果。如果您的搜索包括两个或更多个聚合，如 `count` 或 `sum`，您还可以拆分聚合结果。

启用棚架布局前，请大致考虑您想要提供的比较或趋势。确保搜索结果包括代表这些值的字段或聚合。

生成拆分字段

要使用棚架布局，请确保搜索结果包括您想要用于拆分可视化的字段。拆分字段是您在没有棚架布局的情况下生成可视化可能需要的补充字段。例如，您可以使用以下搜索生成单值可视化。

```
index=_internal | stats count
```

要使用棚架布局，请调整搜索以生成其他字段，以便拆分可视化。

```
index=_internal | stats count by sourcetype
```

您可以拆分 `sourcetype` 字段上的单值以显示搜索结果中每个来源类型的 `count`。

使用其他字段添加见解

您可以生成多个结果字段以为每个可视化段添加更多数据纬度，视使用情况而定。

例如：您可以按客户行为和产品类型聚合最近的零售网站数据。您可以使用搜索结果中一个字段拆分可视化。用户可以使用拆分可视化以在产品类型中比较客户行为或了解产品类型与客户行为的关系。

有关新建搜索的更多信息，请参阅《[搜索参考](#)》中的“统计和图表函数”。

访问棚架布局菜单

您可以在仪表板中新建或编辑可视化时访问棚架布局菜单。

棚架布局不适用于表格可视化或群集地图。

通过可视化访问菜单

如果您正在搜索页面构建可视化，您可以通过可视化选项卡访问棚架配置菜单。

The screenshot shows the Splunk search interface with a search bar containing the query `sourcetype=access_* | stats count by categoryId`. Below the search bar, it says "118,596 个事件 (18/06/06 13:58:19.000 之前) 无事件采样". The "可视化" (Visualization) tab is selected. A modal window titled "使用棚架布局" (Use Shelf Layout) is open, with a checked checkbox "拆分依据" (Split by) and a dropdown set to "categoryId". There are three size options: 小 (Small), 中 (Medium), and 大 (Large). In the background, there are several red cards representing different game categories: ACCESS (6,421), SHOOTER (4,155), SIMULATION (4,335), SPORTS (2,379), STRATEGY (13,809), and another card with 6,039.

通过仪表板访问菜单

1. 单击仪表板中编辑打开仪表板编辑器。
2. 找到您想要应用棚架布局的面板。
3. 单击“更多操作”图标并选择棚架。



配置棚架布局

您可通过棚架布局菜单选择“拆分依据”结果字段或聚合并配置分段。

选择拆分字段或聚合

如果您按字段或聚合拆分可视化，在所选字段中的每个值都会出现单个可视化段。

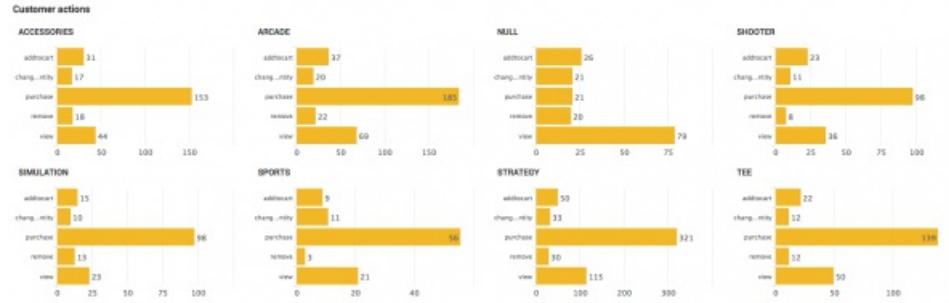
使用 `eval` 命令生成的结果字段会出现在聚合列表中。

如果您没有在此列表中看到想要使用的拆分字段或聚合，请调整搜索确保列表会在搜索结果中生成字段。您可能需要调整搜索以返回其他字段，这些字段不是生成无棚架布局可视化的必需字段。

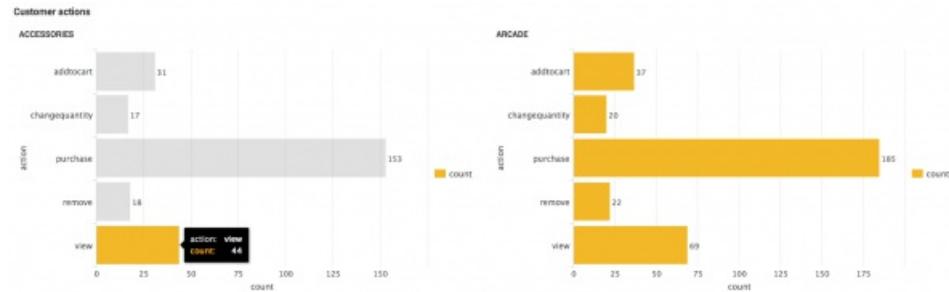
调整分段大小

选择一个分段大小选项。分段大小会影响面板数据密度。面板可以同时显示更多小尺寸分段。较大的分段有助于用户根据分段数量进行更详细的可视化比较。

尺寸较小的分段



尺寸较大的分段



配置刻度共享

棚架布局菜单包括以下可视化类型的刻度共享选项。

- 折线和面积图
- 条形图和柱形图
- 分级统计地图

选择“共享”以在所有分段中使用相同的轴或图例值范围。选择“独立”以在每个分段中使用带有刻度的值的轴或图例值范围。

设置分段格式和外观

使用格式菜单或简单 XML 配置可视化段外观。设置应用棚架布局的可视化格式，其方法与未应用棚架布局设置可视化格式方法相同。每个分段都会配置您应用的格式。

分级统计地图滚动和缩放

在应用棚架布局的分级统计地图中，您可能需要滚动并缩放分段以将其限制在某个特定位置。将滚动和缩放限制到一个分段以避免触发显示其他分段中的更改。侧重此分段后，打开格式菜单并单击“填充当前地图设置”以在所有分段中更新侧重。

棚架布局和仪表板显示

分段密度

棚架布局生成的分段数因搜索结果中拆分字段数或聚合值而异。如果要同时显示的可视化分段过多，仪表板面板可能包括滚动栏。



使用棚架菜单以调整分段大小并在面板中显示更多分段。您还可以使用仪表板编辑器以拖动面板大小或更改简单 XML 中的面板 height 选项。

要更改分段显示的顺序，请调整搜索以排列或更改搜索结果顺序。

面板和行的最佳做法

将使用棚架布局的面板隔在仪表板行中。在同一行中显示其他内容会限制显示棚架布局的内容并很难浏览仪表板。

避免做法	最佳做法
<p>在同一行中放其他面板，显示会受到限制。</p>	<p>整行显示棚架布局面板。</p>

棚架布局中的钻取

使用钻取编辑器或简单 XML 启用并配置钻取。将棚架布局应用到可视化之后，每个可视化段中均可使用钻取。

钻取选项

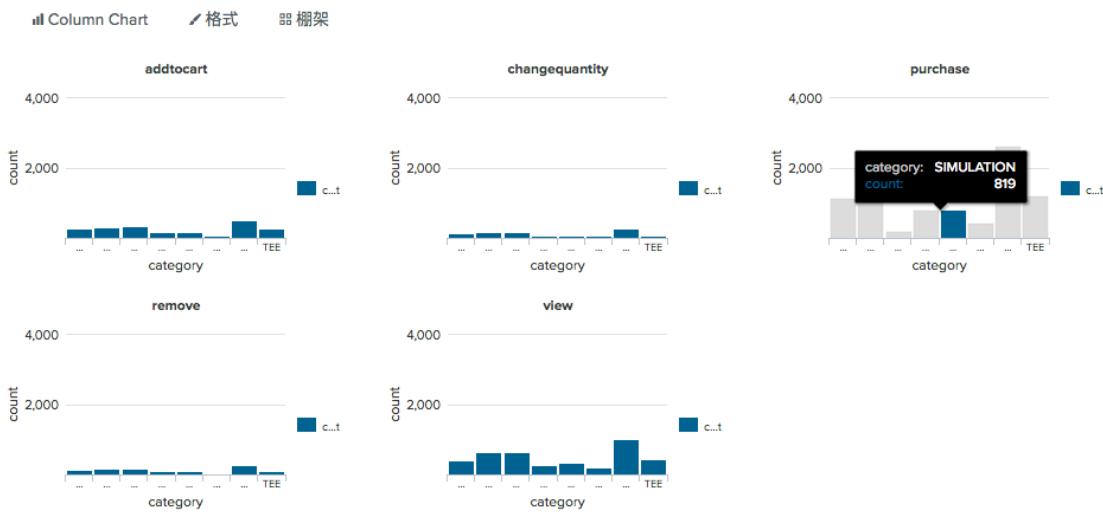
典型的钻取操作（如链接到搜索或外部 URL）可用于使用棚架布局的可视化。根据您想要的行为，您可以配置钻取以捕获并使用来自元素和用户单击的可视化段的详细信息。

示例

此钻取会链接到搜索。默认情况下，辅助搜索会修改初始搜索以包括来自单击的分段的字段值。

例如，棚架布局会按客户行为拆分零售活动可视化。如果用户单击客户行为分段“购买”中的“ARCADE”类别列，则会打开使用这些字段值的辅助搜索。

单击的可视化段和列



生成可视化的搜索

```
... | stats count by action, categoryId | rename categoryId as "category"
```

钻取搜索

```
... | action=purchase | rename categoryId as "category" | search category=ARCADE
```

用于棚架拆分字段的预定义标记

如果棚架布局拆分搜索结果字段，您可以使用预定义标记 `trellis.name` 和 `trellis.value` 访问来自单击的可视化段的拆分字段名称和值。

您可以将这些值传递到钻取目标，如表单或外部 URL。此示例钻取链接到外部零售网站，使用 `trellis.value` 标记在来自单击分段的产品字段值中传递。

```
<drilldown>
<link>
  http://buttercupgames.com?product=$trellis.value$
</link>
</drilldown>
```

聚合在预定义的标记中不可用。

限制

- 在棚架布局配置菜单中，使用 `eval` 命令生成的字段会作为聚合出现。
- 棚架布局不适用于表格可视化或群集地图。
- 预定义标记不适用于用于拆分可视化的聚合。
- 使用棚架布局的可视化不以仪表板 PDF 形式呈现。

在简单 XML 中配置棚架布局

使用以下简单 XML 选项配置棚架布局。

选项名称	类型	默认	描述
<code>trellis.enabled</code>	布尔值	0	启用或禁用 Trellis 布局。默认为 0（禁用）。
<code>trellis.scales.shared</code>	布尔值	1	表示是否要在折线图、面积图、柱形图和条形图共享轴的刻度，或在分级统计地图分段中共享值的范围。使用下列任意值。 <ul style="list-style-type: none"> • 1: 共享刻度 • 0: 独立刻度

trellis.size	字符串	medium	配置可视化段大小。段大小影响拆分可视化的面板显示密度。使用下列任意值。 <ul style="list-style-type: none"> • small • medium • large
trellis.splitBy	结果字段名称	N/A	指示为拆分可视化使用的搜索结果字段或聚合名称。每个值的分段都在此字段中显示。

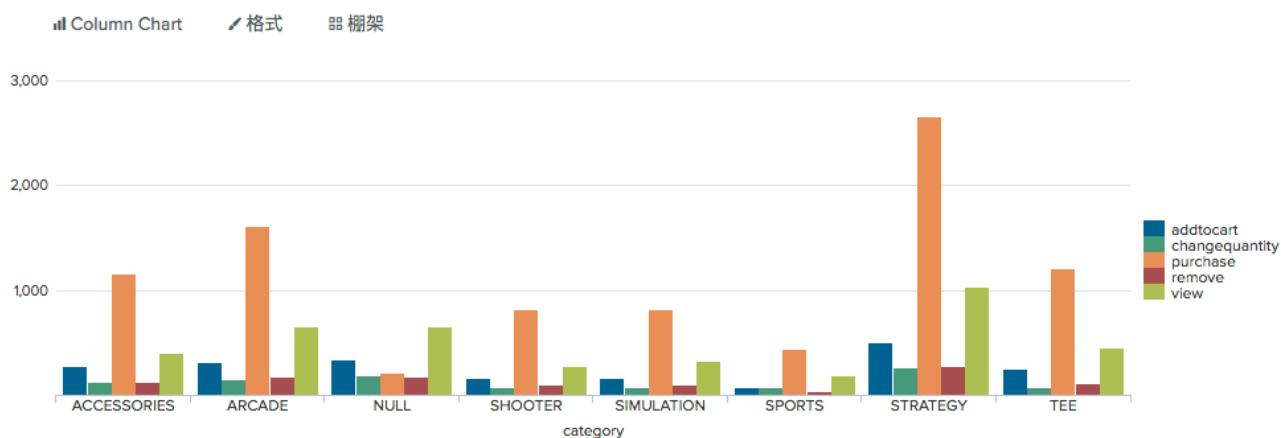
示例

研究销售趋势

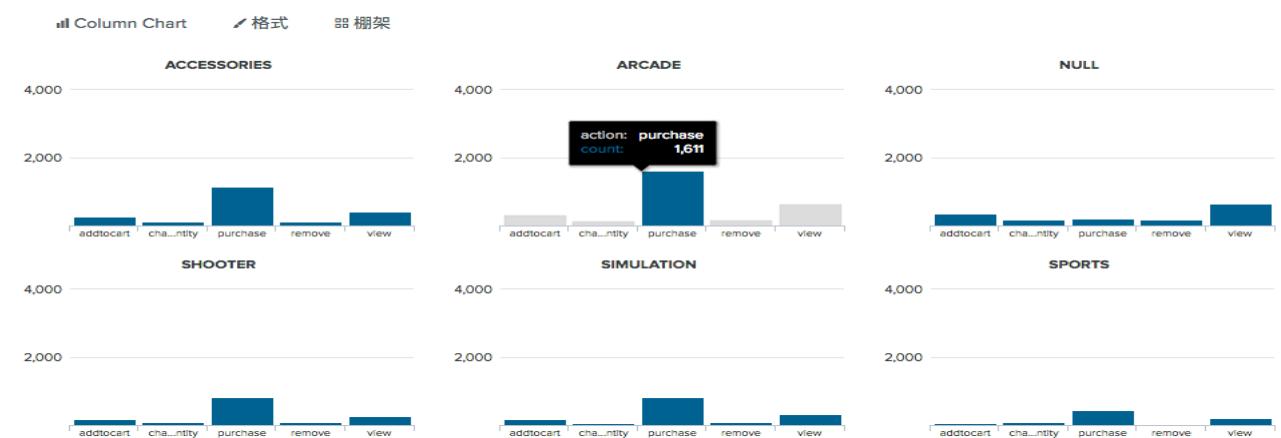
在线零售商分析师会按产品类别研究客户行为。它们会使用以下搜索按产品 category 查找最新的客户 action 事件。

```
source=recent_sales_data action != NULL
| rename categoryId as "category"
| chart count by category, action
```

搜索会生成以下柱形图，显示所有产品类别的客户操作。



分析师可以使用棚架布局将可视化拆分为单独的柱形图，分别代表不同的客户行为类别。分析师可利用棚架布局比较与各行为相关的产品类型的趋势。



仪表板入门

仪表板概览

新建新仪表板或编辑现有仪表板。

快速查看最常用使用案例和新建仪表板的命令，注意，您可以点击“开始”中的链接访问 Splunk 仪表板快速参考指南。

仪表板和表单工作流

使用仪表板涉及以下一个或多个任务。

构建仪表板

- 新建新仪表板
- 添加新可视化到仪表板

有关构建仪表板的更多信息，请参阅“新建仪表板”

编辑仪表板

- 向仪表板添加一个面板
- 编辑仪表板面板和面板可视化
- 管理仪表板搜索

有关编辑仪表板的更多信息，请参阅“编辑仪表板”。

将仪表板转换为表单

- 添加用户输入到仪表板，并将其转换为一张表单
- 编辑表单
- 进行用户输入设置的相关操作

关于表单的更多信息，请参阅“新建和编辑报表”

自定义简单 XML

- 编辑简单 XML 源代码来自定义仪表板或表单。

使用简单 XML 的更多信息，请参阅“编辑简单 XML”

添加互动和动态行为

- 使用标记来捕获和传递数据。
- 添加事件处理程序以执行动态行为。

关于事件处理程序和标记的更多信息，请参阅“将钻取用于仪表板交互”和“仪表板中的标记用法”

工具和框架

要构建和编辑仪表板，使用以下所示的一个或多个工具和框架。

“仪表板编辑器”用户界面

使用 Splunk Web 用户界面来构建和编辑仪表板。

简单 XML

仪表板使用简单 XML 源代码来定义其内容和行为。您可以使用 Splunk Web 中的“仪表板编辑器”来编辑其源代码。

要了解更多信息，请参阅“编辑简单 XML”。

开发人员选项

Splunk Enterprise 用户可以进行额外的仪表板自定义。

- 使用 CSS 和 JavaScript 扩展简单 XML。

有关更多信息，请参阅 Splunk 开发人员门户中的以下资源。

- 使用简单 XML 修改仪表板
- 关于 SplunkJS Stack
- 使用 Splunk Web 框架创建仪表板和可视化

示例

Splunkbase 上的“仪表板示例”应用提供了许多仪表板实现方面的示例，包括源代码。安装此应用，查看示例仪表板并进行互动。

弃用的选项

以下仪表板框架选项自 6.3.0 版本起已弃用：

- 高级 XML
- 模块系统（作为高级 XML 的一部分已弃用）。

有关其他自定义选项的信息，请参阅：为 Splunk 平台构建自定义

已删除选项

以下仪表板框架选项自 7.3.0 版本起已删除。

选项	有关更多信息，请参阅
Django Bindings	Splunk Enterprise 7.3.0 《版本说明》中的已删除功能。

以下仪表板框架选项自 8.1.0 版本起已删除。

选项	有关更多信息，请参阅
可以将简单 XML 仪表板转换为 HTML。	Splunk Enterprise 8.1 《版本说明》中的已删除功能。

关于“仪表板编辑器”

使用 Splunk Web 的“仪表板编辑器”来新建并编辑仪表板。“仪表板编辑器”让用户可访问编辑用户界面和简单 XML 源代码。

编辑用户界面

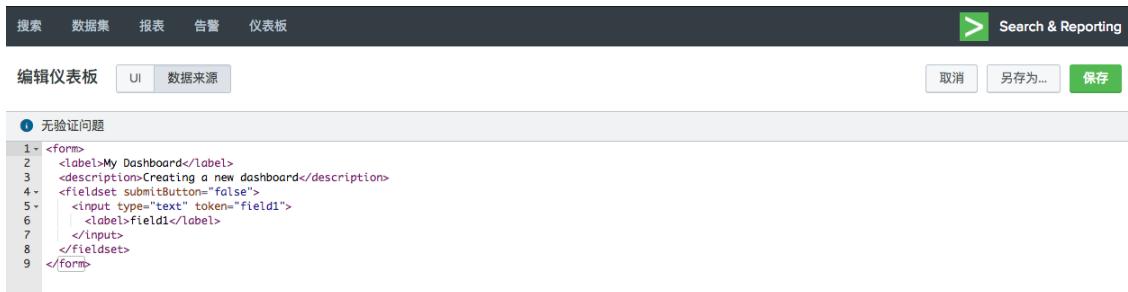
您可以在编辑用户界面中新建和更新仪表板及面板。

The screenshot shows the Splunk Web interface for creating a new dashboard. At the top, there's a navigation bar with links for '搜索' (Search), '数据集' (Data Sets), '报表' (Reports), '告警' (Alerts), and '仪表板' (Dashboards). To the right of the navigation is a 'Search & Reporting' button. Below the navigation, there's a toolbar with buttons for '编辑仪表板' (Edit Dashboard), 'UI' (User Interface), '数据来源' (Data Sources), '+添加面板' (Add Panel), '+添加输入' (Add Input), a dark mode toggle, and buttons for '取消' (Cancel), '另存为...' (Save As...), and '保存' (Save). The main workspace is titled 'My Dashboard' and contains the sub-tutorial 'Creating a new dashboard'. It shows a single panel labeled 'field1' with a text input field. There's also a checkbox for '自动运行仪表板' (Run dashboard automatically) and a note at the bottom: '单击“添加面板”开始操作。' (Click "Add Panel" to start operating.).

要了解更多信息，请参阅“新建仪表板”和“编辑仪表板”。

源代码编辑器

使用“仪表板编辑器”访问和编辑简单 XML 源代码。



1 ~ <form>
2 ~ <label>My Dashboard</label>
3 ~ <description>Creating a new dashboard</description>
4 ~ <fieldset submitButton="false">
5 ~ <input type="text" token="field1">
6 ~ <label>field1</label>
7 ~ </input>
8 ~ </fieldset>
9 ~ </form>

此编辑器在您进行修改时会提供验证、错误消息和警告。

键盘快捷键

与 Ace 代码编辑器快捷键一致的键盘快捷键在仪表板编辑器中可用。

您可以使用 Mac 上的 **Command + Shift + F** 或 Windows 上的 **CTRL + Shift + F** 设置简单 XML 的格式。

在 Splunk Web 中构建和编辑仪表板

新建仪表板

仪表板均在特定应用的上下文中新建。例如，如果使用的是搜索和报表应用，则仪表板使用此应用的上下文。

新建仪表板后，您可以修改其权限，以便共享或管理其他用户对此仪表板的访问权限。您也可以修改应用上下文。

步骤

1. 使用以下各选项中的其中一项。

通过	操作
仪表板页面	单击新建新仪表板
保存可视化	1. 选择另存为 > 仪表板面板 2. 单击新建，使用此面板新建一个新仪表板。

2. 如果您不想使用默认标题，提供标题和 ID，以及仪表板的描述。

3. 指定权限。

4. 选择在经典框架中构建您的仪表板。如果您选择在 Dashboard Studio 中构建，请参阅《Splunk Dashboard Studio》手册中的“在 Dashboard Studio 中创建仪表板”。

5. 保存仪表板。使用以下各选项中的其中一项。

通过	单击
仪表板页面	单击新建仪表板
保存可视化	单击保存

6. 添加面板，将仪表板转换为表单，或编辑仪表板内容。

有关更多信息，请参阅以下主题。

- 向仪表板添加面板
- 编辑仪表板
- 新建和编辑表单
- 配置仪表板权限

使用仪表板面板

仪表板包含一个或多个面板。仪表板面板可使用搜索生成可视化。根据搜索行为的类型和您想要的配置选项选择面板类型。

内联面板

内联面板直接在源代码中包含搜索。此搜索生成的结果会呈现在面板可视化中。您可以使用“仪表板编辑器”编辑内联搜索。

来自报表的面板

此面板类型会使用来自报表的已保存的搜索和可视化。

使用报表中的面板时，不能修改面板中的搜索字符串，但可更改和配置可视化。如果报表搜索有所变化，使用此报表的面板也会进行相应更新。

访问和性能注意事项

根据您的部署情况，您可能需要调整仪表板性能和访问权限的报表配置。例如，根据您的权限，您可以控制是否加速、计划及嵌入报表。您还可以更改报表权限。

用户上下文

仪表板面板中的报表可以报表所有者或报表用户的身份运行。这些设置会影响数据可见性和并发搜索限制。

选项	描述	数据可见性影响	并发搜索限制影响
----	----	---------	----------

以所有者身份运行（默认）	<p>以报表新建者的权限运行报表。</p> <p>计划的报表始终会以报表所有者的权限运行。</p>	<p>以所有者权限运行的报表所呈现的搜索结果可能是部分用户无权查看的。在某些情况下，您可能想提供这种访问权限。在另一些情况下，您可能想限制搜索结果的可见性。</p>	<p>如果一个包含报表备份面板的仪表板同时加载多次，则可能会影响报表所有者的并发搜索限制。当达到限制值时，报表计划程序会使运行的额外报表搜索排入队列，以供后续执行。</p> <p>仪表板用户可能会发现面板加载很慢，而报表所有者可能无法立即运行搜索和报表。</p>
以用户运行	<p>以查看仪表板的用户的权限运行报表。</p> <p>计划的报表无法以用户权限运行。</p>	<p>如果报表访问的数据是当前用户没有权限查阅的，则面板不会呈现这些结果。</p>	<p>当报表运行时，它会计入负载仪表板用户的并发搜索限制，而不是报表所有者。</p>

尽量为仪表板面板使用计划报表

尽可能使用计划报表备份仪表板面板，因为此做法为您的 Splunk 部署缩短搜索处理加载。

计划报表的益处

不使用计划报表可能会影响搜索处理负载和并发搜索限制。例如，对于有五十个用户访问的特定仪表板，如果面板未由计划报表进行备份，则他们的报表会重复运行五十次。

若使用了计划的报表，则每次用户加载仪表板时搜索就不需要重新运行一次。由计划报表备份的面板会显示报表最后一次计划的运行所返回的结果。

使用实时计划报表

若要为仪表板用户显示最近结果，则可使用实时计划报表备份仪表板面板。这种报表类型会一直在后台运行。所以，每次用户加载仪表板时，就不会发起一个新的报表实例。相反，它会显示当前正运行的实时计划报表的结果。

预建面板

在多个仪表板中保存和重用简单 XML 面板。您可以使用一个连接到预建面板的引用，从而在仪表板中显示该面板。直接编辑面板来更改标题、搜索或其中的可视化。

其他信息

- 要了解使用仪表板编辑器添加或编辑仪表板面板的相关信息，请参阅“添加面板至仪表板”。
- 有关面板搜索的详细信息，请参阅“搜索驱动仪表板和表单”。
- 要了解编辑面板可视化的更多相关信息，请参阅“编辑仪表板”和“编辑可视化”。
- 要了解报表的相关使用，请参阅《报表手册》中的“新建和编辑报表”和“计划报表”。

向仪表板添加面板

了解如何添加和编辑仪表板面板。

要了解仪表板面板的类型，请参阅“使用仪表板面板”。

使用“仪表板编辑器”添加面板

使用仪表板的编辑菜单向仪表板添加面板。直接从仪表板或从“仪表板”页面上的仪表板列表访问编辑菜单。

1. 选择编辑打开“仪表板编辑器”。
2. 选择添加面板。
3. 展开其中一个面板类别。
 - 新建
 - 从报表新建
 - 从仪表板复制
 - 添加预建面板
4. (可选) 要搜索特定面板，在过滤器文本框中输入文本。
5. 选择面板并预览该选择。
6. 单击添加到仪表板。

为可用面板过滤搜索

使用搜索字段中的过滤器查找或新建特定面板。该搜索在现有仪表板、面板和报表中查找指定术语。它使用指定搜索术语为新面板提供结果，并链接到包含该术语的现有仪表板和面板。

以下提示对搜索和筛选操作有所帮助。

- 面板标题或面板 ID 为搜索的有用术语。
- 使用可视化元素名称、输入类型、图表类型和其他关键字过滤搜索。例如：
 - 搜索映射以向实现映射可视化的仪表板返回结果或使用映射可视化新建新面板。
 - 搜索多选以获取具有多选表单输入的结果。
- 您可过滤多个术语，但所有术语必须以您在搜索字段中指定的顺序显示。

重新安排仪表板上的面板

拖放面板以重新安排它们在仪表板上的位置。

1. 如果还没有为仪表板选择编辑模式，选择编辑。
2. 选择面板并放到新位置。

新建仪表板的内联面板

当您新建内联面板时，选择可视化并指定该面板的搜索。

1. 选择编辑打开“仪表板编辑器”。
2. 选择添加面板。
3. 扩展面板类别新建并选择数据的可视化。
4. (可选) 输入面板标题。
5. 输入返回要在面板中显示的数据的搜索字符串。
6. (可选) 选择运行搜索来预览搜索结果。
7. 选择搜索的时间范围。
8. 单击添加到仪表板。

从报表中新建面板

当您从报表中新建面板时，从可用报表列表中选择。

1. 选择编辑打开“仪表板编辑器”。
2. 选择添加面板。
3. 扩展面板类别从报表新建以查看可用报表。
(可选) 使用过滤器选项搜索特定报表。请参阅“为可用面板过滤搜索”。
4. 选择报表以查看该报表的预览。
5. 单击添加到仪表板。

从另一个仪表板中复制面板

您可从另一个仪表板中复制面板。该面板在您的仪表板上显示，与复制的面板具有相同的编辑功能。

1. 选择编辑打开“仪表板编辑器”。
2. 选择添加面板。
3. 扩展面板类别从仪表板复制以查看可用报表。
(可选) 使用过滤器选项搜索特定面板。请参阅“为可用面板过滤搜索”。
4. 选择并扩展仪表板。选择面板以查看该面板的预览。
5. 单击添加到仪表板。

通过参考新建和添加面板

您可新建您稍后可通过参考添加到仪表板的面板。如果您计划在各种仪表板中经常重新使用此预建面板，则它很有用。

新建您可从其他仪表板引用的面板有两种方式。

- 将现有面板转换为您可引用的预建面板。
- 从“设置”页面，在简单 XML 代码中新建面板。

通常，使用“仪表板编辑器”新建面板，然后将它转换为预建面板。您还可以在简单 XML 代码中新建此面板。

将现有面板转换为预建面板

仅当面板不包含后期处理搜索时，您才可将该面板转换为预建面板。后期处理搜索为使用 `base` 属性引用其他搜索的搜索。

1. 在包含您要转换的面板的仪表板中，选择编辑 > 编辑面板。
2. 从面板的选项菜单中，选择转换为预建面板。
3. （可选）在打开的对话框中，指定以下内容。
 - **ID**: 面板的文件名。仅允许使用字母数字字符、"-" 字符和 "_"。
 - **面板权限**: 选择专用或在应用中共享。
 - 专用: 只有您拥有查看和编辑面板的权限。
 - 在应用中共享: 应用的其他用户可查看和编辑面板。

在简单 XML 中新建面板

如果这是您第一次使用简单 XML，请参阅“编辑简单 XML”。也可以参阅“Simple XML 参考”了解关于面板配置的更多信息。

1. 从 Splunk Web，转到设置 > 用户界面 > 预建面板。
2. 在“面板”页面中，选择新建以打开“简单 XML 编辑器”。
3. 在“简单 XML 编辑器”中，指定以下内容：
 - **目标应用**: 为面板上下文选择应用。
 - **预建面板 ID**: 输入面板的名称。
您输入的名称为磁盘上的文件名。仅允许使用字母数字字符、"-" 字符和 "_"。
 - **预建面板 XML**: 定义面板元素的简单 XML 代码。
参考面板的简单 XML 代码仅包含 `<panel>` 元素及其子元素。

向仪表板添加预建面板

1. 从仪表板中，选择编辑 > 编辑面板。
2. 选择添加面板。
3. 扩展面板类别添加预建面板以查看可用的参考面板。
(可选) 使用过滤器选项搜索特定面板。请参阅“为可用面板过滤搜索”。
4. 选择参考面板以查看该面板的预览。
5. 单击添加到仪表板。

将预建面板转换为内联面板

您可将预建面板转换为内联面板。预建面板不可以包含后期处理搜索。后期处理搜索为使用 `base` 属性引用其他搜索的搜索。

将预建面板转换为内联面板允许您自定义搜索和可视化。

1. 从仪表板中，选择编辑 > 编辑面板。
2. 从您要转换的预建面板中，单击选项菜单并选择转换为内联面板。

编辑面板标题

面板和可视化各自拥有各自的标题。

您可以在新建面板时指定标题，也可以使用“仪表板编辑器”更改面板标题，但有一个例外。预建面板的标题无法通过“仪表板编辑器”编辑。请参阅“编辑预建面板”了解更多信息。

步骤

1. 在仪表板中找到要编辑的面板。
2. 单击编辑打开“仪表板编辑器”。
3. 使用以下各选项中的其中一项。

选项	操作
编辑用户界面	<ol style="list-style-type: none">1. 在页面左上方编辑仪表板的旁边，确保已勾选 UI 编辑器。2. 单击要编辑的面板标题，并更改标题文本。
编辑简单 XML	<ol style="list-style-type: none">1. 在页面左上方编辑仪表板的旁边，确保已勾选源代码编辑器。2. 在 <code><panel></code> 内找到要编辑的 <code><title></code> 元素。3. 更改面板标题文本。

4. 单击保存。

编辑预建面板

通过预建面板页面访问“面板源代码编辑器”。

步骤

1. 从主页面，导航至设置 > 用户界面 > 预建面板。
2. 找到要编辑的面板，并选择编辑。
3. 编辑简单 XML 源代码。
4. 单击保存。随后，通过引用包含此面板的仪表板中即会对此面板进行相应更新。

从仪表板删除面板

可以使用“仪表板编辑器”或通过编辑简单 XML 代码从仪表板删除面板：

- 从“仪表板编辑器”上，在面板编辑模式中单击面板的选项菜单并选择删除。或者，您可单击面板右上角的删除图标 X。
- 在简单 XML 源代码中，删除 `<panel>` 元素及其内容。

编辑仪表板

使用“仪表板编辑器”自定义仪表板面板、布局或添加交互性。

打开“仪表板编辑器”

1. 从仪表板列表页面，打开要转换的仪表板。
2. 单击编辑打开“仪表板编辑器”。
3. 选择 UI 或来源更改编辑模式。
4. (可选) 预览所进行的仪表板编辑，然后单击保存以保存更改。您也可以随时单击取消以放弃更改。

更改仪表板面板布局

您可以更改仪表板的布局，以便优先安排特定面板或腾出空间容纳额外内容。

1. 从仪表板列表页面，打开要转换的仪表板。
2. 单击编辑打开“仪表板编辑器”。
3. 通过拖放操作重新安排面板的位置。

更改仪表板主题

您可将仪表板主题改为深色或浅色。默认主题是浅色。

1. 单击仪表板中的编辑打开“仪表板编辑器”。
2. 使用深色主题开关更改仪表板的主题。
3. 保存仪表板并刷新浏览器查看更改。

当您导出为 PDF 时，应用深色主题的已保存仪表板将从深色主题转变为浅色。此操作不支持深色主题。

编辑面板搜索

更新驱动特定仪表板面板的搜索。

使用内联搜索时，仪表板搜索栏有语法突出显示和自动完成功能，您可以使用这些功能构建搜索字符串。更多信息，请参阅《搜索手册》中的“协助读取搜索”。

搜索编辑选项

所有搜索类型	报表	内联搜索和内联数据透视表
· 编辑搜索	<ul style="list-style-type: none">在新窗口中查看和编辑报表。在新窗口中打开报表搜索。	<ul style="list-style-type: none">编辑搜索，指定新的内联搜索或数据透视表。

<ul style="list-style-type: none"> ● 删除搜索。 	<ul style="list-style-type: none"> ● 为面板选择其他报表。 ● 选择为本面板的报表指定的可视化。 ● 指定自动刷新间隔延迟和指示器选项。 	<ul style="list-style-type: none"> ● 将内联搜索或数据透视表转换为报表。 ● 指定自动刷新间隔延迟和指示器选项。
---	---	--

步骤

1. 从仪表板列表页面，打开要编辑的仪表板。
 2. 单击编辑打开“仪表板编辑器”。
- 在每个面板的右上方会显示编辑图标。第一个图标代表面板的搜索。搜索图标会随着所使用的搜索类型的不同而有所不同。
3. 选择适用的搜索图标以查看搜索的配置选项。
 4. 选择要更改的搜索配置。此时可能会显示其他配置对话框或窗口，具体取决于所选择的选项。
 5. 在编辑搜索后，单击保存将更改保存到仪表板。

编辑面板可视化

使用“仪表板编辑器”编辑面板可视化，但此操作只适用于不是由数据透视表或数据透视表报表搜索生成的面板。

如果您所操作的是由数据透视表或数据透视表报表搜索生成的可视化，则可使用“数据透视表编辑器”。有关详细信息，请参阅使用“数据透视表编辑器”设计数据透视表图表和可视化。

前提条件

- 请参阅“可视化的数据结构要求”，了解有关以可正确呈现可视化的格式生成搜索结果的详细信息。
- 请参阅“可视化编辑器可用的属性”以查看可视化配置。

步骤

1. 从仪表板列表页面，打开要编辑的仪表板。
 2. 单击编辑打开编辑仪表板。
- 在每个面板的右上方会显示编辑图标。第二个图标代表“可视化挑选器”。此图标会因可视化类型的不同而有所不同。第三个编辑图标代表可视化“格式”菜单。
3. (可选) 使用“可视化挑选器”选择另一种可视化。确保面板搜索以新可视化所需的正确格式生成结果。您可以选择任何可视化，但如果面板搜索结果的格式不是所选可视化所需的正确格式，则可能无法呈现。
 4. (可选) 使用“格式”菜单配置可视化。
 5. 单击保存将更改保存到仪表板。

编辑仪表板源代码

编辑仪表板简单 XML 源代码以便对无法通过用户界面修改的设置进行自定义。仪表板源代码编辑器在您进行修改时会提供交互式验证。

前提条件

- 有关编辑简单 XML 源代码的信息，请参阅“关于编辑简单 XML”。

步骤

1. 从仪表板列表页面，打开要编辑的仪表板。
2. 选择编辑打开“仪表板编辑器”。
3. 单击来源打开仪表板 XML 源代码编辑器。
4. 编辑源代码。
5. (可选) 观察编辑器是否自动提供标记闭合和验证。编辑器会在必要时显示验证警告或错误消息。将鼠标悬停在一行源代码旁边的警告或错误图标文本的上方即可查看此行的消息。
6. (可选) 如果出现验证警告或错误，则保存按钮不可用。如果此按钮不可用，则修正带验证警告或错误的所有代码。
7. 当不再有警告或错误出现时，保存按钮会变为可用。单击保存以保存对源代码的编辑内容。

编辑预建面板

预建面板无法通过“仪表板编辑器”编辑。通过预建面板页面访问“面板源代码编辑器”。

步骤

1. 从主页面，导航至设置 > 用户界面 > 预建面板。
2. 找到要编辑的面板，并选择编辑。
3. 编辑简单 XML 源代码。
4. 单击保存。随后，通过引用包含此面板的仪表板中即会对此面板进行相应更新。

其他资源

- 要了解在仪表板中新建或编辑可视化的相关信息，请参阅“编辑可视化”。
- 有关将仪表板转换成表单并使用这些表单的详细信息，请参阅“新建和编辑表单”。

编辑可视化

编辑可视化以配置其搜索、类型、外观和行为。

可视化组件编辑

您可以在“仪表板编辑器”编辑可视化，也可以在搜索页面中编辑。在任一位置，您都可以调整以下可视化组件。

可视化组件	描述
搜索字符串	使用仪表板搜索编辑器或搜索栏以更改驱动可视化的查询。
类型	使用可视化挑选器选择可视化类型。确保查询针对所选可视化以相应的结构生成结果。
格式和行为	使用格式菜单调整可视化用户界面的外观、钻取和其他设置。

警告：在“仪表板编辑器”中对可视化设置进行的更改会覆盖相关的标记设置和行为。如果您正使用标记来配置仪表板或表单的部分内容，则在“仪表板编辑器”中更新相关元素时要务必小心。例如，如果图表图例的位置由一个表单输入配置，在“格式”菜单中选择图例位置的设置会覆盖该输入所提供的动态标记设置。此时，该输入仍会保留在仪表板中，但无法再配置图例位置。

可视化编辑工作流

编辑可视化搜索、类型或格式的工作流可能会有所不同，具体取决于您编辑时使用的是“仪表板编辑器”还是搜索页面。

仪表板编辑权限

要编辑仪表板面板，您必须具备写入权限。默认情况下，您对自己新建的任何仪表板均具有写入权限。然而，您可能具有其他仪表板的只读权限。`admin` 角色的用户可更改编辑权限。

在“仪表板编辑器”中编辑可视化

1. 在“搜索和报表”应用中，选择“仪表板”选项卡。
2. 找到仪表板以进行编辑。使用以下各选项中的其中一项。

选项	此选项的其他步骤
选择编辑。	无
单击仪表板名称进行查看。	仪表板打开之后，选择编辑。

3. 在正在编辑的面板中，找到用于编辑搜索、可视化类型和格式的图标。选择正在编辑的组件的图标。
4. 编辑所选可视化组件。

在“搜索”页面中编辑可视化

1. 在“搜索和报表”应用中，选择“搜索”选项卡。
2. 输入查询。
3. 显示结果后，选择“可视化”选项卡。
4. 要编辑可视化，使用以下工具之一。

工具	描述
可视化挑选器	更改可视化类型。
格式菜单	更改可视化格式和行为。“格式”选项按可视化类型有所不同。
搜索栏	编辑查询并再次运行，以刷新可视化。

使用“格式”菜单

“格式”菜单配置可立即应用于可视化。

- 您每次进行的编辑都保存至可视化。您可以看到可视化中的每个更改，并可以随意调整。
- 进行编辑时，编辑将在仪表板的简单 XML 源代码中呈现。
- 单击并拖动“格式”菜单，以移动到屏幕的任何位置。
- 关闭“格式”菜单或单击其外部任何地方以退出，并保存更改。

其他资源

格式和其他选项按可视化类型有所不同。要比较可视化，请参阅“可视化参考”。另请参阅“图表配置参考”。

有关使用“数据透视表”编辑可视化的信息，请参阅“使用数据透视表编辑器设计数据透视表图表和可视化”。

新建和编辑表单

让用户可以通过将仪表板转换为表单的方式选择或筛选内容。表单是指包含一个或多个输入的仪表板，如单选按钮或复选框。

新建表单的工作流

新建表单的典型工作流包含以下步骤。有些步骤为可选，而且实际操作时可以不必按照下面的顺序进行。

- 新建一个仪表板，并添加一个或多个输入以将其转换为表单。
- 指定用户可用的选项、默认行为以及如何处理用户选择，以此方式配置输入。
- 操作从输入中捕获所选值的标记。修改搜索和其他内容以使用标记值。
- 根据输入类型，进行所需的其他输入配置。
- 调整输入和面板布局。

添加输入以将仪表板转换为表单

表单是指带用于选择或筛选内容的交互式用户输入的仪表板。当添加输入至仪表板时，顶级源代码元素会从 `<dashboard>` 变为 `<form>`。

步骤

1. 从仪表板列表页面，打开要转换的仪表板。
2. 单击编辑打开“仪表板编辑器”。
3. 从添加输入列表中选择一个或多个输入。选择好输入后，此仪表板即转换为表单。
4. (可选) 拖放输入，重新安排它们的位置。
5. (可选) 将一个输入拖到特定面板中。使用标记使此输入控制仅位于此面板中。
6. 单击保存将更改保存到表单。

表单输入中的标记

使用标记动态响应用户选择。

当添加一个输入至表单时，会为此输入生成一个特别标记。此标记可用于根据用户选择更改面板的内容。例如，使用面板搜索中的标记来修改面板可视化显示的结果。或者，使用此标记来更改面板标签或钻取行为。

下面的示例说明在表单输入中使用标记的常用选项。

在搜索中引用标记

在本示例中，仪表板有一个面板。面板搜索聚合所有来源类型的事件。

```
index=_internal | timechart count by sourcetype
```

将仪表板转换为表单以添加交互性。添加一个文本输入，让用户可指定来源类型来筛选可视化中的事件。

1. 从仪表板中，单击编辑打开“仪表板编辑器”。
2. 选择添加输入 > 文本，以添加一个文本输入。此仪表板转换为表单。
3. 观察输入是否显示在表单的顶部。针对此输入还会生成一个标签和标记。
4. 单击编辑图标打开“输入编辑器”。
5. 将标签文本更改为“来源类型”。
6. 将标记名称更改为 sourcetype_token 使其更具体。表单内的标记名称都必须具有唯一性。
7. 更新面板搜索字符串以使用标记从用户输入中捕获的值。此搜索使用指定的来源类型来筛选事件。
`index=_internal sourcetype=$sourcetype_token$ | timechart count`
观察用于表示搜索中标记的 \${token name} 语法。
8. 单击应用和保存将更新保存到表单中。

现在此表单包含了一个文本输入，使用户可指定要显示在可视化中的来源类型。在用户指定来源类型之前，可视化不会呈现内容，因为标记尚未捕获用于搜索中的值。当文本字段中输入了来源类型后，此搜索使用该值来生成结果，随后可视化即会呈现结果。

添加时间输入到表单

时间输入使用户可应用一个时间范围来筛选显示在一个或多个面板中的事件。

添加时间输入并更新面板搜索，以纳入用户指定的时间范围。

1. 从仪表板或表单中，单击编辑打开“仪表板编辑器”。
2. 选择添加输入 > 时间。
3. (可选) 选择输入编辑图标并更新输入标签和标记名称。
4. (可选) 单击应用保存输入更新。
5. 针对每个要应用时间输入的面板，执行以下更改。
 1. 单击搜索编辑图标。
 2. 选择编辑搜索。
 3. 为时间跨度范围选择共享的时间挑选器。如果表单中有一个以上的时间输入，每个共享的时间挑选器会一起列出其时间输入的独特标记。针对要使用的输入，选择包含此输入标记的共享时间挑选器。
6. 单击保存以保存面板搜索更新。
7. 单击保存以保存表单更新并退出仪表板编辑器。

应用时间输入至面板

一个表单可以有一个或多个时间输入。根据所需的行为，可以全局针对所有面板使用一个时间输入，也可以针对特定面板使用。

全局时间挑选器

当用“仪表板编辑器”新建一个时间输入时，针对此输入会自动生成一个标记。如果删除此标记，则此时间输入即为全局性。此表单中所有未指定时间范围或其他时间输入的面板都会使用此全局时间挑选器。

在配置面板搜索时间范围时，可以选择共享的时间挑选器（全局）来应用此输入。

基于标记的时间挑选器

在配置面板搜索时间范围时，可以选择包含特定标记名称的共享时间挑选器。使用您要应用到面板搜索的输入的标记名称。

未使用时间输入的面板搜索

如果您不想将时间输入应用到特定面板，则可以为面板搜索指定显式时间范围，或使用其他标记值。

配置输入值处理

可以配置输入值填充表单的方式。

当页面加载时提交标记值

要在页面加载时提交标记值，应启用 autorun 行为。

1. 从仪表板中，单击编辑打开“仪表板编辑器”。
2. 勾选 Autorun 仪表板复选框。
3. 单击保存以保存表单更新。

当输入改变时提交标记值

默认情况下，输入会配置为在用户进行了新选择时即提交标记值。要更改此行为，请执行以下步骤。

1. 从仪表板中，单击编辑打开“仪表板编辑器”。
2. 选择要编辑的输入。
3. 取消勾选变更时搜索复选框以禁用此行为，或勾选此复选框进行启用。
4. 保存输入和表单更改。

添加一个“提交”按钮输入

在表单中添加一个“提交”按钮，使用户可以控制提交输入选择的时间。这有助于管理带多个输入的面板或表单的更新频率。通常来说，如果在表单中使用“提交”按钮，则对输入禁用变更时搜索。

表单“提交”按钮的位置无法更改。

1. 从仪表板中，单击编辑打开“仪表板编辑器”。
2. 选择添加输入 > 提交。
3. 根据需要对输入禁用变更时搜索行为，并保存输入更新。
4. 单击保存以保存表单更新。

指定初始和默认输入值

处理没有用户输入值的场景。

默认

当用户没有进行选择时，使用输入的默认值。

初始

只使用文本输入的初始值。仅在表格页面加载时才会出现初始值。如果用户清除了文本字段的内容，则不会重新显示初始值且标记值会设置为一个空字符串。

如果您同时指定了文本输入的初始值和默认值，则只会应用默认值。

为输入指定多个选项

有些表单输入类型可以包含多个静态或动态填充的选项。

- 复选框
- 下拉菜单
- 链接列表
- 单选
- 多选

所有这些输入显示多个选项，而多选和复选框输入可让用户选择多个值。以下任务说明如何为这些输入中的每个输入配置选项。

指定静态选项

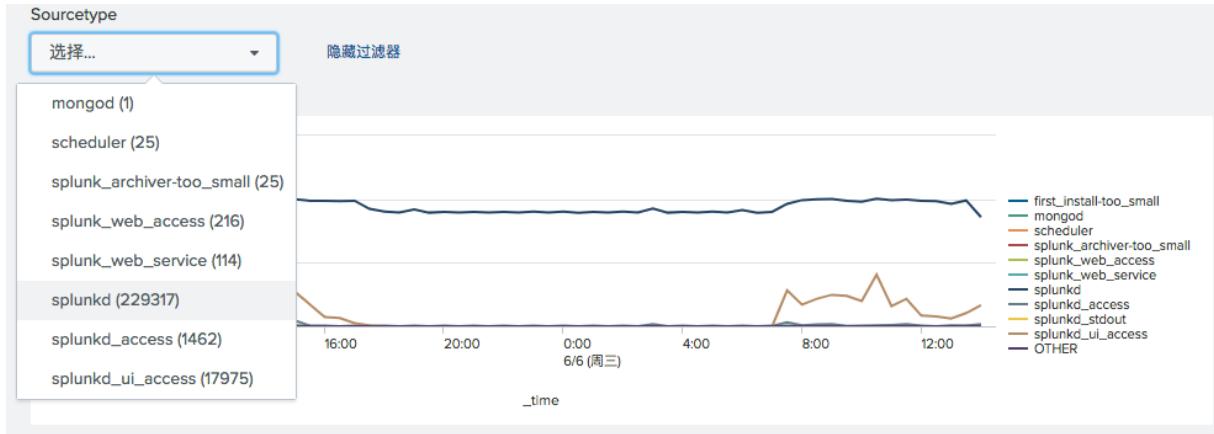
以下示例说明如何指定多个静态选项。本示例使用一个钻取输入，但应用于任意多选项输入。

1. 从仪表板中，选择添加输入 > 下拉。
2. 为输入选择编辑图标。选择静态选项。
3. 为第一个选项指定名称和数值。

4. 对每个其他选项，单击添加选项，并为选项指定名称和数值。
5. (可选) 滚动到默认字段并指定一个默认值。
6. (可选) 拖放选项，重新安排它们的位置。
7. 单击应用以保存输入更改。
8. 单击保存以保存仪表板更改。

指定动态选项

使用搜索来动态生成选项标签和值。



以上步骤说明如何配置动态填充钻取。更新搜索以使用来自输入的标记值的相关步骤并未包含在内。

1. 从仪表板或表单中，添加一个使用以下搜索的折线图面板。

```
index=_internal | timechart count
```

2. 添加一个输入，使用户可针对特定来源类型筛选面板可视化。

1. 单击编辑打开“仪表板编辑器”。
2. 选择添加输入 > 钻取。

3. 配置输入。

1. 选择输入编辑图标。
2. 选择动态选项。
3. 添加以下搜索以生成输入标签和值。

```
index=_internal | stats count by sourcetype | eval label=sourcetype."(.count.)"
```

4. 观察此搜索是否按来源类型聚合事件，并生成结合了来源类型名称和事件计数的标签字段。

5. 针对输入标签和值使用搜索结果字段。指定以下字段。用于标签的字段：label 用于值的字段：sourcetype

4. 单击应用以保存输入更新。

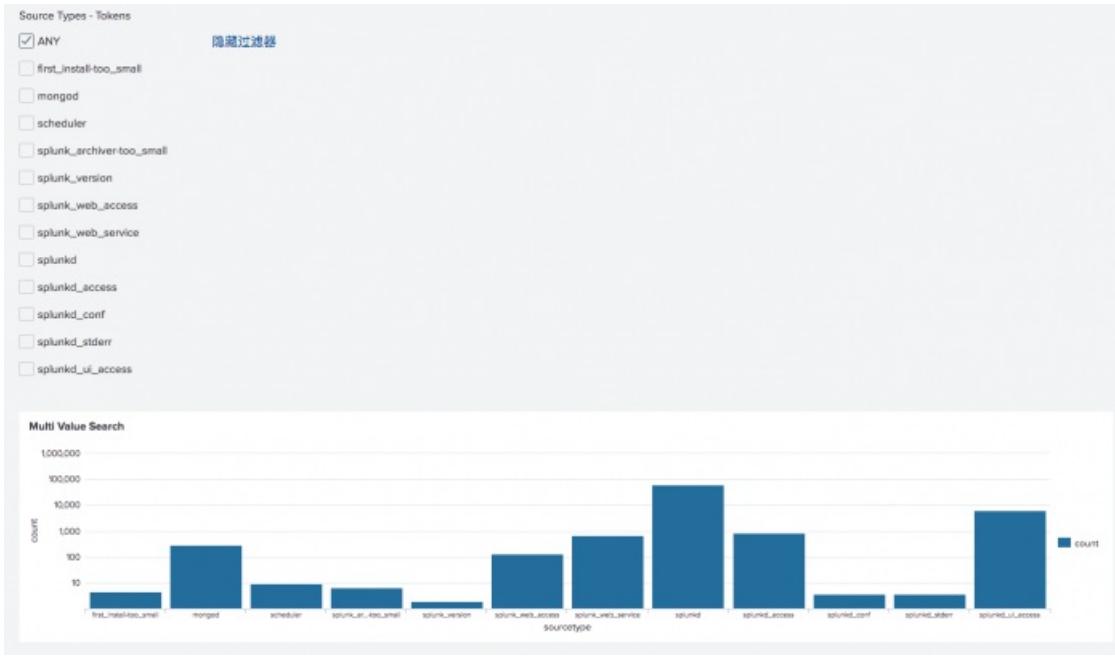
5. 单击保存以保存表单更改。

用户现在可以查看钻取中的事件计数和来源类型名称。

处理多值选择

多选和复选框表单输入可让用户选择多个值。

以下示例面板包含一个复选框，可让用户指定要在图表中呈现的来源类型。



生成多个所选值的搜索

要处理用户在多选或复选框中所选的一个或多个值，使用可为一个或多个值生成结果的搜索。

要指定上面表单中来源类型的值，建立一个搜索字符串，使其表示要返回的值。对于本示例，下面的搜索字符串允许为来源类型选择多个值：

```
(sourcetype="splunkd" OR sourcetype="splunk_web_access" OR sourcetype="splunkd_access")
```

该搜索驱动面板访问复选框和多选的标记值，和其他表单输入不同。使用提交的对标记的修饰符。

```
index=_internal $src_type_tok$ | chart count by sourcetype
```

“输入编辑器”提供编辑字段，可通过复选框或多选指定选择多个值。下面的表格介绍了这些字段，并提供了新建如下搜索字符串的示例值：

```
(sourcetype="selected value" OR sourcetype="selected value" OR ... )
```

编辑器字段	描述	示例值
标记前缀	作为输入元素值的前缀的字符串。 对于多个选择，通常是左圆括号括起选择值的字符串。	(
标记后缀	附加到输入元素值的字符串。 对于多个选择，通常是右圆括号括起选择值的字符串。)
标记值前缀	作为输入元素值的前缀的字符串。可以是正则表达式。默认值是一个左双引号 ("")。 通常，这是选择多个值的子字符串的左边部分。	sourcetype="
标记值后缀	附加到输入元素值的字符串。可以是正则表达式。默认值是一个右双引号 ("")。 通常，这是选择多个值的子字符串的右边部分。	"
分隔符	位于每个选定值之间的字符串。通常，使用大写来指定 "OR" 或 "AND"。不要指定引号，而要在字符串前和字符串后指定一个空格字符。 默认值： " "	OR

下面的过程显示如何为复选框或多选输入启用多个选择。

1. 从仪表板中，单击编辑打开“仪表板编辑器”。
2. 选择添加输入。选择复选框或多选。
3. 指定标签、变更时搜索和标记。
4. 指定选择，如“使用静态选项指定选择”和“使用动态选项指定选择”中所述。
5. 使用上表中的编辑字段，构建多选搜索字符串。
(推荐) 使用预览功能来验证多选搜索字符串。
6. (可选) 指定一个默认值。
7. 单击应用。单击完成。

表单输入示例

本部分提供了一个关于每个表单输入的示例，以及实现此示例的关键字段列表。

复选框

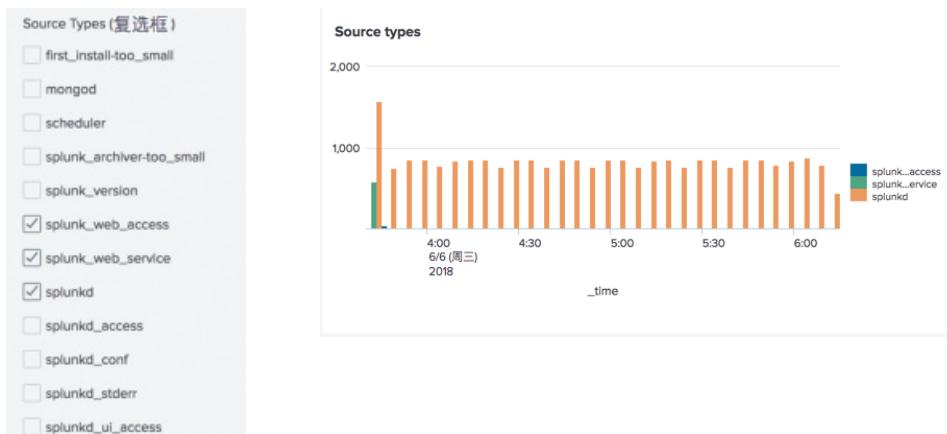
本示例使用复选框输入来指示时间图表中显示哪个来源类型。填充搜索指定可选择的选项。默认选择三种来源类型：

```
splunk_web_access
splunk_web_service
splunkd
```

本示例启用了变更时搜索。选择后，表单即开始加载。

面板在默认列图表中显示结果，使用的是下列基本搜索。可视化使用为标记指定的值引用输入值。在本例中，标记名称为 `src_type_tok`。

```
index=_internal $src_type_tok$ | timechart count by sourcetype
```



常规设置

为输入指定标签以及变更时搜索行为。本示例启用了变更时搜索。

标记选项

使用标记选项来指定由复选框输入返回的值。

对于标记字段，为返回值的标记指定一个名称。可视化的基本搜索引用了本标记。在本示例中，指定 `src_type_tok`。

使用如下字段，为返回的值构建搜索。当编辑这些字段时，“输入编辑器”中的预览字段会更新。

- 标记前缀
- 标记后缀
- 标记值前缀
- 标记值后缀
- 分隔符

下面表格中列出的示例值构建了如下搜索字符串：

(sourcetype="splunkd" OR sourcetype="splunk_web_access" OR ...)

在动态新建复选框后，可从默认字段选择那些默认启用的复选框。

静态选项

使用静态选项，为输入显式定义复选框的名称和值。

本示例的静态选项留空。它使用一个填充搜索，为输入定义复选框。

动态选项

引用报表或定义一个内联填充搜索，为输入定义复选框。

本示例使用了如下内联搜索：

```
| metadata type=sourcetypes index=_internal
```

该示例对所有时间运行该搜索。

使用字段名称，为复选框指定一个名称/值对。本示例同时为用于标签的字段和用于值的字段指定 sourcetype 字段。

复选框输入的示例值

本表格为复选框输入示例列出了示例值。

编辑器字段	示例值
常规	
标签	Source Types (Check Box)
变更时搜索	已启用
标记选项	
标记	src_type_tok
默认	splunk_web_access splunk_web_service splunkd
标记前缀*	(
标记后缀*)
标记值前缀*	sourcetype="
标记值后缀*	"
分隔符*	OR
动态选项	
内容类型	Inline Search
搜索字符串	metadata type=sourcetypes index=_internal
时间范围	All time
用于标签的字段	sourcetype
用于值的字段	sourcetype

*这些字段构建动态新建复选框的搜索字符串。对于“分隔符”字段，确保指定了开始和结束空格。

下拉输入

本示例使用下拉输入来指示：哪种来源类型显示为时间图表。面板以条形图显示结果，使用的是下列基本搜索。

```
index=_internal sourcetype=$src_type Tok$ | timechart count by sourcetype
```

标记 \$src_type_tok\$ 引用由下拉列表指定的值。



示例使用静态选项，为下拉列表定义选择。

示例为标记前缀指定 splunk。每个选定的值将标记前缀添加为值的前缀。

下拉列表有一个默认值。

该示例用“提交”按钮运行搜索。对选择的更改不会生效，直到您点击“提交”按钮。

编辑器字段	示例值
常规	
标签	Source Types (Dropdown)
变更时搜索	未指定
标记选项	
标记	src_type_tok
默认	Daemon
标记前缀	splunk
静态选项	
名称 : 值	Daemon : d
名称 : 值	Web Service : _web_service
名称 : 值	Web Access : _web_access
名称 : 值	Daemon Access : d_access

链接列表

本示例使用链接列表输入，指示哪种来源类型显示为时间图表。面板以条形图显示结果，使用的是下列基本搜索。这基本上与添加下拉输入的工作流程相同。

```
index=_internal sourcetype=$src_type Tok$ | timechart count by sourcetype
```

标记 \$src_type Tok\$ 引用由链接列表指定的值。例如：



示例使用静态选项，为链接列表定义选择。

示例为标记前缀指定 `splunk`。每个选定的值将标记前缀添加为值的前缀。

链接列表输入有一个默认值。

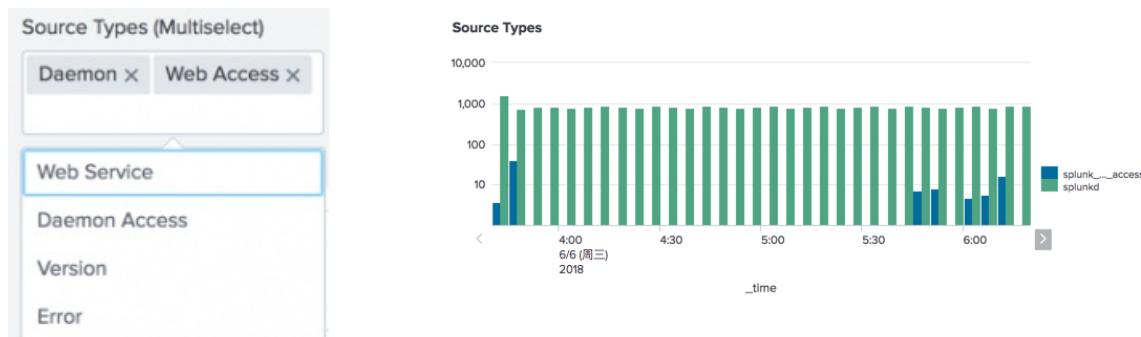
该示例用“提交”按钮运行搜索。对选择的更改不会生效，直到您点击“提交”按钮。

编辑器字段	示例值
常规	
标签	源类型（链接列表）
变更时搜索	未指定
标记选项	
标记	<code>src_type_tok</code>
默认	<code>Daemon</code>
标记前缀	<code>splunk</code>
静态选项	
名称 : 值	<code>Daemon : d</code>
名称 : 值	<code>Web Service : _web_service</code>
名称 : 值	<code>Web Access : _web_access</code>
名称 : 值	<code>Daemon Access : d_access</code>

多选

本示例使用多选输入，指示哪种来源类型显示在时间图表中。面板在默认列图表中显示结果，使用的是下列基本搜索。

```
index=_internal $src_type_tok$ | timechart count by sourcetype
```



示例使用静态选项，为下拉列表定义选择。

默认选择两种来源类型：

```
Daemon  
Web Access
```

本示例启用了**变更时搜索**。选择后，表单即开始加载。

对于一个多选输入，应通过构建如下搜索字符串来定义要选择的多选值。

```
(sourcetype="splunkd" OR sourcetype="splunk_web_access" OR ...)
```

标记 `src_type_tok` 在搜索中引用生成面板内容的这一搜索字符串。构建搜索字符串的字段已在下表中表明。

编辑器字段	示例值
常规	
标签	来源类型（多选）
变更时搜索	已启用

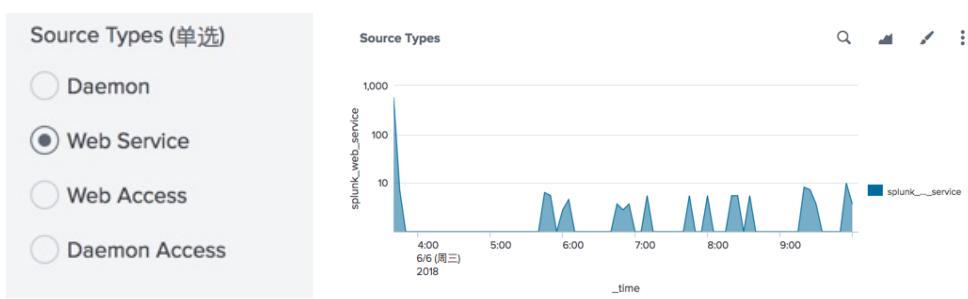
标记选项	
标记	src_type_tok
默认	Daemon Web Access
标记前缀*	(
标记后缀*)
标记值前缀*	sourcetype="
标记值后缀*	"
分隔符*	OR
静态选项	
名称 : 值	Daemon : splunkd
名称 : 值	Web Service : splunk_web_service
名称 : 值	Web Access : splunk_web_access
名称 : 值	Daemon Access : splunkd_access
名称 : 值	Version : splunk_version
名称 : 值	Error : splunkd_stderr

*这些字段构建提供标记值的搜索字符串。对于“分隔符”字段，确保指定了开始和结束空格。

单选输入

本示例使用一个单选输入，指示哪种来源类型显示为时间图表。面板以面积图显示结果，使用了下列基本搜索。

```
index=_internal sourcetype=$src_type Tok$ | timechart count by sourcetype
```



标记 \$src_type Tok\$ 引用由下拉列表指定的值。

示例使用静态选项，为下拉列表定义选择。

单选输入有一个默认值。

本示例启用了变更时搜索。选择后，表单即开始加载。

编辑器字段	示例值
常规	
标签	Source Types (Radio)
变更时搜索	已启用
标记选项	
标记	src_type Tok
默认	Web Service
静态选项	
名称 : 值	Daemon : splunkd

名称 : 值	Web Service : splunk_web_service
名称 : 值	Web Access : splunk_web_access
名称 : 值	Daemon Access : splunkd_access

文本输入

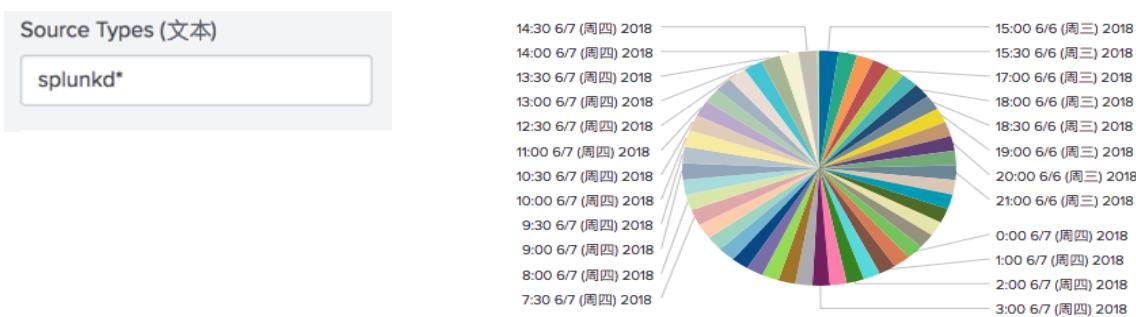
本示例使用文本输入，指示哪种来源类型显示为时间图表。面板以饼图显示结果，使用的是下列基本搜索。

```
index=_internal sourcetype=$src_type_tok$ | timechart count by sourcetype
```

标记 \$src_type_tok\$ 引用在文本输入中指定的值。

本示例指定了一个初始值 splunkd*，没有指定默认值。初始加载开始后，即开始应用种子值。当指定新值时，表单会重新加载。

因为没有默认值，所以空的文本输入不返回任何结果。

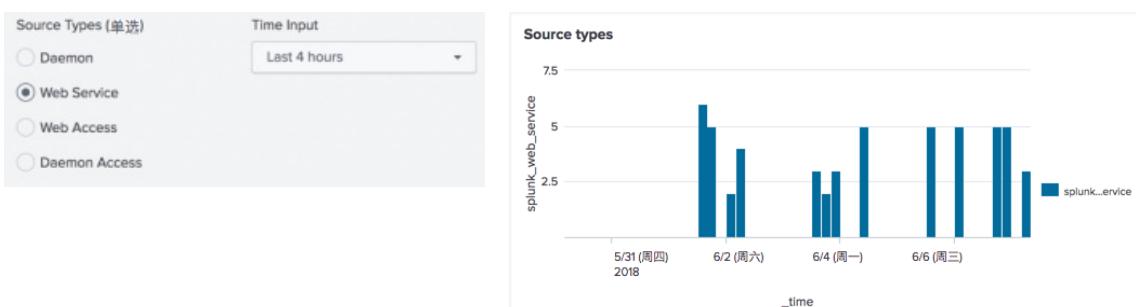


编辑器字段	示例值
常规	
标签	来源类型（文本输入）
变更时搜索	已启用
标记选项	
标记	src_type_tok
默认	未指定
初始	splunkd*

时间输入

本示例显示如何用时间输入，为表单中的面板指定时间范围。该表单包含一个单选输入，指示哪种来源类型显示为时间图表。面板以柱形图显示结果，使用的是下列基本搜索。

```
index=_internal sourcetype=$src_type_tok$ | timechart count by sourcetype
```



示例指定 `time_input_tok`，以在面板中引用时间输入。

在“面板编辑器”中，选择编辑搜索字符串。从时间跨度范围下拉列表选择共享的时间挑选器 (`time_input_tok`)。

时间输入的默认值是过去 4 天。

该示例为时间输入启用了变更时搜索。当选择了新的时间范围时，表单会加载。

编辑器字段	示例值
<u>常规</u>	
标签	Time Input
<u>变更时搜索</u>	已启用
<u>标记选项</u>	
标记	time_input_tok
默认	Last 4 days

用简单 XML 新建仪表板

编辑简单 XML

您可以使用交互式编辑器新建和编辑仪表板，而无需编辑简单 XML 源代码。但是，一些仪表板的高级功能在交互式编辑器中不可用。您可通过编辑底层的简单 XML 代码来访问这些功能。

编辑仪表板源代码

编辑仪表板简单 XML 源代码以便对无法通过用户界面修改的设置进行自定义。仪表板源代码编辑器在您进行修改时会提供交互式验证。

前提条件

如果您不熟悉简单 XML，编辑源代码之前请先查看以下信息。

- “仪表板和表单”中的“仪表板和表单结构和元素”
- “简单 XML 参考”中的“可用选项和元素”

步骤

1. 从仪表板列表页面，打开要编辑的仪表板。
2. 选择编辑打开“仪表板编辑器”。
3. 单击来源打开源代码编辑器。
4. 编辑源代码。
编辑器会提供自动标记闭合和验证。必要时还会显示警告或错误消息。将鼠标悬停在源代码行旁边的警告或错误图标即可查看详细信息。
5. 如果保存按钮已禁用，则修正带验证警告或错误的所有代码。否则，单击保存以保存编辑。

XML 文件中的特殊字符

简单 XML 文件中部分字符有特殊含义。要使源代码分析器不将这些字符处理为特殊字符，在两边为它们加上 `<![CDATA[]]>` 标记。

```
<![CDATA[
<content_with_special_characters>
]]>
```

您也可以使用 HTML 实体转义这些字符。

字符	描述	HTML 实体
'	撇号	'
?	问号	?
'	加号	+
"	引号	"
<	左尖括号	<
>	右尖括号	>
&	& 号	&

仪表板简单 XML 代码的只读权限

将 `showsource` 查询参数附加到仪表板 URL，以访问只读版本的仪表板源代码。请参阅以下示例。

`https://host:port/en-US/app/my_app/my_dashboard?showsource`

注意：只读源代码的访问权限只适用于简单 XML 仪表板。只读的 HTML 或 高级 XML 源代码无法通过 URL 访问。

其他信息

编辑简单 XML 之前，请查看以下资源。

- “仪表板和表单剖析”中的“简单 XML 仪表板和表单结构”。
- “简单 XML 参考”和“图表配置参考”，查看有关简单 XML 元素和选项的详细信息。

Splunk Enterprise 用户可以使用第三方编辑器编辑简单 XML。但 Splunk Cloud 用户不行。请参阅“使用第三方 XML 编辑器”。

搜索驱动仪表板和表单

搜索会在仪表板和表单中生成可视化和其他内容。您还可以使用搜索在仪表板中实施动态行为或交互行为。

了解可用搜索类型和如何在简单 XML 中使用这些类型。

搜索类型和使用方法概述

您可以根据您正在新建的内容或行为在仪表板中使用一个或多个搜索类型。

内联搜索

内联搜索直接存在于仪表板或可视化中。编辑仪表板面板时您可以新建或修改内联搜索。

每个可视化都可以拥有自己内联搜索。您还可以在仪表板中将内联搜索用作基本搜索。基本搜索需要处理后搜索以在仪表板面板中修改结果和生成可视化。

内联搜索以“快速模式”运行，这意味着可能不会提取所有字段。为确保提取所有字段，您可以执行以下操作之一：

- 添加

```
<Your_search> | fields * | ...
```

至你的搜索。

- 添加

```
fieldname=*
```

至你的搜索。

已引用的报表搜索

使用另存为报表的搜索生成仪表板内容。通过引用报表将报表的搜索和可视化添加到仪表板或表单。

您可以编辑仪表板以调整引用的报表中的可视化和时间范围。但是，您无法在仪表板中直接编辑搜索。编辑报表以更改搜索。

更改报表搜索之后，仪表板中已引用的报表搜索会自动更新。

搜索以填充表单输入

您可以使用搜索以动态生成表单输入选择。显示选择用户在表单中看到的标签和值时要使用的结果字段。

后期处理搜索

处理后搜索会对来自基本搜索的结果实施其他处理。您可以使用多个处理后搜索以生成来自相同基本搜索的不同结果。您还可以使用处理后搜索填充表单输入。

预建面板

如果您想要重复使用搜索和其他内容，请新建预建面板。要更改预建面板搜索，请直接编辑预建面板。

预建面板的改变会自动出现在使用面板的仪表板中。

使用“数据透视表”生成的搜索

您可以生成数据透视表以便导出到仪表板。更多信息，请参阅《数据透视表手册》中的“使用‘数据透视表编辑器’设计数据

透视表格”。

在简单 XML 中新建搜索

<search> 元素会在简单 XML 源代码中定义搜索。搜索元素包括子元素，如搜索字符串的 <query> 和时间范围的元素。

您可以使用 <search> 元素定义生成仪表板或表单内容的搜索。您还可以使用 <search> 生成表单输入选择或定义处理后搜索。

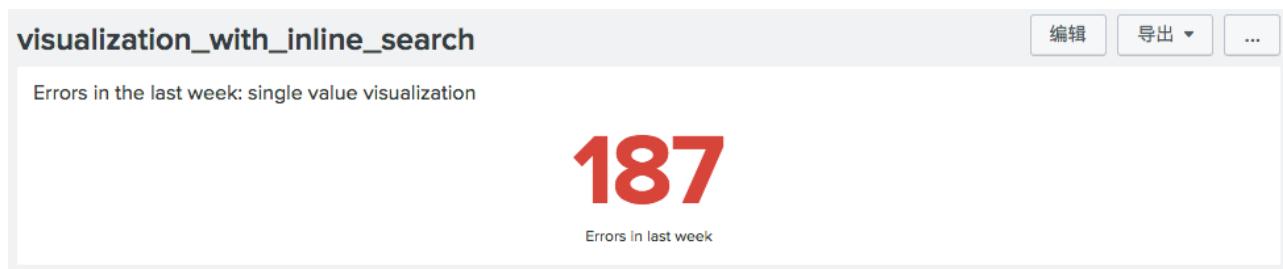
请参阅“[简单 XML 参考](#)”了解有关 <search> 元素、子元素和使用情况要求的更多信息。

示例

内联搜索

使用内联搜索生成可视化数据。

此示例中的搜索会生成单值可视化数据，显示上个星期的系统错误计数。



在此可视化的源代码中，<search> 元素包括这些子元素。

- <query> 包括搜索字符串。
- <earliest> 和 <latest> 定义搜索时间范围。

简单 XML 源代码

```
<panel>
  <single>
    <title>Errors in the last week: single value visualization</title>

    <search>
      <!-- Search string -->
      <query>index=_internal source="*splunkd.log"
        ( log_level=ERROR OR log_level=WARN*
        OR log_level=FATAL OR log_level=CRITICAL )
        | stats count as log_events</query>

      <!-- search time range -->
      <earliest>-7d@h</earliest>
      <latest>now</latest>
    </search>

    <option name="underLabel">Errors in the last week</option>
    <option name="useColors">1</option>
  </single>
</panel>
```

来自报表的引用搜索

使用并修改已引用的保存的搜索以生成仪表板面板内容。

引用来自报表的保存的搜索您可以使用来自报表的初始时间范围和可视化，或您可以在简单 XML 中修改。要更改搜索字符串，请编辑报表。

要在仪表板简单 XML 中使用已保存的搜索，请首先为 `<search>` 元素添加 `ref` 引用属性。引用表示要为仪表板面板添加的报表名称。

示例

以下示例显示您如何在仪表板面板中使用和修改已引用的保存搜索。

- **引用已保存的搜索**

此仪表板面板源代码包括来自报表的保存的搜索。在报表中定义的搜索时间范围和可视化未修改。

```
<panel>
  <title>Referenced saved search</title>
  <chart>
    <title>Sales by product code</title>
    <search ref="saved_search_simple_example">
    </search>
  </chart>
</panel>
```

- **修改搜索时间范围**

此示例将使用 `<earliest>` 和 `<latest>` 调节器更改搜索时间范围。面板搜索使用自定义时间范围。

```
<panel>
  <title>Referenced saved search with custom time range</title>
  <chart>
    <title>Sales by product code in the last week</title>
    <search ref="saved_search_simple_example">
      <earliest>-7d@h</earliest>
      <latest>now</latest>
    </search>
  </chart>
</panel>
```

- **修改可视化类型**

本示例会针对搜索结果使用不同的可视化。

```
<panel>
  <title>Referenced saved search with custom time range and visualization</title>
  <chart>
    <title>Sales by product code in the last week</title>
    <search ref="saved_search_simple_example">
      <earliest>-7d@h</earliest>
      <latest>now</latest>
    </search>
    <option name="charting.chart">bar</option>
  </chart>
</panel>
```

填充表单输入的搜索

使用搜索生成表单输入选择。

您可针对以下表单输入，使用搜索以动态填充选择。

- 复选框
- 下拉菜单
- 多选
- 单选按钮

不要使用实时搜索填充表单输入选项。输入选择不会随着搜索结果更改而更新。

示例

用户可使用表单选择产品类别，以查看该类别的当前销售总计。

Search populated form input

Select a Product category

ACCESSORIES [隐藏过滤器](#)

ARCADE

SHOOTER

SIMULATION

SPORTS

STRATEGY

TEE

Count for ACCESSORIES

\$6,429

在此简单 XML 源代码中，输入包括用于搜索的、可生成输入选项的 `<search>` 元素。`fieldForLabel` 和 `fieldForValue` 元素显示结果字段以用于选择标签和值。

静态 `<initialValue>` 表示在用户做出选择前要使用的初始选择值。

用户选择类别之后，输入会捕获 `category` 标记中的所选值。此表单中单值可视化可使用标记进行动态更新。面板搜索中包括标记值，以针对所选类别生成结果。标记值也会出现在面板标题中。

```

<form>
  <label>Search populated form input</label>
  <fieldset autoRun="true" submitButton="false">
    <input type="radio" token="category" searchWhenChanged="true">
      <label>Select a Product category</label>
      <default>ACCESSORIES</default>
      <search>
        <query>source="tutorial*" NOT null | stats count by categoryId</query>
        <earliest>-7d@h</earliest>
        <latest>now</latest>
      </search>
      <fieldForLabel>categoryId</fieldForLabel>
      <fieldForValue>categoryId</fieldForValue>
      <initialValue>ACCESSORIES</initialValue>
    </input>
  </fieldset>
  <row>
    <panel>
      <single>
        <title>Count for $category$</title>
        <search>
          <query>source="tutorial*" categoryId=$category$ | stats count</query>
        </search>
        <option name="rangeValues">[0,300,700,1000]</option>
        <option name="unit">$</option>
        <option name="unitPosition">before</option>
        <option name="useColors">1</option>
      </single>
    </panel>
  </row>
</form>

```

使用标记将动态值添加到搜索

标记是动态数据的引用，如搜索结果计数或用户指定值。使用搜索中的标记访问动态值并生成更多自定义结果。

要使用搜索中的标记，请在标记名称周围使用 `$...$` 分隔符。搜索运行时，标记引用的动态值将替换 `$<token_name>$`。

示例

此搜索字符串中包括 `$series_tok$` 标记以代表动态 `series` 字段值。此值可能来自于表单输入中的一个用户选择。

```
index=_internal source=*metrics.log group="per_sourcetype_thruput" series=$series_tok$ | table sourcetype eps, kb, kbps
```

搜索可以生成代表用户已选的 `$series_tok$` 值的可视化。

除了搜索，标记也可以用于捕获用户输入值并控制动态仪表板行为。请参阅“[仪表板中的标记用法](#)”了解详细信息。

后期处理搜索

处理后搜索会对来自基本搜索的结果实施其他处理。基本搜索可以是全局搜索或仪表板内的任何其他搜索。在处理后 `<search>` 中使用 `base` 属性来表示基本搜索 ID。

您可以使用单个处理后搜索生成结果或您可以将多个处理后搜索链接起来。

最佳实践

使用这些最佳实践以确保处理后搜索按预期运行。

使用转换基本搜索

基本搜索应该是一种转换搜索，以统计表的形式返回搜索结果。

非转换基本搜索可能产生以下搜索结果并导致超时问题。如果您观察仪表板中的这些问题，请检查基本搜索以确保它是转换搜索。

无返回结果

如果基本搜索是非转换搜索，您必须在基本搜索中明确说明使用 `| fields` 命令时基本搜索中会在后处理搜索中用到什么字段。例如：如果您的后处理搜索将搜索一段时间内畅销 buttercup game 类别，您将使用类似以下内容的搜索命令。

```
| fields _time, categoryId, action
```

事件保存

如果基本搜索是一个非转换搜索，则 Splunk 平台仅保留其返回的前 500,000 个事件。处理后搜索不会处理超出此 500,000 个事件限值的事件，以静默方式忽略这些事件。这会生成不完整的处理后搜索数据。

此搜索结果保存限制匹配 `limits.conf` 中的 `max_count` 设置。设置默认为 500,000。

客户端超时

如果处理后操作花费时间过长，可能会超出 Splunk Web 客户端超时值 30 秒。

collect

当用于基本搜索时，`collect` 命令不适用于后期处理搜索。使用内联搜索而非基本搜索以使用 `collect` 命令。

有关转换搜索的更多信息，请参阅《[搜索手册](#)》中的转换命令和搜索。

不要引用未在基本搜索中引用的后处理搜索中的字段

后处理搜索完全取决于基本搜索中出现的字段。如果您没有在基本搜索中引用特定字段，那么也不要在处理后搜索中引用。转换命令中使用的字段在后处理搜索中自动可用。转换命令不在基本搜索中使用时，基本搜索中没有引用的字段在后处理搜索中显示为空。在此情形下，处理后搜索不返回结果。

限制基本搜索结果和处理后复杂性

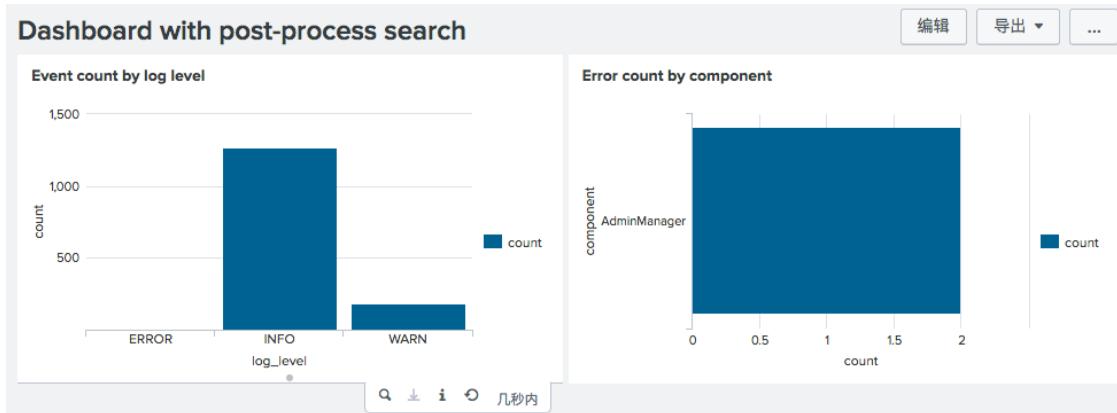
将大量搜索结果传递到处理后搜索会导致服务器超时问题。在此情景中，考虑调整基本搜索以减少该搜索返回的结果和字段数。您还可以考虑减少基本搜索结果的处理后操作的复杂度。

示例

以下示例显示如何使用基本搜索和处理后搜索。

基本处理后搜索

此示例中的基本搜索使用的是 `<stats>` 转换命令。两个处理后搜索以不同的方式使用基本搜索结果。



基本搜索

```
index=_internal source=*splunkd.log | stats count by component, log_level
```

首个处理后搜索

```
| stats sum(count) AS count by log_level
```

第二个处理后搜索

```
| search log_level=error | stats sum(count) AS count by component
```

仪表板源代码

```
<dashboard>
  <label>Dashboard with post-process search</label>

  <!-- Example uses stats transforming command -->
  <!-- This limits events passed to post-process search -->
  <search id="baseSearch">
    <query>
      index=_internal source=*splunkd.log | stats count by component, log_level
    </query>
  </search>

  <row>
    <panel>
      <chart>
        <title>Event count by log level</title>

        <!-- post-process search -->
        <search base="baseSearch">
          <query>
            stats sum(count) AS count by log_level
          </query>
        </search>

      </chart>
    </panel>
    <panel>
      <chart>
        <title>Error count by component</title>

        <!-- post-process search -->
        <search base="baseSearch">
          <query>
            search log_level=error | stats sum(count) AS count by component
          </query>
        </search>
      </chart>
    </panel>
  </row>
</dashboard>
```

```

</search>

<option name="charting.chart">bar</option>
</chart>
</panel>
</row>
</dashboard>

```

链接的处理后搜索

将两个或多个后期处理搜索一并链接。首先进行基本搜索和处理后搜索。将第一个处理后搜索用作另一个处理后搜索的基本搜索。

仪表板源代码

```

<search id="baseSearch">
    <query>index=_internal</query>
    <earliest>-60m@m</earliest>
    <latest>now</latest>
</search>

<search base="baseSearch" id="post_process_1">
    <query>sourcetype=splunkd</query>
</search>

<search base="post_process_1" id="post_process_2">
    <query>stats count</query>
</search>

```

复杂的处理后搜索

新建包括统计聚合（如百分位或标准偏差）的复杂基本搜索时，请使用摘要索引命令。

像以下命令这样的摘要索引命令为处理后搜索提供了更多灵活性。

- sistats
- sitimechart
- sitop
- sichart
- sirare

有关摘要索引的更多信息，请参阅《报表手册》中的“使用摘要索引提高报表效率”和“关于转换命令和搜索”。

示例

此示例包括使用 `sistats` 摘要索引的命令的基本搜索。

基本搜索按 `_internal` 索引的来源和来源类型报告事件大小（最小、平均、最大）。将 `sistats` 计数与不同的 `group-by` 子句结合使用。如果不包含这些，则您将失去分布式搜索中的映射减少所带来的益处。

基本搜索

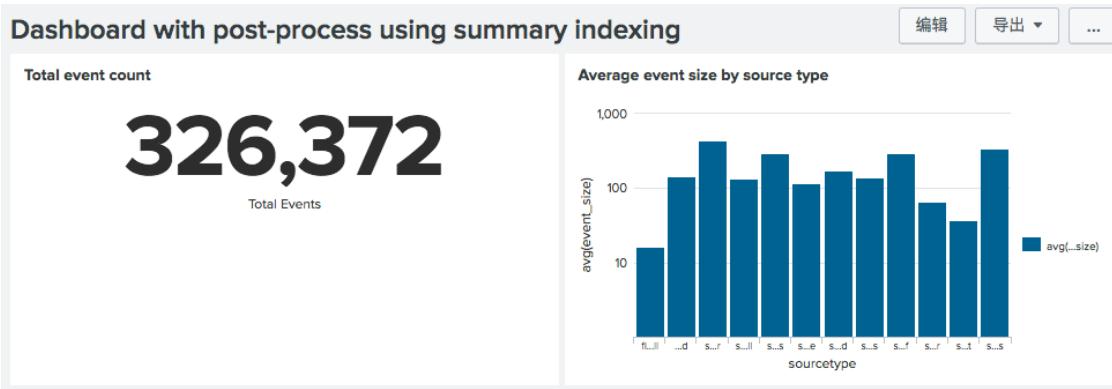
```
index=_internal | eval event_size=len(_raw) <br />| sistats count min(event_size) avg(event_size) max(event_size)<br />by source sourcetype
```

后期处理 1

```
| stats count
```

后期处理 2

```
| stats avg(event_size) by sourcetype
```



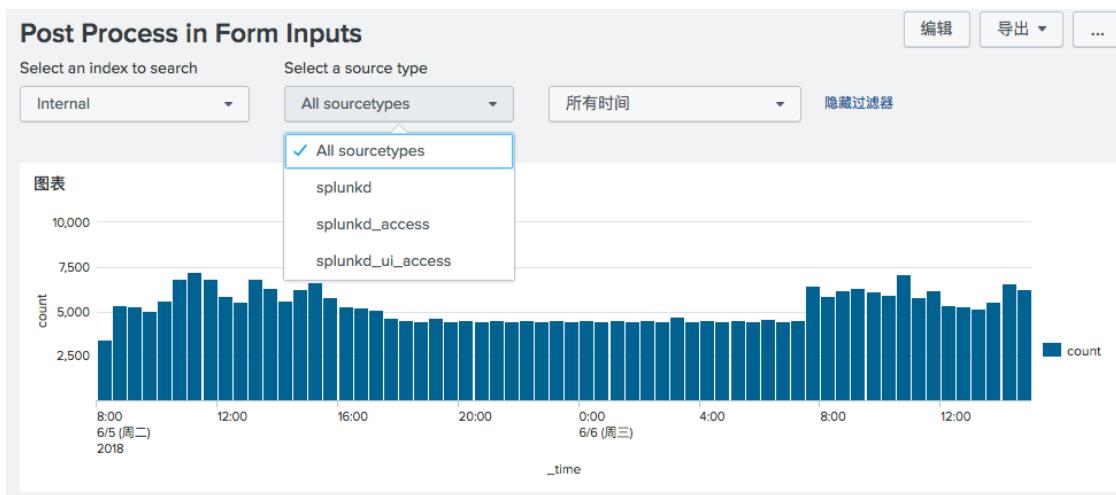
仪表板源代码

```
<dashboard>
  <label>Dashboard with post-process using summary indexing</label>
  <!-- Base search with summary indexing transforming command -->
  <search id="baseSearch">
    <query>
      index=_internal | eval event_size=len(_raw)
      | sstats count min(event_size) avg(event_size) max(event_size)
      by source sourcetype
    </query>
  </search>
  <row>
    <panel>
      <single>
        <title>Total event count</title>
        <search base="baseSearch">
          <query>stats count</query>
        </search>
        <!-- post-process search -->
        <option name="rangeColors">["0x53a051","0x0877a6","0xf8be34","0xf1813f","0xdc4e41"]</option>
        <option name="underLabel">Total Events</option>
      </single>
    </panel>
    <panel>
      <chart>
        <title>Average event size by source type</title>
        <search base="baseSearch">
          <query>stats avg(event_size) by sourcetype</query>
        </search>
        <!-- post-process search -->
        <option name="charting.axisY.scale">log</option>
      </chart>
    </panel>
  </row>
</dashboard>
```

使用处理后搜索填充表单输入

使用处理后搜索填充表单输入

用户可使用此表单中的第一个输入选择要搜索的索引。此输入静态定义选项。第二次输入使用处理后搜索动态定义选项。



基本搜索

```
index=_internal | stats count by sourcetype
```

处理后生成输入选项

```
| search sourcetype=splunkd*
```

表单源代码

```
<form>
  <label>Post Process in Form Inputs</label>

  <!-- Global search for post process by dropdown input -->
  <search id="searchInput">
    <query>index=_internal | stats count by sourcetype</query>
    <earliest>-60min</earliest>
    <latest>now</latest>
  </search>

  <fieldset submitButton="false">

    <!-- Input with statically defined choices -->
    <input type="dropdown" token="index_tok" searchWhenChanged="true">
      <label>Select an index to search</label>
      <choice value="_internal">Internal</choice>
      <choice value="*"/>All public indexes</choice>
      <default>_internal</default>
    </input>

    <!-- Input with dynamically populated choices -->
    <input type="dropdown" token="sourcetype_tok" searchWhenChanged="true">
      <label>Select a source type</label>

      <!-- Default choice defined statically -->
      <choice value="*"/>All sourcetypes</choice>
      <default>*</default>

      <!-- Post-process search to populate additional choices -->
      <search base="searchInput">
        <query>search sourcetype=splunkd*</query>
      </search>
      <fieldForLabel>sourcetype</fieldForLabel>
      <fieldForValue>sourcetype</fieldForValue>

    </input>
    <input type="time" token="time_tok" searchWhenChanged="true">
      <label></label>
```

```

<default>
  <earliest>-24h@h</earliest>
  <latest>now</latest>
</default>
</input>
</fieldset>
<row>
  <panel>
    <chart>
      <title>Chart</title>
      <search>
        <query>
          index=$index_tk$ sourcetype=$sourcetype_tk$ | timechart count
        </query>
        <earliest>$time_tk.earliest$</earliest>
        <latest>$time_tk.latest$</latest>
      </search>
    </chart>
  </panel>
</row>
</form>

```

面板搜索控制

单击仪表板面板上的刷新和停止按钮以生成新的搜索结果或停止运行搜索任务。在搜索正在运行时，面板中的停止按钮替代刷新按钮。可视化呈现来自已停止的搜索任务的可用结果，时间戳则显示最近任务的时间。

停止搜索按钮默认可见。您可以使用仪表板源代码中的 `link.stopSearch.visible` 简单 XML 选项隐藏此按钮。请参阅“简单 XML 引用”以了解更多详细信息。

停止处理后搜索

停止后期处理搜索导致该后期处理搜索的基本搜索在任何其使用的位置停止。如果同一基本搜索用于多个面板，搜索也将在那些面板中停止。

搜索头群集中已引用的实时搜索的故障排除

在搜索头群集化 (SHC) 部署中，如果您正在搜索头上引用仪表板中的保存的实时搜索，实时搜索在返回初始结果之后可能不会继续流出数据。

此问题有两个解决方法。

选项	示例仪表板源代码	性能注意事项
改在仪表板面板中使用内联实时搜索。	<pre> <search> <query>index=_internal stats count </query> <earliest>rt-5m</earliest> <latest>rtnow</latest> </search> </pre>	此搜索类型只在用户查看仪表板时运行。但是，对于通过搜索头或其他成员访问仪表板的每个用户，会衍生出新的实时搜索。
新建已保存的计划搜索。 在内联面板搜索中使用 <code>loadjob</code> 命令，以使用保存的搜索结果更新仪表板。	<pre> <search> <query> loadjob savedsearch="admin:search:SavedSearch" </query> </search> </pre>	只有一个已保存的搜索实例在计划时间运行（不考虑访问仪表板的用户数量）。

其他搜索资源

如果您之前未使用过 Splunk 平台和搜索处理语言 (SPL)，可以从[搜索教程](#)开始。此教程将介绍“搜索和报表”应用程序。教程将通过添加数据至 Splunk 部署、搜索数据以及建立简单报表和仪表板进行逐步指导。

《[搜索手册](#)》包含关于新建和优化搜索、检索事件、指定时间范围和使用子搜索的详细信息。

[搜索参考](#)是“搜索处理语言”(SPL) 的参考指导。[搜索参考](#)包含带有语法、描述和各示例的搜索命令目录。

仪表板和表单

使用仪表板和表单来可视化、组织和共享数据见解。

仪表板和表单有一行或多行面板。每个面板都包含可视化，如图表、表格或地图。在每个面板中，搜索可生成可视化的数据。

表单与仪表板不同，因为表单包括供用户互动的 `<input>` 元素，如文本框或单选按钮。您可以通过自定义驱动可视化的搜索或更改其他行为，在表单中配置元素（如面板）以响应用户输入。

有关建立 `<dashboard>` 或 `<form>` 的详细信息，请参阅“简单 XML 参考”。

仪表板和表单剖析

请参阅“简单 XML 参考”了解有关仪表板和表单元素层次结构的完整信息。

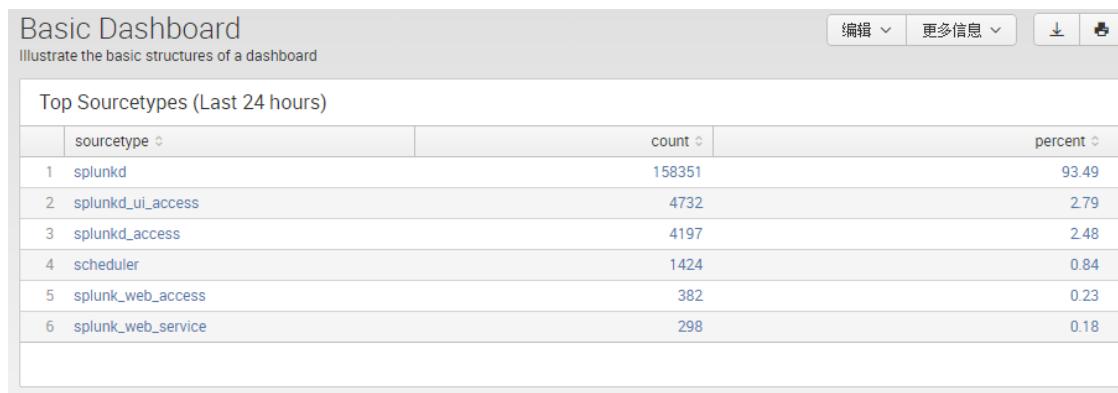
元素	描述
顶级元素	<code><dashboard></code> 或 <code><form></code>
标题	<code><label></code> （可选）
描述	<code><description></code> （可选）
全局搜索	全局搜索用于与后期处理搜索结合使用。后期处理搜索有限制。请参阅“处理后限制”。 <code><search id="[identifier]"></code>
表单输入（仅用于表单）	<code><fieldset></code> <code><input></code> <code><text></code> <code><checkbox></code> <code><dropdown></code> <code><multiselect></code> <code><radio></code> <code><search></code> （用于填充输入选择）
行	每行包含一个或多个面板。 <code><row></code>
面板	每个面板包含一个可选标题、可选输入和一个或多个可视化。有关可用面板的类型，请参阅“仪表板面板”。 <code><panel></code>
可视化	可视化显示从搜索返回的数据。 <code><chart></code> <code><event></code> <code><map></code> <code><single></code> <code><table></code>
搜索	可视化的搜索。 <code><search id="[identifier]"></code> 后期处理搜索的基本搜索。 <code><search base="[id]"></code> 后期处理搜索引用基本搜索。 <code><search ref="[report] [app="[app name]"]></code> 从报表引用搜索。应用的引用为可选。
选项	特定于可视化的属性： <code><option name="[option name]"></code>

仪表板示例

本主题显示了仪表板后面的源简单 XML 代码。在熟悉简单 XML 源代码后，您可以进一步自定义仪表板。

基本仪表板

此实例使用一些简单的 XML 元素新建基本的仪表板。



```
<dashboard>
  <!-- A title for the dashboard -->
  <label>Basic Dashboard</label>

  <!-- Provide a description -->
  <description>Illustrate the basic structures of a dashboard</description>

  <!-- Place panels within rows -->
  <row>

    <!-- This basic dashboard has only a single panel -->
    <panel>

      <table>
        <title>Top Sourcetypes (Last 24 hours)</title>

        <!-- A search powers the panel -->
        <search>
          <query>
            index=_internal | top limit=100 sourcetype | eval percent = round(percent,2)
          </query>
          <!-- Specify a time range for the search -->
          <earliest>-24h@h</earliest>
          <latest>now</latest>
        </search>

        <!-- Use options to further define how to display result data -->
        <option name="wrap">true</option>
        <option name="rowNumbers">true</option>
      </table>
    </panel>
  </row>

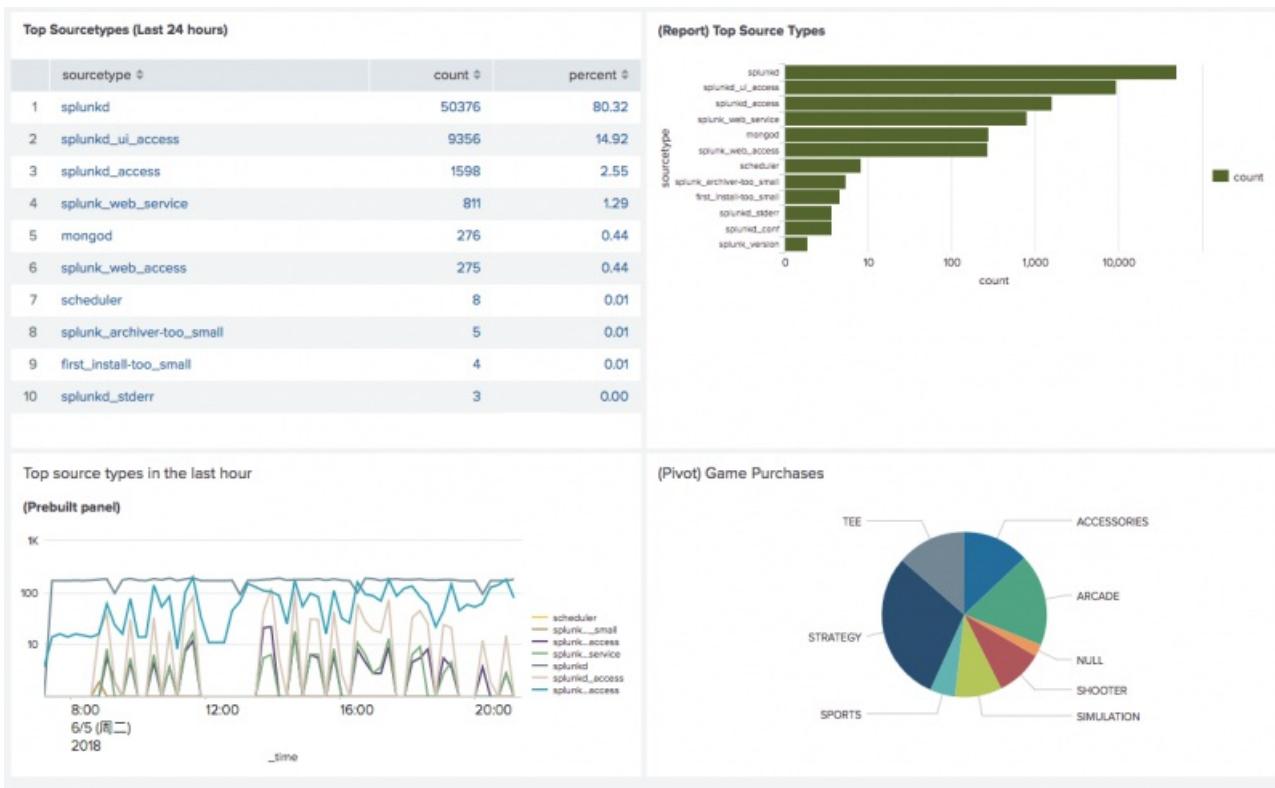
</dashboard>
```

搜索驱动面板

此仪表板说明了以下搜索：

- 内联搜索
- 另存为报表的搜索
- 来自预建面板的搜索

- 源自数据透视表的内联搜索



```

<dashboard>
<label>Searches power dashboards</label>
<description>Show the various searches to power a panel.</description>
<!-- This row contains three panels -->
<row>
  <panel>
    <table>
      <title>(Inline Search) Top Source Types</title>
      <!-- Inline Search -->
      <search>
        <query>
          index=_internal | top limit=100 sourcetype
          | eval percent = round(percent,2)
        </query>
        <earliest>-24h@h</earliest>
        <latest>now</latest>
      </search>
      <option name="rowNumbers">true</option>
    </table>
  </panel>
  <panel>
    <chart>
      <title>(Report) Top Source Types</title>
      <!-- Reference to a search saved as a report -->
      <search ref="Top Source Types Report" />
    </chart>
  </panel>
</row>
<row>
  <panel ref="top_source_types_in_the_last_hour" app="search" />

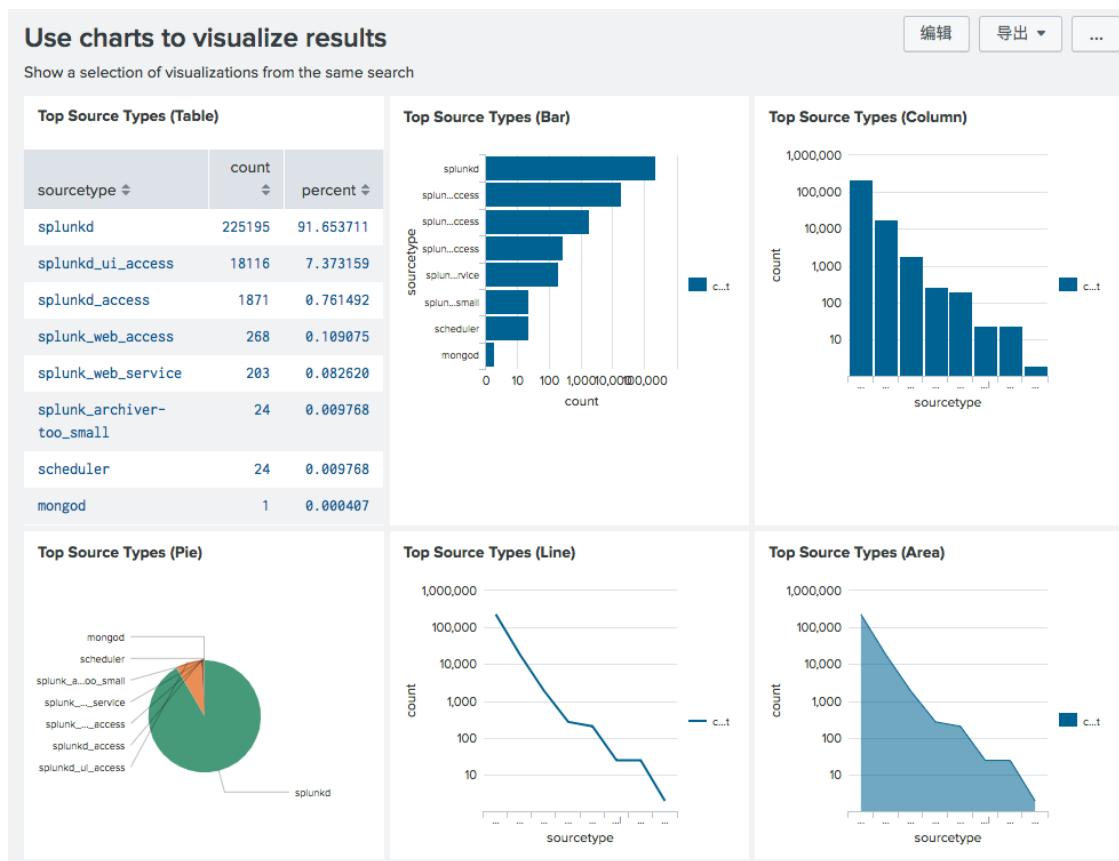
  <panel>
    <chart>
      <title>(Pivot) Game Purchases</title>

```

```
<!-- Inline search derived from a pivot -->
<search>
  <query>
    | pivot Buttercup_Games Successful_purchases count(Successful_purchases)
      AS "Count of Successful purchases" SPLITROW product_name
      AS "product name" SORT 100 product_name
  </query>
</search>
<option name="charting.chart">pie</option>
</chart>
</panel>
</row>
</dashboard>
```

使用面板可视化搜索结果

您可以在表格或事件列表中显示搜索结果，但也可以指定各种图表。使用 `<chart>` 元素，通过 `<option>` 子元素指定图表类型。



```
<dashboard>
  <label>Use charts to visualize results</label>
  <description>Show a selection of visualizations from the same search</description>
  <row>
    <panel>
      <!-- Display results as a table. Uses an          -->
      <!-- inline search, equivalent to the <searchName> -->
      <!-- specified for the other panels           -->
      <table>
        <title>Top Source Types (Table)</title>
        <search>
          <query>
            index=_internal | top limit=10 sourcetype
          </query>
          <earliest>-24h</earliest>
          <latest>now</latest>
```

```

        </search>
    </table>
</panel>
<panel>
    <!-- display same search as various charts -->
    <chart>
        <title>Top Source Types (Bar)</title>
        <search>
            <query>
                index=_internal | top limit=10 sourcetype
            </query>
            <earliest>-24h</earliest>
            <latest>now</latest>
        </search>
        <!-- specify the chart type with this <option> to <chart> -->
        <option name="charting.chart">bar</option>
        <option name="charting.axisY.scale">log</option>
    </chart>
</panel>
<panel>
    <chart>
        <title>Top Source Types (Column)</title>
        <search>
            <query>
                index=_internal | top limit=10 sourcetype
            </query>
            <earliest>-24h</earliest>
            <latest>now</latest>
        </search>
        <option name="charting.chart">column</option>
        <option name="charting.axisY.scale">log</option>
    </chart>
</panel>
</row>
<row>
<panel>
    <chart>
        <title>Top Source Types (Pie)</title>
        <search>
            <query>
                index=_internal | top limit=10 sourcetype
            </query>
            <earliest>-24h</earliest>
            <latest>now</latest>
        </search>
        <option name="charting.chart">pie</option>
    </chart>
</panel>
<panel>
    <chart>
        <title>Top Source Types (Line)</title>
        <search>
            <query>
                index=_internal | top limit=10 sourcetype
            </query>
            <earliest>-24h</earliest>
            <latest>now</latest>
        </search>
        <option name="charting.chart">line</option>
        <option name="charting.axisY.scale">log</option>
    </chart>
</panel>
<panel>
    <chart>
        <title>Top Source Types (Area)</title>
        <search>
            <query>
                index=_internal | top limit=10 sourcetype
            </query>

```

```

<earliest>-24h</earliest>
<latest>now</latest>
</search>
<option name="charting.chart">area</option>
<option name="charting.axisY.scale">log</option>
</chart>
</panel>
</row>
</dashboard>

```

带实时搜索的仪表板

您可以使用 Splunk 仪表板编辑器构建实时仪表板，或使用简单 XML 编码仪表板。本示例显示了如何编码简单 XML。

要启用实时搜索，使用 `<search>` 元素的 `<earliest>` 和 `<latest>` 子元素。例如，如果您要启用实时搜索并在表格中显示数据，请指定以下内容：

```





```

您还可以为实时仪表板设置窗口。例如，如果您需要只显示最近 5 分钟内的实时事件。

```





```

有关设置搜索窗口的更多信息，请参阅《搜索手册》中的“在您的搜索中指定实时时间范围窗口”。

为图表中的字段指定自定义颜色

使用 `charting.fieldColors` 简单 XML 属性以自定义图表中的字段颜色。您选择的颜色在每次图表显示时都一样，不管仪表板中其他图表或颜色规范如何。

有关此属性的详情信息，请参阅“图表配置参考”中的 `charting.fieldColors`。

示例

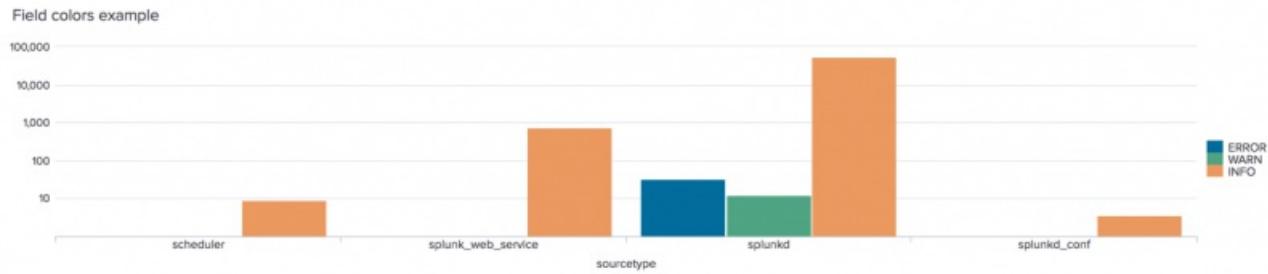
以下示例显示如何根据来源类型为显示错误计数的图表指定颜色。该示例使用此搜索。

```

index = _internal log_level=* | stats count(eval(log_level="ERROR")) as ERROR count(eval(log_level="WARN")) as WARN
count(eval(log_level="INFO")) as INFO by sourcetype

```

如果没有 `charting.fieldColors`，可视化将基于数值的返回顺序使用默认字段颜色映射。此处 `ERROR` 显示为蓝色。

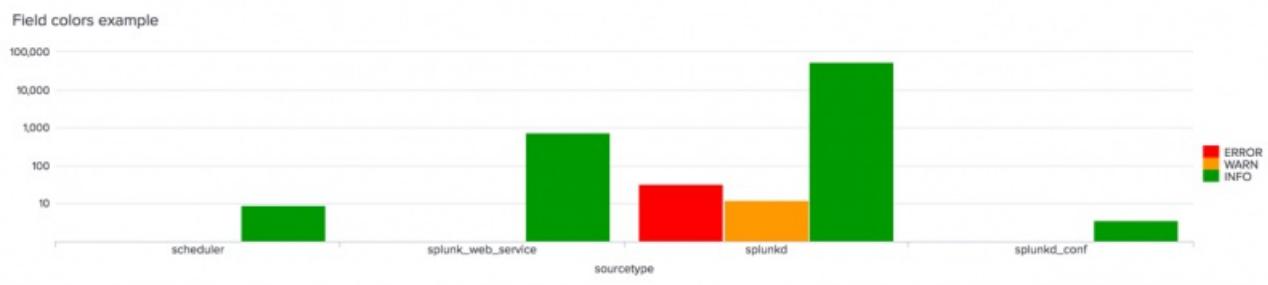


要更改字段颜色映射，请添加 `charting.fieldColors` 属性至仪表板的简单 XML 源代码。例如，如下 `charting.fieldColors` 配置为每个日志级别定义这些颜色。

- INFO: 绿色
- WARN: 橙色
- ERROR: 红色

```
<option name="charting.fieldColors">
  {"ERROR": 0xFF0000, "WARN": 0xFFFF00, "INFO":0x009900, "NULL":0xC4C4C0}
</option>
```

添加 `charting.fieldColors` 之后，图表看起来就像现在这个样子。



下面的代码实现了带自定义字段颜色的类似图表。

```
<panel>
  <html>
    Use <tt>eval</tt> function in the search to transpose
    the value of the log_level field into individual fields
    for <tt>charting.fieldcolors</tt>.
  </html>
  <chart>
    <title>Field colors example</title>
    <search>
      <query>
        index = _internal log_level=* | stats
        count(eval(log_level=="ERROR")) as ERROR
        count(eval(log_level=="WARN")) as WARN
        count(eval(log_level=="INFO")) as INFO
        by sourcetype
      </query>
      <earliest>-7d@h</earliest>
      <latest>now</latest>
    </search>
    <option name="charting.axisY.scale">log</option>
    <option name="charting.chart">column</option>
    <option name="charting.fieldColors">
      {"ERROR": 0xFF0000, "WARN": 0xFFFF00, "INFO":0x009900, "NULL":0xC4C4C0}
    </option>
    <option name="charting.legend.placement">right</option>
  </chart>
```

```
</panel>
```

为可视化指定属性

简单 XML 提供了一组简单 XML 元素，以定义可应用于所有可视化的属性。对于特定于某些可视化类型的属性（例如，`<chart>` 或 `<map>`），请使用 `<option>` 元素指定属性。

使用特定元素或 `<option>` 元素不同。有关指定面板属性的详细信息，请参阅“简单 XML 参考”和“图表配置参考”。

下表汇总了所有可视化可用的一些元素。

标记	描述
<code><title></code>	字符串 为您的面板添加标题，如失败的登录。此标题显示在面板顶部。
<code><earliest></code> <code><latest></code>	Splunk 时间格式 将您的搜索结果限制在特定时间窗口内，从最早时间开始并以最晚时间结束。指定“rt”以启用实时搜索。

以下带 `<chart>` 元素的面板示例显示了如何指定一个标题和一个内联搜索。它限制搜索结果在 5 小时窗口和三个字段：

```
<dashboard>
  <label>My dashboard</label>
  <row>
    <panel>

      <table>
        <title>Top users, five hours ago</title>
        <search>
          <query>
            host=production | top users
          </query>
          <earliest>-10h</earliest>
          <latest>-5h</latest>
        </search>
        <fields>host,ip,username</fields>
      </table>

    </panel>
  </row>
</dashboard>
```

下例使用 `<option>` 元素为 `<table>` 指定了各种属性。

```
<dashboard>
  <label>My dashboard</label>
  <row>
    <panel>

      <table>
        <title>Errors in the last 24 hours</title>
        <search>
          <query>
            Errors in the last 24 hours
          </query>
        </search>
        <option name="count">15</option>
        <option name="displayRowNumbers">true</option>
        <option name="maxLines">10</option>
        <option name="segmentation">outer</option>
      </table>

    </panel>
  </row>
</dashboard>
```

```

<option name="softWrap">true</option>
</table>

</panel>
</row>
</dashboard>

```

以下示例指定了柱形图可视化，以及 X 轴和 Y 轴的显示名称。

```

<dashboard>
  <label>My dashboard</label>
  <row>
    <panel>
      <chart>
        <search>
          <query>
            sourcetype=access_* method=GET | timechart count by categoryId
            | fields _time BOUQUETS FLOWERS
          </query>
          <earliest>-7d</earliest>
          <latest>now</latest>
        </search>
        <title>Views by product category, past week (Stacked)</title>
        <option name="charting.axisTitleX.text">Views</option>
        <option name="charting.axisTitleY.text">Date</option>
        <option name="charting.chart">column</option>
      </chart>
    </panel>
  </row>
</dashboard>

```

使用 HTML 面板显示静态文本

HTML 面板显示内联 HTML。使用 HTML 面板添加文档、链接、图像和其他 Web 内容到仪表板。

HTML 标记间的内容会根据指定的 HTML 格式进行显示。相对链接引用均相对于当前视图位置。HTML 面板不使用任何其他常规面板选项，也没有需要为 HTML 设置的任何特定选项。

有关使用 HTML 面板的详细信息，请参考“简单 XML 参考”中的 `<html>` 元素条目。

Illustrate HTML panel

Show usage of an HTML panel to display static text.

This is an **HTML panel** providing links to system reports.

- Errors in the last 24 hours
- Errors in the last hour
- Indexing workload
- License Usage

(Report) Top Source Types

sourcetype	count	percent
splunkd	55149	78.21
splunkd_ui_access	11966	16.97
splunkd_access	1924	2.73
splunk_web_service	854	1.21
splunk_web_access	323	0.46
mongod	276	0.39
scheduler	9	0.01
splunk_archiver-too_small	6	0.01
first_install-too_small	4	0.01
splunkd_stderr	3	0.00

在示例中，锚点标记使用特别 Splunk 定位符访问系统报表： @go?s=

```

...
<row>
  <panel>
    <html>

```

```

<p>This is an <i><b>HTML panel</b></i> providing links to system reports.</p>
<ul>
  <li>
    <p><a href="@go?s=Errors in the last 24 hours">Errors in the last 24 hours</a></p>
  </li>
  <li>
    <p><a href="@go?s=Errors in the last hour">Errors in the last hour</a></p>
  </li>
  <li>
    <p><a href="@go?s=Indexing workload">Indexing workload</a></p>
  </li>
  <li>
    <p><a href="@go?s=License Usage Data Cube">License Usage</a></p>
  </li>
</ul>
</html>
</panel>
. . .
</row>

```

配置钻取

使用钻取链接到搜索、另一个仪表板或外部网站。您还可以使用钻取触发同一个仪表板中的上下文变化。

请参阅“将钻取用于仪表板交互”以了解更多信息。

表单示例

表单与仪表板类似，但它为用户提供界面，以便为一个或多个搜索术语提供值，其中通常会使用文本框、下拉菜单或单选按钮等。表单会向用户屏蔽基本搜索的具体细节 - 它允许用户只专注于他们正在寻找的词语和结果。结果可显示在表格、事件列表，或任何仪表板提供的可视化中。

本主题包括介绍如何新建表单的基本示例。有关使用更加强大的来源数据的其他示例，请参阅 Splunk 仪表板示例应用。此示例显示如何使用标记传入表单中的值。有关标记实现的详细信息，请参阅“仪表板中的标记用法”。

基本表单示例

表单的用户输入定义输入的选择值的标记。表单中的搜索使用标记以指定要在搜索中使用的值。搜索使用 "\$...." 作为标记值的分隔符来访问该标记值。

例如，以下代码段定义使用 `sourcetype_tok` 标记代表用户选择的下拉选项。它还定义下拉的选项。

```

<input type="dropdown" token="sourcetype_tok">
  <label>Select a source type</label>
  <default>splunkd</default>
  <choice value="splunkd">splunkd</choice>
  <choice value="splunk_web_access">splunk_web_access</choice>
  <choice value="splunkd_ui_access">splunkd_ui_access</choice>
</input>

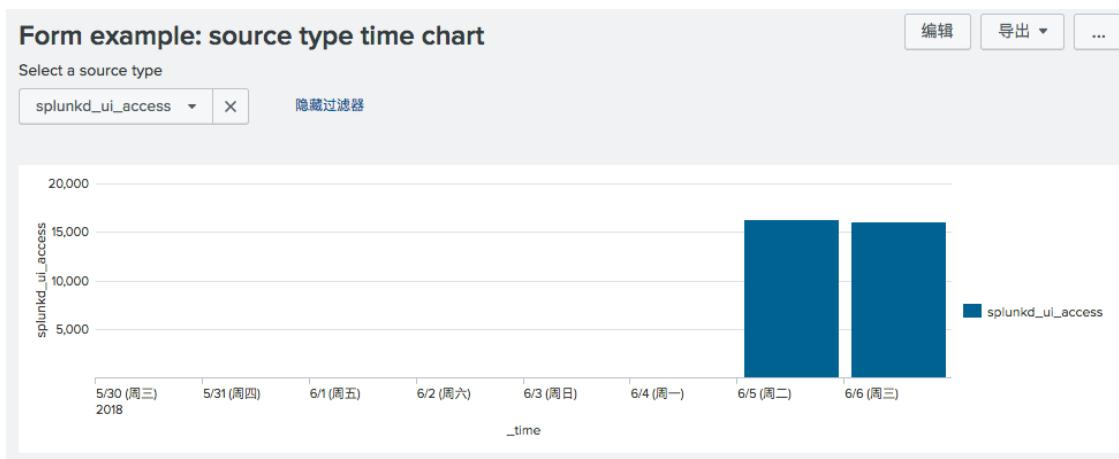
```

表单中的搜索引用该标记。在以下代码段中，`$sourcetype_tok$` 代表来自下拉选项的值。

```

<search>
  <query>
    index = _internal sourcetype=$sourcetype_tok$
    | timechart count by sourcetype
  </query>
  <earliest>-7d</earliest>
  <latest>-0d</latest>
</search>

```



以下是实现此表单的简单 XML。

```

<form>
  <label>Form example: source type time chart</label>

  <!--autoRun means the search runs as soon as it is loaded. -->
  <!-- Do not need a submit button -->
  <fieldset autoRun="true" submitButton="false">
    <input type="dropdown" token="sourcetype_tok">
      <label>Select a source type</label>
      <default>splunkd</default>
      <choice value="splunkd">splunkd</choice>
      <choice value="splunk_web_access">splunk_web_access</choice>
      <choice value="splunkd_ui_access">splunkd_ui_access</choice>
    </input>
  </fieldset>

  <row>
    <panel>
      <chart>
        <search>
          <query>
            index = _internal sourcetype=$sourcetype_tok$
            | timechart count by sourcetype
          </query>
          <earliest>-7d</earliest>
          <latest>-0d</latest>
        </search>
      </chart>
    </panel>
  </row>
</form>

```

具有时间输入示例的表单

您可向表单添加一个或多个时间输入。如果您添加单个时间输入，则时间输入的标记没有必要。时间输入驱动表单中所有搜索的数据。

但是，如果您向表单添加其他时间输入，则指定每个时间输入的标记。表单中的搜索引用该标记以指示要使用的时间输入。

以下代码段新建了定义用于本地使用的时间输入的标记。

```

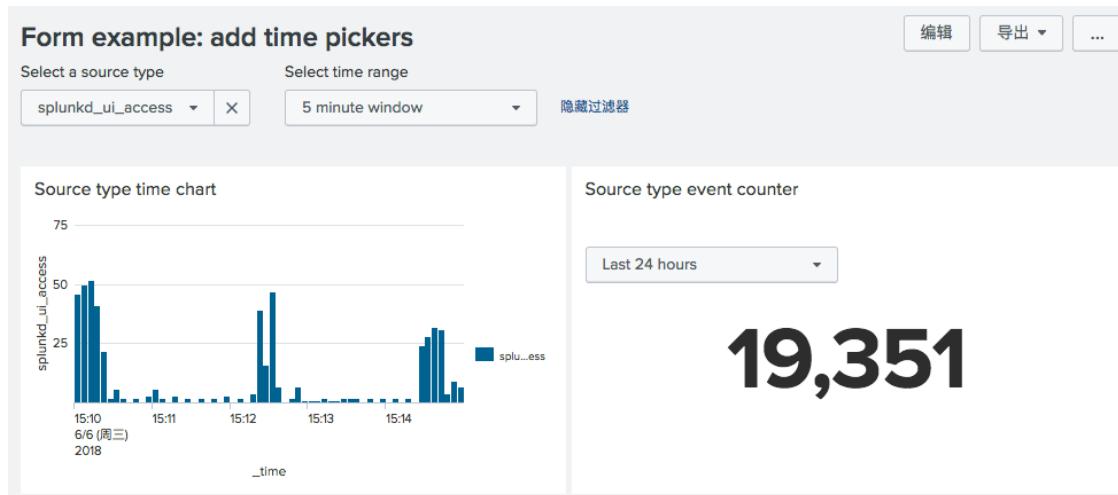
<input type="time" token="time_tok" searchWhenChanged="true">
  <label></label>
  <default>
    <earliest>-24h@h</earliest>
    <latest>now</latest>
  </default>
</input>

```

访问本地时间输入时，使用时间输入标记的 `earliest` 和 `latest` 修饰符。

```
<search>
  <query>
    index=_internal sourcetype=$sourcetype_tok$
    | stats count as sourcetype</query>
    <earliest>$time_tok.earliest$</earliest>
    <latest>$time_tok.latest$</latest>
  </search>
```

以下示例使用驱动“来源类型时间图表”面板的全局计时器。“来源类型事件计数器”面板仅包含此面板的本地时间。



```
<form>
  <label>Form example: add time pickers</label>
  <fieldset autoRun="true" submitButton="false">
    <input type="dropdown" token="sourcetype_tok">
      <label>Select a source type</label>
      <default>splunkd</default>
      <choice value="splunkd">splunkd</choice>
      <choice value="splunk_web_access">splunk_web_access</choice>
      <choice value="splunkd_ui_access">splunkd_ui_access</choice>
    </input>

    <!-- Global timer. Not token is necessary -->
    <input type="time" searchWhenChanged="true">
      <label>Select time range</label>
      <default>
        <earliest>-7d@h</earliest>
        <latest>now</latest>
      </default>
    </input>

  </fieldset>
  <row>
    <panel>
      <title>Source type time chart</title>
      <chart>
        <search>
          <query>index = _internal sourcetype=$sourcetype_tok$
            | timechart count by sourcetype</query>
        </search>
      </chart>
    </panel>
    <panel>
      <title>Source type event counter</title>

      <!-- Local timer. Use tokens to access selected time. -->
      <input type="time" token="time_tok" searchWhenChanged="true">
        <label></label>
      </input>
    </panel>
  </row>
</form>
```

```

<default>
  <earliest>-24h@h</earliest>
  <latest>now</latest>
</default>
</input>

<single>
<search>
<query>
  index=_internal sourcetype=$sourcetype_tok$
  | stats count as sourcetype</query>

  <!-- Use the earliest and latest modifiers to the time input token -->
  <earliest>$time_tok.earliest$</earliest>
  <latest>$time_tok.latest$</latest>

</search>
</single>
</panel>
</row>
</form>

```

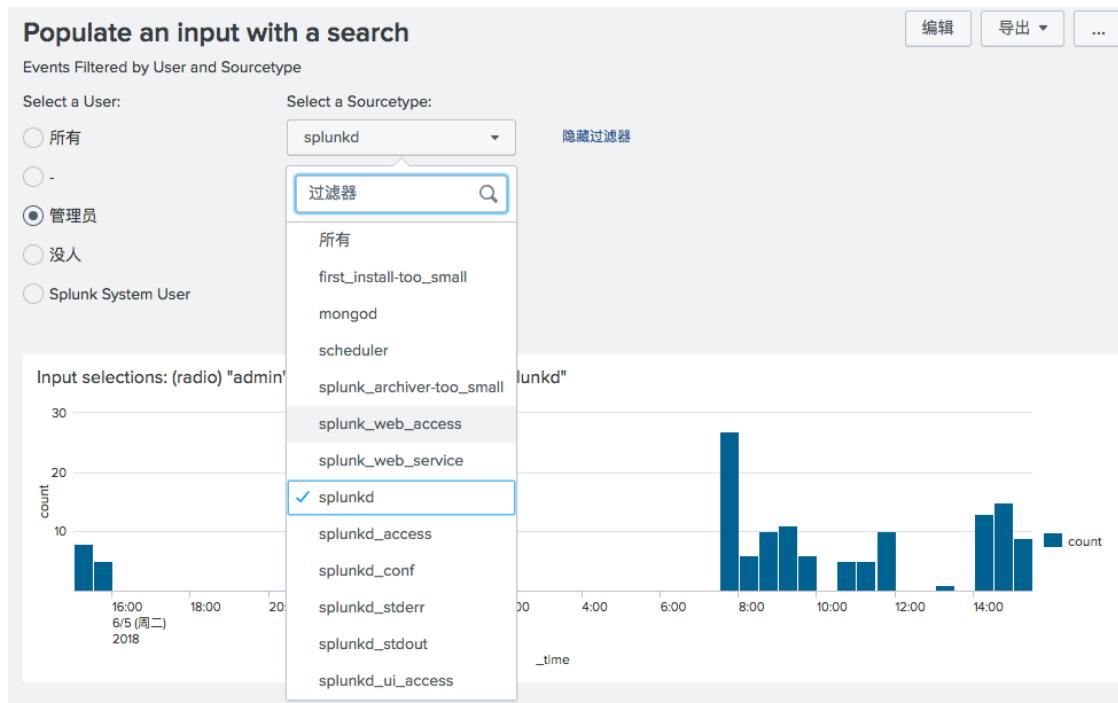
到表单的静态和动态输入

以下表单输入需要用户选择的多个选项。您可静态定义此输入或使用搜索动态填充表单的输入。

- 复选框
- 下拉菜单
- 多选
- 单选

以下示例中的搜索比较选项的静态和动态定义。下拉列表使用填充搜索定义选项。

- 填充 `<search>`
返回该选项的标签和值要使用的字段。
- `<fieldForLabel> <fieldForValue>`
`<input>` 元素的子元素。这些元素指定要使用的字段以填充下拉选项。



```

<form>
<label> Populate an input with a search</label>
<description>Events Filtered by User and Sourcetype</description>

```

```

<!-- Do not need a Search Button. Inputs search when changed -->

<fieldset autoRun="true" submitButton="false">

    <!-- Static definition of choices -->
    <input type="radio" token="username_tok" searchWhenChanged="true">
        <label>Select a User:</label>

        <!-- Define the default value -->
        <default>All</default>

        <!-- Hard-code the choices -->
        <choice value="*">All</choice>
        <choice value="-"></choice>
        <choice value="admin">Admin</choice>
        <choice value="nobody">Nobody</choice>
        <choice value="splunk-system-user">Splunk System User</choice>
    </input>

    <!-- Dynamic definition of choices -->
    <input type="dropdown" token="sourcetype_tok" searchWhenChanged="true">
        <label>Select a Sourcetype:</label>
        <prefix>sourcetype=</prefix>
        <suffix>"</suffix>

        <!-- Define the default value -->
        <default>splunkd</default>

        <!-- Hard-code the choice for "All" -->
        <choice value="*">All</choice>

        <!-- Define the other choices with a populating search -->
        <search>
            <query>
                index=_internal | stats count by sourcetype
            </query>
        </search>
        <fieldForLabel>sourcetype</fieldForLabel>
        <fieldForValue>sourcetype</fieldForValue>
    </input>

</fieldset>
<row>
    <panel>
        <!-- Use tokens from the <input> elements in the panel title -->
        <title>
            Input selections: (radio) "$username_tok$", (dropdown) $sourcetype_tok$
        </title>

        <chart>
            <!-- search for the visualization, references the input tokens-->
            <search>
                <query>
                    index=_internal user=$username_tok$ $sourcetype_tok$ | timechart count
                </query>
                <earliest>-24h@h</earliest>
                <latest>now</latest>
            </search>
        </chart>
    </panel>
</row>
</form>

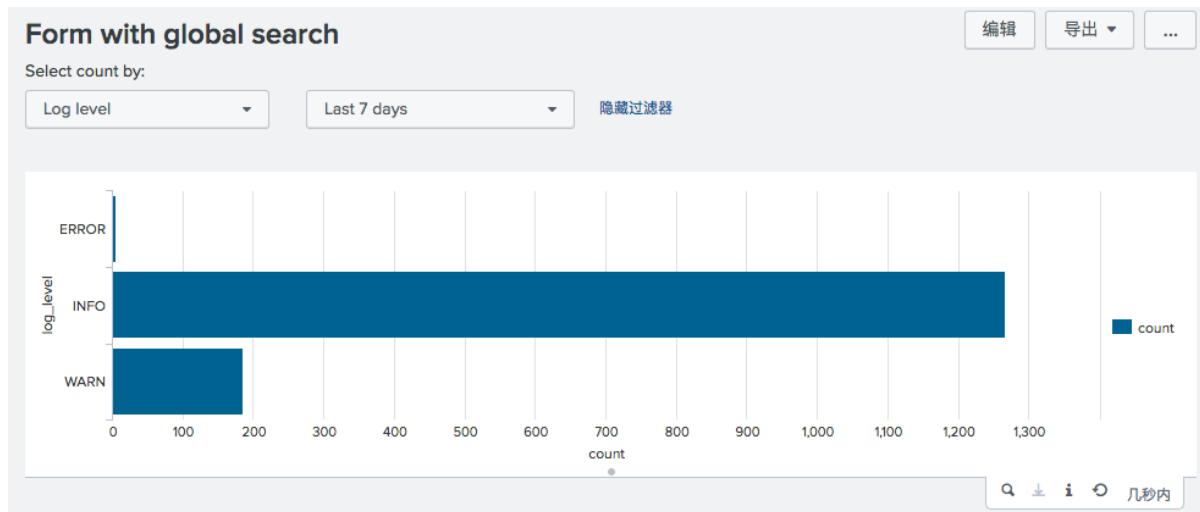
```

新建带全局搜索的表单

您可新建使用驱动各种面板中数据的全局搜索的表单。这种情况是后期处理搜索的另一个表单。由于各种限制，您在使用后期

处理搜索时应格外注意。许多情况下，后期处理搜索并不始终是使用搜索资源的最有效方法。请仔细阅读主题“处理后搜索”。该主题讨论了在实现处理后搜索前要考虑的处理后限制和其他因素。

以下示例显示了具有全局搜索的表单。



全局搜索使用转换搜索命令，以避免您可传递到后期处理搜索的 10,000 个事件这一数量限制。

```
<search id="global_search">
  <query>
    index=_internal source=*splunkd.log | stats count by component, log_level
  </query>
</search>
```

下拉选项的值包括后期处理搜索：

```
<fieldset autoRun="true" submitButton="false">
  <input type="dropdown" token="stats_tok" searchWhenChanged="true">
    <label>Select count by:</label>
    <default>Log level</default>
    <choice value="stats sum(count) AS count by log_level">Log level</choice>
    <choice value="search log_level=error | stats sum(count) AS count by component">Component</choice>
  </input>
```

表单中的面板使用来自下拉选项的标记访问所选的选项。

```
<search base="global_search">
  <query>
    $stats_tok$
  </query>
</search>
```

以下是针对具有全局搜索的表单的完整代码：

```
<form>

  <label>Form with global search</label>
  <search id="global_search">
    <query>
      index=_internal source=*splunkd.log | stats count by component, log_level
    </query>
  </search>

  <fieldset autoRun="true" submitButton="false">
    <input type="dropdown" token="stats_tok" searchWhenChanged="true">
      <label>Select count by:</label>
      <default>Log level</default>
      <choice value="stats sum(count) AS count by log_level">Log level</choice>
      <choice value="search log_level=error | stats sum(count) AS count by component">Component</choice>
    </input>
  </fieldset>
```

```
<input type="time">
  <default>Last 7 days</default>
</input>
</fieldset>
<row>
  <panel>
    <chart>
      <option name="charting.chart">bar</option>
      <search base="global_search">
        <query>
          $stats_tok$
        </query>
      </search>
    </chart>
  </panel>
</row>
</form>
```

使用第三方 XML 编辑器

大多数情况下，您可以使用 Splunk Web 仪表板编辑器编辑简单 XML。请参阅“关于仪表板编辑器”了解更多。

如果您正在使用 Splunk Enterprise，您也可以使用第三方编辑器与部署中的仪表板源代码文件一起使用。

Splunk Cloud 用户无法使用第三方编辑器，因为他们没有访问仪表板源代码文件的权限。如果您有 Splunk Cloud，请使用 Splunk Web 中的仪表板编辑器。

仪表板和表单的源代码文件

仪表板和表单的源代码文件可能包含以下各项。

- 简单 XML
- JavaScript
- CSS
- 由引用导入的静态 HTML 和图像文件

文件用法要求

文件系统写入权限

您必须拥有对 Splunk 部署文件系统的写入权限，才能访问简单 XML 文件以及 CSS 和 JavaScript 支持文件。如果没有写入权限，请与管理员联络。

仪表板来源文件权限

复制仪表板来源文件后，请确保您可以读取和写入这些文件。文件上的读取和写入权限独立于仪表板用户写入权限进行定义。

文件目录和位置

使用源代码文件的本地目录

编辑仪表板编辑器中的简单 XML 时，源代码文件更改写入到 /local 目录。将使用第三方编辑器编辑的仪表板源代码文件放入 /local 目录。

警告：不要将简单 XML 源文件放入 /default 目录。部署和应用更新时，/default 目录中的文件会被覆盖。

有关目录和文件优先顺序的更多信息，请参阅“配置文件优先顺序”。

文件位置和权限

源代码文件位置取决于文件类型和权限。

简单 XML 和预建面板来源文件

应用的 /views 目录包含以下文件。

- 简单 XML 文件
- 通过仪表板中参考可用的面板文件。请参阅“通过引用新建和添加面板”了解更多信息。
- 旧高级 XML 文件

将简单 XML 和面板源代码文件放在每个权限类型的以下位置。

权限类型	位置
在应用中共享	\$SPLUNK_HOME/etc/apps/<app>/local/data/ui/views/<file_name>
专用	\$SPLUNK_HOME/etc/users/<user>/<app>/local/data/ui/views/<file_name>

旧 HTML 文件

应用中的 /html 目录包含让仪表板转换成 HTML（不再支持转换成 HTML）的源文件。

将 HTML 文件放到每个权限类型的以下位置。

权限类型	位置
在应用中共享	\$SPLUNK_HOME/etc/apps/<app>/local/data/ui/html/<dashboard_file_name>
专用	\$SPLUNK_HOME/etc/users/<user>/<app>/local/data/ui/html/<dashboard_file_name>

显示 Splunk Web 中的源代码文件更改

要显示仪表板源代码文件的更改，请使用 debug/refresh 端点刷新 Splunk 部署中的配置。

`http://localhost:8000/debug/refresh`

刷新实例后，重新加载已编辑的仪表板。

导入 CSS、JavaScript 和其他静态文件

仪表板可以导入 CSS 和 JavaScript 文件，以及图像文件和静态 HTML 文件。这些文件在如下位置。文件不能放在子目录中。

`$SPLUNK_HOME/etc/apps/<app_name>/appserver/static/`

默认情况下，本目录包含以下两个文件：

- dashboard.css
- dashhboard.js

您可以编辑这一位置的默认文件或添加其他 CSS 和 JavaScript 文件。您还可以添加希望从仪表板引用的任何 HTML 文件。

导入 JavaScript 和 CSS 文件

使用 `<dashboard>` 或 `<form>` 元素中的 `script` 和 `stylesheet` 属性，从应用默认位置导入 JavaScript 或 CSS 文件。也可引用其他应用中的脚本和 CSS 文件。

示例

从同一个应用导入文件

```
<dashboard script="myScript.js" stylesheet="myStyles.css">
. . .
</dashboard>
```

从其他应用导入文件

```
<dashboard script="myApp:myScript.js" stylesheet="myApp:myStyles.css">
. . .
</dashboard>
```

钻取和仪表板交互

使用钻取构建仪表板交互性

用户单击仪表板中的数据点、表格行或其他可视化元素时，您可能想要分享其他的数据见解。使用钻取在仪表板中构建此交互。

钻取如何运作

钻取是一种配置工具，用于配置对用户单击仪表板或表单中可视化的响应。在单个可视化中配置钻取行为。您可以对仪表板中的每个可视化单独进行钻取配置。根据可视化类型，您还可以启用可视化中特定元素的钻取，如表格行或单元格。

钻取操作

用户在钻取已启用的情况下单击可视化元素时，即进行您配置的钻取操作。

链接到目标

钻取可以将来源仪表板或表单链接到用户单击打开的外部目标。目标可以是辅助搜索、其他仪表板、表单或网站。

如果您链接到网站，请确保使用有效解码的 URL。例如：任何该被认为是 URL 链接中的问号的问号（?）应改为 %3F。您还可以新建可以在 XML 中的多个地方使用的编码 URL 字符标记。

触发当前仪表板中的交互行为

钻取还会触发在同一个仪表板或表单中的上下文更改。例如，您可以根据单击值显示或隐藏内容。

使用标记自定义钻取

标记就像是程序变量。标记名称代表可以更改的值，如表单输入中的用户选择。您可以使用标记名称访问其代表的值。在钻取中，您可以使用标记捕获来自当前仪表板的上下文值或单击元素的值。您还可以定义自定义标记以帮助实施交互行为。

您可以配置钻取将目标中的标记设为捕获来源值，将标记值传递到目标搜索、仪表板或 URL。以这种方式设置标记值，您可以在目标中显示自定义内容。

您还可以使用标记值触发当前仪表板中的交互变化，如内容显示或更多特定的搜索结果。配置当前仪表板中的元素以侦听和响应这些更改。

钻取中可用的标记

代表仪表板事件的几个预定义标记类型在钻取上下文中可用。您可以使用这些标记访问单击字段、搜索事件和其他动态值。

请参阅“仪表板中的标记用法”以了解关于使用以下标记类型的详细信息。

表单输入更改事件

表单输入使用标记代表用户在输入中选择的值。如果钻取目标是表单，您可以将来自来源仪表板的值传递到目标表单中的输入标记，以便用户可以看到为已选值自定义的内容。

要确定表单输入的标记名称，请检查该输入的简单 XML 源代码。

搜索事件

预定义标记代表搜索进程和完成事件。将搜索事件处理程序包括可视化元素 `<search>` 中，以获取搜索任务或结果属性。您可以使用标记以将这些值传递到 `<drilldown>` 元素。

在页面加载时设置的标记

在浏览器中加载仪表板时，您可以使用 `<init>` 元素设置标记值。您可以使用 `<drilldown>` 中的 `<init>` 元素访问标记值。

图表导航和选择事件

您可以访问代表用户在一些图表类型中的平移和缩放或所选择事件的标记值。请参阅“图表控制”以了解关于使用这些标记的更多信息。

预定义单击事件标记

在 Splunk 软件中预定义一些可以用于钻取的标记。您可以使用这些标记捕获来自仪表板的用户操作或其他值。例如，您可以使用预定义的 \$click.value2\$ 标记捕获单击的表单元格值。

请参阅“简单 XML 参考”中的“预定义钻取标记”以获取每个可视化可用的预定义标记列表。

自定义标记

除了预定义标记，您可以新建自定义标记，用于新建动态或条件式显示行为。这些标记可以代表更改的其他值，如搜索结果。

选择钻取操作

根据您想要的互动行为类型和您正在与用户共享的数据见解选择钻取操作。

要查看最常用使用案例和如何使用钻取操作的示例，注意您可以点击“开始”中的链接访问 Splunk 仪表板快速参考指南。

操作	类型	行为和配置
链接到搜索	链接到目标	在浏览器中打开搜索页面。辅助搜索会自动生成以显示单击值的结果。您还可以新建自定义搜索。
链接到不同的仪表板或表单	链接到目标	在浏览器中打开目标仪表板或表单。使用标记将值传递到目标并将自定义内容显示为单击值或其他来源值。
链接到 URL	链接到目标	在浏览器中打开外部网站。将来源标记值作为查询字符串参数传递到 URL。
管理当前仪表板或表单中的标记值	触发当前仪表板中的交互	当用户单击仪表板或表单中的元素时，设置、取消设置或筛选标记值。 不要链接到不同的位置，请使用标记值更改在同一仪表板中配置交互行为。例如，您可以使用仪表板中的 depends 或 rejects 属性，在设置标记之后，控制面板显示或隐藏行为。

钻取默认和自定义

部分钻取组件有默认设置。您可以根据组件使用钻取编辑器或简单 XML 进行自定义。

钻取组件	默认配置	自定义位置
已启用？	如果您正在构建一个新的可视化或仪表板，默认禁用钻取。如果您正在将现有的仪表板迁移到软件 6.6 或以上版本，默认保留之前的钻取设置（包括钻取启用）。	使用钻取编辑器或简单 XML 启用或禁用钻取。
已启用钻取的可视化中的元素	因可视化而异。例如，您可以启用表格行上或单个表格单元格中的钻取以捕获更多特定单击值。 查看简单 XML 参考的默认设置和选项。	使用简单 XML 调整钻取位置。
打开已链接的搜索、仪表板或 URL 的浏览器选项卡	在钻取编辑器中，默认选择在新的选项卡中打开。 在简单 XML 中，默认在同一个选项卡中打开钻取。	在钻取编辑器中，您可以不选择在新的选项卡中打开钻取目标。在简单 XML 中，将 target="blank" 属性添加到 <link> 以便在新的选项卡中打开目标。

默认设置和源代码同步

新的仪表板内容默认禁用钻取。要禁用钻取，将 <option name="drilldown">none</option> 简单 XML 元素添加到想要保存到仪表板的可视化。

为避免同步问题，不要从仪表板源代码中删除此 <option>。您可以使用钻取编辑器更改钻取配置或编辑 <option name="drilldown"> 元素，无需删除该元素。

访问钻取编辑器

您可以使用钻取编辑器以启用或配置钻取操作。某些高级配置（如条件式链接）只在简单 XML 中可用。

步骤

1. 在您想要配置钻取的仪表板中，单击编辑。
2. 找到您正在添加或更新钻取的面板。单击右侧的其他选项图标。选择编辑钻取。

编辑仪表板 UI 数据来源 + 添加面板 + 添加输入 ▾ 取消 另存为... 保存

Basic Dashboard

Illustrate the basic structures of a dashboard

无标题

Top Sourcetypes (Last 24 hours)

sourcetype	count	91.87
1 splunkd	226250	
2 splunkd_ui_access	15734	6.39
3 splunkd_access	3356	1.36
4 splunk_web_service	466	0.19
5 splunk_web_access	413	0.17
6 splunk_archiver-too_small	25	0.01
7 scheduler	25	0.01

Edit Drilldown

3. 使用编辑器启用和配置钻取操作。

有关在钻取编辑器和简单 XML 中配置特定钻取操作的详细信息，请参阅[选择钻取操作](#)中的选项和链接主题。

链接到搜索

您可以新建将用户链接到单击值搜索结果的钻取。用户可以查看事件以获得有关单击值的更多信息。

链接到搜索如何运作

链接到搜索，用户即可查看其他字段、值和与单击值相关的其他数据。您可以使用默认搜索或自定义用户单击打开的搜索。

使用默认搜索

辅助搜索会自动生成以显示有关单击值的更多信息。此搜索和驱动来源可视化的搜索类似，但是会生成更具有针对性的单击值结果。

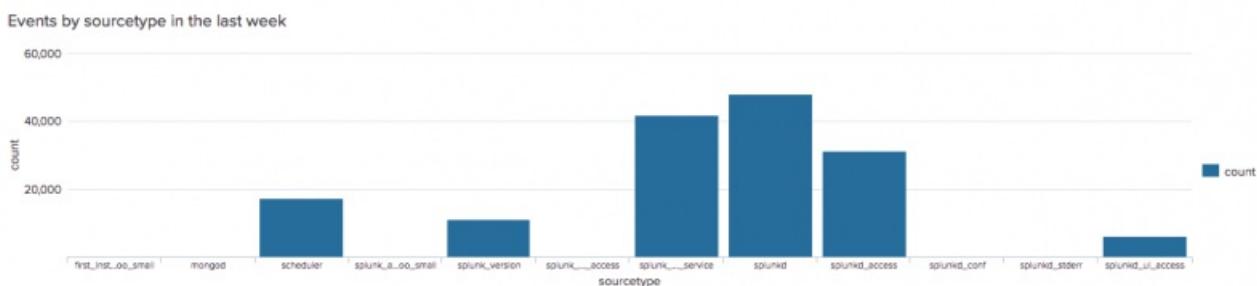
自定义搜索

您可以自定义辅助搜索以生成不同的结果。例如，您可能想要显示单个数据集的结果或包括搜索字符串中的不同字段或命令。

您可以使用预定义标记包括搜索中的单击值。

示例

此柱形图会按来源类型显示上周的事件计数。



此图表是使用以下搜索字符串生成的。

```
index = _internal | stats count by sourcetype
```

链接到默认搜索的钻取已在图表上启用。如果用户单击图表中的 mongod 来源类型列，则会打开辅助搜索。此搜索会删除聚合并生成 mongod 来源类型值的事件列表。

用户可以查看在柱形图中无法使用的 mongod 来源类型的详细信息。

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

- Search Bar:** index=_internal sourcetype=mongod
- Results Summary:** ✓ 230 个事件 (18/05/31 13:00:00.000 至 18/06/07 13:17:33.000) 无事件采样
- Time Range:** 过去 7 天
- Event Count:** 230
- Mode:** 事件 (230)
- Visualizations:** 统计信息 可视化
- Time Range Controls:** 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
- Result Table Headers:** 列表 格式 每页 20 个 1 2 3 4 5 6 7 8 下一步 >
- Result Data:** Two events are listed:

 - Event 1: 18/06/06 9:09:48.122Z I COMMAND [ftdc] serverStatus was very slow: { after basic: 0, after asserts: 12, after backgroundFlushing: 23, after connections: 23, after dur: 23, after extraInfo: 136, after globalLock: 2021, after locks: 2071, after network: 2071, after opLatencies: 2071, after opCounters: 2071, after opCountersRepl: 2071, after repl: 2081, after security: 2081, after storageEngine: 2081, after tcmalloc: 2081, at end: 2091 }
host = debianSplunk | source = /opt/splunk/var/log/splunk/mongod.log | sourcetype = mongod
 - Event 2: 18/06/05 8:28:12.308Z I ACCESS [conn11] Successfully authenticated as principal __system on local
host = debianSplunk | source = /opt/splunk/var/log/splunk/mongod.log | sourcetype = mongod

在钻取编辑器中配置钻取

您可以使用钻取编辑器启用钻取并配置链接到搜索。

要在钻取中新建条件式行为或其他高级行为，请使用简单 XML。如果使用现有的高级配置在面板中访问钻取编辑器，则会出现错误消息。

前提条件

在软件版本 6.6.0 中，部分默认钻取设置是新的。请参阅“将钻取用于仪表板交互”中的钻取默认设置和自定义。

步骤

- 从您想要配置钻取的仪表板中，单击编辑打开仪表板编辑器。
- 找到您正在配置钻取的面板。单击其他选项按钮并选择编辑钻取。

The screenshot shows the Splunk dashboard editor with the following details:

- Dashboard Title:** Basic Dashboard
- Panel Type:** Top Sourcetypes (Last 24 hours)
- Table Headers:** sourcetype, count, %
- Table Data:** A list of sourcetypes and their counts:

sourcetype	count	%
1 splunkd	226250	91.87
2 splunkd_ui_access	15734	6.39
3 splunkd_access	3356	1.36
4 splunk_web_service	466	0.19
5 splunk_web_access	413	0.17
6 splunk_archiver-too_small	25	0.01
7 scheduler	25	0.01
- Context Menu:** The 'Edit Drilldown' button is highlighted with a red arrow.

- 选择链接到搜索。
- 选择搜索类型。
 - “自动”会生成默认搜索以删除聚合并筛选来自单击元素的值。
 - 选择“自定义”以输入搜索字符串和时间范围。
- (可选) 选择在新的浏览器选项卡中打开搜索。
- 单击应用以应用钻取设置。

7. 单击保存以保存仪表板更改。

在简单 XML 中配置钻取

单击编辑以打开仪表板编辑器并单击来源以访问简单 XML 源代码。

钻取默认和自定义

在软件版本 6.6.0 中，部分默认钻取设置是新的。请参阅“将钻取用于仪表板交互”中的钻取默认设置和自定义。

启用钻取

查找可视化中的 `<option name="drilldown">none</option>` 元素。更改选项以启用和侧重钻取。例如，在表格可视化中，使用 `<option name="drilldown">cell</option>` 启用表格单元格上的钻取。

启用后，钻取会链接到同一浏览器选项卡中的默认搜索。

搜索语法

默认搜索

为启用钻取的可视化使用简单 XML `<option>` 的可视化。例如，气泡图中的以下源代码将添加链接到搜索的钻取。

```
<option name="charting.drilldown">all</option>
```

参阅“简单 XML 参考”以查看每个可视化要使用的 `<option>` 名称和语法。

自定义搜索

在您的仪表板源代码中，添加 `<drilldown>` 元素以自定义已链接的搜索。

此示例使用的是 `target` 属性以在新浏览器选项卡中打开搜索。钻取会链接到 `search` 页面并使用 `q` 参数传入自定义搜索字符串。

```
<drilldown>
  <link target="_blank">search?q=index=_internal | stats count by sourcetype</link>
</drilldown>
```

链接到自定义搜索示例

打开辅助搜索之后，您可以自定义钻取更改用户看到的结果。

默认搜索

此搜索将生成在零售网站上聚合客户行为的表格。

```
source="my_retail_data_source" | stats count by action
```

Retail actions today	
action	count
addtocart	44
purchase	40
view	34
remove	14
changequantity	11

链接到默认搜索的钻取已在表格中启用。默认搜索会按照来源类型删除聚合并为已选来源类型列筛选事件。如果用户单击 `addtocart` 操作，则会打开以下辅助搜索。

```
source="my_retail_data_source" action="addtocart"
```

默认搜索会筛选已选操作的结果。您可能想要显示更多特定详细信息。要覆盖此默认行为，请在钻取编辑器或简单 XML 中新建自定义辅助搜索。

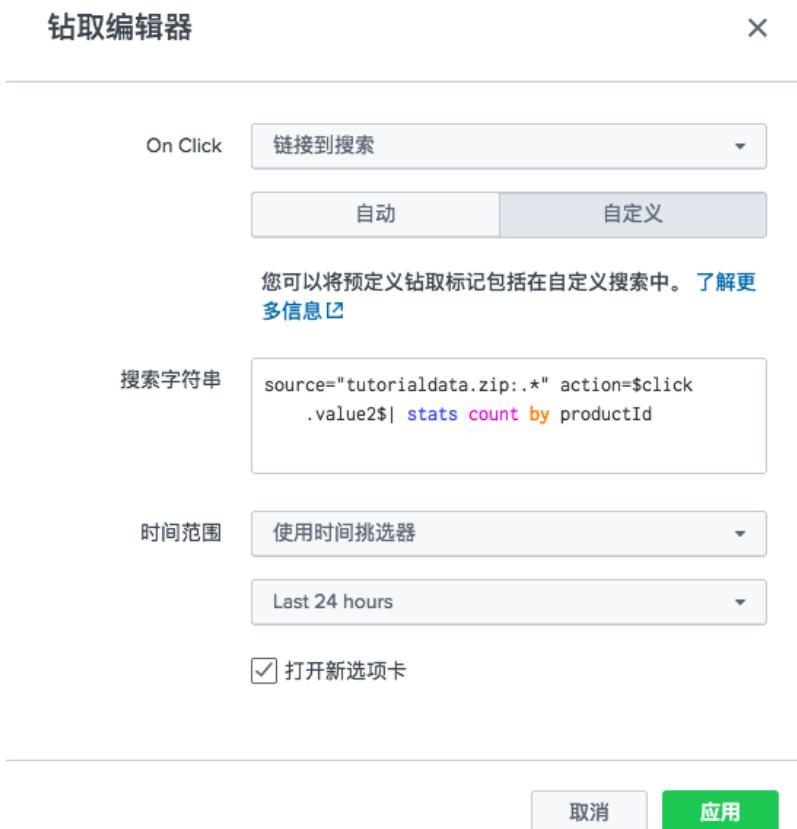
自定义搜索

自定义钻取搜索向用户显示有关用户行为所涉产品的更多信息。以下搜索字符串使用 \$click.value2\$ 预定义标记捕获用户单击的操作并针对该操作筛选产品计数。

```
source="my_retail_data_source" action=$click.value2$ | stats count by productId
```

在钻取编辑器中自定义搜索

在钻取编辑器中，您可以将默认搜索更改为自定义搜索。需要时，输入搜索字符串并配置时间范围参数。



在简单 XML 中自定义搜索

您可以使用简单 XML 新建相同的自定义搜索行为。在表格可视化元素中，添加以下源代码。

```
<drilldown>
  <link target="_blank">search?q=source="my_retail_data_source" action=$click.value2$ | stats count by productId</link>
</drilldown>
```

钻取使用 \$click.value2\$ 预定义标记捕获用户单击的操作并将其用于搜索。

您可以为搜索添加自定义时间范围参数。使用 <![CDATA[]]> 包装脚本或 HTML 字符实体转义 & 符号或其他特殊字符。

此示例将时间范围设为过去 24 小时。

```
<drilldown>
  <link target="_blank">
    <![CDATA[
      search?q=source="my_retail_data_source" action=$click.value2$ | stats count by productId&earliest=-24h@h&latest=now
    ]]>
  </link>
</drilldown>
```

有关语法的详细信息，请参阅“简单 XML 参考”中的 `<link>` 元素。

链接到仪表板

设置钻取以将用户链接到目标仪表板或表单。此钻取操作可显示与用户单击值相关的用户仪表板内容。

链接到仪表板如何运作

表格显示零售网站的客户活动（如购买或浏览）。表格聚合了事件以显示哪个产品和产品种类最近有活动。

Buttercup Games customer actions in the past week		
productId	categoryId	count
BS-AG-G09	ARCADE	543
CU-PG-G06	SPORTS	555
DB-SG-G01	STRATEGY	926
MB-AG-T01	TEE	801
SC-MG-G10	SIMULATION	983
SF-BVS-01	NULL	20
WC-SH-A01	ACCESSORIES	672
WC-SH-G04	SHOOTER	951

您可以使用钻取将用户链接到仪表板，显示用户单击的产品类别相关的更多数据。

例如，目标仪表板可能有显示此类别的购买和删除计数的单值可视化。它也可能包括按照状态显示相对购买计数的分级统计地图。以下钻取 `<link>` 会在新的浏览器窗口中打开此目标仪表板。

```
<link target="_blank">/app/search/customer_purchase_removal_map</link>
```

使用参数自定义目标内容

将值从来源传递到目标显示目标中的自定义内容。您可以配置钻取以捕获来源仪表板中单击值或其他值，并将该值作为参数传递到目标。

例如，您可以在表格可视化上启用钻取。您可以使用 `$click.value2$` 预定义标记访问单击的表格单元格中的值。您可以配置钻取以将目标内容中的标记设为已捕获的 `$click.value2$`。用户单击后，钻取会打开带有设置为单击值的参数的目标。

设置目标表单中的标记

如果您要设置目标表单中的标记值，请使用 `form.` 作为表单标记名称的前缀。例如，使用以下配置将目标表单中的 `host` 标记设置为来自来源的单击表格单元格值。

```
form.host = $click.value2$
```

仪表板标记名称不需要前缀。要将目标仪表板中的 `host` 标记设置为单击表格单元格值，请使用 `host = $click.value2$`。

在钻取编辑器中配置钻取

您可以使用钻取编辑器配置链接到外部仪表板或 URL。使用钻取编辑器可以在来源和目标之间传递参数。

要在钻取中新建条件式行为或其他高级行为，请使用简单 XML。如果使用现有的高级配置在面板中访问钻取编辑器，则会出现错误消息。

前提条件

在软件版本 6.6.0 中，部分默认钻取设置是新的。请参阅“将钻取用于仪表板交互”中的钻取默认设置和自定义。

步骤

1. 从您想要配置钻取的仪表板中，单击编辑打开仪表板编辑器。
2. 找到您正在配置钻取的面板。单击其他选项按钮并选择编辑钻取。

sourcetype	count	percent
splunkd	226250	91.87
splunkd_ui_access	15734	6.39
splunkd_access	3356	1.36
splunk_web_service	466	0.19
splunk_web_access	413	0.17
splunk_archiver-too_small	25	0.01
scheduler	25	0.01

3. 选择链接到仪表板。
4. 选择目标应用和仪表板。

On Click: 链接到仪表板

应用: Search & Reporting

仪表板: 选择...

打开新选项卡

参数: = x

+ 新增

使用参数设置目标仪表板中的标记值。例如 form.host = \$click.value2\$ 或 host = \$row.host\$ [了解更多信息](#)

取消 应用

5. (可选) 单击高级以输入要在目标仪表板中设置的参数名称和值。您可以使用从来源捕获的值 (如 \$click.value\$) 以配置目标中的参数。
6. 单击应用以应用钻取设置。
7. 单击保存以保存仪表板更改。

在简单 XML 中配置钻取

通过将 `<drilldown>` 元素放入表格或图表开始构建动态钻取。

指定钻取目标

在 `<drilldown>` 元素中，使用 `<link>` 元素表示钻取目标并在目标仪表板或表单中自定义内容。

```
<drilldown>
  <link>...</link>
</drilldown>
```

`<link>` 元素包含目标路径和您正在从来源传到目标的任何标记价值。这些示例显示了用于指定目标路径和传递值的语法。

目标和行为	语法
-------	----

在您的 Splunk 部署中链接到仪表板。	<p>使用包含仪表板或表单 ID 的相对路径。</p> <pre><link> [relative path]/[dashboard or form id] </link></pre>
链接到您的 Splunk 部署中的表单。通过传递从来源获取的标记值显示表单中的自定义内容。使用标记值填充表单输入。	<p>在相对路径后添加一个 ? 符号。将目标中的标记设置为从数据来源传递来的值。此示例将目标表单中的标记设置为数据来源中的值。</p> <p>使用 form. 作为目标表单中标记的前缀，如此处所示。</p> <pre><link> [relative path]/[dashboard or form id]? form.[target_token_name]=[\$source_value\$] </link></pre>
将 <earliest> 和 <latest> 时间范围调节器从数据来源搜索传递到目标中的搜索。	<p>添加 &earliest=\$earliest\$&latest=\$latest\$ 到目标路径和标记值。使用 <! [CDATA[...]]> 包装确保 & 符号解释正确。</p> <pre><link> <! [CDATA[[relative path]/[dashboard or form id]? form.[target_token_name]=[\$source_value\$]&earliest=\$earliest\$&latest=\$latest\$]> </link></pre>

其他信息

- 关于 <link> 和 <drilldown> 元素的详细信息，请参阅“简单 XML 参考”。
- 有关使用和自定义标记的信息，请参阅“仪表板中的标记用法”。

条件式链接

您可能想根据来源仪表板或表单中用户单击的特定元素来配置链接到不同目标的条件式链接。要这么做，请将 <condition> 元素添加到 <drilldown>。<condition> 元素包括要使用的条件式 <link> 目标和值。

<condition> 中的表格 field 或图表 series 属性表示要针对条件式链接进行评估的字段或系列值。

示例

仪表板中所含表格有 A、B 和 C 三列。

如果用户单击 A 列中的值，则会打开含有设为捕获值的标记的表单。

```
<drilldown>

<condition field="A">
  <link> [relative_path]/[target_form_id]?form.[target_token]=${value_from_source} $ </link>
</condition>
[...]

</drilldown>
```

从多值字段中捕获值

多值字段可在一次事件中出现多次。每次字段出现在事件中时，都可以有一个不同的值。您可以配置钻取以根据用户单击的值链接到特定的目标。

设置表格中的钻取时，通常会使用 \$click.name\$ 或 \$click.name2\$ 以捕获用户在列或行中单击的值。但是，如果要使用多值字段，请使用 \$click.value2\$ 捕获所选值进行钻取。使用带 field 属性的 <condition> 元素将列选择限制为多值字段。

请参阅《知识管理器手册》中的“配置多值字段”以了解关于在您的数据中使用多值字段的更多信息。

在另一个浏览器选项卡中打开目标

默认情况下，在简单 XML 中，钻取目标会作为来源仪表板或表单在同一个浏览器选项卡中打开。您可以将 target="blank" 属性添加到 drilldown 元素以在新的浏览器选项卡中打开目标。

示例源代码

```

<dashboard>
  <label>Example linking drilldown</label>

  <row>
    <panel>
      <table>

        <title>Sourcetypes by source (Drilldown to a form)</title>
        <search>
          <query>
            index=_internal | stats dc(sourcetype) by sourcetype, source
          </query>
          <earliest>-60m</earliest>
          <latest>now</latest>
        </search>
        <option name="count">15</option>
        <option name="showPager">true</option>

        <drilldown target="blank">
          <!-- Access the input on the target form, which is in the same app -->
          <!-- sourcetype.tok is the token for an input to the target form -->
          <link>
            form_for_drilldown?form.sourcetype_tok=$click.value$ 
          </link>
        </drilldown>

      </table>
    </panel>
  </row>
</dashboard>

```

简单 XML 示例

链接到表单的仪表板

目标表单路径

以下示例的目标是 `form_for_drilldown` 表单。此表单的相对路径是

`/app/search/form_for_drilldown`

目标标记配置

在链接到目标仪表板或表单之前，请先检查其中的标记是否可用。确保配置目标及其标记，以在钻取操作中使用传递到目标的值。

此目标表单中有用户可用于选择来源类型值的钻取输入。输入使用 `sourcetype` 标记代表所选值。此标记用于生成图表的搜索中，显示此来源类型的结果。

目标表单源代码

```

<form>
  <label>Target form for drilldown</label>
  <fieldset autoRun="true" submitButton="false">
    <input type="dropdown" token="sourcetype">
      <label>Select a source type</label>
      <default>splunkd</default>
      <search>
        <query>
          index = _internal | stats count by sourcetype
        </query>
      </search>
      <fieldForLabel>sourcetype</fieldForLabel>
      <fieldForValue>sourcetype</fieldForValue>
    </input>
  </fieldset>
</row>

```

```

<panel>
  <chart>
    <search>
      <query>index = _internal sourcetype=$sourcetype$
        | timechart count by sourcetype</query>
      <earliest>-7d</earliest>
      <latest>-0d</latest>
    </search>
  </chart>
</panel>
</row>
</form>

```

来源仪表板

设置将来源仪表板链接到目标表单的钻取。在目标表单中使用标记捕获来源并设置值。用户单击仪表板中的表格行时，会打开表单显示自定义内容。

钻取配置

此钻取使用 `<link>` 元素以表示要打开的表单并设置表单中的 `sourcetype` 标记值。

```

<drilldown>
<link>
<![CDATA[
 /app/search/form_for_drilldown?form.sourcetype=$row.sourcetype$&earliest=$earliest$&latest=$latest$]]>
</link>
</drilldown>

```

在 `<link>` 元素中，用户单击仪表板中的表格行之后，以下钻取组件会配置链接和标记设置。

组件	钻取此组件配置的行为	详细信息
目标表单路径	表示用户单击表格行后要打开的表单。	<code>/app/search/form_for_drilldown</code>
标记名称和值	标记会根据仪表板中用户单击的表格行自定义表单内容。	<p>要将标记值从来源仪表板传递到目标表单，查询字符串参数是否包含在路径中的 <code>?</code> 符号之后。</p> <p><code>form.sourcetype=\$row.sourcetype\$</code></p> <p>用户单击仪表板中的表格行之后，将 <code>sourcetype</code> 值从此行传递到表单。将表单中 <code>form.sourcetype</code> 标记设置为用户单击的表格行的 <code>\$row.sourcetype\$</code> 值。</p> <p><code>earliest=\$earliest\$&latest=\$latest\$</code></p> <p>将表单中的 <code>earliest</code> 和 <code>latest</code> 时间范围修饰符设置为来源仪表板中的 <code>\$earliest\$</code> 和 <code>\$latest\$</code> 值。</p> <p><code><![CDATA[...]]></code> 标记可确保 <code>&</code> 字符解释正确。</p>

完成仪表板源代码

```

<dashboard>
<label>Dashboard linking to a form</label>
<row>

  <table>
    <search>
      <query>
        index=_internal group="per_sourcetype_thruput" |
        chart sum(kbps) over series
      </query>
      <earliest>-60m</earliest>
      <latest>now</latest>
    </search>
    <title>Top sourcetypes (drilldown example)</title>
    <option name="count">15</option>
    <option name="showPager">true</option>
  </table>
</row>

```

```

<drilldown>
  <link>
    <![CDATA[
      /app/search/form_for_drilldown?form.sourcetype=$row.sourcetype$&earliest=$earliest$&latest=$latest$
    ]]>
  </link>
</drilldown>
</table>

</row>
</dashboard>

```

链接到 URL

链接到外部网站并与仪表板用户共享相关内容。

您可以链接到 URL 以帮助用户找到有关其单击的值的更多信息，如 Splunk Answers 上相关用户的文章或零售网站上的产品页面。

链接到 URL 如何运作

使用钻取以链接到 URL 与链接到仪表板或表单相似。用户单击来源仪表板中的元素时，钻取可以在浏览器窗口中打开一个目标外部网站。

使用参数自定义目标内容

要自定义浏览器中打开的内容，您可以将查询字符参数包括在您使用的 URL 中。您可以配置钻取以捕获来源仪表板中单击值或其他值，并将该值作为参数传递到目标。

例如，您可以在表格可视化上启用钻取。您可以使用 \$click.value2\$ 预定义标记访问单击的表格单元格中的值。您可以配置钻取以将目标内容中的标记设为已捕获的 \$click.value2\$。用户单击后，钻取会打开带有设置为单击值的参数的目标。

在钻取编辑器中配置钻取

您可以使用钻取编辑器配置链接到外部 URL。钻取编辑器还可将查询字符串参数包括在目标 URL 中。

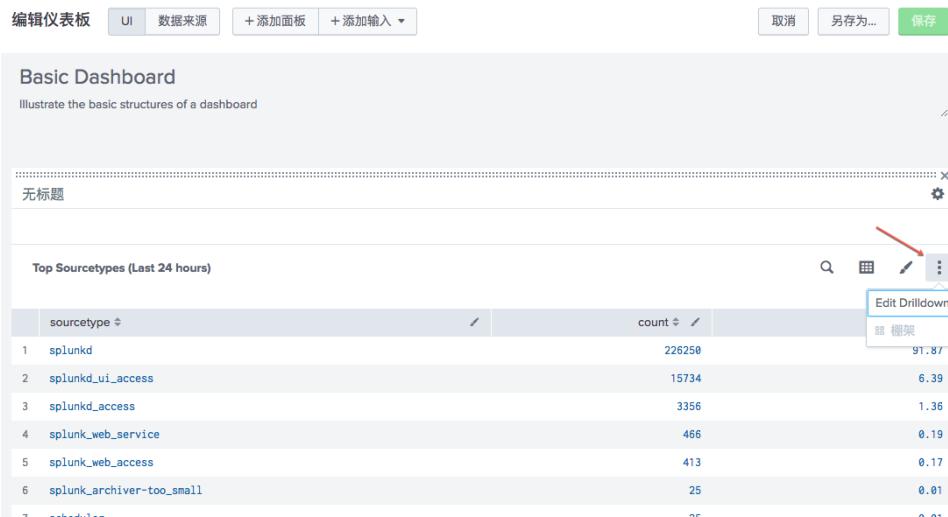
要在钻取中新建条件式行为或其他高级行为，请使用简单 XML。如果使用现有的高级配置在面板中访问钻取编辑器，则会出现错误消息。

前提条件

在软件版本 6.6.0 中，部分默认钻取设置是新的。请参阅“将钻取用于仪表板交互”中的钻取默认设置和自定义。

步骤

- 从您想要配置钻取的仪表板中，单击编辑打开仪表板编辑器。
- 找到您正在配置钻取的面板。单击其他选项按钮并选择编辑钻取。



- 选择链接到 URL。

4. 键入完整的目标 URL，包括 `http://` 或 `https://` 前缀。将任意查询字符串参数添加到 URL。例如，使用 `http://buttercupgames.com?product=$click.value$` 以传入来源仪表板中的单击产品值。
5. 单击应用以应用这些钻取设置。
6. 单击保存以保存这些仪表板更改。

在简单 XML 中配置钻取

您可以配置钻取以链接到 URL、传递参数并在简单 XML 中新建条件式链接行为。

语法

使用您想要在浏览器中显示的完整的资源 URL。您可以添加可选的查询字符串参数以自定义用户可以看到的内容。

```
<drilldown>
  <link>
    [target_URL]?q=[$source_value$]
  </link>
</drilldown>
```

条件式链接

您可能想要根据上下文值（如搜索结果或用户单击）配置条件式链接到不同的目标或传入不同的查询字符串参数。要这么做，请为 `<drilldown>` 添加 `<condition>` 元素。

要评估用户单击位置，您可以使用表格 `field` 或 `<condition>` 中的图表 `series` 属性。

您还可以使用 `<condition match="" " " >` 语句评估上下文值并有条件地触发链接或其他操作。请参阅“仪表板中的标记用法”中的“定义条件式匹配”以了解详细信息。

示例：链接到不同的目标

此钻取会根据用户单击的列从表格链接到不同目标 URL。

如果用户单击 A 列中的值，钻取会将单击字段值作为查询字符串参数传递到 URL。如果用户单击 B 列中的值，钻取会将此值传递到 URL。

```
<drilldown>
  <condition field="A">
    <link>[target_URL]?q=$[value_from_field_A]$</link>
  </condition>

  <condition field="B">
    <link>[other_target_URL]?q=$[value_from_field_B]$</link>
  </condition>
</drilldown>
```

示例：使用自定义逻辑计算搜索结果

以下钻取会设置搜索事件处理程序中的标记，以捕获表示失败的登录事件计数的 `$result.count$` 属性。该钻取使用 `<condition match="" " " >` 元素评估失败登录的次数。如果事件多于 5,000 个，钻取会连接到内部 runbook，以对登录失败进行故障排除。

```
<single>
  <search>
    <query>souce="recent_login_events" type=failed_login | stats count</query>
    <earliest>-24h@h</earliest>
    <latest>now</latest>
    <done>
      <set token="count">$result.count$</set>
    </done>
  </search>
  <option name="colorMode">block</option>
  <option name="useColors">1</option>
  <option name="drilldown">all</option>
  <drilldown>
    <condition match="$count$ > 5000">
      <link>http://companydocs.com/failed_login_runbook
      </link>
    </condition>
  </drilldown>
```

```
</drilldown>
</single>
```

从多值字段中捕获值

多值字段可在一次事件中出现多次。每次字段出现在事件中时，都可以有一个不同的值。您可以配置钻取以根据用户单击的值链接到特定的目标。

设置表格中的钻取时，通常会使用 `$click.name$` 或 `$click.name2$` 以捕获用户在列或行中单击的值。但是，如果要使用多值字段，请使用 `$click.value2$` 捕获所选值进行钻取。使用带 `field` 属性的 `<condition>` 元素将列选择限制为多值字段。

请参阅《知识管理器手册》中的“配置多值字段”以了解关于在您的数据中使用多值字段的更多信息。

其他信息

- 要了解关于编辑简单 XML 的更多信息，请参阅“[编辑简单 XML](#)”。
- 关于 `<drilldown>` 和 `<link>` 元素的详细信息，请参阅“[简单 XML 参考](#)”。

示例

链接到 *Splunk Answers* 上的搜索结果

将单击图表中元素的用户链接到 Splunk Answers 社区论坛上的相关搜索结果。

```
<link>
  http://answers.splunk.com/search.html?q=$click.value$
</link>
```

钻取包括 `<link>` 元素中的以下组件。

组件	钻取此组件配置的行为
外部网站的 URL <pre><link> http://answers.splunk.com/search.html?q=\$click.value\$ </link></pre>	此次 URL 指向 Splunk Answers 的搜索页面。
参数设置标记名称和值 <pre><link> http://answers.splunk.com/search.html?q=\$click.value\$ </link></pre>	<code>\$click.value\$</code> 预定义标记将捕获来自图表的单击值。此值会作为查询字符串参数传递到 Answers 搜索 URL。 在此示例中， <code>q Answers</code> 搜索术语参数会获得单击值且搜索会生成。当用户单击值之后，Answers 站点会加载，用户可以看到此值的搜索结果。

完成表单源代码

```
<form>
  <label>Form Search</label>

  <fieldset>
    <!-- Use the html tag to specify text to display -->
    <html>
      <p>Enter a sourcetype in the field below. This view returns the most recent 1000 events for that sourcetype.</p>
      <p>In the Matching Events, click in the series column to open the value clicked in a new form</p>
    </html>

    <!-- The default input is a text box with no initial value -->
    <input token="sourcetype" />

    <!-- Include a time picker -->
    <input type="time">
      <default>Last 30 days</default>
    </input>
```

```

</fieldset>

<row>
<panel>
<!-- output the results as a 50 row events table --&gt;
&lt;table&gt;
&lt;title&gt;Matching events&lt;/title&gt;

<!-- search with replacement token delimited with $ --&gt;
&lt;search&gt;
&lt;query&gt;
    index=_internal group="per_sourcetype_thruput" series=$sourcetype$
    | chart sum(kbps) over series
&lt;/query&gt;
&lt;/search&gt;

&lt;option name="count"&gt;50&lt;/option&gt;

&lt;!-- $click.value$ captures the value clicked by the user --&gt;
&lt;!-- and passes it to the website as a query parameter --&gt;
&lt;drilldown&gt;
&lt;link&gt;
    http://answers.splunk.com/search.html?q=$click.value$
&lt;/link&gt;
&lt;/drilldown&gt;
&lt;/table&gt;
&lt;/panel&gt;
&lt;/row&gt;
</pre>

```

</form>

管理当前仪表板中的标记值

使用钻取更新标记值并触发当前仪表板中的响应行为。不要链接到搜索仪表板或其他仪表板，您可以构建钻取（用户单击仪表板中的元素时可管理标记值）。根据仪表板配置，这些标记值更改可以促进不同的动态行为。

管理标记值如何运作

管理标记值是在当前仪表板中新建响应钻取行为的一部分。在钻取中配置标记值更改前，在仪表板中计划您想要的行为。例如，可以在用户单击后显示或隐藏内容。您还可以 `<set>` 标记值（是搜索字符串的一部分）以在仪表板中生成更符合需求的可视化。

在钻取中，您可以 `set`、`unset` 或使用 `eval` 以在用户单击后更改标记值。设置或更新标记值不会导致本身的动态仪表板行为。要新建响应更改，请在仪表板中配置元素以侦听这些标记更新。

例如，您可能想要在用户单击仪表板中特定表格时显示相关面板。您可以使用钻取编辑器或简单 XML 以在此表格中配置钻取以设置自定义 `show_content` 标记。然后，您可以编辑仪表板源代码为面板添加 `depends` 属性，这样面板只会在已设置 `show_content` 标记的情况下显示。

此话题中的使用案例和示例显示了当前仪表板中响应行为的不同选项。

- [生成自定义内容](#)
- [显示或隐藏内容](#)
- [配置条件式行为](#)

在钻取编辑器和简单 XML 中管理和响应标记值

您可以使用钻取编辑器以 `set`、`unset` 或 `eval` 标记值。新建这些配置后，您可以使用简单 XML 设置同一仪表板中的标记值的响应。

前提条件

- 更改标记值前，请在当前仪表板中计划您想要的响应行为。通常，您可以新建或使用现有的标记（您在钻取中 `set`、`unset` 和 `eval` 这些标记的值）以调用响应行为。确保标记可用且已放置好，以配置您想要的行为。必要时，可以在仪表板元素中新建标记或参考标记。
- 自 6.6.0 版本起，新增了一些默认钻取设置。请参阅“将钻取用于仪表板交互”中的钻取默认设置和自定义。

步骤

1. 从您想要配置钻取的仪表板中，单击编辑打开仪表板编辑器。
2. 找到您正在配置钻取的面板。单击其他选项按钮并选择编辑钻取。

The screenshot shows the Splunk UI dashboard editor. At the top, there are tabs for '编辑仪表板' (Edit Dashboard), 'UI' (selected), '数据来源' (Data Sources), '+ 添加面板' (Add Panel), and '+ 添加输入' (Add Input). On the right, there are buttons for '取消' (Cancel), '另存为...' (Save As...), and a green '保存' (Save) button. Below the tabs, the title 'Basic Dashboard' is displayed, followed by the subtitle 'Illustrate the basic structures of a dashboard'. The main content area shows a table titled 'Top Sourcetypes (Last 24 hours)'. The table has columns for sourcetype, count, and percentage. The data is as follows:

sourcetype	count	%
1 splunkd	226250	91.87
2 splunkd_ui_access	15734	6.39
3 splunkd_access	3356	1.36
4 splunk_web_service	466	0.19
5 splunk_web_access	413	0.17
6 splunk_archiver-too_small	25	0.01
7 scheduler	25	0.01

3. 选择管理此仪表板上的标记值。
4. 选择并配置标记操作。您可以在钻取中包含一个或更多标记操作。
 - 要 set 标记，请输入要设置的标记名称和新值。
 - 要 eval 标记值，请输入标记名称和决定标记值的 eval 表达式。
 - 要 unset 或删除标记值，请输入标记名称。
5. 单击应用以应用钻取设置。
6. 单击来源打开源代码编辑器。
7. 使用简单 XML 配置响应标记值更新的行为。例如，使用 depends 面板属性以进行标记设置，确定面板是否显示。
8. 单击保存以保存仪表板更改。

在简单 XML 中管理和响应标记值

您可以使用简单 XML 管理和响应标记值。配置标记值更改前，请在当前仪表板中计划您想要的响应行为。检查仪表板源代码以确保您需要的标记可用。您可以新建或编辑标记以使用您构建的行为。

例如，如果您想要显示自定义可视化内容，确保驱动可视化的搜索字符串包括您可以用来自定义结果的标记。您可以配置钻取以 <set> 该标记，这样搜索会筛选集值。

用于筛选结果的带有标记的示例可视化搜索字符串

```
index = _internal | stats count by $count_field$
```

将此标记设置为单击字段名称的示例钻取

此钻取使用预定义的 \$click.value\$ 标记捕获单击值。会将自定义 \$count_field\$ 标记设为该值。然后，搜索字符串就可以筛选单击字段的结果。

```
<drilldown>
  <set token="count_field">$click.value$</set>
</drilldown>
```

配置详细信息

在启用钻取的仪表板上单击编辑以打开仪表板编辑器，然后选择来源以访问仪表板源代码。

找到您正在添加或更新钻取的元素。添加 <drilldown> 元素并 set、unset 或 eval 子元素以配置用户单击后标记值的更改方式。

请查看以下示例了解有关在简单 XML 中新建响应行为的详细信息。

- [生成自定义内容](#)
- [显示或隐藏内容](#)
- [配置条件式行为](#)

生成自定义内容

用户单击仪表板元素时，您可以使用标记更新来生成自定义内容。例如，使用搜索字符串中的标记显示可以反映单击值的可视化。

示例

分级统计地图显示美国的最近销售活动。用户单击州之后，单值可视化会向用户显示所选状态的销售总计。

用户单击分级统计地图中的加利福尼亚后，此屏幕显示仪表板。



配置动态行为

用户单击地图中州之后设置标记。标记将捕获所选州值。

代表地图上的单击州的标记用于单值搜索字符串以筛选结果。搜索会生成特定于所选州的可视化。

仪表板源代码

在分级统计地图中，`<drilldown>` 将 `selected_state` 标记设置为单击位置。

```
<map>
  <title>Sales events in the United States this week
  </title>
  [...]
  <drilldown>
    <set token="selected_state">$click.value$</set>
  </drilldown>
  [...]
</map>
```

在同一个仪表板中，单值搜索将使用此标记生成所选州的销售总计。此搜索类似于驱动分级统计地图的搜索，但此搜索使用 `selected_state` 值筛选和聚合事件。

单值 `<title>` 还使用 `selected_state` 标记。

```
<single>
  <title>Sales events for $selected_state$</title>
  [...]
  <search>
    <query>source="my_data_source" | iplocation IP | lookup geo_us_states longitude as lon, latitude as lat | search
featureId=$selected_state$| stats count</query>
    <earliest>-7d@h</earliest>
    <latest>now</latest>
    <sampleRatio>1</sampleRatio>
```

```
</search>
[...]
</single>
```

显示或隐藏内容

要在用户单击后显示或隐藏内容，请使用您在仪表板元素中以 `depends` 或 `rejects` 属性更新的标记。您可以在设置或取消设置标记之后，用这些属性控制显示或隐藏行为。

隐藏元素不会阻止任何搜索元素在后台的运行。

配置动态显示

您可能只想在用户单击仪表板中的元素时显示面板。为面板添加一个 `depends` 属性针对要显示的面板设置 `show_panel` 标记。

```
<panel depends="$show_panel$">
```

用户单击仪表板中的元素后，请使用上下文钻取 `<set> show_panel` 标记。

```
<drilldown>
  <set token="show_panel">true</set>
</drilldown>
```

在单击事件之前，标记设置取消，面板不显示。用户单击已配置上下文钻取的元素之后，设置 `show_panel` 标记并显示面板。

示例

此仪表板会按来源类型显示有事件计数的表格。用户单击特定表格行之后，会出现其他可视化。可视化将显示所选源类型的事

件。

用户单击表格中的 `splunkd_conf` 源类型后，此屏幕显示仪表板。

The screenshot shows a dashboard with two main sections. On the left, there is a table titled "Event counts by sourcetype" with the following data:

sourcetype	count
first_install-too_small	8
mongod	230
scheduler	58
splunk_archiver-too_small	49
splunk_web_access	861
splunk_web_service	968
splunkd	468642
splunkd_access	5567
splunkd_conf	2
splunkd_stderr	3

Below the table are navigation controls: "«上一页" (Previous page), "1" (selected), "2" (next), "下一页»" (Next page), and search/filter buttons.

On the right, there is a panel titled "Recent events for splunkd_conf" showing two log entries:

i	时间	事件
>	18/06/05 8:28:09.205	{ [-] component: ConfDeployment data: { [+] } datetime: 06-05-2018 08:28:09.205 +0100 log_level: INFO } 显示为原始文本 host = debianSplunk source = /opt/splunk/var/log/splunk/conf.log sourcetype = splunkd_conf
>	18/06/05 8:25:38.914	{ [-] component: ConfDeployment data: { [+] } datetime: 06-05-2018 08:25:38.914 +0100 log_level: INFO } 显示为原始文本 host = debianSplunk source = /opt/splunk/var/log/splunk/conf.log sourcetype = splunkd_conf

控制面板显示

此示例中的动态行为包括在用户单击表格行之后显示面板和生成自定义搜索结果。首先 `<drilldown>` 会设置控制面板显示的标记。事件列表面板使用 `depends` 属性以针对要显示的面板设置 `show_panel`。

自定义仪表板内容

在 `<drilldown>` 中设置标记还有助于在仪表板中生成自定义内容。此示例中的 `selected_value` 标记设置为单击来源类型值。

驱动事件列表可视化的搜索使用 `selected_value` 标记生成单击来源类型的结果。也可以使用 `selected_value` 标记自定义面板标题。

仪表板源代码

```
<dashboard>
  <row>
    <panel>
      <table>
        <title>Event counts by sourcetype</title>
        <search>
          <query>index=_internal | stats count by sourcetype</query>
        </search>
        <drilldown>
          <set token="show_panel">true</set>
          <set token="selected_value">$click.value$</set>
        </drilldown>
      </table>
    </panel>
    <panel depends="$show_panel$">
      <event>
        <title>Recent events for $selected_value$</title>
        <search>
          <query>index=_internal sourcetype=$selected_value$ </query>
          <earliest>$earliest$</earliest>
          <latest>$latest$</latest>
        </search>
        <option name="count">5</option>
      </event>
    </panel>
  </row>
</dashboard>
```

配置条件式行为

您可能想要根据用户单击的元素或值显示不同的仪表板内容。您可以使用 `<drilldown>` 中的 `<condition>` 元素定义条件式标记设置。这有助于自定义仪表板中响应行为。

示例

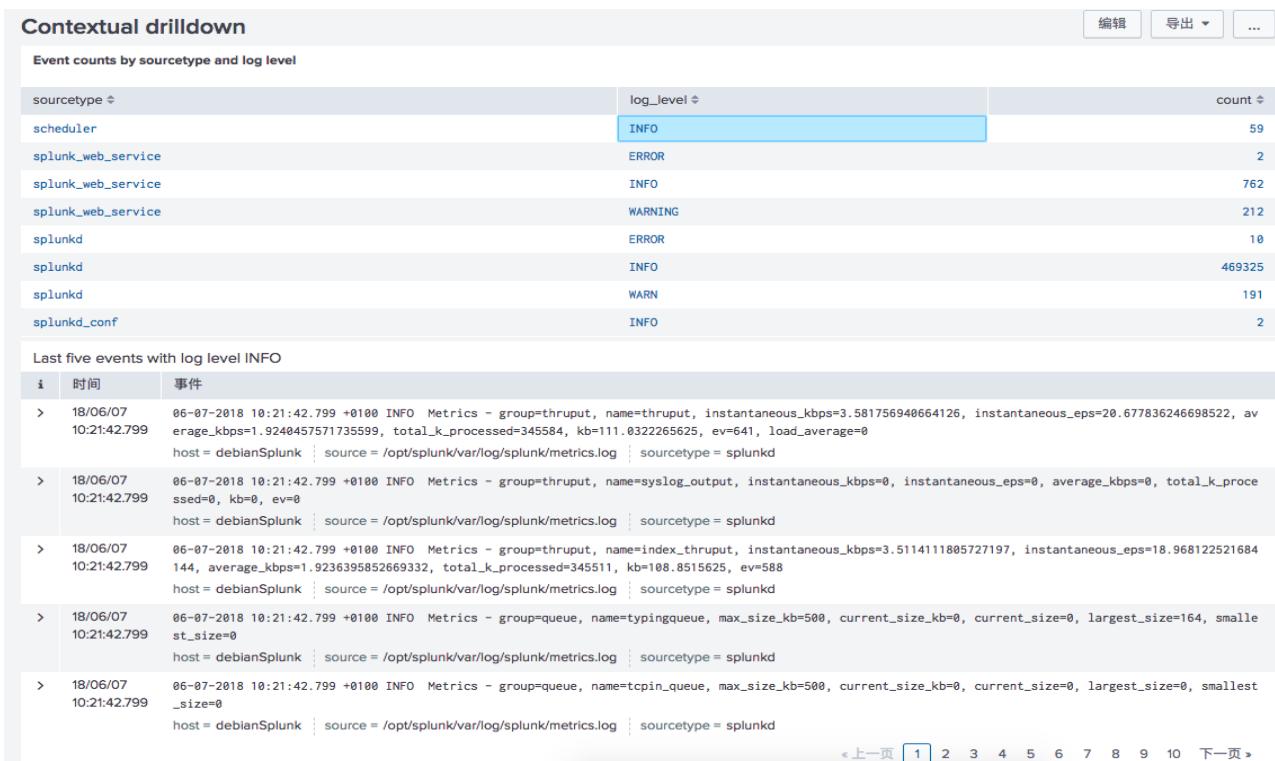
表格将按 `sourcetype` 和 `log_level` 显示事件计数。

Event counts by sourcetype and log level		
sourcetype	log_level	count
scheduler	INFO	8
splunk_web_service	INFO	675
splunk_web_service	WARNING	48
splunkd	ERROR	5
splunkd	INFO	49682
splunkd	WARN	168
splunkd_conf	INFO	3

如果用户单击表格中的 `sourcetype` 值，仪表板将显示所选来源类型的单值聚合事件。



如果用户单击 `log_level` 值，将显示所选日志等级的事件清单。



设置条件式钻取行为

上下文 `<drilldown>` 将 `<condition>` 元素包括在内以根据用户单击位置设置相应的标记值。

要处理不同单击位置，表格中的每个 `field` 或列都有 `<condition>` 元素。例如，如果用户单击 `sourcetype` 列中的值，`<condition>` 会定义标记设置。

```
<condition field="sourcetype">
  <set token="selected_sourcetype">$click.value2$</set>
  <set token="show_single_value">true</set>
  <unset token="show_event_list"></unset>
</condition>
```

在此 `<condition>` 的钻取操作会设置条件式内容自定义和显示。

条件式行为	源代码（位于 <code><condition></code> ）	详细信息
生成自定义搜索结果	<pre><set token="selected_sourcetype">\$click.value2\$</set> <set token="show_single_value">true</set> <unset token="show_event_list"></unset></pre>	<p><code>selected_sourcetype</code> 标记值代表已单击的来源类型。</p> <p><code>\$click.value2\$</code> 预定义标记将捕获单击表格单元值。标记值是生成自定义可视化的搜索的一部分。</p>

控制面板显示

```
<set token="show_single_value">true
</set>
<unset token="show_event_list">
</unset>
```

要控制用户单击来源类型之后显示哪些面板，请 `set show_single_value` 标记并 `<unset> show_event_list`。

结合 `depends` 属性，这些标记更新会触发响应的隐藏和显示行为。

与配置用于处理 `log_level` 列中用户单击的 `<condition>` 相似。

仪表板源代码

```
<dashboard>
  <label>Contextual drilldown</label>
  <row>
    <panel>
      <table>
        <title>Event counts by sourcetype and log level</title>
        <search>
          <query>index=_internal | stats count by sourcetype, log_level</query>
        </search>
        <drilldown>
          <condition field="sourcetype">
            <set token="selected_sourcetype">$click.value2$</set>
            <set token="show_single_value">true</set>
            <unset token="show_event_list"></unset>
          </condition>
          <condition field="log_level">
            <set token="selected_log_level">$click.value2$</set>
            <set token="show_event_list">true</set>
            <unset token="show_single_value"></unset>
          </condition>
        </drilldown>
      </table>
    </panel>
  </row>
  <row>
    <panel depends="$show_single_value$">
      <title>Event count for $selected_sourcetype$</title>
      <single>
        <search>
          <query>index=_internal sourcetype=$selected_sourcetype$ | stats count</query>
        </search>
        <option name="colorMode">block</option>
        <option name="drilldown">all</option>
        <option name="rangeColors">["0x65a637", "0x6db7c6", "0xf58f39", "0xd93f3c"]</option>
        <option name="rangeValues">[0,30,100]</option>
        <option name="underLabel">events</option>
        <option name="useColors">1</option>
      </single>
    </panel>
    <panel depends="$show_event_list$">
      <title>Last five events with log level $selected_log_level$</title>
      <event>
        <option name="count">5</option>
        <search>
          <query>index=_internal log_level=$selected_log_level$</query>
        </search>
      </event>
    </panel>
  </row>
</dashboard>
```

仪表板中的标记用法

标记就像是程序变量。标记名称代表可以更改的值，如表单输入中的用户选择。您可使用标记访问并传递这些值以新建更多交互仪表板。

在 Splunk 软件预定义某些标记，以提供环境、上下文或用户单击事件信息。例如，您可以使用钻取中的 `$click.value2$` 预定

义标记访问用户单击的表格单元格值。

您还可以新建自定义标记以实施交互行为。例如，定义您可以设置或取消设置的 \$show_panel\$ 标记以控制面板显示。

要快速查看通用标记命令，注意您可以点击“开始”中的链接访问 Splunk 仪表板快速参考指南。

使用案例

您可以使用标记在许多上下文中新建交互仪表板行为。

使用情况下 下文	描述
搜索字符串	通过将标记包含在内来代表动态值，自定义搜索字符串。搜索运行时会使用标记值。
搜索事件处理 程序	搜索事件处理程序代表搜索状态更改（如搜索已完成、正在搜索或取消的时间）。您可以将事件处理程序添加到 <search> 元素并使用处理程序中的预定义标记访问搜索任务元数据或第一个结果行数据。 您可以将来自搜索处理程序的标记值传递到其他仪表板元素以控制行为或内容。
表单输入	表单输入使用标记代表用户选择或键入的值。当添加一个输入至表单时，会为此自动生成一个标记。必要时，您可以自定义标记名称。 如果表单有多个时间挑选器输入，标记会将单个时间挑选器与表单中的一个或多个可视化连接。用户时间范围选择会控制使用该标记的可视化的搜索时间范围。 在表单中使用 map 命令时，使用两个美元符号 (\$\$) 指定变量字符串。例如， \$\$count\$\$。
设置页面加载 时的标记	通过在 <init> 元素设置标记值，在仪表板加载时显示自定义初始内容。
钻取	使用标记配置钻取行为。使用预定义和自定义标记，您可以自定义链接搜索、仪表板或 URL 中的内容。您还可以使用标记在同一个仪表板中新建交互行为。
定义图表平移 和缩放区域	使用预定义标记定义图表的平移和缩放区域。

在搜索中使用标记

标记在仪表板中捕获和传递数值。标记值来自不同的来源，包括表单输入和可视化的预定义标记值。搜索可以访问标记值。

在搜索中，标记名称语法使用 \$...\$ 分隔符。比如，如果您将表单输入标记定义为 field_tok，则您可以在搜索中将标记指定为 \$field Tok\$。以下是一个示例：

```
<search>
index=_internal source=*splunkd.log | stats count by $field Tok$
</search>
```

有关访问标记值的高级语法，请参阅“[标记过滤器](#)”。

定义搜索标记

您可以为仪表板设置搜索标记，以显示搜索任务元数据或控制仪表板行为。

使用搜索标记有多种方式。如下为一些使用案例示例。

- 包括可视化标题中的搜索结果计数。
- 如果搜索不返回任何结果，则运行其他搜索或隐藏面板。
- 如果搜索出现故障，则隐藏或显示面板。

使用搜索标记还有多种高级选项。选项包括以下内容：

- 使用 HTML 显示可视化元素下面的搜索时间范围。
- 建立自定义 HTML 元素并将搜索结果作为标记嵌入。
- 基于特定标记 eval 表达式的结果定义标记值。

搜索事件元素和任务属性

您可以在简化 XML 仪表板中使用若干搜索事件处理程序。

处理程序名称	访问搜索任务属性？	访问第一个结果行？
<progress>	是	是
<done>	是	是
<cancelled>	否	否
<error>	否	否
<fail>	否	否

在搜索事件处理程序中，您可以使用标记访问特定任务属性。例如，以下为部分常用任务元数据标记。

- \$job.earliestTime\$: 初始任务开始时间。
- \$job.latestTime\$: 搜索任务的最晚时间记录。
- \$job.resultCount\$: 搜索任务返回的结果数。
- \$job.runDuration\$: 完成搜索需要的时间（以秒为单位）。
- \$job.messages\$: 搜索任务生成的错误和/或调试消息列表。

要了解更多搜索任务属性的内容，请参阅《搜索手册》中的“查看搜索任务属性”。

用于动态显示的搜索标记示例

如下为 <search> 元素的示例，所针对的是，如果不返回任何搜索结果，则仪表板将隐藏面板。

```
<search id="search_logic">
    <query>$index_switcher$ | top sourcetype</query>
    <earliest>-60m@m</earliest>
    <latest>now</latest>

    <progress>
        <!-- match attribute for condition uses eval-like expression (see Splunk search language 'eval' command) -->
        <!-- logic: if resultCount is 0, then show a static html element, and hide the chart element -->
        <condition match="'job.resultCount'== 0">
            <set token="show_html">true</set>
        </condition>
        <condition>
            <unset token="show_html"/>
        </condition>
    </progress>
</search>
```

关于更多的示例，请参阅“Splunk 仪表板示例应用”。

为仪表板自定义逻辑

将自定义逻辑添加到带有 <condition match=" "> 和 <eval> 元素的仪表板。

对于 <condition> 和 <eval> 元素，所有来自事件以及已提交标记模型的数据都将在 Eval 表达式中用作变量。

标记语法

自软件版本 6.4 起，您可以使用 \$...\$ 分隔符或 <eval> 或 <condition match=" "> 语句中的标记的单引号分隔符。例如，以下这两种选项都是有效的。

- <condition match="\$job.resultCount\$ > 0">

- <condition match="'job.resultCount' > 0">

定义条件匹配

使用 `<condition match=" ">` 元素以定义条件式行为。以下示例根据结果计数任务属性控制标记值。

```
<condition match="$job.resultCount$ == 0">
<set token="show_table_query">true</set>
</condition>
```

您还可以使用仪表板 `eval` 表达式以定义匹配条件。如下为根据所选时间范围跨度是否超过一天而使用 `<condition match=" ">` 以设置标记值的示例。

```
<condition match="relative_time(now(), earliest) - relative_time(now(), latest) > 86400">
    <!-- Selected time range spans more than a day, use summary search -->
<set token="table_query">index=my_summary_index | timechart count</set>
</condition>
```

故障排除任务属性访问权限

默认情况下，任务属性在仪表板内不可用。如果源代码中的条件式逻辑语句无法像预期地那样应用于任务属性，添加搜索事件处理程序以访问自定义标记中的任务属性。请在条件式逻辑语句中使用自定义标记。

在此示例中，`$search_results$` 标记在 `<search>` 事件处理程序中获得 `$job.resultCount$` 任务属性值。条件式逻辑语句会评估 `$search_results$` 标记并相应地设置 `$show_panel$` 标记。

```
[...]
<search>
    <query>index=_internal </query>
    <earliest>-24h@h</earliest>
    <latest>now</latest>
    <done>
        <set token="search_results">$job.resultCount$</set>
    </done>
</search>
<drilldown>
    <condition match="$search_results$ != 0">
        <set token="showPanel">true</set>
    </condition>
</drilldown>
[...]
```

使用条件式语句中的字符串

如果您正在使用 `<condition match=" " ">` 语句评估字符串值（如来自第一个结果行的源类型名称），将转义双引号放在字符串周围。这将可防止仪表板分析器将引号作为特殊字符处理。

以下示例设置条件式标记设置，该设置因第一个结果行中的 `sourcetype` 字段值而异。第一个结果行中的 `sourcetype` 字段值是 `mongod`，将 `"show_table"` 标记设为 `true`。

要指定条件式匹配语句中的 `"mongod"` 字符串，请用同等的 HTML 字符实体代替双引号。

```
<condition match="'result.sourcetype'=='mongod'">
<set token="show_table">true</set>
</condition>
```

关于使用仪表板源代码中的特殊字符的更多信息，请参阅“[编辑简单 XML](#)”。

定义标记筛选和格式

您可以使用 `eval` 表达式逻辑以定义标记筛选和格式。比如，您可以将标记值设置到 `eval` 表达式的结果。

仪表板 `<eval>` 表达式功能

仪表板 `eval` 表达式具有和用于 SPL 查询的 `eval` 表达式语法相同的语法和语义。大部分同样的 `eval` 表达式功能在仪表板 `eval` 表达式和 SPL 版本的 `eval` 之间都是相同的。然而，也有一些重要的例外情况。

无法提供的仪表板 eval 表达式功能

- commands(X)
- searchmatch(X)
- exact(X)
- 加密哈希功能:

```
*md5(X)
*sha1(X)
*sha256(X)
*sha512(X)
*sigfig(X)
*spath(X, "Y")
```

eval 对于仪表板具有不同行为的表达式功能

- relative_time(X,Y): 使用客户端时区。
- strftime(X,Y): 使用客户端时区。
- strptime(X,Y): 使用客户端时区。

注意仪表板 eval 表达式中的正则表达式使用 JavaScript 正则表达式引擎的语法和语义，这也是非常重要的。这并不是用于 SPL eval 表达式的相同引擎。如果您正在搜索标记中使用正则表达式，请检查以确保语法和语义匹配 JavaScript。

要了解更多关于 eval 表达式功能的内容，请参阅《[搜索参考](#)》中的 eval。

自定义逻辑示例

您可以在 <condition> 事件处理程序元素中使用 Eval 表达式。以下是一个示例：

```
<condition match="[eval expression]">
. . . [conditional actions] . . .
</condition>
```

您还可以基于 eval 表达式的结果计算标记值。以下是一个示例：

```
<eval token="new_token">[eval expression]</eval>
```

定义表单输入的标记

所有表单输入具有为用户所选的输入值定义标记的标记属性。表单输入还具有进一步修改标记值的子 <prefix> 和 <suffix> 元素。对于多选选项，有可修改标记值的其他元素。请参阅“[定义多选输入的标记](#)”。

此代码段定义下拉列表的标记。下拉列表的所选选项提供标记的值。

```
<input type="dropdown" token="sourcetype_tok">
<label>Select a source type</label>
<default>splunkd</default>
<choice value="splunkd">splunkd</choice>
<choice value="splunk_web_access">splunk_web_access</choice>
<choice value="splunkd_ui_access">splunkd_ui_access</choice>
</input>
```

请参阅“[表单输入示例](#)”。

定义多选输入的标记

多选输入使用 <prefix>、<suffix>、<valuePrefix>、<valueSuffix> 和 <delimiter> 元素构建所选选项的多选搜索。多选搜索（即输入的标记值）确保输入将所有选择值传递给表单的搜索。

以下代码段显示如何构建多选标记的值。如果用户从多选输入选择 splunkd 和 splunk_web_access，则标记值为以下搜索片段：

```
(sourcetype = "splunkd") OR (sourcetype = "splunk_web_access")
```

搜索片段源自：

```

<prefix> + <valuePrefix> + [choice value] + <valueSuffix> + <delimiter> . . . + <suffix>
(           sourcetype = "         splunkd           "           _OR_           )
<input type="multiselect" token="sourcetype_tok">
<label>Select one or more source types</label>
<choice value="splunk_web_access">splunk_web_access</choice>
<choice value="splunkd">splunkd</choice>
<choice value="splunk_ui_access">splunk_ui_access</choice>
<choice value="splunkd_access">splunkd_access</choice>
<!--      Build multi-selection search:
(sourcetype ="value1" OR sourcetype ="value2" OR ...)>
-->
<prefix>(</prefix>
<valuePrefix>sourcetype ="/</valuePrefix>
<valueSuffix>"</valueSuffix>
<delimiter> OR </delimiter>
<suffix>)</suffix>
</input>

```

请参阅“[多选输入示例](#)”。

定义时间输入的标记

如果您拥有具有使用不同时间挑选器的面板的表单，则为时间输入使用标记，以指示用于每个面板的时间挑选器。要从时间挑选器访问最早和最晚值，使用以下针对标记的修饰符：

- \$timer_tok.earliest\$
- \$timer_tok.latest\$

不定义标记的时间输入是全局的。从这样的时间挑选器所选的值应用于所有不另外指定时间挑选器的可视化。

请参阅“[时间输入示例](#)”。

定义具有表单输入的条件式操作的标记

您可定义表单输入的条件式操作的标记。标记的值根据您指定的条件更改。例如，您可基于标记的条件值修改搜索或选择要显示的不同可视化。

条件式操作包括：

- 基于标记值修改搜索。
- 基于条件隐藏或显示面板和面板内容。
- 基于标记值选择要打开的视图。

条件式操作对表单输入和动态钻取可用。表单输入使用以下元素的各种组合：

元素	描述
<change>	您定义的条件的容器元素。
<condition>	基于输入选择的值设置条件。在条件式输入示例中，这是下拉列表的所选选项的值。
<link>	基于条件指定目标的链接。
<set>	定义标记的不同值。仪表板中的 <search> 元素获取此标记的值。 在条件式输入示例中，定义 earliest_tok 的标记值。
<unset>	删除之前设置的标记。 这对取决于要设置标记的条件式操作很有用。

请参阅“[具有表单输入的条件式操作](#)”中的示例。

用于访问表单输入的标签和值的预定义标记

Splunk® Enterprise 提供预定义标记以访问表单输入的标签和值。标记在以下输入中可用：

- 复选框
- 下拉列表
- 多选
- 单选按钮

标记	描述
标签	包含表单输入选项的指定名称。
值	包含表单输入选项的值。

这些标记对于自定义搜索或将所选的选项的标签放置于标题或面板或可视化的描述中很有用。

请参阅“访问表单输入的标签和值”。

设置页面加载时的标记

在仪表板或表单中添加一个 `<init>` 元素以重用内容或新建一个模板。当仪表板页面加载时会设置此元素内的标记值。

指南

在 `<dashboard>` 或 `<form>` 元素内，将页面加载时要设置的内容放置在以下标记对之间。

```
<init>
</init>
```

- 可以使用以下事件处理程序指定 `<init>` 标记内的标记设置。
 - `<condition>`
 - `<eval>`
 - `<link>`
 - `<set>`
 - `<unset>`
- 对于包含 `<init>` 元素的仪表板和表单，PDF 计划是禁用的。
- `<init>` 元素内所做的标记设置会覆盖 URL 查询字符串参数内所做的任何设置。
- 页面加载时的标记设置仅适用于简单 XML 仪表板。

示例

此表单设置了一个页面加载时的应用名称标记。该标记值通过 `|s$` 过滤器用于面板标签和搜索中，以在值的两边加上引号。

```
<form>
  <label>Application Monitoring: Exchange</label>
  <init>
    <set token="app_name">my_app_name</set>
  </init>
  <row>
    <panel>
      <title>Activity Monitoring: $app_name$</title>
      <search>
        <query>index=main app=$app_name|s$</query>
      </search>
    </panel>
  </row>
</form>
```

使用全局标记访问环境信息

访问与用户、Splunk 平台实例和使用全局标记的环境相关的详细信息。以下为可用标记：

名称	描述
----	----

\$env:user\$	当前用户的用户名
\$env:user_realname\$	当前用户的全名。
\$env:user_email\$	当前用户的电子邮件地址。
\$env:app\$	当前应用上下文
\$env:locale\$	当前区域
\$env:page\$	当前打开的页面
\$env:product\$	当前实例的产品类型
\$env:instance_type\$	表示当前实例是 Splunk Cloud 还是本地部署
\$env:is_cloud\$	表示当前实例是否是 Splunk Cloud。此标记只有当 "true" 的时候才会设置。
\$env:is_enterprise\$	表示当前实例是否是 Splunk Enterprise 部署。此标记只有当 "true" 的时候才会设置。
\$env:is_hunk\$	表示当前实例是否是 Hunk 部署。此标记只有当 "true" 的时候才会设置。
\$env:is_lite\$	表示当前实例是否是 Splunk Light 部署。此标记只有当 "true" 的时候才会设置。
\$env:is_lite_free\$	表示当前实例是否使用 Splunk Light Free 许可证。此标记只有当 "true" 的时候才会设置。
\$env:is_free\$	表示当前实例是否使用 Splunk Enterprise Free 许可证。此标记只有当 "true" 的时候才会设置。
\$env:version\$	当前实例的产品版本

定义动态钻取的标记

动态钻取的预定义标记

Splunk® Enterprise 为动态钻取提供预定义标记。预定义标记根据用户在可视化中单击的位置捕获值。

根据可视化类型不同，预定义的标记可用性和捕获的值有所不同。请参阅“简单 XML 参考”中的“预定义钻取标记”部分查看所有预定义标记的完整列表。

使用 `<drilldown>` 元素定义条件式操作的标记

您可以使用条件式钻取行为的标记，例如：

- 基于条件设置标记值。
- 为可视化中的多值字段选择一个值。
多值字段是多次显示不同值的字段。
- 基于标记值选择要打开的视图。
- 基于条件隐藏或显示面板。

条件式操作对表单输入和条件式钻取都可用。定义条件式钻取的标记使用以下标记的各种组合：

元素	描述
<drilldown>	定义仪表板或表单中字段的链接目标。您还可使用 <condition> 设置自定义操作的标记。
<condition>	将钻取操作的范围限制到特定字段。
<selection>	使用 <set> 元素为图表的平移和缩放功能设置时间窗口。 适用于面积图、柱形图或折线图。 请参阅《简单 XML 参考》中的“图表控件和 <selection> 条目”。
<link>	为钻取指定目标的链接。
<set>	定义标记的不同值。

<code><unset></code>	删除之前设置的标记值。 使用取决于要设置标记的条件式操作。
----------------------------	----------------------------------

使用 `<set>` 元素定义标记

使用 `<set>` 元素定义条件式使用的标记。在使用 `<set>` 元素定义标记时，您可使用另一个标记的值。例如，以下代码段定义 `sourcetype_tok` 标记。此标记捕获为字段 `sourcetype` 从 `<table>` 元素单击的值。

```
<drilldown>
  <condition field="sourcetype">
    <set token="sourcetype_tok">$click.value2$</set>
  </condition>
</drilldown>
```

您可在搜索中使用 `sourcetype_tok` 标记：

```
index=_internal sourcetype=$sourcetype Tok$ | timechart count by sourcetype
```

使用 `<condition>` 元素为可视化中多值字段选择一个值

多值字段是指在一个事件中出现多次，且每次出现都有不同值的字段。请参阅《知识管理员》手册中的“配置多值字段”。

如果具有显示多值字段的仪表板，您可以使用 `<condition>` 元素指定特定于单击字段值的钻取位置。以下示例基于字段的特定链接到不同的目标。`<link>` 元素获取每个条件的不同的预定义标记。

```
<drilldown>
  <condition field="badges">
    <link>
      /app/foursquare_vegas/vegas_badge_1?form.badge=$click.value2$
    </link>
  </condition>

  <condition field="venue">
    <link>
      /app/foursquare_vegas/vegas_venue_1?form.venue=$row.venue$
    </link>
  </condition>

  <condition field="links">
    <link>
      http://www.yelp.com/search?find_desc=$row.venue$&find_loc=Las+Vegas,+NV
    </link>
  </condition>
</drilldown>
```

获取标记的语法

使用 `$...$` 分隔符以访问标记值。例如，以下可视化的搜索访问 `field Tok` 标记。先前在 `field Tok` 标记中定义的表单输入。

```
index=_internal source=*splunkd.log | stats count by $field Tok$
```

标记过滤器

标记过滤器确保您正确捕获标记值。

筛选	描述
引号中的 wrap 值 <code>\$token_name s\$</code>	确保标记引用的值用引号括起来。在带引号的值内，转义所有引号字符“”。
HTML 格式 <code>\$token_name h\$</code>	请确保标记值对 HTML 格式有效。 默认情况下， <code><HTML></code> 元素的标记值使用此过滤器。
URL 格式 <code>\$token_name u\$</code>	请确保标记值用作 URL 有效。 默认情况下， <code><link></code> 元素的标记值使用此过滤器。

阻止元字符执行
\$token_name|n\$

防止默认标记过滤器运行。标记中没有字符会进行转义。

以下代码段使用 `|s` 过滤器将从标记返回的值用引号引起起来：

```
<search>
  <query>
    index=_internal sourcetype=$sourcetype_tok|s$ | timechart count by sourcetype
  </query>
</search>
```

如果 `sourcetype_tok` 的值为 `access_combined`, 则它构建以下搜索字符串：

```
index=_internal sourcetype="access_combined" | timechart count by sourcetype
```

转义 \$ 标记分隔符字符

如果您包括包含 `$` 字符的静态文本，则使用 `$$` 以转义标记分隔符值。

合并文本值与标记值

您可将从标记返回的值与文本值合并。基于标记值使用 `<set>` 元素设置条件式操作。

以下模板使用静态文本合并从预定义标记捕获的值 `click.value`。它将 `NewToken` 的值用引号括起来。

```
<set token="NewToken">sourcetype=$click.value|s$</set>
```

如果 `click.value` 的值为 `access_combined`, 则 `NewToken` 的值为以下搜索片段：

```
sourcetype="access_combined"
```

您可使用 `<set>` 元素的 `prefix` 和 `suffix` 属性指定标记值的静态文本。以下示例设置 `NewToken` 的值。它和模板示例是等效的：

```
<set token="NewToken" prefix="sourcetype="" suffix=""">$click.value$</set>
```

访问标记以显示或隐藏用户界面组件

您可使用标记值以按条件显示或隐藏用户界面组件。以下元素包含属性 `depends` 和 `rejects`。使用 `<set>` 和 `<unset>` 元素设置这些属性获取的标记值。

隐藏元素不会阻止任何搜索元素在后台的运行。

- `<row>`
- `<panel>`
- `<chart>`
- `<event>`
- `<html>`
- `<map>`
- `<single>`
- `<table>`
- `<input>`

例如，仅当已设置 `showChart` 标记时显示 `<chart>` 元素。

```
<chart depends="$showChart$">
```

定义平移和缩放图表控制的标记

Splunk® Enterprise 使用预定义标记以实现图表上的缩放功能。使用缩放功能，您可选择图表中数据系列的部分，它将在单独的图表中打开。请参阅“平移和缩放图表控制”。

在 `<selection>` 元素（即图表的子元素）内设置预定义标记的值。使用原始图表中的标记值显示缩放到选择的新图表。

标记	描述
----	----

<code>start</code>	在图表中选择的起始点和终点捕获 X 轴的值。
<code>end</code>	仅在图表的上下文中有效。将值分配到您定义的标记以访问仪表板中其他位置的值。
<code>start.<field></code>	捕获选择的 Y 轴值的值。<field> 代表在图表中显示的系列。
<code>end.<field></code>	仅在图表的上下文中有效。将值分配到您定义的标记以访问仪表板中其他位置的值。

有关显示如何缩放到时间图表中选择的示例，请参阅“平移和缩放图表控制”。

使用 *SplunkJS Stack* 的标记

如果您正在使用具有 JavaScript 扩展功能的 SplunkJS Stack，请参阅“Splunk 开发人员门户”上的“标记和数据绑定”以了解如何使用具有 JavaScript 的标记。

标记用法示例

表单输入示例

本示例显示表单输入中标记的基本用法。它使用下拉列表选择时间图表的来源类型。请参阅“定义表单输入的标记”。

<input> 元素定义由可视化的搜索获取的 sourcetype_tok。



```

<form>
  <label>Form example: source type time chart</label>
  <fieldset autoRun="true" submitButton="false">
    <input type="dropdown" token="sourcetype_tok">
      <label>Select a source type</label>
      <default>splunkd</default>
      <choice value="splunkd">splunkd</choice>
      <choice value="splunk_web_access">splunk_web_access</choice>
      <choice value="splunkd_ui_access">splunkd_ui_access</choice>
    </input>
  </fieldset>
  <row>
    <panel>
      <chart>
        <search>
          <query>
            index = _internal sourcetype=$sourcetype_tok$
            | timechart count by sourcetype
          </query>
          <earliest>-7d</earliest>
          <latest>-0d</latest>
        </search>
      </chart>
    </panel>
  </row>
</form>

```

多选输入示例

此示例显示如何使用静态文本和标记值构建表单输入的搜索字符串。这对构建多选选项很有用。请参阅“[定义多选输入的标记](#)”。

此示例使用 `<prefix>`、`<suffix>`、`<valuePrefix>`、`<valueSuffix>` 和 `<delimiter>` 元素构建多选搜索字符串。当用户选择 `splunkd` 和 `splunk_web_access` 时，它生成以下搜索字符串：

```
(sourcetype ="splunkd" OR sourcetype ="splunk_web_access")
```



```
<form>
<label>Form with multiselect</label>
<fieldset autoRun="false" submitButton="true">
<html>
<p>
  <strong>Multiselect choices</strong>
</p>
</html>
<input type="multiselect" token="sourcetype_tok" searchWhenChanged="false">
<label>Select one or more source types</label>
<choice value="">All</choice>
<choice value="splunk_web_access">splunk_web_access</choice>
<choice value="splunkd">splunkd</choice>
<choice value="splunk_ui_access">splunk_ui_access</choice>
<choice value="splunkd_access">splunkd_access</choice>

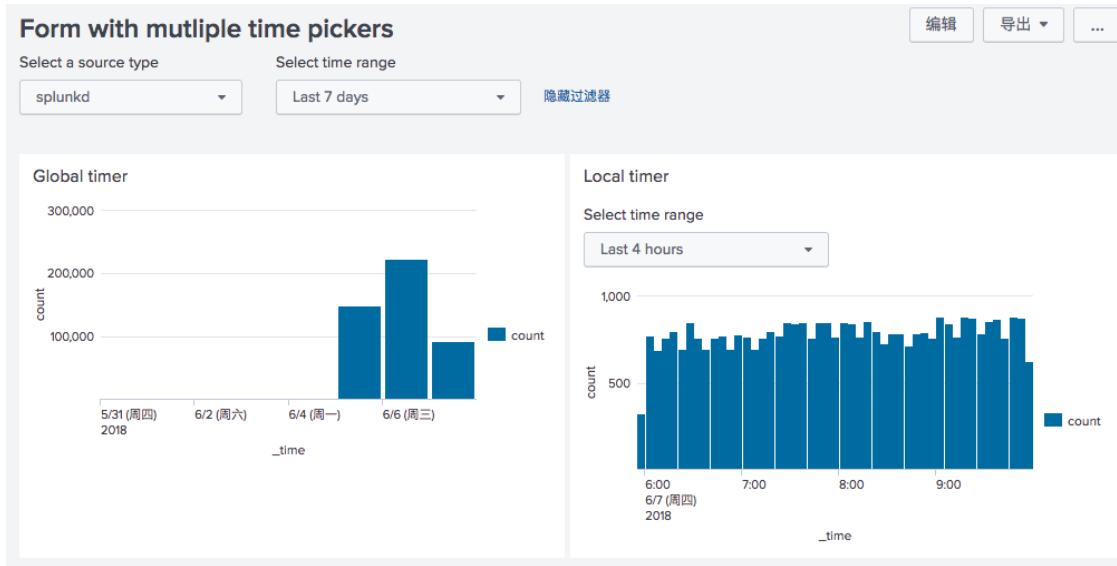
<!--      Build multiselect search:
  (sourcetype ="value1" OR sourcetype ="value2" OR ...)<!-->
<prefix>(</prefix>
<valuePrefix>sourcetype = "</valuePrefix>
<valueSuffix>"</valueSuffix>
<delimiter> OR <delimiter>
<suffix>)</suffix>

</input>
</fieldset>
<row>
<panel>
<title></title>
<chart>
<search>
  <query>index = _internal $sourcetype_tok$ | stats count by sourcetype</query>
  <earliest>-24h</earliest>
  <latest>now</latest>
</search>
<option name="charting.chart">line</option>
<option name="charting.axisY.scale">log</option>
</chart>
</panel>
</row>
</form>
```

时间输入示例

此示例显示如何使用表单中的全局和本地时间挑选器。它还显示如何访问时间输入标记的预定义修饰符。请参阅“[定义时间输入的标记](#)”。

此示例显示具有全局时间挑选器和本地时间挑选器的表单。<chart> 元素包含本地时间挑选器，并使用 local_time_input_tok 标记的修饰符访问最早和最晚值。



```

<form>
  <label>Form with mutliple time pickers</label>
  <description></description>
  <fieldset submitButton="false">
    <input type="dropdown" token="source_tok" searchWhenChanged="true">
      <label>Select a source type</label>
      <choice value="">All</choice>
      <search>
        <query>index=_internal | stats count by sourcetype</query>
        <earliest>-7d@h</earliest>
        <latest>now</latest>
      </search>
      <fieldForLabel>sourcetype</fieldForLabel>
      <fieldForValue>sourcetype</fieldForValue>
      <prefix>sourcetype=</prefix>
      <suffix></suffix>
      <default>splunkd</default>
    </input>

    <!-- Do not define token for global timer -->
    <input type="time" searchWhenChanged="true">
      <label>Select time range</label>
      <default>
        <earliest>-7d@h</earliest>
        <latest>now</latest>
      </default>
    </input>
  </fieldset>
</row>
<panel>
  <title>Global timer</title>
  <chart>
    <search>
      <query>index=_internal $source_tok$ | timechart count</query>
    </search>
  </chart>
</panel>
<panel>
  <title>Local timer</title>
  <!-- Define token for local timer -->
  <input type="time" searchWhenChanged="true" token="local_time_input_tok">
    <label>Select time range</label>
    <default>
      <earliest>-24h@h</earliest>
      <latest>now</latest>
    </default>
  </input>
  <chart>
    <search>
      <query>
        index=_internal $source_tok$ | timechart count
      </query>
    <!-- Use modifiers to token for a timer -->
    <earliest>$local_time_input_tok.earliest$</earliest>
    <latest>$local_time_input_tok.latest$</latest>
  </chart>
</panel>

```

```

</search>
</chart>
</panel>
</row>
</form>

```

具有表单输入的条件式操作

此示例显示如何使用具有表单输入的条件式操作。请参阅“[定义具有表单输入的条件式操作的标记](#)”。

此示例使用 `<change>`、`<condition>` 和 `<set>` 元素按条件设置所选时间的标签和设置最早时间标记。搜索获取最早时间标记以设置搜索的边界。此示例将 `label` 和 `value` 预定义标记用于输入选项。请参阅“[用于访问表单输入的标签和值的预定义标记](#)”。



注意：所有输入元素（时间输入除外）需要显示标记属性。在此示例中，输入元素定义标记 `period_tok`。但是，搜索从不获取此标记。

```

<form>
  <label>Use tokens with conditional input choices</label>
  <fieldset submitButton="false">
    <input type="radio" token="period_tok">
      <label>Select a time range</label>
      <choice value="-24h@h">Last 24 Hours</choice>
      <choice value="-7d@h">Last 7 Days</choice>
      <choice value="-30d@h">Last 30 Days</choice>
      <default>Last 24 Hours</default>

      <!-- set condition based on the label defined by <choice> -->
      <!-- Within each condition, specify a custom label for display -->
      <!-- Capture the selected value in the token, earliest_tok -->
      <change>
        <condition label="Last 24 Hours">
          <set token="date_label">Yesterday</set>
          <set token="earliest_tok">$value$</set>
        </condition>
        <condition label="Last 7 Days">
          <set token="date_label">Last week</set>
          <set token="earliest_tok">$value$</set>
        </condition>
        <condition label="Last 30 Days">
          <set token="date_label">Last month</set>
          <set token="earliest_tok">$value$</set>
        </condition>
      </change>
    </input>
  </fieldset>

```

```

<row>
  <panel>
    <title>Conditional Inputs</title>
    <chart>

      <!-- Display selected label in the title -->
      <title>$date_label$</title>

      <search>
        <query>index = _internal | timechart count by sourcetype</query>
        <!-- use the value of earliest_tok -->
        <!-- to set the time range -->
        <earliest>$earliest_tok$</earliest>
        <latest>now</latest>
      </search>

      <option name="charting.axisY.scale">log</option>
      <option name="charting.axisTitleX.text">Time periods</option>
      <option name="charting.axisTitleY.text">Events</option>
    </chart>
  </panel>
</row>
</form>

```

访问表单输入的标签和值

此示例显示如何使用标记访问表单输入的标签和值。请参阅“用于访问表单输入的标签和值的预定义标记”。

此示例使用可视化标题中所选单选按钮的标签。它使用所选单选按钮的值确定搜索的边界。



```

<form>
  <label>Use tokens with input choices to capture input labels and values</label>
  <fieldset submitButton="false">
    <input type="radio" token="period_tok">
      <label>Select a time range</label>
      <choice value="-24h@h">Last 24 Hours</choice>
      <choice value="-7d@d">Last 7 Days</choice>
      <choice value="-30d@d">Last 30 Days</choice>
      <default>Last 24 Hours</default>

    <change>
      <!-- use predefined input tokens to set -->
      <!-- tokens for the selected label and value -->
      <set token="date_label">$label$</set>
      <set token="earliest_tok">$value$</set>
    </change>

    </input>
  </fieldset>

```

```

<row>
  <panel>
    <title>Conditional Inputs</title>
    <chart>
      <!-- Display selected label in the title -->
      <title>Source Type by $date_label$</title>

      <search>
        <query>index = _internal | timechart count by sourcetype</query>
        <!-- use the value of earliest_tok -->
        <!-- to set the time range -->
        <earliest>$earliest_tok$</earliest>
        <latest>now</latest>
      </search>

      <option name="charting.axisY.scale">log</option>
      <option name="charting.axisTitleX.text">Time period</option>
      <option name="charting.axisTitleY.text">Events</option>
    </chart>
  </panel>
</row>
</form>

```

图表控制

本主题介绍查看图表中的数据的高级行为。

平移和缩放图表控制

平移和缩放功能可突出显示图表详细信息，并有选择性地在一个单独的面板中查看详细信息。平移和缩放在如下图表中可用：

- 柱形图
- 折线图
- 面积图

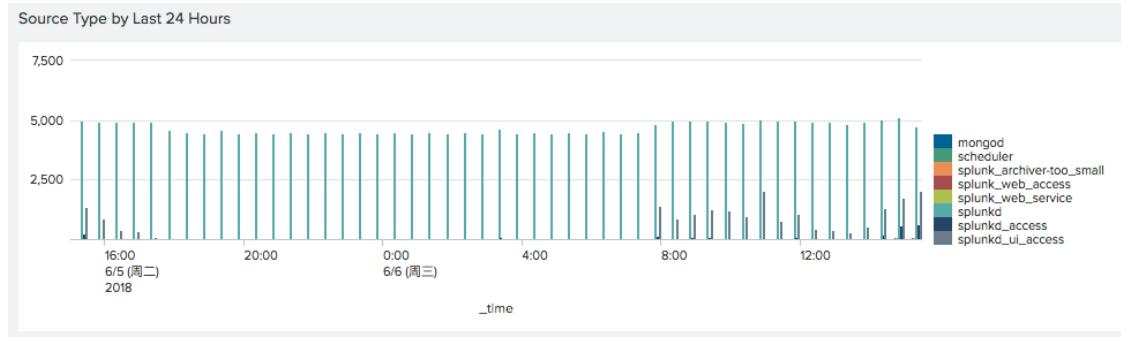
下面的示例显示如何使用平移和缩放图表的功能。

平移和缩放行为

以下仪表板显示图表，该图表显示七天时间内的来源类型。Y 轴使用对数刻度，以提供更多有意义的图形。此面板指定以下搜索。

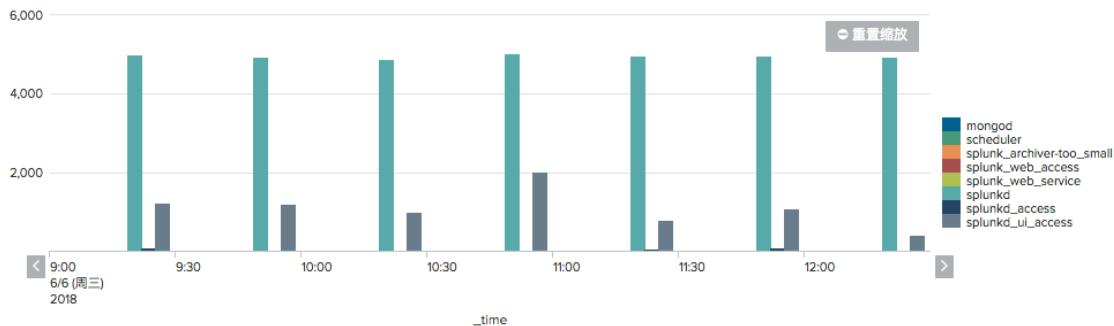
```
index=_internal | timechart count by sourcetype
```

下面的屏幕截图选择了两天的结果。



生成的图表放大了被选中部分，现在显示所选区域的详细信息。

- 使用沿着 X 轴的左箭头和右箭头移动选中的窗口，查看之前的或之后的图表。
- 单击重置缩放，返回到原始图表。

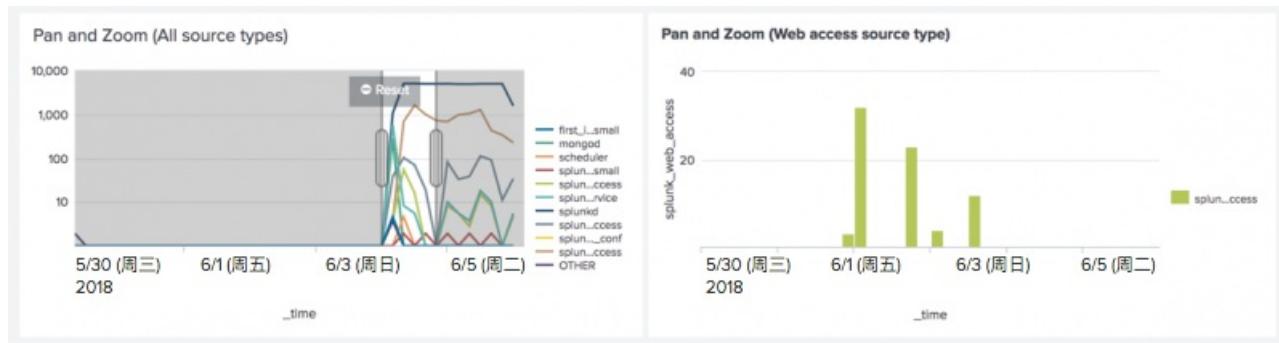


缩放到另一图表

您可指定平移和缩放行为以在一个单独的图表中显示结果。以下示例使用的基本示例与上文的“平移和缩放行为”中演示的示例相同。左边的图表列出了所有来源类型，也显示所选的一天。另一个图表仅针对选中的时间范围列出 `splunk_web_access` 来源类型。

您可拖动左边图表中的时间范围的边缘，以扩展时间范围。您也可移动选中的时间范围到左边或右边，以指定一个更早或更晚的时间范围。

下边的图表显示实现平移和缩放行为的标记值。



实现细节

要在单独的图表中显示缩放结果，首先要在简单 XML 中编辑基本图表。使用 `<selection>` 元素，为选中的时间范围设置标记值。

注意：有关标记的信息，请参阅“仪表板中的标记用法”。 “定义平移和缩放图表控制”部分为特定于平移和缩放行为的标记提供了详细信息。

```
$start$  
$end$
```

在选中时间范围的起始点和终点捕获 X 轴值的预定义标记。在本例中，捕获时间图表的起始点和终点时间。值以 epoch 时间表示。

```
$start.splunk_web_access$  
$end.splunk_web_access$
```

在选中的起始点和终点捕获指定系列的 Y 轴值。在本例中，值为字段 `splunk_web_access` 的事件数量。

`start` 和 `end` 标记仅在图表上下文中有效。将这些值分配给您定义的标记，以便您在整个仪表板中访问这些值。

```
<chart>  
  <title>Pan and Zoom (All source types)</title>  
  <search>  
    <query>  
      index=_internal | timechart count by sourcetype  
    </query>  
    <earliest>-7d@h</earliest>  
    <latest>now</latest>  
  </search>  
  . . .
```

```

<selection>
  <set token="selection_earliest">$start$</set>
  <set token="selection_latest">$end$</set>
  <set token="start_splunk_web_access">$start.splunk_web_access$</set>
  <set token="end_splunk_web_access">$end.splunk_web_access$</set>
</selection>
. .
</chart>

```

在目标图表中，使用 `$selection_earliest$` 和 `$selection_latest$` 访问选中的时间范围。

```

<chart>
  <title>Pan and Zoom (Web access source type)</title>
  <search>
    <query>
      index=_internal sourcetype=splunk_web_access
      | timechart count by sourcetype
    </query>
    <earliest>$selection_earliest$</earliest>
    <latest>$selection_latest$</latest>
  </search>
. .
</chart>

```

HTML 面板显示了由 `$start$` 和 `$selection$` 标记捕获的值。

```

<html>
  <h3>Token values for the splunk_web_access selection</h3>
  <table border="0" cellpadding="12" cellspacing="0">
    <tr>
      <td>
        <p><b>Time range (epoch time)</b></p>
        <p><b>$selection_earliest$</b>: $selection_earliest$<br /><b>$selection_latest$</b>: $selection_latest$</p>
      </td>
      <td>
        <p><b>Count at the begining and end of time range.</b></p>
        <p><b>$start_splunk_web_access$</b>: $start_splunk_web_access$<br /><b>$end_splunk_web_access$</b>: $end_splunk_web_access$</p>
      </td>
    </tr>
  </table>
</html>

```

图表叠加

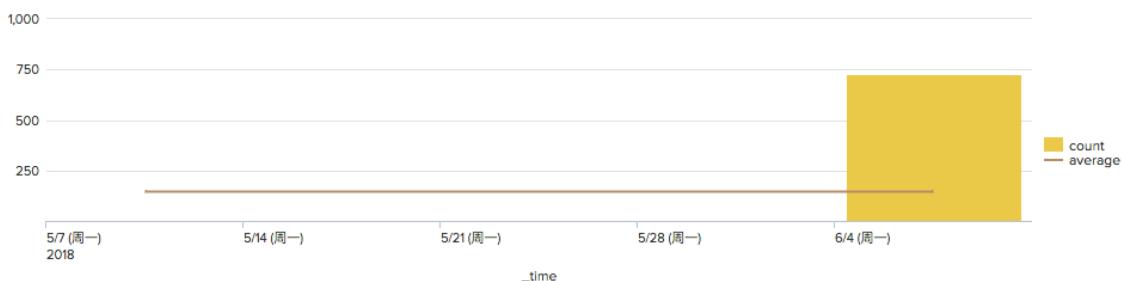
使用图表叠加，在单个图表上表示两个不同的系列。可在柱形图、面积图或另一个折线图的顶部，将搜索结果的一个系列突出显示为折线图。

使用叠加时，可在单个轴或双轴上指定叠加值。使用单个轴情况下，可绘制针对同一 Y 轴的叠加值和搜索结果。对于双轴，可指定第二个 Y 轴来表示叠加值。

图表叠加示例（单个轴）

本示例显示了 `splunk_web_access` 来源类型事件在以周为单位的时间图表上的计数。在本图表上叠加的是每周这些事件的平均计数。

Chart Overlay (Single Axis)



下面是新建本图表的搜索：

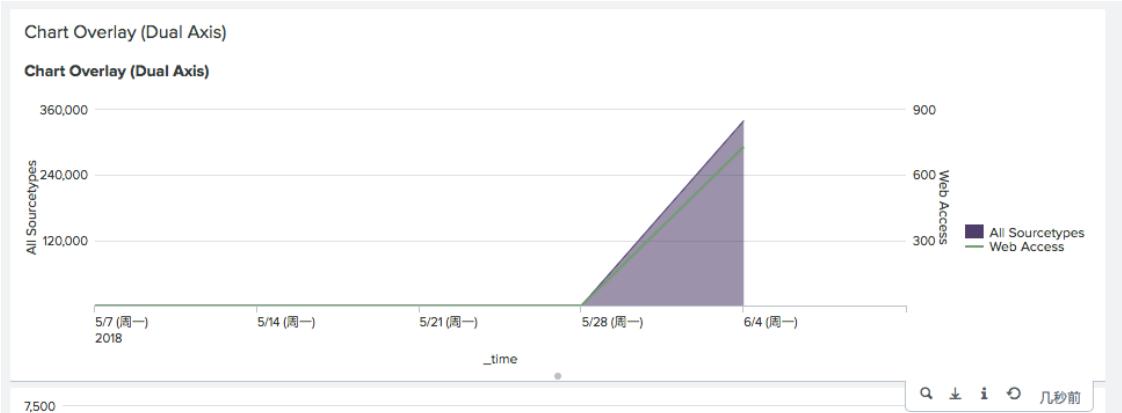
```
index=_internal sourcetype=splunk_web_access | timechart span=1week count | eventstats avg(count) as average | eval average=round(average,0)
```

可使用“可视化编辑器”来新建叠加。

1. 从仪表板，单击编辑 > 编辑面板。
2. 添加指定以下内容的面板：
 - 内容标题：图表叠加（单个轴）
 - 搜索字符串：以上列出的搜索字符串。
 - 时间范围：30 天。
3. 对于图表叠加面板，单击编辑属性图标。单击图表叠加。
4. 在叠加字段中单击。从可选字段中选择平均值，作为叠加。
5. 对于按轴查看，单击关闭。
本示例没有指定第二个 Y 轴。

图表叠加示例（双轴）

本示例对照所有来源类型的总数，叠加了 `splunk_web_access` 来源类型的事件计数，该图表对照单独的 Y 轴，绘制了“Web 访问”的总数。



下面是新建本图表的搜索：

```
index=_internal sourcetype=* | timechart span=1week count as "All Sourcetypes" count(eval(sourcetype="splunk_web_access")) as "Web Access"
```

可使用“可视化编辑器”来新建叠加。

1. 从仪表板，单击编辑 > 编辑面板。
2. 添加指定以下内容的面板：
 - 内容标题：图表叠加（双轴）
 - 搜索字符串：以上列出的搜索字符串。
 - 时间范围：30 天。
3. 对于图表叠加面板，单击编辑属性图标。单击图表叠加。
4. 在叠加字段中单击。从可选字段中选择 Web 访问，作为叠加。
5. 对于按轴查看，单击打开，以指定第二个 Y 轴。
6. 对于标题，单击自定义。在相邻文本字段中，键入 Web 访问以指定第二个轴的标题。

7. 对于刻度，单击继承，以便继承第一个 Y 轴的刻度选择。

管理和共享仪表板

配置仪表板权限

了解如何管理仪表板和面板搜索权限。

管理仪表板权限

一个仪表板即为一个知识对象。您为自己和其他人配置仪表板权限的能力取决于您的角色。

下表列出了新的 Splunk 平台实现随附的默认角色所包含的权限管理功能。

默认 Splunk 角色	权限管理能力
用户	新建您个人专用的仪表板。
高级用户、管理员	新建您个人专用的仪表板。 与某个应用的用户或所有应用的用户共享专用仪表板。 按角色设置对仪表板的读写访问权限。

您的实现可能针对用户设有不同的角色集。或者它可能有默认角色，但权限管理功能可能会在它们之间有所不同。如果想了解您的角色的权限管理功能的更多信息，请与 Splunk 管理员联系。有关基于角色的知识对象权限管理的更多信息，请参阅《知识管理器手册》中的“管理知识对象权限”。

管理面板搜索权限

驱动仪表板面板的搜索是独立于仪表板的知识对象。此搜索有其自己的可配置权限。内联或即席搜索，而不是已保存的搜索不是知识对象，因此无需权限即可查看由即席搜索驱动的可视化。为限制访问即席搜索，管理员必须限制访问搜索依赖的其中一个知识对象，如索引或来源。

面板搜索权限

面板搜索可使用新建此搜索的人（搜索所有者）的权限来运行，或查看仪表板的人（搜索用户）的权限来运行。搜索用户上下文会影响结果以及不同用户可在仪表板面板中看到的内容。

根据您想提供的结果数据访问权限，您可以在报表列表页面中调整搜索的权限上下文。在此页面中找到搜索，选择编辑 > 编辑权限，然后修改设置以决定是用所有者还是用户上下文来运行搜索。

有关设置仪表板和其他知识对象权限的其他信息，请参阅《知识管理员》手册中的“管理知识对象权限”。

指定新仪表板的权限

通过搜索或仪表板页面新建新仪表板时，可以配置其权限。选择以下各选项中的其中一项。

选项	描述
专用	只有您拥有查看和编辑仪表板的权限。仪表板对其他用户不可见。
在应用中共享	对属于在仪表板新建时所用的应用上下文的其他用户，仪表板为可见。例如，如果您在搜索和报表应用中新建了一个仪表板，则此仪表板对此上下文中的其他用户可见。其他用户可能也可以对此仪表板进行编辑，具体取决于他们的权限。

更新仪表板权限

新建仪表板后，您可以更改权限：

1. 导航到搜索和报表中的仪表板页面。
2. 找到要更新权限的仪表板。
3. 在操作下，选择编辑 > 编辑权限
4. 根据您的角色和权限，指定以下信息。
 - 选择所有者使此仪表板为专用。
 - 选择应用将此仪表板在当前应用上下文中共享或在 Splunk 平台实例的所有应用中共享。

- 赋予读取和写入权限
- 为其他系统用户和/或角色配置读取（查看）和写入（编辑）权限。

生成仪表板 PDF

仪表板 PDF 生成包括以下选项。

- 生成并保存仪表板 PDF。
- 打印仪表板 PDF。
- 计划 PDF 电子邮件交付。

这里是 PDF 生成的一些限制。有关详细信息，请参阅“PDF 生成限制”。

有关以电子邮件附件的形式发送计划报表 PDF 的信息，请参阅《报表手册》中的“计划报表”。

生成和打印仪表板 PDF

生成仪表板 PDF

1. 在仪表板中，选择导出 > 导出 PDF。所生成的 PDF 在浏览器窗口中显示。
2. 从浏览器窗口查看、下载或打印 PDF。

打印仪表板 PDF

1. 在仪表板中，选择导出 > 打印。将打开您浏览器的默认打印驱动程序及打印设置。

实时搜索和集成的 PDF 生成

PDF 生成为实时搜索提供特别时间范围处理。实时搜索、报表或仪表板 PDF 显示搜索时间窗（相对于 PDF 生成时间）的结果。例如，为时间窗为五分钟的实时搜索生成 PDF 时，PDF 显示过去五分钟的搜索结果。

搜索时间范围为“实时所有时间”的仪表板面板 PDF 将一直显示搜索结果。

计划 PDF 交付

经授权的用户可为仪表板计划 PDF 交付。要在搜索中向需要 SMTP 身份验证的邮件服务器发送电子邮件通知，您必须分配到 admin 角色。要在搜索中向不需要 SMTP 身份验证的邮件服务器发送电子邮件通知，需要 list_settings 功能。默认情况下，只有 admin、splunk-system-role 和 can_delete 角色分配了 list_settings 功能。

如果您想要允许不再属于任何角色的用户在搜索中使用 sendemail 命令发送电子邮件通知，您必须为他们分配 list_settings 功能。关于角色和功能的更多信息，请参阅《确保 Splunk Enterprise 安全》中的“关于定义具有功能的角色”。要设置 PDF 交付，选择导出 > 计划 PDF 交付。确保电子邮件通知设置在计划 PDF 交付之前已配置。

有关配置告警的更多信息，请参阅《告警手册》中的“配置电子邮件通知设置”。

计划的 PDF 交付不适用于包含表单的仪表板。

在计划的仪表板交付中使用标记

Splunk 软件提供标记，您可以使用这些标记在电子邮件字段中包含搜索生成的信息。对于计划的 PDF 交付，您可在下面的电子邮件字段中使用标记：

- 主题
- 消息
- 页脚

用下面的语法访问标记值：

\$<token-name>\$

例如，将下面的标记放入计划的 PDF 交付的主题字段，参考包含仪表板的应用。

来自 \$app\$ 的搜索结果

对电子邮件通知可用的标记

您可以使用标记用搜索、服务器或仪表板信息动态填充电子邮件通知。

请参阅“在电子邮件通知中使用标记”以了解有关仪表板元数据和其他可用标记的详细信息。

仪表板的计划 PDF 交付

仪表板的计划 PDF 交付：

- 对于要计划的仪表板，选择导出 > 计划 PDF 交付。
- 选择计划 PDF 交付复选框以启用 PDF 交付。

编辑 PDF 计划

仪表板 Buttercup Games

计划 PDF

计划 每小时运行 ▾

时间 15 分钟(整点后)

发送电子邮件至 用逗号分隔的电子邮件地址列表。
显示抄送和密件抄送

优先级 正常 ▾

主题 Splunk Dashboard: '\$dashboard.label\$'

消息 A dashboard was generated for
\$dashboard.label\$

类型 HTML 和纯文本 纯文本

纸张大小 Letter ▾

纸张布局 纵向 横向

发送测试电子邮件 预览 PDF

取消 保存

- 选择一个计划。

如果您选择了运行 Cron 计划，请参阅 cron 示例。

- 指定电子邮件详情。

您可在主题和消息字段中使用标记。

- 发送、抄送，以及密送给电子邮件收件人。
指定一个逗号分隔的电子邮件收件人列表。
- 优先级
优先级是否强制执行取决于您的电子邮件客户端。
- 主题
- 消息

- 选择纸张大小和纸张布局。

- 单击保存以保存计划交付设置。

要中止仪表板 PDF 的计划电子邮件交付

- 对于要中止 PDF 交付的仪表板，选择导出 > 计划 PDF 交付。
- 取消选择计划 PDF 交付。
- 单击保存以保存计划交付设置。

计划视图报表

当您计划交付的 PDF 时，新建名为计划视图的报表。计划视图不出现在设置下的搜索、报表和告警中。它们只作为 savedsearches.conf 中的段落出现。计划视图的命名约定是 _ScheduledView_<dashboard_name>，dashboard_name 是相应仪表板的名称。这是监视正在运行以生成这些仪表板的搜索数的最佳做法，特别是当您遇到了部署的并发搜索限制问题时。

删除仪表板时，相应的计划视图被孤立，但仍然存在。默认情况下，每 24 个小时删除一次孤立的计划视图。如果您想要更改或禁用设置频率，您可以在 limits.conf 中使用以下设置。

设置	描述	默认
enable_reaper = <boolean>	控制计划视图获取程序是否运行。获取程序删除孤立的计划视图。	true
reaper_freq = <integer>	控制计划视图获取程序运行的频率，以秒为单位。	86400 (24 小时)。

不要更改默认目录中的配置文件。有关如何编辑配置文件的信息，请参阅“关于配置文件”。

指定 PDF 交付的 cron 计划

您可以使用 cron 符号定义自定义交付计划。选择 Cron 选项输入一个计划。

Cron 参数

指定 cron 表达式时，只有五个 cron 参数可用，而非六个。用于年的第六个参数（在 cron 符号的其他形式中常见）不可用。

cron 参数，* * * * *，对应于 minute hour day month day-of-week。

表达式示例

以下为 cron 表达式的一些示例。

```
*/5 * * * *      Every 5 minutes.
*/30 * * * *     Every 30 minutes.
0 */12 * * *     Every 12 hours, on the hour.
*/20 * * * 1-5   Every 20 minutes, Monday through Friday.
0 9 1-7 * 1       First Monday of each month, at 9am.
```

用于 PDF 打印的其他配置

Splunk Enterprise 用户可以为 PDF 打印指定以下配置。

- 要打印的最大表格行号
- 生成 PDF 的超时设置
- 是否包含徽标
- 允许使用非拉丁字体

注意：如果您使用的是 Splunk Cloud 并想更改这些设置，请向 Splunk 支持提交问题。

配置表格中的行号

对于仪表板面板中的简单结果表，默认会生成 1000 行。如果您的仪表板表格所包含的行数超过 1000，则仅会为 PDF 呈现前 1000 行，必要时会打印结果到多个页面。

Splunk Enterprise 用户可以在 limits.conf 文件中覆盖为 PDF 生成的默认行数。

要配置可打印到 PDF 的表格最大行号：

- 打开 \$SPLUNK_HOME/etc/system/local/limits.conf 进行编辑。
若不存在，则新建此文件。
- 在 [pdf] 段落中指定以下属性：

```
[pdf]
max_rows_per_table = <unsigned int>
```

注意：该设置将为您的 Splunk 部署中的所有表格配置 PDF 设置。

配置生成 PDF 的超时设置

生成 PDF 的默认超时是 3,600 秒，如 limits.conf 所指定。完成速度很慢的复杂搜索可能需要额外时间以生成 PDF。

要配置生成 PDF 的超时：

1. 打开 \$SPLUNK_HOME/etc/system/local/limits.conf 进行编辑。
若不存在，则新建此文件。
2. 指定生成 PDF 要等待的秒数。该属性在 [pdf] 段落中：

```
[pdf]
render_endpoint_timeout = <unsigned int>
```

注意：该设置将为您的 Splunk 部署中的所有 PDF 配置 PDF 生成超时设置。

配置是否为 PDF 包含 Splunk 徽标

所生成的 PDF 中默认会包含 Splunk 徽标。您可以覆盖 alert_actions.conf 中的默认设置。

要在生成的 PDF 中包含 Splunk 徽标：

1. 打开 \$SPLUNK_HOME/etc/system/local/alert_actions.conf 进行编辑。
若不存在，则新建此文件。
2. 在 [email] 段落中指定以下属性：

```
[email]
reportIncludeSplunkLogo=0
```

注意：该设置会为 Splunk 部署中的所有生成的 PDF 配置设置。

允许在 PDF 中使用非拉丁字体

Splunk 软件准备了一系列拉丁字体，以及一组 CID 字体以处理日文、韩文、简体中文和繁体中文。

通过更改 alert_actions.conf 中的 reportCIDFontList 参数，您可以控制 Splunk 软件加载 CID 字体的方式。使用空格分隔的列表指定字体。如果多个字体要为给定字符代码提供字形，则使用来自列表第一个字体的字形。

reportCIDFontList 参数在 [email] 段落中。在此对字体使用进行任何更改：

```
$SPLUNK_HOME/etc/system/local/alert_actions.conf
```

以下为默认支持的 CID 字体：

```
gb cns jp kor
```

这些分别指简体中文、繁体中文、日文和韩文。

要跳过加载任何 CID 字体，在 alert_actions.conf 的本地版本中，将 reportCIDFontList 的值留空。

如果希望您的 PDF 使用另一种非拉丁字体（如 Cyrillic 或 Greek），则须请管理员将 Unicode 字体添加到 \$SPLUNK_HOME/share/splunk/fonts。如果尚不存在，请新建 fonts 目录。

注意：当安装多个字体时，这些字体会以名称的字母顺序排列存放。例如，如果您安装了 Cyrillic 和 Greek 字体，Splunk 软件会始终选择 Cyrillic 字体，除非您在 \$SPLUNK_HOME/share/splunk/fonts 中更改了文件名称使 Greek 字体排在前面。

PDF 生成限制

集成的 PDF 生成功能可能存在一些限制。

- 对于某些要求文本从右到左显示的语言（如希伯来语），他们的 PDF 在呈现时其文本会遵循从左到右的顺序。
- 若仪表板一行中有多个面板，则此类仪表板的 PDF 生成后，每行只有一个面板。
- PDF 生成仅对于以简单 XML 构建的仪表板可用。
- 您无法生成表单的 PDF。
- PDF 生成将忽略 JSChart 图表库不支持的图表自定义。完成后的 PDF 将以 JSChart 中呈现的方式显示面板，并移除不支持的自定义。
- 此操作不支持深色主题。导出为 PDF 时以深色主题保存的仪表板将切换为浅色主题。

复制和管理仪表板

您可以复制仪表板或选择一个仪表板使其显示在应用的主屏幕上。

带大量仪表板的部署的缓存也可以进行调整。

复制仪表板

通过仪表板页面或“仪表板编辑器”新建一个仪表板的副本。

步骤

通过	操作
仪表板页面	<ol style="list-style-type: none">找到要设为主页仪表板的仪表板。选择编辑 > 复制。(可选) 更新所复制的仪表板的标题和 ID，并提供描述。单击复制仪表板。
仪表板编辑器	<ol style="list-style-type: none">单击 ... 按钮并选择复制。(可选) 更新所复制的仪表板的标题和 ID，并提供描述。单击复制仪表板。

设置主页仪表板

配置仪表板使其显示在应用的主页面。

步骤

通过	操作
仪表板列表页面	<ol style="list-style-type: none">找到要设为主页仪表板的仪表板。选择编辑 > 设置为主页仪表板。
仪表板编辑器	<ol style="list-style-type: none">单击 ... 按钮并选择设置为主页仪表板。

调整 UI 缓存以处理大量仪表板

带有几百个或者更多仪表板的 Splunk Enterprise 部署的 UI 性能可能运行较慢。

要改进 UI 性能，请增加 web.conf 配置文件中的默认 max_view_cache_size 设置。例如，如果您有 700 个仪表板，则您可以将设置增加至 1,000。

有关更多信息，请参阅 web.conf 规范文件。

简单 XML 引用

简单 XML 引用

您可以使用简单 XML 源代码构建仪表板和表单。使用仪表板源代码编辑器访问和编辑简单 XML。在某些情况下，简单 XML 提供仪表板用户界面编辑器中没有的自定义选项。

概述

元素

简单 XML 源代码有父级和子级元素，以 `<dashboard>` 或 `<form>` 根元素开头。使用元素构建仪表板或表单。比如，您可以使用 `<row>` 元素组织仪表板中的一个或多个 `<panel>` 子元素。`<panel>` 可以包含如 `<table>` 或 `<map>` 等可视化元素。

属性和选项

大多数简单 XML 元素有可以用以配置仪表板外观和行为的属性和选项。

在可视化元素中，您可以使用选项配置格式、交互性和其他组件，如图表中的图例位置或是要使用的颜色。

属性和选项有类型之分，如数字或文本。一些属性和选项有默认设置和其他要求，如接受的值范围。

使用简单 XML 引用

获取有关简单 XML 元素的引用信息以新建仪表板和表单。

新建仪表板或表单。配置结构和布局。	添加和配置可视化	配合搜索以驱动仪表板内容	添加交互性
<ul style="list-style-type: none">仪表板或表单<code>row</code>面板	<ul style="list-style-type: none">使用可视化元素<code>event</code><code>table</code><code>chart</code><code>map</code><code>single value</code><code>html</code>	<ul style="list-style-type: none"><code>search</code>	<ul style="list-style-type: none"><code>fieldset</code> (表单)<code>input</code> (表单)钻取预定义钻取标记<code>Eval</code>、<code>Link</code>、<code>Set</code> 和 <code>Unset</code>

仪表板或表单

`<dashboard>` 或 `<form>` 根元素在仪表板简单 XML 源代码的顶部显示。`<form>` 根元素表示包含一个或多个输入的仪表板。

仪表板元素层次结构

简单 XML 中的仪表板定义使用以下父级和子级的元素层次。

```
<dashboard>
  <init> (0..1)
  <label> (0..1)
  <description> (0..1)
  <search> (0..1)
  <row> (1..n)
    <panel> (0..n)
      <search> (0..n)
    <chart> | <event> | <html> | <map> | <single> | <table> | <viz> (1..n)
      <search> (0..n, for each visualization element)
```

表单元素层次结构

简单 XML 中的表单元素使用以下父级和子级的元素层次结构。与仪表板不同，表单有包含 `<input>` 元素的 `<fieldset>` 元素。

```
<form>
  <init> (0..1)
```

```

<label> (0..1)
<description> (0..1)
<search> (0..1)
<fieldset> (1)
  <input> (1..n)
<row> (1..n)
<panel> (0..n)
  <search> (0..n)
<chart> | <event> | <html> | <map> | <single> | <table> | <viz> (1..n)
  <search> (0..n, for each visualization element)

```

属性

使用以下属性配置 `<dashboard>` 和 `<form>` 根元素。

名称	类型	默认	描述
hideChrome	布尔值	false	隐藏 Splunk 栏、应用栏和页脚。 针对此属性和以下所有 <code>hide<element_name></code> 属性，如果它们指定为没有值的 URL 查询字符串参数，则按 "true" 处理它们。比如，以下查询字符串都按 "true" 进行处理。 <code><dashboard_url>?hideChrome<dashboard_url>?hideChrome=true</code>
hideAppBar	布尔值	false	隐藏列出可用应用的栏。
hideEdit	布尔值	false	隐藏仪表板编辑界面。如果启用，使用设置 > 用户界面 > 视图或仪表板页面编辑仪表板。
hideExport	布尔值	false	设置为 true 隐藏仪表板导出菜单。
hideFilters	布尔值	false	隐藏 <code><form></code> 输入以增加面板显示空间。对 <code><dashboard></code> 不适用。
hideSplunkBar	布尔值	false	隐藏提供主页和设置页链接的栏。
hideTitle	布尔值	false	隐藏在 <code><label></code> 和 <code><description></code> 元素中定义的文本。
isDashboard	布尔值	true	用于内部使用。
isVisible	布尔值	true	指示仪表板或表单是否出现在应用仪表板列表页面和导航菜单中。
onunloadCancelJobs	布尔值		指示是否在用户导航出仪表板或表单时取消搜索任务。
refresh	整数	0	指定 refresh 间隔（秒）。间隔过后仪表板或表单重新加载。 设置刷新时间会重新运行仪表板上的所有搜索。这将防止用户从其 Splunk 实例中注销。尽管此行为在某些 NOC 和 SOC 环境中很有用，但如果要阻止此行为但保留 refresh 设置，则应指示用户在离开系统之前先离开有 refresh 设置的仪表板。这样就会阻止刷新的发生。
	字		要加载的以逗号分隔的自定义 .js 文件列表。这些文件必须位于 appserver/static 目录的文件夹或子文件夹中。 <code>\$SPLUNK_HOME/etc/apps/<app_name>/appserver/static/</code>

script	字符串	<p>要从另一个应用引用自定义 .js 文件，则需在引用文件时指定应用的名称。例如，使用如下引用。</p> <pre><dashboard script="myApp:myScript.js"></pre>	
stylesheet	字符串	<p>用于仪表板的自定义样式表的逗号分隔列表。这些样式表文件必须位于以下目录的文件夹或子文件夹中。 \$SPLUNK_HOME/etc/apps/<app_name>/appserver/static/</p> <p>要从另一个应用引用自定义 css 文件，则须在引用文件时指定此应用的名称。例如，使用如下引用。</p> <pre><dashboard stylesheet="myApp:myStyles.css"></pre>	
theme	字符串	<p>将仪表板或表单主题从 dark 更改为 light。如果未设置主题或将主题设为 light，仪表板或表单将以浅色模式呈现。</p> <p>您必须保存仪表板并刷新浏览器查看主题更改。</p> <p>要仅为了便于查看而更改仪表板主题且不保存更改，您可将主题指定为 URL 查询字符串参数。例如，以下参数将以深色主题呈现仪表板。<dashboard_url>?theme=dark 注意：此操作将覆盖已保存的仪表板状态。您必须删除 URL 查询字符串并刷新页面以查看实际保存的仪表板主题。</p>	
version	字符串	1.1	<p>添加 version="1.1" 以验证仪表板是否在具有所有 jQuery 安全性更新的最新视图中像预期那样运行。版本 1.1 只包含 jQuery 版本 3.5 或更高版本。不要指定任何其他版本。</p>

属性示例

使用 hideEdit 属性将编辑界面从仪表板上隐去。

```
<dashboard hideEdit="true">
...
</dashboard>
```

使用 refresh 属性以在 30 秒后重新加载表单。

```
<form refresh="30">
...
</form>
```

子元素

<dashboard> 或 <form> 根元素可以包含以下一个或多个子元素。

元素	描述	示例
<description>	<p>仪表板或表单的可选文本说明。</p> <p>如果还使用了 <label>，描述以较小的字体出现在标签下方。</p>	<pre><dashboard> <label>Sales this month</label> <description>The following panels show monthly sales totals in the United States.</description> <row> . </row> </dashboard></pre>
<fieldset>	<p>在 <form> 中使用以组织表单输入。对 <dashboard> 不适用。</p> <p><fieldset> 有两个属性：</p> <ul style="list-style-type: none"> • <autoRun>，默认为 false。 • <submitButton>，默认为 true。 <p>如果 <submitButton> 设置为 false，则会发生两件事：</p> <ul style="list-style-type: none"> • <autoRun> 会被忽略，并按照设置为 true 的方式操作。 • 元素 <input> 的属性 <searchWhenChanged> 会被忽略，并按照设置为 true 的方式操作。 	<pre><form> <label>Events by sourcetype</label> . <fieldset> <input type="text" token="series"> <label>Enter a source type</label> <default></default> <initialValue>splunkd</initialValue> </input> </fieldset> . </form></pre>

<init>	包含页面加载时标记更新的元素。比如，设置标记值在仪表板打开时显示具体搜索结果。 有关设置页面加载时标记的更多信息，请参阅“仪表板中的标记用法”。	<pre><dashboard> <init> <set token="selected_sourcetype">mongod</set> </init> . . </dashboard></pre>
<label>	仪表板、表单或表单输入的可选文本标签。	<pre><dashboard> <label>Recent login activity</label> . . </dashboard></pre>
<row>	在仪表板或表单中组织 <panel> 元素。查看行以获得更多详细信息	
<search>	<p>仪表板或表单中的全局搜索元素。</p> <p>仪表板或表单可以包含一个或多个全局 <search> 元素。</p> <p>如果仪表板或表单包含全局搜索，使用 <panel> 元素中的后期处理搜索以便在面板中显示结果。</p> <p>查看 search 以了解更多详细信息。</p>	

fieldset (表单)

<fieldset> 包含 <form> 输入，如复选框或单选按钮。

元素层次

```
<form>
<fieldset autoRun="[Boolean]" submitButton="[Boolean]">
<html> (0..n)
<input type="[input type]" token="[search token]"> (1..n)
<default> (0..1)
<fieldForLabel> (0..1)
<fieldForValue> (0..1)
<initialValue> (0..1)
<label> (0..1)
<prefix> (0..1)
<search> (0..1)
<selectFirstChoice> (0..1)
<suffix> (0..1)
```

属性

名称	类型	默认	描述
autoRun	布尔值	False	表示是否在加载页面时运行搜索。
submitButton	布尔值	True	表示是否显示“提交”按钮。

如果 submitButton 设置为 false，则会发生两件事：

- autoRun 会被忽略，并按照设置为 true 的方式操作。
- 元素 <input> 的属性 searchWhenChanged 会被忽略，并按照设置为 true 的方式操作。

子元素

<fieldset> 包含一个或多个 <input> 元素。

示例

```

<fieldset autoRun="true" submitButton="false">
  <input type="text" token="series">
    <label>sourcetype</label>
    <default></default>
    <initialValue>splunkd</initialValue>
    <suffix>*</suffix>
  </input>
</fieldset>

```

input（表单）

输入元素定义表单的用户交互界面。选择元素，如单选按钮或复选框，让用户单击或选择选项。您可以使用搜索以动态填充选择元素。其他输入，如时间或文本，允许用户输入内容或更改搜索时间范围。

使用属性配置用户输入并使用子元素定义输入内容。一些子元素在多个输入类型中共享。其他元素因输入类型而异。

输入属性

在任意表单输入中使用这些属性。

名称	类型	描述
depends	逗号分隔的列表	必须定义列表中的所有标记以使输入呈现。这些标记可能用于表单输入中或钻取上下文。
id	文本（最小两个字符）	输入标识符。 仅字母数字和下划线字符有效。id 不能以数字或下划线字符开始。
rejects	逗号分隔的列表	如果已定义此列表中的一个或多个标记，阻止输入呈现。这些标记可能用于表单输入中或钻取上下文。
searchWhenChanged	布尔值	指定在选择更改时运行搜索。默认为 false。
token	标记名称	标记代表用户从此输入中选择的值。
type		以下输入类型中的一个。 <ul style="list-style-type: none"> • checkbox • dropdown • link • multiselect • radio • text • time

共享的输入子元素

使用 `<input>` 元素中的这些子元素。有一些使用例外。

名称	描述	使用例外
<change>	请参阅 change	不可用于多选择输入。
<condition>	请参阅 condition（输入）	不可用于多选择输入。
<default>	输入的默认值。如果用户不选择或输入值，将使用此值。覆盖 initialValue。	
<earliest> 和 <latest>	定义 <search> 时间范围的最早和最晚时间。使用相对时间调节器，如“在搜索中指定时间修饰符”中所述；或将 UNIX Epoch 时间格式用作绝对时间。	对文本或时间输入不可用。
<fieldForLabel> 和 <fieldForValue>	在动态填充的选择输入中，这些元素表示可用于每个选择的标签和值的搜索结果字段。与为填充输入选择生成结果的 <search> 元素一起使用。	对文本或时间输入不可用。
<initialValue>	输入的初始值。此值用于用户选择或输入值之前。	
<label>	输入标签。	

<prefix>	添加到所选值的前缀。比如，您可以在字符串值的开头添加引号，并使用 <suffix> 在字符串值后添加右引号。前缀可以是字符串或正则表达式。	
<search>	动态填充输入选项的搜索。使用 <search> 元素的 ref 属性以从报表引用搜索。请参阅 <search>。	在文本输入中不可用。
<suffix>	附加到所选值的后缀。后缀可以是字符串或正则表达式。	

复选框子元素

除了共享的输入子元素，您可以在 <checkbox> 中使用以下子元素。

元素	类型	默认	描述
<delimiter>	文本		一个将放在每个选中值之间的字符串。通常，使用大写来指定 "OR" 或 "AND" - 不要指定引号，而要在文本前和文本后指定一个空格字符。
<valuePrefix>	文本		作为输入元素值的前缀的字符串。可以是正则表达式。
<valueSuffix>	文本		附加到输入元素值的字符串。可以是正则表达式。

下拉列表子元素

除了共享的输入子元素，您可以在 <dropdown> 中使用以下子元素。

元素	类型	默认	描述
<allowCustomValues>	布尔值	false	如果为 true，则启用键入到输入的文本字段的自定义值的选择。
<choice value=[value]>	文本		value 必填。指定要用于选项的值。 为单选或下拉菜单元素指定选择。<choice> 是用于特定值的标签。
<selectFirstChoice>	布尔值	false	表示列出的第一个项目是否为默认的输入项目。<default> 的值是否存在，<selectFirstChoice> 是否被忽略。
<showClearButton>	布尔值	true	指示用于下拉列表的清除按钮是否存在。 当存在时，用户单击清除按钮以更改用于下拉列表默认值的选择。

链接子元素

除了共享的输入子元素，您可以在 <link> 中使用以下子元素。

元素	类型	默认	描述
<choice value=[value]>	文本		value: Required. 指定要用于选项的值。 指定链接输入元素的选择。<choice> 是用于特定值的标签。
<selectFirstChoice>	布尔值	false	表示列出的第一个项目是否为默认的输入项目。覆盖 <initialValue> 的任何值。<default> 的值是否存在，<selectFirstChoice> 是否被忽略。

多选择子元素

除了共享的输入子元素，您可以在 <multiselect> 中使用以下子元素。

二进制	类	单选	组合
-----	---	----	----

元素	型	默认	描述
<allowCustomValues>	布尔值	false	如果为 true，则启用键入到输入的文本字段的自定义值的选择。
<delimiter>	文本		一个将放在每个选中值之间的字符串。通常，使用大写来指定 "OR" 或 "AND" - 不要指定引号，而要在文本前和文本后指定一个空格字符。
<valuePrefix>	文本		作为输入元素值的前缀的字符串。可以是正则表达式。
<valueSuffix>	文本		附加到输入元素值的字符串。可以是正则表达式。

单选子元素

除了共享的输入子元素，您可以在 <radio> 中使用以下子元素。

元素	类型	默认	描述
<choice value=[value]>	文本		<p>value 必填。代表单选按钮选择值。 为单选或下拉菜单元素指定选择。<choice> 是特定值的标签。</p>
<selectFirstChoice>	布尔值	false	表示列出的第一个项目是否为输入的默认已选项目。如果 <default> 的值存在，将忽略 <selectFirstChoice>。

文本子元素

请参阅“共享的输入子元素”了解可用元素和例外。

时间子元素

请参阅“共享的输入子元素”了解可用元素和例外。

更改（表单输入）

使用 <change> 元素以定义表单如何对用户输入做出响应。用户做出选择或键入输入时，将发生在 <change> 元素中为该输入配置的操作。

<change> 元素在以下 <input> 类型中可用。

- <checkbox>
- <dropdown>
- <radio>
- <text>
- <time>

使用标记定义对用户输入的响应

在 <change> 元素中，您可以定义能够帮助您管理表单中的动态行为或显示的操作，如标记设置或其他标记更新。

条件响应

使用 <change> 元素中的一个或多个 <condition> 元素定义特定用户输入的条件响应。请参阅 <condition> 以了解更多信息。

元素层次

```
<input>
  <change>
    ( <set> | <unset> | <link> | <eval> ) (1..n)
      <condition> (0..n)
        ( <set> | <unset> | <link> | <eval> ) (1..n)
```

属性

无

子元素

您可以在 `<change>` 元素中使用以下子元素。

名称	描述
<code><set></code>	设置或更新标记值。
<code><unset></code>	取消之前设置的标记值。
<code><link></code>	链接到目标，如另一个仪表板、表单或外部网站。
<code><eval></code>	筛选或设置标记值的格式。
<code><condition></code>	使用 <code><change></code> 元素中的 <code><condition></code> 元素定义用户输入的条件响应。

示例

使用 `<change>` 元素捕获输入中的所选标签和值。

```
<form>
  <label>Use tokens with input choices to capture input labels and values</label>
  <init>
    <set token="date_label">Last 7 Days</set>
    <set token="earliest_tok">-7d@d</set>
  </init>
  <fieldset submitButton="false">
    <input type="radio" token="period_tok">
      <label>Select a time range</label>
      <choice value="-24h@h">Last 24 Hours</choice>
      <choice value="-7d@d">Last 7 Days</choice>
      <choice value="-30d@d">Last 30 Days</choice>
      <default>Last 7 Days</default>

    <change>
      <!-- use predefined input tokens to set -->
      <!-- tokens for the selected label and value -->
      <set token="date_label">$label$</set>
      <set token="earliest_tok">$value$</set>
    </change>

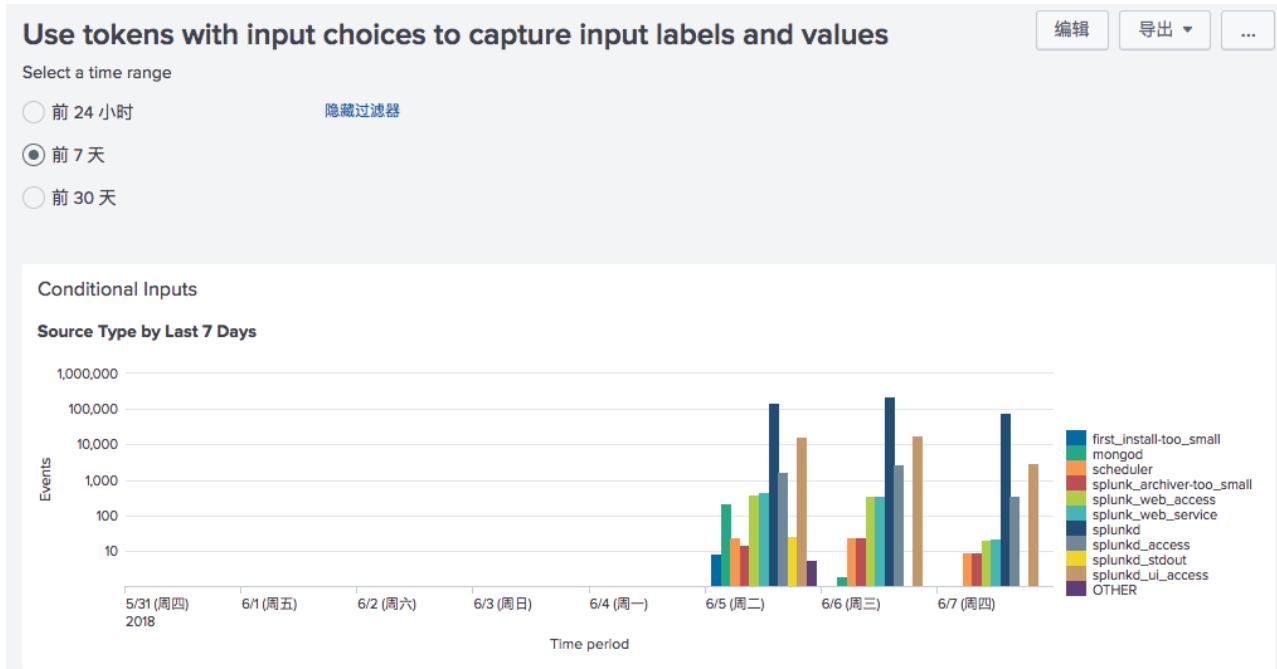
    </input>
  </fieldset>

  <row>
    <panel>
      <title>Conditional Inputs</title>
      <chart>
        <!-- Display selected label in the title -->
        <title>Source Type by $date_label$</title>

        <search>
          <query>index = _internal | timechart count by sourcetype</query>
          <!-- use the value of earliest_tok -->
          <!-- to set the time range -->
          <earliest>$earliest_tok$</earliest>
          <latest>now</latest>
        </search>

        <option name="charting.axisY.scale">log</option>
        <option name="charting.axisTitleX.text">Time period</option>
        <option name="charting.axisTitleY.text">Events</option>
      </chart>
    </panel>
  </row>
</form>
```

```
</row>
</form>
```



条件（表单输入）

使用表单输入 `<change>` 元素中的 `<condition>` 定义用户输入的条件式响应。

`<condition>` 元素对多选输入不可用。

关于将 `<condition>` 元素用作钻取的一部分的信息，请参阅 `<condition>`（钻取）。

属性

名称	类型	默认	描述
label	文本	*	指定将条件应用于哪个输入标签元素。 * 将条件应用于所有输入 <code><label></code> 元素。
match=	文本		指定评估匹配的条件。 例如，当搜索未返回任何结果时，您可以使用 <code><condition match="'job.resultCount' == 0"></code> 以指定一个条件以应用。
value	文本	*	指定将条件应用于哪个输入值元素。 * 将条件应用于所有输入 <code><value></code> 元素。

子元素

使用 `<condition>` 中的以下子元素定义条件标记设置或其他行为。请参阅 `Eval`、`Link`、`Set` 和 `Unset` 以了解更多详细信息。

名称	描述
<code><set></code>	设置标记值。
<code><unset></code>	取消之前设置的标记值。
<code><link></code>	链接到目标，如另一个仪表板、表单或外部网站。
<code><eval></code>	处理或设置标记值的格式。

元素层次

```

<change>
  <condition>
    ( <set> | <unset> | <link> | <eval> ) (1..n)

```

示例

使用条件式输入选择搜索的预设时间范围。

所选选项的标记在图表的标题中显示。所选值的条件式标记驱动图表的数据。

```

<form>
  <label>Use tokens with conditional input choices</label>
  <fieldset submitButton="false">
    <input type="radio" token="period_tok">
      <label>Select a time range</label>
      <choice value="-24h@h">Last 24 Hours</choice>
      <choice value="-7d@h">Last 7 Days</choice>
      <choice value="-30d@h">Last 30 Days</choice>
      <default>Last 7 Days</default>

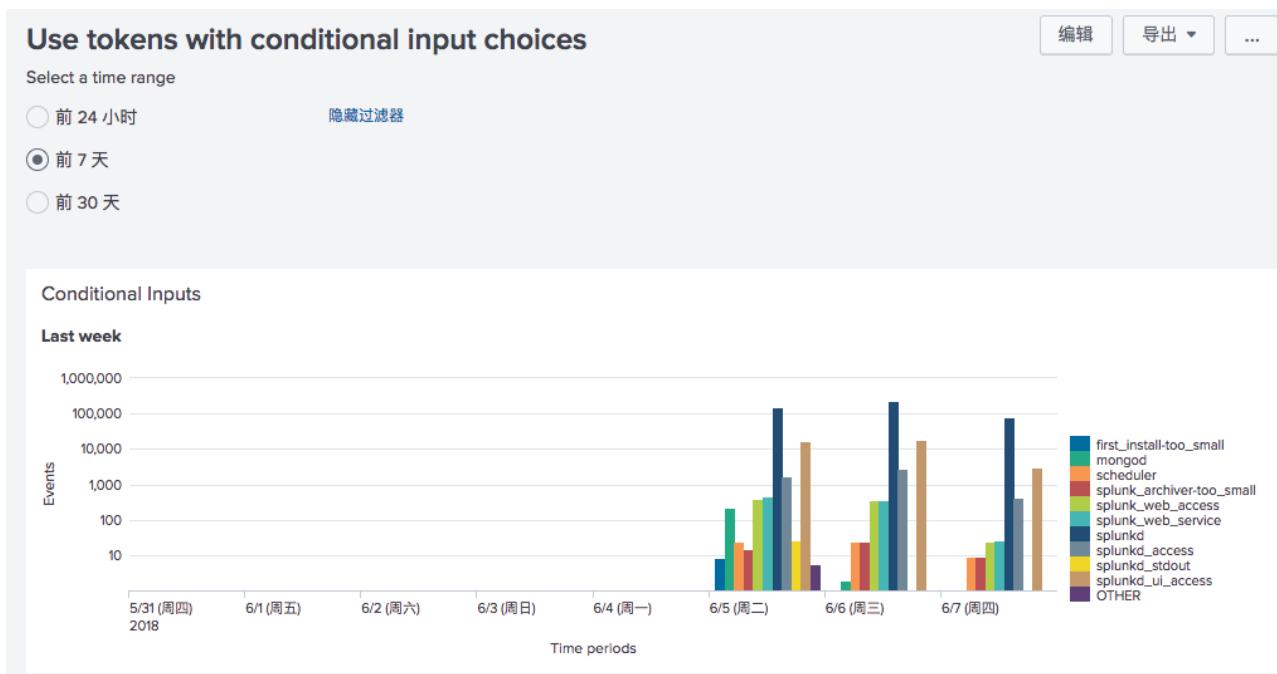
      <!-- set condition based on the label defined by <choice> -->
      <!-- Within each condition, specify a custom label for display -->
      <!-- Capture the selected value in the token, earliest_tok -->
      <change>
        <condition label="Last 24 Hours">
          <set token="date_label">Yesterday</set>
          <set token="earliest_tok">$value$</set>
        </condition>
        <condition label="Last 7 Days">
          <set token="date_label">Last week</set>
          <set token="earliest_tok">$value$</set>
        </condition>
        <condition label="Last 30 Days">
          <set token="date_label">Last month</set>
          <set token="earliest_tok">$value$</set>
        </condition>
      </change>
    </input>
  </fieldset>
  <row>
    <panel>
      <title>Conditional Inputs</title>
      <chart>

        <!-- Display selected label in the title -->
        <title>$date_label$</title>

        <search>
          <query>index = _internal | timechart count by sourcetype</query>
          <!-- use the value of earliest_tok -->
          <!-- to set the time range -->
          <earliest>$earliest_tok$</earliest>
          <latest>now</latest>
        </search>

        <option name="charting.axisY.scale">log</option>
        <option name="charting.axisTitleX.text">Time periods</option>
        <option name="charting.axisTitleY.text">Events</option>
      </chart>
    </panel>
  </row>
</form>

```



row

在仪表板或表单中，一个 `row` 包含一个或多个 `<panel>` 子元素。使用 `row` 配置面板分组和布局。

属性

使用 `<row>` 元素中的以下属性。

名称	类型	默认	描述
depends	逗号分隔的 标记列表		来自标记列表的所有标记必须进行定义，以便在仪表板中呈现此行。但是，未定义的标记不会阻止行中的搜索在后台运行。
rejects	逗号分隔的 标记列表		来自此列表的所有标记必须进行定义，以便阻止此行呈现在仪表板中。
id	文本		<p>行标识符。</p> <p>仅字母数字和下划线字符有效。id 不能以数字或下划线字符开始。</p> <p>以下术语预留给内部使用，且不能用于 id。</p> <ul style="list-style-type: none"> • dashboard • search • default • submitted • footer • url • header

子元素

`<row>` 通常包含一个或多个 `<panel>` 元素。还可能有包含 `<html>` 元素的 `<row>`。但是，单个 `<row>` 无法同时包含 `<panel>` 和 `<html>`。

面板

在 `<row>` 中，使用 `<panel>` 包含一个或多个可视化。您可以使用面板管理可视化分组和布局。您还可以动态显示或隐藏面板。

面板对齐

面板中的两个或多个可视化元素垂直对齐，单值可视化除外。同一面板中的两个或多个值可视化水平分组。

面板类型

在简单 XML 中有两个可用 `<panel>` 类型。

类型	描述	要求	编辑选项	限制
内联	包含一个或多个可视化元素。	N/A	使用仪表板编辑用户界面或简单 XML 源代码新建和更新内联面板。	N/A
引用	显示预建面板的目录	需要 <code>ref</code> 属性以使预建面板显示。 选择性地添加 <code>app</code> 引用。		无法使用面板编辑器编辑引用面板。 引用面板无法识别简单 XML 中指定的 <code><panel></code> 子元素。

有关预建面板的更多信息，请参阅“仪表板面板”和“通过引用新建和添加面板”。

元素层次

内联面板

```
<row>
  <panel> (0..n)
    <title> (0..1)
    <search> (0..n)
    <chart> | <event> | <html> | <map> | <single> | <table> | <viz> (1..n)
```

引用面板

```
<row>
  <panel ref="[panel name]" [app="[app name]"]> (0..n)
  <!-- Other <panel> child elements ignored -->
```

属性

使用 `<panel>` 元素中的以下属性。

名称	类型	默认	描述
ref	文本		只有引用面板需要。 引用预建面板的名称。预建面板名称在设置 > 用户界面 > 面板下显示。
app	文本	对包含仪表板的应用为默认选项。	对引用面板为可选项。 引用包含预建面板的应用的名称。面板应用名称在设置 > 用户界面 > 面板下显示。
depends	逗号分隔的标记列表		此列表中的所有标记必须进行定义，以便在仪表板中呈现此面板。
id	文本		面板标识符。 仅字母数字和下划线字符有效。 <code>id</code> 不能以数字或下划线字符开始。 以下术语预留给内部使用，且不能用于 <code>id</code> 。 <ul style="list-style-type: none">• dashboard• search• default• submitted• footer• url• header

rejects 逗号分隔的标记列表。

来自此列表的所有标记必须进行定义，以便阻止此面板呈现在仪表板中。

子元素

使用 `<panel>` 子元素配置内联面板。引用面板忽视 `<panel>` 子元素。

元素	描述	示例
<code><title></code>	可选 <code><title></code> 面板标题。 面板标题可以提供一组可视化的上下文。面板中的每个可视化元素也可以有自己的标题。	<pre><form> ... <row> <panel> <title>Video game sales</title> <table> ... </table> </panel> </row> </form></pre>
<code><search></code>	面板的基本搜索。在面板可视化中使用有后期处理搜索的基本面板 <code><search></code> 元素。	
可视化元素	面板可能包含以下一个或多个可视化类型。 <code><chart></code> <code><event></code> <code><html></code> <code><map></code> <code><single></code> <code><table></code> <code><viz></code>	

面板示例

此 `<panel>` 元素显示单值可视化和图表分组。

```
<dashboard>
  <label>Dashboard Panel Example</label>
  <description></description>
  <row>
    <panel>
      <chart>
        <title>Chart grouping</title>
        <search>
          <query>
            index=_internal source="*splunkd.log"
            ( log_level=ERROR OR log_level=WARN*
              OR log_level=FATAL OR log_level=CRITICAL )
            | stats count as log_events
            | rangemap field=log_events low=1-100 elevated=101-300 default=severe
          </query>
          <earliest>-7d@h</earliest>
          <latest>now</latest>
        </search>
        <option name="charting.chart">radialGauge</option>
      </chart>
      <chart>
        <search>
          <query>
            index=_internal source="*splunkd.log"
            ( log_level=ERROR OR log_level=WARN*
              OR log_level=FATAL OR log_level=CRITICAL )
            | stats count as log_events
            | rangemap field=log_events low=1-100 elevated=101-300 default=severe
          </query>
          <earliest>-7d@h</earliest>
          <latest>now</latest>
        </search>
        <option name="charting.chart">markerGauge</option>
      </chart>
    </panel>
  </row>
  <row>
```

```

<panel>
  <single>
    <title>Single value grouping</title>
    <search>
      <query>
        index=_internal source="*splunkd.log"
        ( log_level=ERROR OR log_level=WARN*
        OR log_level=FATAL OR log_level=CRITICAL )
        | stats count as log_events
        | rangemap field=log_events low=1-100 elevated=101-300 default=severe
      </query>
      <earliest>-7d@h</earliest>
      <latest>now</latest>
    </search>
    <option name="beforeLabel">Found</option>
    <option name="afterLabel">errors</option>
  </single>
  <single>
    <search>
      <query>
        index=_internal source="*splunkd.log"
        ( log_level=ERROR OR log_level=WARN*
        OR log_level=FATAL OR log_level=CRITICAL )
        | stats count as log_events
        | rangemap field=log_events low=1-100 elevated=101-300 default=severe
      </query>
      <earliest>-7d@h</earliest>
      <latest>now</latest>
    </search>
    <option name="beforeLabel">Found</option>
    <option name="afterLabel">errors</option>
  </single>
</panel>
</row>
</dashboard>

```

使用可视化元素

使用以下一个或多个元素添加可视化到 `<panel>`。

元素	描述
<code><event></code>	事件列表
<code><nowiki><table></nowiki></code>	统计表
<code><chart></code>	折线图、条形图、面积图、气泡图和散点图
<code><map></code>	群集地图和分级统计地图
<code><single></code>	单值可视化
<code><html></code>	自定义 <code>html</code> 内容
<code><viz></code>	自定义可视化。请参阅《开发用于 <code>Splunk Web</code> 的视图和应用》中的“简单 XML 中的自定义可视化”。

使用可视化属性和选项

像其他简单 XML 元素一样，可视化将属性用于标识及管理显示。有几个可以用于任何可视化类型的共享属性。一些可视化有其他可用的属性。

每个可视化有几个称为属性的可用于配置的 `<option>`。共享选项可以用于所有可视化。其他 `<option>` 属性特定用于一个可视化类型。

选项语法

使用以下选项在可视化元素中标记语法。

```
<option name="[option_name]">[option_value]</option>
```

如，使用以下选项显示面板中的导出按钮。

```
<option name="link.exportResults.visible">true</option>
```

共享属性

使用以下属性识别和控制任何可视化元素的显示。

名称	类型	描述
depends	必须设置的、以逗号分隔的标记列表，以显示面板、行或可视化。	来自标记列表的所有标记必须进行定义，以便呈现此可视化。如， <code><chart depends="\$show1\$"></code> 表示图表只在设置 \$show1\$ 标记时显示。隐藏元素不会阻止任何搜索元素在后台的运行。
rejects	必须设置的、以逗号分隔的标记列表，以隐藏可视化。	来自此列表的所有标记必须进行定义，以便阻止呈现此可视化。例如： <code><table rejects="\$one\$, \$two\$"></code> 表示设置 \$one\$ 或 \$two\$ 标记之后，表格隐藏。
id	文本	可视化标识符。 仅字母数字和下划线字符有效。id 不能以数字或下划线字符开始。 以下术语预留给内部使用，且不能用于 id。 <ul style="list-style-type: none">• dashboard• search• default• submitted• footer• url• header

共享选项

Trellis 布局选项

Trellis 布局适用于任何可视化类型，除了群集地图和表。要了解更多信息，请参阅“使用 Trellis 布局拆分可视化”。

选项名称	类型	默认	描述
trellis.enabled	布尔值	0	启用或禁用 Trellis 布局。默认为 0（禁用）。
trellis.scales.shared	布尔值	1	表示是否要在折线图、面积图、柱形图和条形图共享轴的刻度，或在分级统计地图分段中共享值的范围。使用下列任意值。 <ul style="list-style-type: none">• 1: 共享刻度• 0: 独立刻度
trellis.size	字符串	medium	配置可视化段大小。段大小影响拆分可视化的面板显示密度。使用下列任意值。 <ul style="list-style-type: none">• small• medium• large
trellis.splitBy	结果字段名称	N/A	指示为拆分可视化使用的搜索结果字段或聚合名称。每个值的分段都在此字段中显示。

搜索、检查、刷新和导出选项

使用以下 `<option>` 设置配置在搜索中打开行为并管理其他面板用户界面元素。

选项名称	类型	默认	描述
link.exportResults.visible	布尔值	默认为 link.visible	在面板底部显示导出按钮。
link.inspectSearch.visible	布尔值	默认为 link.visible	在面板底部显示检查按钮。
link.openPivot.visible	布尔值	默认为 link.visible	在面板底部显示在数据透视表中打开按钮。
link.openSearch.search	搜索字符串	默认为面板搜索	指定当用户单击在搜索中打开按钮时打开搜索。
link.openSearch.searchEarliestTime	时间调节器	默认为面板搜索最早时间。	用于由 link.openSearch.search 指定的备选搜索的最早时间。
link.openSearch.searchLatestTime	时间调节器	默认为面板搜索最晚时间。	用于由 link.openSearch.search 指定的备选搜索的最晚时间。
link.openSearch.text	文本	Open in Search	指定在搜索中打开按钮的自定义标签。
link.openSearch.viewTarget	视图名称	search	指定当用户单击在搜索中打开按钮时使用的目标视图。
link.openSearch.visible	布尔值	默认为 link.visible	在面板底部显示在搜索中打开按钮。
link.visible	布尔值	true	在面板底部显示链接按钮。
refresh.time.visible	布尔值	true	在面板中显示刷新时间指示器。 使用 <search> 元素中的 <refresh> 属性以配置刷新行为。
refresh.link.visible	布尔值	true	在面板中显示刷新链接。 使用 <search> 元素中的 <refresh> 属性以配置刷新行为。

event

使用 event 元素以添加事件列表到 <panel>。

i	时间	事件
>	18/06/07 3:01:00.307	06-07-2018 03:01:00.307 +0100 WARN TelemetryHandler - 1528239600.000000 host = debianSplunk source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
>	18/06/06 15:42:34.796	06-06-2018 15:42:34.796 +0100 WARN DispatchSearchMetadata - could not read metadata file: /opt/splunk/var/run/splunk/dispatch/admin__admin__search__search1_1528296154.601/meta data.csv host = debianSplunk source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
>	18/06/06 15:42:34.796	06-06-2018 15:42:34.796 +0100 WARN DispatchSearchMetadata - could not read metadata file: /opt/splunk/var/run/splunk/dispatch/admin__admin__search__search1_1528296154.601/meta data.csv host = debianSplunk source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
>	18/06/06 15:42:34.794	06-06-2018 15:42:34.794 +0100 WARN DispatchSearchMetadata - could not read metadata file: /opt/splunk/var/run/splunk/dispatch/admin__admin__search__search1_1528296154.601/meta data.csv host = debianSplunk source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
>	18/06/06 15:42:34.793	06-06-2018 15:42:34.793 +0100 WARN DispatchSearchMetadata - could not read metadata file: /opt/splunk/var/run/splunk/dispatch/admin__admin__search__search1_1528296154.601/meta data.csv host = debianSplunk source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd

属性

您可以在 <event> 元素中使用可视化的任何共享属性。

子元素

您可以在 <event> 列表中使用以下子元素。

名称	类型	描述	示例
----	----	----	----

<fields>	逗号分隔的列表	限制搜索结果到这些字段。已列出字段的顺序决定事件列表中字段的顺序。	<pre> <dashboard> <label>Fields Example</label> <row> <panel> <event> <search> <query> index=_internal timechart count by sourcetype </query> <earliest>-7d@d</earliest> <latest>now</latest> </search> <fields>_time, splunkd, splunk_web_access, splunk_web_service</fields> </event> </panel> </row> </dashboard> </pre>
----------	---------	-----------------------------------	---

选项

除了可视化的共享选项，您还可以使用以下选项配置事件列表。

选项名称	类型	默认	描述
count	整数		要显示的最大行数。
list.drilldown	以下一个值： full inner outer none	full	指定为事件列表启用钻取。 full: 启用整个条目钻取。 inner: 启用事件列表的内部元素钻取。 outer: 启用事件列表的外部元素钻取。 none: 禁用钻取。
list.wrap	布尔值	true	表示是否要包括事件列表内容。
maxLines	整数		要为每个结果/事件显示的最大行号。
raw.drilldown	以下一个值： full inner outer none	full	指定在原始事件列表中启用的钻取。 full: 启用整个条目钻取。 inner: 启用事件列表的内部元素钻取。 outer: 启用事件列表的外部元素钻取。 none: 禁用钻取。
rowNumbers	布尔值	false	指示是否显示行号。
showPager	布尔值	true	切换是否分页显示。
table.sortColumn	文本		指定排序表格的列。
table.sortDirection	以下一个值： asc desc	asc	指定表格中的项目的排序方向。
table.drilldown	以下一个值： all none	all	指示是否为表格启用钻取功能。 all: 启用钻取。 none: 禁用钻取。
table.wrap	布尔值	true	指示表格中的文本是否换行。
	以下一个值：		

type	list raw table	list	指示显示事件的格式。
------	----------------------	------	------------

弃用的事件选项

属性	类型	默认	描述	方式
钻取	字符串	all	启用或禁用钻取类型。	使用已键入的钻取选项 (list.drilldown、table.drilldown、raw.drilldown) 或 <drilldown> 元素配置钻取行为。
entityName	字符串	events	显示列表中的事件或结果。	使用 type 以指定要显示的内容。
分段	字符串	none	指定在钻取时可单击的事件元素。	使用 list.drilldown 或 raw.drilldown 以指定每个事件中可单击的元素。
softWrap	布尔值		配置事件换行。	使用 list.wrap 或 table.wrap 配置事件换行。

示例

```
<dashboard>
  . .
  <row>
    <panel>
      <title>Events in the last 24 hours</title>
      <event>
        <search>
          <query>index=_internal</query>
          <earliest>-24h@h</earliest>
          <latest>now</latest>
          <sampleRatio>1</sampleRatio>
        </search>
        <option name="count">20</option>
        <option name="list.drilldown">full</option>
        <option name="list.wrap">1</option>
        <option name="maxLines">5</option>
        <option name="raw.drilldown">full</option>
        <option name="rowNumbers">0</option>
        <option name="table.drilldown">all</option>
        <option name="table.sortDirection">asc</option>
        <option name="table.wrap">1</option>
        <option name="type">list</option>
      </event>
    </panel>
  </row>
  . .
</dashboard>
```

table

<table> 元素定义统计表可视化。



属性

您可以在 `<table>` 中使用任何共享属性。

子元素

您可以在 `<table>` 中使用以下子元素。

名称	类型	描述	示例
<code><fields></code>	逗号分隔的列表	限制搜索结果到这些字段。列出的字段顺序决定表列的顺序。	<pre> <dashboard> <label>Fields Example</label> <row> <panel> <table> <search> <query> index=_internal timechart count by sourcetype </query> <earliest>-7d@d</earliest> <latest>now</latest> </search> <fields>_time, splunkd, splunk_web_access, splunk_web_service</fields> </table> </panel> </row> </dashboard> </pre>

选项

除了可视化的共享选项，您可以使用以下选项配置表。

名称	类型	默认	描述
count	整数	10	要显示的最大行数。
dataOverlayMode	下一个值： none heatmap highlow	none	指示要显示的叠加类型。
drilldown	下一个值： cell row	cell	启用行或单元格级别的钻取，或禁用钻取。 cell: 启用表单元格钻取。 row: 启用表行钻取。

	none		none: 禁用钻取。
rowNumbers	布尔值	false	切换行号的显示。
showPager	布尔值	true	切换是否分页显示。
totalsRow	布尔值	false	设置为 true 以添加列总计行到表。
percentagesRow	布尔值	false	设置为 true 以添加列百分比行到表。
wrap	布尔值	true	启用结果表格中的文本换行。

设置列的格式

您可以在表列中使用颜色和其他格式以显示上下文或突出值。设置表列的格式使用一种不同于其他可视化选项的语法。要了解简单 XML 中的设置表列格式，请参阅“表列简单 XML”。

示例

下面的表格面板示例使用内联搜索，显示五行，并禁用行号：

```
<dashboard>
  <label>Dashboard with Table</label>
  <row>
    <panel>
      <table>
        <title>Top source types in the last 24 hours</title>
        <search>
          <query>
            index=_internal group=per_sourcetype_thruput
            | chart sum(kb) by series | sort -sum(kb)
          </query>
          <earliest>-24h</earliest>
          <latest>now</latest>
        </search>
        <option name="count">5</option>
        <option name="rowNumbers">0</option>
      </table>
    </panel>
  </row>
</dashboard>
```

表格迷你图

表格迷你图显示每个表行的最近行为模式。您可以在简单 XML 中设置迷你图的格式。



单值迷你图与表格迷你图效果不同。有关更多详细信息，请参阅 `single_value`。

在简单 XML 中配置迷你图格式无法更改 PDF 格式中的迷你图外观。迷你图在 PDF 中不以其他格式出现。

生成迷你图

要使用此处介绍的格式选项，您的搜索必须在可视化中生成迷你图。要新建迷你图，请使用 `chart` 或 `stats` 命令 `sparkline()`

函数。更多详细信息，请参阅《搜索手册》中的“为搜索结果添加迷你图”。

设置语法和属性格式

`<format>` 元素包含迷你图的格式设置规则。包括 "sparkline" 类型属性和迷你图正在追踪的 `field`。

```
<format type="sparkline" field="[field name]">
...
</format>
```

将 `<option>` 子元素放在 `<format>` 中以配置迷你图外观。

设置元素属性格式

使用以下属性配置 `<format>` 元素。

名称	类型	描述
<code>type</code>	字符串	必填。使用 "sparkline"。
<code>field</code>	迷你图正在追踪的搜索结果字段	必填。使用您的搜索中 <code>sparkline()</code> 命令正在使用的字段生成迷你图。如，您可以使用此搜索生成 <code>trend</code> 字段的迷你图。 <code>... chart count sparkline(count, 1h) as trend by sourcetype ...</code> 将 <code>trend</code> 用作 <code>field</code> 值以设置迷你图的格式。 <code><format type="sparkline" field="trend"></code> ... <code></format></code>

格式选项

使用 `<format>` 元素中的 `<option>` 元素以定义迷你图外观。一些选项是迷你图的常见选项。其他选项特定于某种迷你图表类型。

常见迷你图选项

属性	类型	默认	描述
<code>chartRangeMax</code>	数字	n/a	指定一个最大迷你图范围的替代值。
<code>chartRangeMin</code>	数字	n/a	指定一个最小迷你图范围的替代值。
<code>height</code>	CSS 样式	auto	图表高度。使用任意有效 CSS 宽度。例如， <code>1.5em</code> 或 <code>20px</code> 。
<code>tooltipPrefix</code>	文本		工具提示中所显示字段前的文本。
<code>tooltipSuffix</code>	文本		附加到工具提示里显示的每个字段的文本。
<code>type</code>	(<code>bar</code> <code>discrete</code> <code>line</code>)	折线图	迷你图类型

迷你图条形图表选项

属性	类型	默认	描述
<code>barSpacing</code>	数字		每个条形之间的距离（以像素为单位）。
<code>barWidth</code>	数字		每个条形的宽度（以像素为单位）。
<code>colorMap</code>	请参阅 描述		将字段值映射到已选颜色。 例如，如果您想要所有 <code>-2</code> 的值显示黄色，则使用 <code>colorMap: { '-2': '#ff0' }</code> 。 您还可以使用值数组，而不是映射以指定每个条形图的颜色。比如，如果您的图表有值 <code>1</code> 、 <code>3</code> 和 <code>1</code> ，您可以使用 <code>colorMap=["red", "green", "blue"]</code> 。

迷你图离散图表选项

属性	类型	默认	描述
lineColor	CSS 样式		折线图和离散图用于将画线的颜色指定为一个 CSS 值字符串。
lineHeight	数字	图形高度的 30%	每条线的高度（以像素为单位）。
thresholdColor	CSS 颜色		结合 thresholdValue 一起使用的 CSS 颜色。
thresholdValue	CSS 颜色		使用 thresholdColor 而不是 lineColor 绘制少于此阈值的值。

迷你图折线图表选项

属性	类型	默认	描述
fillColor	CSS 颜色 false		指定填入图形下面的区域的颜色为一个 CSS 值。设置为 false 以禁用填充。
highlightLineColor	CSS 颜色	#f22	当鼠标移上去时，所示垂直线的 CSS 颜色。 设置为空值以禁用。
highlightSpotColor	CSS 颜色	#f5f	当鼠标移上去时，所显示点的颜色。 设置为空值以禁用。
lineColor	CSS 样式		折线图和离散图用来指定画线的颜色为一个 CSS 值字符串
lineWidth	数字	1	线的宽度（以像素为单位）。
maxSpotColor	CSS 颜色		针对最大值标记显示的 CSS 颜色。 设置为 false 或一个空的字符串，以将其隐藏。
minSpotColor	CSS 颜色		针对最小值标记显示的 CSS 颜色。 设置为 false 或一个空的字符串，以将其隐藏。
normalRangeMax	数字（请参阅描述）		配合 normalRangeMin 使用以定义一个正常或符合预期的值范围阈值。迷你图中出现的条形图显示哪些值在此范围内，哪些在范围外。
normalRangeMin	数字		配合 normalRangeMax 使用以定义一个正常或符合预期的值范围阈值。迷你图中出现的条形图显示哪些值在此范围内，哪些在范围外。
spotColor	CSS 颜色		最终值标记的 CSS 颜色。 设置为 false 或一个空的字符串，以将其隐藏。
spotRadius	数字	1.5	所有圆点标记的半径（以像素为单位）。
valueSpots	请参阅描述		绘制值点的点和颜色。可以是一个范围。 例如，要使所有小于 50 的值呈现绿色，高于 50 的值呈现红色，则使用 {'<50': 'green', '>50': 'red'}。
width	CSS 样式	auto	图表宽度。指定任意有效的 CSS 宽度（例如，1.5em 或 20px）。

示例

简单 XML 源代码生成带有条形图表迷你图的表格。

```
<dashboard>
  <label>Sparkline Example</label>
  <row>
    <panel>
```

```

<table>
  <title>Basic Sparkline Bar w/ Color Map</title>
  <!-- Set span for each sparkline datapoint to be 1 hour -->
  <search>
    <query>
      index=_internal | chart count sparkline(count, 1h) as trend by sourcetype | sort -count
    </query>
    <earliest>-24h@h</earliest>
    <latest>now</latest>
  </search>
  <option name="count">3</option>

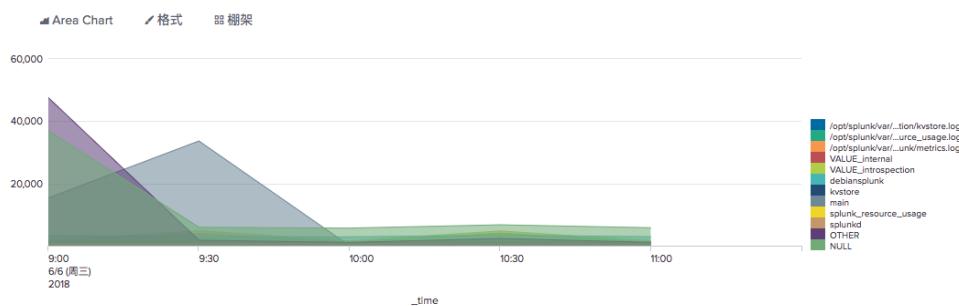
  <!-- Set sparkline options here; make sure that field matches field name of the search results -->
  <format type="sparkline" field="trend">
    <option name="type">bar</option>
    <option name="height">40</option>
    <!-- Use colorMap to map specific values to selected colors -->
    <option name="colorMap">
      <option name="2000:">#5379AF</option>
      <option name=":1999">#9ac23c</option>
    </option>
    <option name="barWidth">5px</option>
  </format>
</table>
</panel>
</row>
</dashboard>

```



chart

使用 `<chart>` 元素添加柱形图、条形图、折线图、面积图、气泡或散点图到 `<panel>`。您还可以使用 `<chart>` 元素添加仪表可视化到 `<panel>`。



生成图表的搜索可能是内联搜索或保存的报表。保存的报表可能包含图表格式设置。默认使用这些设置，但是您可以使用简单 XML 源代码中的选项和属性覆盖它们。

关于保存报表的更多信息，请参阅“新建和编辑报表”。

属性

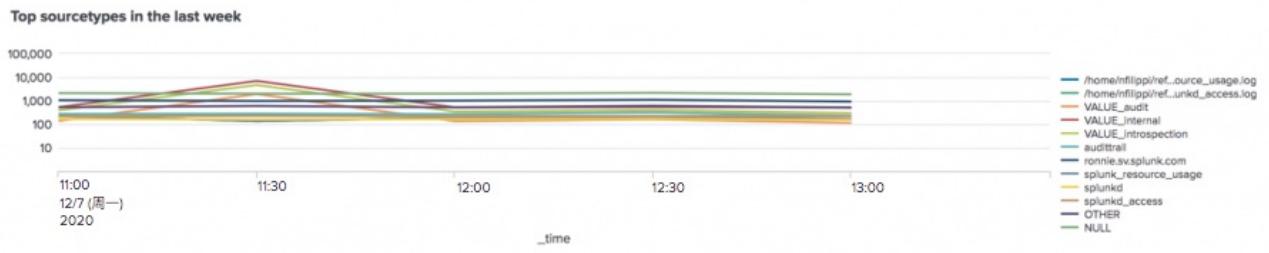
在图表中使用可视化的任何共享属性。

选项

除了可视化的共享选项，您可以使用一般图表配置的以下选项。有关完整的图表选项列表，请参阅“图表配置引用”。

名称	类型	默认	描述
charting.chart	area bar column fillerGauge line markerGauge pie radialGauge scatter	column	设置图表类型。确定您正在使用的搜索为图表类型生成数据格式正确的结果。 注意：如果使用标记设置 charting.chart 类型，在编辑模式下打开时可视化挑选器不可用于面板。
charting.legend.placement	top left bottom right none	right	图例位置，相对于图表
charting.<option_name>			支持图表的格式设置选项。请参阅“自定义图表引用”以请参阅每个图表类型的可用选项。
height	100–10000 之间的数	250	图表高度（以像素为单位）

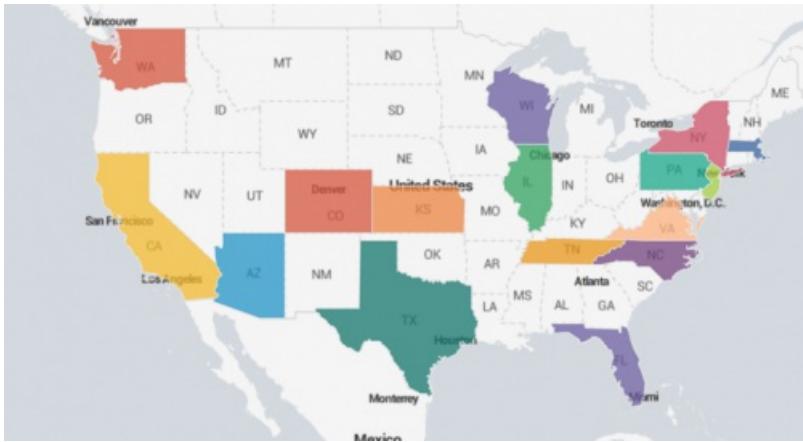
示例



```
<form>
  . .
  <row>
    <panel>
      <title>Chart example</title>
      <chart>
        <title>Top sourcetypes in the last week</title>
        <search>
          <query>index=_internal | timechart sum(kb) by series | head 5</query>
          <earliest>-4h@m</earliest>
          <latest>now</latest>
        </search>
        <option name="height">200</option>
        <option name="charting.chart">line</option>
        <option name="charting.axisY.scale">log</option>
        <option name="charting.chart.nullValueMode">connect</option>
      </chart>
    </panel>
  </row>
  . .
</form>
```

map

使用 `<map>` 元素以添加 Choropleth 或群集地图到 `<panel>`。



属性

除了可视化的共享属性，您可以在 `<map>` 元素中使用以下属性。

一般地图选项

除了可视化的共享选项，您可以使用以下选项配置 Choropleth 和群集地图。

名称	类型	默认	描述
drilldown	all none	all	使用 all 启用钻取或使用 none 禁用钻取。
mapping.fieldColors	一个或多个 <code><field> : <color_hexvalue></code> 映射。		映射到十六进制颜色值（0xRRGGBB）以定义特定系列颜色的字段名称列表（以逗号隔开）。
mapping.map.center	(lat, long)		地图的初始中心点。纬度值可以在 -85 至 85 的范围内，本范围外的值将被切除。经度值可以在 -180 至 180 的范围内，本范围外的值将被缩小为在范围内。
mapping.map.scrollZoom	布尔值	false	当用户在地图上用鼠标滚动时，指示地图是否缩放。
mapping.map.panning	布尔值	true	当拖拽时指示地图是否平移。
mapping.map.zoom	数字	2	地图的初始缩放级别。
mapping.map.fitBounds	(南纬、西经、北纬、东经)		适合地图查看区域的初始边界。纬度值可以在 -85 至 85 的范围内，本范围外的值将被切除。 经度值可以在 -180 至 180 的范围内，本范围外的值将被缩小为在范围内。 为该属性指定的值将有效覆盖分配给中心或缩放属性的任何值。
mapping.seriesColors	列表	Default*	逗号隔开的十六进制颜色值列表（0xRRGGBB）。列表表示没有分配具体 fieldColors 颜色的系列的样本颜色。
mapping.showTiles	布尔值	true	指定是否要显示或隐藏地图图块。
mapping.tileLayer.tileOpacity	文本	1	指定图块的不透明度。值可以从 0（透明）到 1（不透明）。
mapping.tileLayer.url	URL 模板	请参阅描述	基于以下模板请求平铺的 URL。 http://(s).tile.openstreetmap.org/(z)/(x)/(y).png
mapping.tileLayer.subdomains	[string, ...]	[a,b,c]	分布平铺请求到的子域列表。更多子域允许同时请求更多平铺。 请参见以下示例。
mapping.tileLayer.minZoom	整数	0	平铺集的最小缩放级别。
			平铺集的最大缩放级别。

<code>mapping.tileLayer.maxZoom</code>	整数	7	使用任何非负整数指定最大缩放级别。
<code>mapping.tileLayer.invertY</code>	布尔值	False	是否为平铺请求反向 y 坐标。TMS 服务器使用反向 y 轴编号。
<code>mapping.tileLayer.attribution</code>	字符串	请参阅描述	显示在地图右下角的版权属性。默认值： Map data (c) 2012 OpenStreetMap contributors, CC-BY-SA. 请参见以下示例。
<code>mapping.type</code>	marker choropleth	请参阅描述	要呈现的地图类型。默认为 marker (群集地图)。

Choropleth 地图选项

名称	类型	默认	描述
<code>mapping.choroplethLayer.colorBins</code>	整数	5	指定要使用的颜色数据箱数。
<code>mapping.choroplethLayer.colorMode</code>	"sequential" "divergent" "categorical")	'auto'	为 Choropleth 形状指定要使用的颜色模式。可能使用的模式有“序列”、“分散”或“分类”。
<code>mapping.choroplethLayer.maximumColor</code>	文本	DB5800	为最高值形状指定要使用的颜色。
<code>mapping.choroplethLayer.minimumColor</code>	文本	2F25BA	仅当颜色模式是分散时使用。为最低值形状指定要使用的颜色。
<code>mapping.choroplethLayer.neutralPoint</code>	文本	0	仅当颜色模式是分散时使用。颜色选项板从使用最小值颜色到最大值颜色转换的数值。
<code>mapping.choroplethLayer.shapeOpacity</code>	指定形状的不透明度。值可以从 0 (透明) 到 1 (不透明)。	文本	0.75
<code>mapping.choroplethLayer.showBorder</code>	布尔值	true	指定每个形状是否显示边框。
<code>mapping.showTiles</code>	布尔值	true	决定地图图块是否显示。
<code>mapping.tileLayer.tileOpacity</code>	文本	1	指定图块的不透明度。值可以从 0 (透明) 到 1 (不透明)。

群集地图选项

名称	类型	默认	描述
<code>mapping.data.maxClusters</code>	整数	100	要在群集地图中呈现的最大群集数。 警告： 设置本选项为大量群集会显著降低性能。使用一个小于 1000 的值。
<code>mapping.markerLayer.markerOpacity</code>	数字	0.8	群集地图标记的不透明度。值可以从 0 (透明) 到 1 (不透明)。
<code>mapping.markerLayer.markerMinSize</code>	数字	10	群集地图标记的最小大小 (以像素为单位)。
<code>mapping.markerLayer.markerMaxSize</code>	数字	50	群集地图标记的最大大小 (以像素为单位)。

示例

以下示例说明了如何使用不同的地图配置。

`mapping.data.maxClusters`

以下示例将群集的最大数设为 250。

```
<map>
  <option name="mapping.data.maxClusters">250</option>
</map>
```

mapping.fieldColors 和 mapping.seriesColors

以下示例分别配置 "foo" 和 "bar" 字段为红色 (0xFF0000) 和绿色 (0x00FF00)，并配置所有其他字段为蓝色 (0x0000FF)。

```
<map>
  <option name="mapping.fieldColors">{foo:0xFF0000,bar:0x00FF00}</option>
  <option name="mapping.seriesColors">[0x0000FF]</option>
</map>
```

mapping.map.fitBounds example

以下示例初始化地图视图为旧金山周围边界。

```
<map>
  <option name="mapping.map.fitBounds">
    (37.5,-123,38,-122)
  </option>
</map>
```

mapping.tileLayer.*

以下示例配置客户端以请求来自 openstreetmap.org 的平铺（这是默认配置）。

```
<map>
  <option name="mapping.tileLayer.url">http://{s}.tile.openstreetmap.org/{z}/{x}/{y}.png</option>
  <option name="mapping.tileLayer.subdomains">a,b,c</option>
  <option name="mapping.tileLayer.maxZoom">18</option>
  <option name="mapping.tileLayer.attribution">
    Map data (c) 2012 OpenStreetMap contributors, CC-BY-SA.
  </option>
</map>
```

地图示例，使用 foursquare 数据

本示例假定您正新建 foursquare 数据索引为源 foursquare。

```
<map>
  <title>Roma</title>
  <search>
    sourcetype=foursquare
    | geostats latfield=checkin.geolat longfield=checkin.geolong count by checkin.user.gender
  </search>
  <option name="mapping.data.maxClusters">500</option>
  <option name="mapping.markerLayer.markerMaxSize">20</option>
  <option name="mapping.map.fitBounds">(41.3,12.7,41.5,12.8)</option>
  <option name="mapping.seriesColors">[0x0060DD]</option>
  <option name="mapping.map.zoom">4</option>
</map>
```

完整分级统计地图示例

```
<dashboard>
  . . .
  <row>
    <panel>
      <title>choropleth map</title>
      <map>
```

```

<search>
  <query>source="my_mapping_data_source" | iplocation clientip | lookup geo_us_states latitude as lat longitude as lon
| stats count by featureId | geom geo_us_states</query>
  <earliest>-24h@h</earliest>
  <latest>now</latest>
  <sampleRatio>1</sampleRatio>
</search>
<option name="drilldown">all</option>
<option name="mapping.choroplethLayer.colorBins">5</option>
<option name="mapping.choroplethLayer.colorMode">auto</option>
<option name="mapping.choroplethLayer.maximumColor">0xFFB600</option>
<option name="mapping.choroplethLayer.minimumColor">0x2F25BA</option>
<option name="mapping.choroplethLayer.neutralPoint">0</option>
<option name="mapping.choroplethLayer.shapeOpacity">0.75</option>
<option name="mapping.choroplethLayer.showBorder">1</option>
<option name="mapping.data.maxClusters">100</option>
<option name="mapping.legend.placement">bottomright</option>
<option name="mapping.map.center">(0,0)</option>
<option name="mapping.map.panning">1</option>
<option name="mapping.map.scrollZoom">0</option>
<option name="mapping.map.zoom">2</option>
<option name="mapping.markerLayer.markerMaxSize">50</option>
<option name="mapping.markerLayer.markerMinSize">10</option>
<option name="mapping.markerLayer.markerOpacity">0.8</option>
<option name="mapping.showTiles">1</option>
<option name="mapping.tileLayer.maxZoom">7</option>
<option name="mapping.tileLayer.minZoom">0</option>
<option name="mapping.tileLayer.tileOpacity">1</option>
<option name="mapping.type">choropleth</option>
</map>
</panel>
</row>
. .
</dashboard>

```

single value

<single> 元素定义 <panel> 中的单值可视化。



属性

您可以使用 <single> 值元素中的任意可视化共享属性。

选项

除了可视化的共享选项，您可以使用以下选项配置单值可视化。

使用以下选项配置 <single> 值可视化。

注意：在格式菜单中进行的配置可以覆盖简单 XML 设置。

选项名称	类型	默认	描述
colorBy	下一个值： trend value	value	指明是以单值显示颜色更改还是以趋势指示器显示。 要使用此选项，useColors 选项必须设置为 true。 如果您使用 value，值的范围决定使用的颜色。 按照趋势着色只有在可视化搜索使用 timechart 命令时可用。 如果您使用 trend，指示器显示黑色（没有更改）、绿色（正）或红色（负）。使用

			trendColorInterpretation 选项配置正值和负值解释。
colorMode	以下一个值： block none	none	指定单值还是背景显示值范围颜色。 使用 block 以在白色文本的背景中显示颜色。使用 none 以在白色背景的单值上显示颜色。
drilldown	以下一个值： all none	none	使用 all 以启用单值钻取。使用 none 以禁用钻取。
field	字段名称	默认为返回的第一个字段	指示可视化中要显示哪个字段的单值。
numberPrecision	字符串	0	指定要显示的小数位位数。对于十进制精确度，请使用 0. 显示几位数，后面最多跟上四个零。例如，0.0 或 0.00。
rangeColors	字符串阵列	默认为标准范围颜色：红、橙、黄、蓝和绿。	使用字符串队列指定十六进制颜色值的任意数。按照对应 rangeValues 值的顺序列出颜色。十六进制值格式应为 0xFFFFFFFF 或 FFFFFFFF。 如果 rangeColors 值数量大于范围，将忽略超出的颜色值。如果 rangeValues 值数量多于 rangeColors 十六进制颜色，若单值属于没有颜色映射的范围，则单值会呈现出深灰色。
rangeValues	数组	无	使用数字阵列以指定单值的范围。如果您正在按值使用颜色，范围决定单值颜色。使用 rangeColors 选项以指定映射到 rangeValues 值的颜色。
showSparkline	布尔值	true	表示是否显示单值迷你图（如果可用）。 迷你图只适用于包括 timechart 搜索命令的搜索。
showTrendIndicator	布尔值	true	显示或隐藏单值趋势指示器。趋势指示器只在可视化查询包括 timechart 命令时可用。
trendColorInterpretation	以下一个值： standard inverse	standard	指定大于 0 的字段值显示为正（标准）或负（颠倒）趋势。
trendDisplayMode	以下一个值： percent absolute	absolute	指定 delta 值显示为百分比还是绝对量。
trendInterval	SPL 时间调节器	auto	指示计算趋势 delta 的开始时间。将评估从开始时间到最近数据点的趋势。 为时间调节器使用搜索语法，以指示范围。
underLabel	字符串		可视化的标题。
useColors	布尔值	false	启用或禁用可视化颜色。为值和趋势颜色选项设置为 true，使其可用。
useThousandSeparators	布尔值	true	指定数字值是否包括千分位分隔符。例如，1,000 包括一个千分位分隔符。
unit	简短的文本标签	无	指定单值旁显示标签。单位文本应简短。通常可以使用缩写，如 MB 或符号，如 \$。
unitPosition	以下一个值： before after	after	指定单位标签应在单值前还是单值后显示。

弃用的选项

属性	类型	默认	描述	方式
additionalClass	CSS 类名称		要添加到结果容器的 CSS 类名称。	使用 colorBy、rangeValues 和 rangeColors 以配置值的颜色映射。
afterLabel	字符串		可视化标签	使用 underLabel 以包含标题或使用 unit 为单值添加测量单位。
beforeLabel	字符串		可视化标签	使用 underLabel 以包含标题或使用 unit 为单值添加测量单位。
classField	字符串		将第一个结果的 classField 值作为附加 CSS 类添加到结果容器中。	使用 colorBy、rangeValues 和 rangeColors 以配置值的颜色映射。
linkFields	字符串	result	指示可单击进行钻取的可视化元素。	单值本身可单击进行钻取。使用 <drilldown> 元素以配置钻取行为。
linkSearch	搜索字 字符串		搜索可单击进行钻取的结果的所属元 素。	单值本身可单击进行钻取。使用 <drilldown> 元素以配置钻 取行为。
linkView	仪表板 或表单		与 linkSearch 搜索结合使用以进行 钻取的仪表板或表单。	使用 <drilldown> 元素配置钻取行为，包括链接到仪表板或 表单。
refresh.auto.interval	整数	0	指定可视化刷新间隔。要禁用面板刷 新，请指定为 0 或一个负整数。	使用 refresh 属性配置仪表板或表单刷新行为，或使用 <search> 元素 <refresh> 子元素配置面板刷新行为。

示例

```

<dashboard>
  .
  .
  <panel depends="$show_single_value$">
    <title>Event count for $selected_sourcetype$</title>
    <single>
      <search>
        <query>index=_internal sourcetype=$selected_sourcetype$ | stats count</query>
      </search>
      <option name="colorMode">block</option>
      <option name="drilldown">all</option>
      <option name="rangeColors">["0x65a637", "0x6db7c6", "0xf58f39", "0xd93f3c"]</option>
      <option name="rangeValues">[0,30,100]</option>
      <option name="underLabel">events</option>
      <option name="useColors">1</option>
    </single>
  </panel>
  .
  .
</dashboard>

```

html

显示内联的 HTML 内容。

属性

除了可视化的共享属性，您可以在 <html> 元素中使用以下属性。

名称	类型	默认	描述
encoded	布尔值	false	仅用于内部使用。
			将 HTML 或图像文件的内容放入 <html> 面板。对于 HTML 文件和图像文件，目录位置和简单 XML 语法有所不同。 同一个应用上下文中的 HTML 文件 <html src=" <file_name>.html"></file_name>

src	字符串	<pre></html> 不同应用上下文中的 HTML 文件 <html src="<other_app_name>:<file_name>.html"> </html></other_app_name></pre> <p>图像文件</p> <pre><html> <img src="/static/app/<app_name>/images/<file_name>.png"> </html></pre> <p>请参阅以下说明了解关于保存 HTML 和图像文件的位置，以及如何从不同应用上下文引用文件。</p>
tokens	布尔值	true 如果为 false，则禁用 <html> 面板的标记替换。

在仪表板面板中使用 HTML 文件。

步骤

- 将 HTML 文件放在以下目录中。 \$SPLUNK_HOME/etc/apps/<app_name>/appserver/static
- 在 <html> 面板中，使用此语法指示当前应用上下文中的文件。

```
<html src=".html">
</html>
```

如果您正在从另一个应用上下文指定 HTML 文件，使用此语法。

```
<html src=":<file_name>.html">
</html>
```

在仪表板面板中使用图像文件

步骤

- 将图像文件放在以下目录中。 \$SPLUNK_HOME/etc/apps/<app_name>/appserver/static/images

如果 /images 目录不存在，新建一个目录，并将文件放入其中。

- 测试以下 URL，验证图像文件路径可以访问。
`http://<host>:<port>/static/app/<app_name>/images/<image>`

比如，使用此 URL 验证 my_image.png 文件可访问。

`http://localhost:8000/static/app/search/images/my_image.png`

- 在 <html> 面板中，使用此语法指示当前应用上下文中的文件。

```
<html>

</img>
</html>
```

选项

没有 <html> 元素的子选项。

示例

```
<dashboard>
  <label>test_db</label>
  <row>
    <panel>
      <html>
        <!-- Use an image from the current app's /static/images directory -->
        </img>
      </html>
    </panel>
  </row>
</dashboard>
```

```

</html>
</panel>
<panel>
<!-- Use an HTML file from the webhook app. -->
<html src="alert_webhook:my_html_file.html">
</html>
<!--Use an image from the webhook app static/images directory -->
<html>
</img>
</html>
</panel>
</row>
</dashboard>

```

search

使用 `<search>` 元素在仪表板、表单或面板中定义搜索。您还可以使用 `<search>` 以动态定义输入选择。

搜索类型

`<search>` 元素可以定义以下任意搜索类型。

搜索类型	描述
内联	直接在仪表板、表单或面板中定义搜索。使用 <code><query></code> 元素指定搜索字符串。您可以添加时间范围调节器和其他选项以配置搜索。
报表引用	在面板中使用报表搜索和可视化。为 <code><search></code> 元素添加 <code>ref</code> 属性和报表名称。 您可以配置引用报表的可视化并为搜索添加自定义时间范围调节器。您无法在简单 XML 中修改搜索字符串。编辑报表以调整搜索字符串。当您编辑报表搜索时，引用此报表的面板自动更新。
为输入选项填充搜索	将 <code><search></code> 用作表单输入的子元素以填充复选框、下拉、多选或单选输入的选项。表示 <code><fieldForLabel></code> 和 <code><fieldForValue></code> 搜索结果字段将填充输入选择标签和选择值。 不要将实时搜索用于填充搜索。生成实时搜索结果时，输入选择标签和值不更新。
基本搜索	基本搜索为后期处理搜索生成转换结果以进行修改。基本搜索可以是全局搜索，在 <code><dashboard></code> 中或 <code><form></code> 级别定义。您还可以在简单 XML 中使用 <code><panel></code> 级的基本搜索。 确保所有的基本搜索满足以下要求。 <ul style="list-style-type: none"> 在基本搜索中使用转换命令来生成转换结果。非转换基本搜索可能导致性能和超时问题。 基本搜索必须有 <code><id></code> 属性以供后期处理搜索引用。
后期处理搜索	后期处理搜索接受来自基本搜索的已转换结果，并对这些结果实施其他搜索处理。使用 <code>base</code> 和 <code>id</code> 属性以引用后期处理搜索的基本搜索 ID。 在基本搜索中指定 <code><earliest></code> 和 <code><latest></code> 元素。后期处理搜索忽略在后期处理 <code><search></code> 元素中定义的时间调节器。 有关后期处理搜索的更多信息，请参阅本手册中的“后期处理搜索”。

元素层次

您可以将 `<search>` 元素放入以下任意父级元素中。

- `<form>`
- `<dashboard>`
- `<panel>`
- `<chart>`
- `<event>`
- `<map>`
- `<single>`
- `<table>`

属性



名称	类型	默认	描述
app	文本		应用的名称。 结合使用 <code>app</code> 属性和 <code>ref</code> 属性，以引用不在当前应用的报表。
base	文本		在后期处理搜索中，引用此仪表板、表单或面板中的基本搜索。将 <code>id</code> 属性与 <code>base</code> 结合使用以指示后期处理搜索应使用的基本搜索。
depends	一个或多个标记的列表		列出的所有标记必须经过定义以方便搜索分发。如果搜索不分发，面板不呈现。
id	文本（最小两个字符）		搜索标识符。在后期处理搜索中，使用此标识符引用基本搜索。 确保搜索标识符满足这些要求。 <ul style="list-style-type: none"> • 只能使用字母数字或下划线字符。 • <code>id</code> 不能以数字或下划线字符开始。 • 以下术语预留给内部使用，且不能用于 <code>id</code>。 <ul style="list-style-type: none"> ◦ dashboard ◦ default ◦ footer ◦ header ◦ search ◦ submitted ◦ url
ref	文本		引用报表。添加报表搜索和可视化到仪表板或表单。 如果您正在另一个应用中引用报表，则使用 <code>app</code> 属性指定该应用。
rejects	一个或多个标记的列表		如果定义此列表中的一个或多个标记，阻止搜索分发。如果搜索不分发，面板不呈现。

子元素

在 `<search>` 中使用以下子元素。

元素	类型	默认	描述
<code><cache></code>	对于已保存的搜索，使用下列值中的一个。 <ul style="list-style-type: none"> • <code>true</code> • <code>false</code> • <code>scheduled</code> • <code>[integer]</code> 	<code>scheduled</code>	<ul style="list-style-type: none"> • <code>true</code>: 可能的话，始终使用已存在的保存的搜索任务中的结果。 • <code>false</code>: 不要使用之前存在的保存的搜索任务中的结果。 • <code>scheduled</code>: 重新使用之前运行的计划保存的搜索任务。 • <code>[integer]</code>: 秒数表示最大保存的搜索任务结果时间。只使用比此秒数更新的结果。
<code><cancelled></code>	N/A	N/A	当搜索取消时执行操作。
<code><done></code>	N/A	N/A	基于已完成的搜索事件执行操作。包含任务属性和第一个结果行。
<code><error></code>	N/A	N/A	当出现搜索错误事件，如无效查询时，请执行操作。
<code><earliest></code> 和 <code><latest></code>	文本		<p>指定搜索的最早和最晚时间参数的可选时间表达式。</p> <p>后期处理搜索会忽略子元素 <code><earliest></code> 和 <code><latest></code>。而会使用来自基本搜索的 <code><earliest></code> 和 <code><latest></code> 元素。</p> <p>您可将时间指定为相对时间或绝对时间。对于相对时间，使用相对时间调节器，如《搜索手册》中的“在搜索中指定相对时间范围”部分所介绍。对于绝对时间，指定时间为 UNIX epoch 时间格式。</p> <p>注意：对于简单 XML 中的绝对时间来说，UNIX epoch 时间格式与查询中所使用的 SPL 绝对时间格式有所不同。</p>
<code><progress></code>			执行搜索进度事件的操作。访问任务属性和第一个结果行。

<query>	文本		搜索字符串。
<refresh>	整数或相对时间表达式	不刷新	<p>表示内联或保存的搜索的延迟或间隔时间。此设置不会应用于后期处理搜索，这种搜索会在其基本搜索刷新时自动刷新。</p> <p>整数以秒处理。对于相对时间表达式，使用 SPL 语法。例如，1h5m 或 5m。</p> <p>使用 <refreshType> 设置指定与搜索完成或分发相关的刷新行为。</p> <p>可以使用可视化中的 <refresh.display> 设置来指定刷新进度指示器。</p>
<refreshType>	interval 或 delay	delay	<p>表示刷新倒计时的开始时间。使用 delay 在搜索完成时开始计时。</p> <p>使用 interval 在搜索分配后时开始倒计时。如果搜索的运行时间大于配置的时间，则此搜索任务会取消，并会分发一个新任务。</p>
<sampleRatio>	数字		事件示例比例。要了解更多信息，请参阅《搜索手册》中“带有报表与仪表板面板的事件示例”。

示例

来自内联搜索的基本搜索

```
<search id=[base ID]>
  <query>[search string]</query> (1)
  <earliest> (0..1)
  <latest> (0..1)
```

来自报表的基本搜索

```
<search id=[base ID] [ref=[report name]]>
  <earliest> (0..1)
  <latest> (0..1)
```

后期处理搜索

```
<search base=[base ID] (0..n)
  <query>[post-process search string]</query> (1)
```

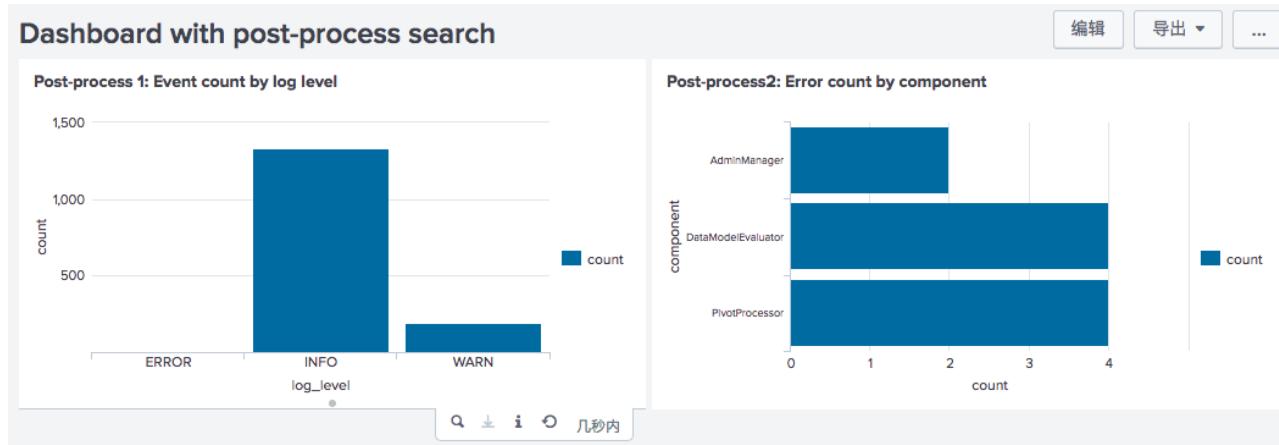
具有基本搜索和两个后期处理搜索的仪表板

```
<dashboard>
  <label>Dashboard with post-process search</label>
  <description></description>
  <!-- Example uses stats transforming command -->
  <!-- This limits events passed to post-process search -->
  <search id="baseSearch">
    <query>
      index=_internal source=*splunkd.log | stats count by component, log_level
    </query>
    <earliest>-30d</earliest>
    <latest>now</latest>
  </search>
  <row>
    <panel>
      <chart>
        <title>Post-process 1: Event count by log level</title>
        <!-- post-process search -->
        <search base="baseSearch">
          <query>
            stats sum(count) AS count by log_level
          </query>
        </search>
      </chart>
    </panel>
  </row>
</dashboard>
```

```

<panel>
  <chart>
    <title>Post-process2: Error count by component</title>
    <!-- post-process search -->
    <search base="baseSearch">
      <query>
        search log_level=error | stats sum(count) AS count by component
      </query>
    </search>
    <option name="charting.chart">bar</option>
  </chart>
</panel>
</row>
</dashboard>

```

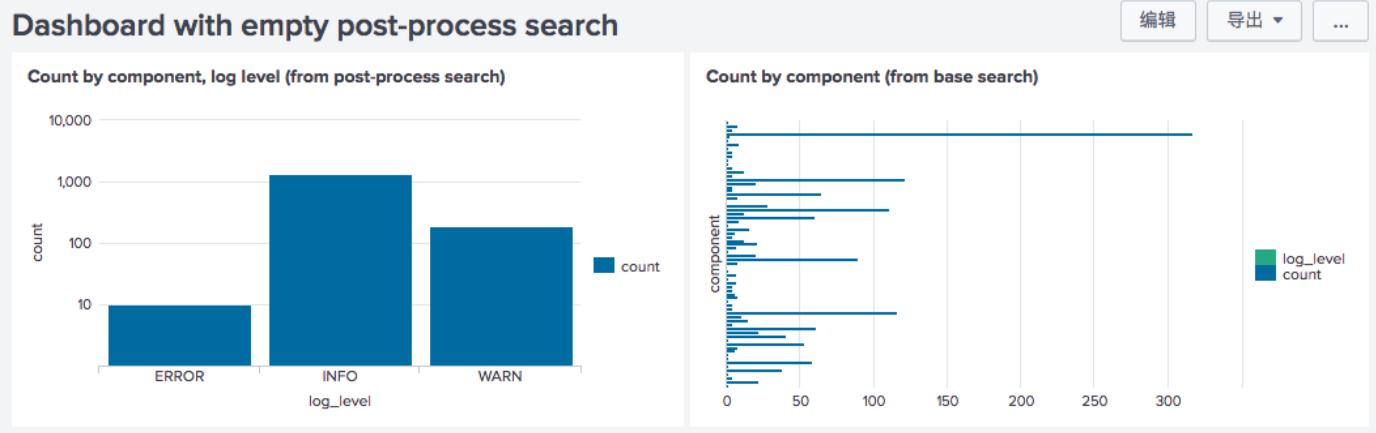


带空的后期处理搜索的仪表板

```

<dashboard>
  <label>Dashboard with empty post-process search</label>
  <description></description>
  <!-- Example uses stats transforming command -->
  <!-- This limits events passed to post-process search -->
  <search id="baseSearch">
    <query>index=_internal source=*/splunkd.log | stats count by component, log_level</query>
    <earliest>-30d</earliest>
    <latest>now</latest>
  </search>
  <row>
    <panel>
      <chart>
        <title>Count by component, log level (from post-process search)</title>
        <!-- post-process search -->
        <search base="baseSearch">
          <query>stats sum(count) AS count by log_level</query>
        </search>
        <option name="charting.axisY.scale">log</option>
      </chart>
    </panel>
    <panel>
      <chart>
        <title>Count by component (from base search)</title>
        <!-- empty post-process search -->
        <search base="baseSearch" />
        <option name="charting.chart">bar</option>
      </chart>
    </panel>
  </row>
</dashboard>

```



selection (面积图、柱形图和折线图)

在面积图、柱形图或折线图中使用 `<selection>` 元素以配置平移和缩放时间窗口参数或设置其他标记值。

请参阅“图表控制”以了解关于使用图表平移和缩放的更多信息。

父元素

```
<chart>
<option name="charting.chart">area</option> | <option name="charting.chart">column</option> |<option
name="charting.chart">line</option>
```

使用预定义的标记来捕获时间窗口的最早和最晚时间，以及为字段捕获该时间窗口内的最早和最晚值。

示例

```
<selection>
  <set token="selection.earliest">$start$</set>
  <set token="selection.latest">$end$</set>
  <set token="start.[fieldname]">$start.[fieldname]$</set>
  <set token="end.[fieldname]">$end.[fieldname]$</set>
</selection>
```

您还可以在 `<selection>` 元素中 `<link>` 到目标仪表板、表单或外部网站。

属性

无

示例

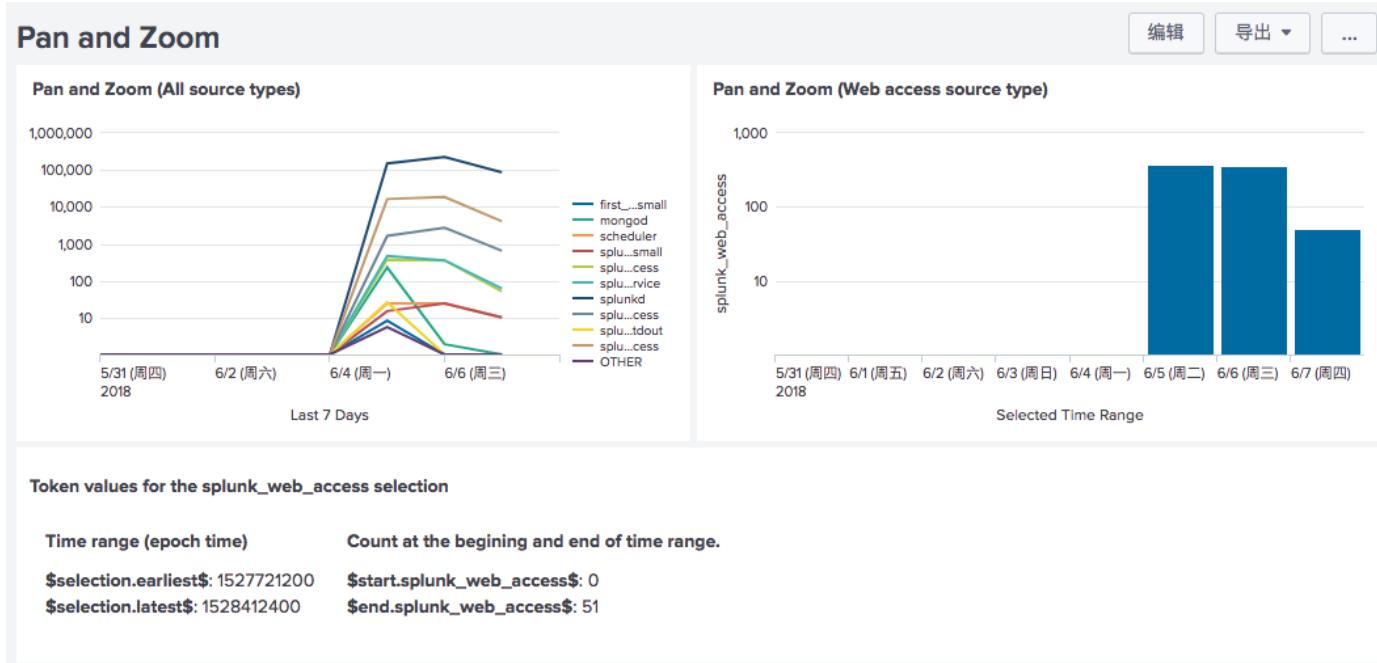
左边图表的选择部分放大为右边的图表，并包括选择区域的详细信息。

```
<dashboard>
<label>Pan and Zoom</label>
<row>
  <panel>
    <chart>
      <title>Pan and Zoom (All source types)</title>
      <search>
        <query>
          index=_internal | timechart count by sourcetype
        </query>
        <earliest>-7d@h</earliest>
        <latest>now</latest>
      </search>
      <option name="charting.axisX.scale">linear</option>
      <option name="charting.axisY.scale">log</option>
    </chart>
  </panel>
</row>
```

```

<option name="charting.chart">line</option>
<selection>
    <set token="selection.earliest">$start$</set>
    <set token="selection.latest">$end$</set>
    <set token="start.splunk_web_access">$start.splunk_web_access$</set>
    <set token="end.splunk_web_access">$end.splunk_web_access$</set>
</selection>
<option name="charting.axisTitleX.text">Last 7 Days</option>
</chart>
</panel>
<panel>
<chart>
    <title>Pan and Zoom (Web access source type)</title>
    <search>
        <query>
            index=_internal sourcetype=splunk_web_access
            | timechart count by sourcetype
        </query>
    <earliest>$selection.earliest$</earliest>
    <latest>$selection.latest$</latest>
    </search>
    <option name="charting.chart">column</option>
    <option name="charting.legend.placement">none</option>
    <option name="charting.legend.masterLegend">null</option>
    <option name="charting.axisX.scale">linear</option>
    <option name="charting.axisY.scale">log</option>
    <option name="charting.axisTitleX.text">Selected Time Range</option>
</chart>
</panel>
</row>
<row>
<panel>
<html>
    <h3>Token values for the splunk_web_access selection</h3>
    <table border="0" cellpadding="12" cellspacing="0">
        <tr>
            <td>
                <p><b>Time range (epoch time)</b></p>
                <p>
                    <b>$selection.earliest$</b>: $selection.earliest$<br/>
                    <b>$selection.latest$</b>: $selection.latest$<br/>
                </p>
            </td>
            <td>
                <p><b>Count at the begining and end of time range.</b></p>
                <p>
                    <b>$start.splunk_web_access$</b>: $start.splunk_web_access$<br/>
                    <b>$end.splunk_web_access$</b>: $end.splunk_web_access$<br/>
                </p>
            </td>
        </tr>
    </table>
</html>
</panel>
</row>
</dashboard>

```



钻取

钻取使您建立对用户输入或互动的动态响应。使用以下元素以配置钻取行为。

请参阅“将钻取用于仪表板交互”了解使用仪表板和表单钻取的详细信息。

使用 `<drilldown>` 元素以开始实施钻取行为。`<drilldown>` 元素包含定义对用户单击的响应的子元素。

钻取操作

在 `<drilldown>` 元素中，使用 `<set>`、`<unset>` 或 `<eval>` 将标记值作为建立动态行为更新或在当前仪表板或表单中显示。使用 `<link>` 以打开搜索、另一个仪表板或外部网站。您可以通过单击将标记值传递到连接目标。

钻取条件

通过在 `<drilldown>` 中添加 `<condition>` 元素，为不同用户操作定义条件响应。

将操作或条件用作钻取子元素。

您无法将操作和条件作为 `<drilldown>` 的直接子元素结合起来。如果您正在定义条件钻取行为，您无法在 `<drilldown>` 元素中直接包含操作元素。如果您正在直接从 `<drilldown>` 元素定义操作，您无法直接在钻取中添加 `<condition>` 元素。

属性

无

元素层次

将 `<drilldown>` 元素放入以下任意可视化父元素。

- `<chart>`
- `<event>`
- `<map>`
- `<single>`
- `<table>`

子元素

使用 `<drilldown>` 中的以下子元素配置用户单击钻取启用的元素时发生的操作。

```
<drilldown>
( <link> | <set> | <unset> ) (1..n) | <condition> (1..n)
```

示例

将值传递给表单

```
<table>
<search>index=_internal</search>

<!-- Pass the clicked row's 'count'-column value -->
<!-- to populate a destination form's 'foo' token. -->
<drilldown>
  <link>
    /app/search/simple_xml_form?form.foo=$row.count$
  </link>
</drilldown>
</table>
```

将参数传递给表单

```
<table>
<search>index=_internal</search>

<!-- Pass the clicked cell's value, earliest time, -->
<!-- and latest time to a destination form's -->
<!-- token ('foo') and search parameters -->
<drilldown>
  <link>
    <![CDATA[
/app/search/simple_xml_form?form.foo=$click.value2$&earliest=$earliest$&latest=$latest$
  ]]>
  </link>
</drilldown>
</table>
```

将来自图表的值传递给网站

```
<chart>
<search>
  index=_internal | chart count by sourcetype
</search>
<option name="charting.chart">column</option>

<!-- $click.value$ captures the value clicked by the user -->
<!-- From the x-axis of a column chart and passes -->
<!-- it to the website as a query parameter -->
<drilldown>
  <link>
    http://splunkbase.splunk.com/integrated_search/?q=$click.value$
  </link>
</drilldown>
</chart>
```

condition (钻取)

定义对用户单击仪表板或表单中特定字段的条件响应。如果 `<condition>` 元素不存在，钻取操作适用于任何字段上的单击。

请参阅 `<condition>` (输入) 以了解关于在表单输入中使用 `<condition>` 的详细信息。

属性

名称	类型	默认	描述
field	文本	*	在实现钻取、或设置或取消设置标记的地方指定搜索字段。

子元素

请参阅 `Eval`、`Link`、`Set` 和 `Unset`。

示例

请参阅 `<set>` 示例，了解使用 `<condition>` 标签为页面内钻取设置标记。

`Eval`、`Link`、`Set` 和 `Unset`

管理标记值

更新标记值以在仪表板和表单中新建动态显示和行为。配合 `<drilldown>` 或 `<change>` 元素使用 `eval`、`link`、`set` 和 `unset` 定义对用户交互的响应。

元素层次

```
<input>
<change>
  ( <set> | <unset> | <link> | <eval> ) (1..n)
    <condition> (0..n)
      ( <set> | <unset> | <link> | <eval> ) (1..n)

<drilldown>
  ( <set> | <unset> | <link> | <eval> ) (1..n)
    <condition> (0..n)
      ( <set> | <unset> | <link> | <eval> ) (1..n)
```

`Eval`

筛选或设置标记值的格式。关于更多信息，请参阅“对于仪表板 `eval` 表达式的自定义逻辑”。

属性

名称	类型	默认	描述
token	文本	无	<p>值由 <code><eval></code> 表达式生成的标记。</p> <p>在 <code><eval></code> 表达式中，您可以将 <code>\$...\$</code> 分隔符或单引号分隔符用作标记。例如，以下这两种选项都是有效的。</p> <ul style="list-style-type: none">• <code>\$my_token\$</code>• <code>'my_token'</code>

示例

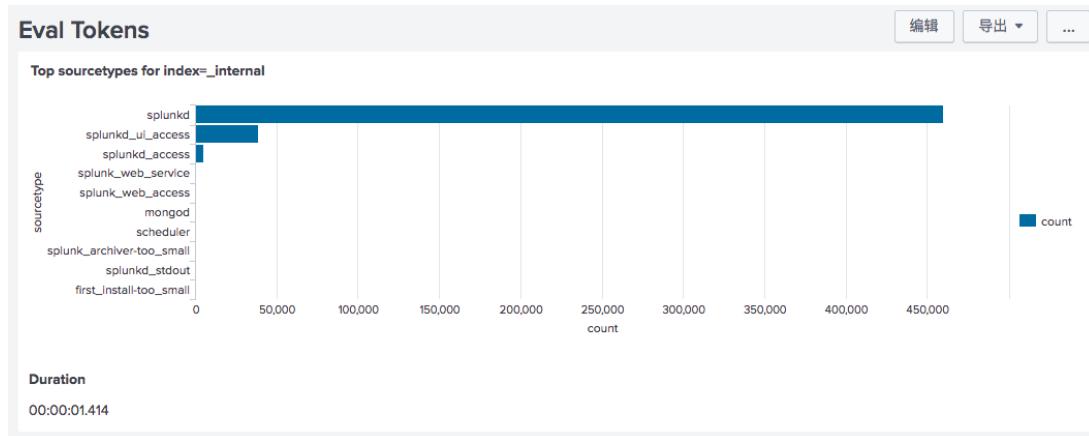
此示例配合 `<progress>` 搜索事件处理程序使用 `<eval>` 以在仪表板中计算和显示任务持续时间。

```
<dashboard stylesheet="eval_tokens.css">
  <label>Eval Tokens</label>
  <row>
    <panel>
      <title></title>
      <search id="search_logic">
        <query>index=_internal | top sourcetype</query>
        <earliest>0</earliest>
        <latest>now</latest>
        <progress>
          <eval token="duration">toString(tonumber($job.runDuration$),"duration")</eval>
        </progress>
      </search>
      <chart>
        <title>Top sourcetypes for index=_internal</title>
        <search base="search_logic" />
```

```

<option name="charting.chart">bar</option>
</chart>
<html>
  <h3>Duration</h3>
  <div class="custom-result-value">$duration$</div>
</html>
</panel>
</row>
</dashboard>

```



Link

作为对钻取单击或表单输入的响应，链接到仪表板、表单或外部网站。

属性

名称	类型	默认	描述
target	文本		<p>显示钻取目标打开的浏览器窗口。</p> <p>对应于 <code><a></code> HTTP 标记的 <code>target</code> 属性。</p> <ul style="list-style-type: none"> “<code>_blank</code>”：在新窗口中打开目标。 “<code>_self</code>”：在当前窗口中打开目标。 <code><optional_string></code>：使用一个任意字符串，以在新窗口中打开目标。之后每次用户单击请求此钻取时，目标在同一窗口中打开。

弃用属性

名称	类型	描述	方式
field	字段名称	(仅用于 <code><drilldown></code>) 指定从指定列或行捕获的表格中的值。不能同时用 <code>series</code> 属性指定。	使用 <code><condition></code> 标签指定字段。
series	系列名	(仅用于 <code><drilldown></code>) 指定从特定系列捕获的表格中的值。不能同时用 <code>field</code> 属性指定。	使用 <code><condition></code> 标签指定系列。

链接路径语法

`<link>` 元素包含目标路径和您正在从来源传到目标的任何标记值。使用以下语法选项中的一种。

目标和行为	语法
在您的 Splunk 部署中链接到仪表板。	<p>使用包含仪表板或表单 ID 的相对路径。</p> <pre><link> [relative path]/[dashboard or form id] </link></pre>
	在相对路径后添加一个 ? 符号。将目标中的标记设置为从数据来源传递来的值。此示例将目

<p>链接到您的 Splunk 部署中的表单。通过传递从来源获取的标记值显示表单中的自定义内容。使用标记值填充表单输入。</p>	<p>标表单中的标记设置为数据来源中的值。</p> <p>使用 <code>form.</code> 作为目标表单中标记的前缀，如此处所示。</p> <pre><link> [relative path]/[dashboard or form id]? form.[target_token_name]=[\$source_value\$] </link></pre>
<p>将 <code><earliest></code> 和 <code><latest></code> 时间范围调节器从数据来源搜索传递到目标中的搜索。</p>	<p>添加 <code>&earliest=\$earliest&latest=\$latest</code> 到目标路径和标记值。使用 <code><![CDATA[...]]></code> 包装确保 <code>&</code> 符号解释正确。</p> <pre><link> <![CDATA[[relative path]/[dashboard or form id]? form.[target_token_name]=[\$source_value\$]&earliest=\$earliest&latest=\$latest]]> </link></pre>
<p>使用 URL 和查询参数来将值传递给目标 Web 页面。</p>	<pre><link>[target_URL]?q=[\$source_value\$] </link></pre>

另请参阅“仪表板中的标记用法”，了解可用的标记筛选器。

示例

使用具有条件式输入的 `<link>` 打开新页面。

```
<form>
. . .
<fieldset>
<input type="dropdown" token="openNewPageToken">
<label></label>
<default>Select a page to open</default>
<choice value="">Select a page to open</choice>
<choice value="manager_page">Buttercup Games dashboard</choice>
<choice value="splk_page">Splunk home page</choice>
<change>
<condition value="manager_page">
<link target="_blank">
    /app/search/buttercup_games
</link>
</condition>
<condition value="splk_page">
<link target="_blank">
    http://splunk.com
</link>
</condition>
</change>
</input>
</fieldset>
. . .
</form>
```

设置

设置或更新其他仪表板或表单元素可以使用的标记值。您可以将标记设置为新建动态行为或显示的一部分，例如将用户已选值从表单输入传递到搜索或管理面板隐藏或显示行为。

元素层次

表单输入

```
<change>
<condition> (optional)
<set>
```

钻取

```
<drilldown>
  <condition> (optional)
    <set>
```

属性

名称	类型	描述	示例
token	标记名称	必填。 使用您正在设置或更新其值的标记。 此示例将 <code> \$s\$</code> 标记筛选器包含在内以指示标记值应作为字符串处理。	<code><set token="[token_name]"> sourcetype=\$click.value \$s\$</set></code>
prefix	文本	添加到标记值开头的字符串。 此示例在标记值两边附加引号 <code>prefix</code> 和 <code>suffix</code> 。	<code><set token="[token_name]"> prefix="sourcetype="" suffix=""">\$click.value\$</set></code>
suffix	文本	附加到标记值的字符串。 此示例在标记值两边附加引号 <code>prefix</code> 和 <code>suffix</code> 。	<code><set token="[token_name]"> prefix="sourcetype="" suffix=""">\$click.value\$</set></code>

示例

单击表格，会设置一个标记，用于图表可视化的搜索。

```
<dashboard>
  <label>In-page Drilldown</label>
  <row>
    <panel>
      <table>
        <title>Set sourcetype token on click</title>
        <search>
          <query>
            index=_internal | stats count by sourcetype
          </query>
          <earliest>-1h</earliest>
          <latest>now</latest>
        </search>
        <drilldown>
          <condition field="sourcetype">
            <set token="sourcetype">$click.value2$</set>
          </condition>
        </drilldown>
      </table>
      <chart>
        <title>Chart for $sourcetype$</title>
        <search>
          <query>
            index=_internal sourcetype=$sourcetype$ | timechart count by sourcetype
          </query>
          <earliest>-1h</earliest>
          <latest>now</latest>
        </search>
      </chart>
    </panel>
  </row>
</dashboard>
```

unset

使用 `<unset>` 以清除之前设置的标记值。当您取消设置标记时，再次设置前此值为空。取消设置标记值可以帮助您在仪表板和

表单中实现动态显示或其他行为。

属性

名称	类型	描述
token	标记名称	必填。使用您正在取消设置其值的标记。

示例

配合仪表板面板中的 `depends` 和 `rejects` 使用 `<set>` 和 `<unset>` 以更改在不同用户单击时出现的可视化。

```
<dashboard>
  <label>Example for <set> and <unset></label>
  <row>
    <panel>
      <table>
        <title>Set sourcetype token</title>
        <search>
          <query>
            index=_internal | stats count by sourcetype
          </query>
          <earliest>-1h</earliest>
          <latest>now</latest>
        </search>
        <drilldown>
          <!-- For the sourcetype field clicked: -->
          <!-- Set token to display a chart -->
          <!-- Unset token to display a table -->
          <condition field="sourcetype">
            <set token="sourcetype">$row.sourcetype$</set>
            <set token="showChart">foo</set>
            <unset token="showTable"></unset>
          </condition>
          <!-- For any other field clicked: -->
          <!-- Set token to display a table -->
          <!-- Unset token to display a chart -->
          <condition field="*"/>
            <set token="sourcetype">$row.sourcetype$</set>
            <set token="showTable">foo</set>
            <unset token="showChart"></unset>
          </condition>
        </drilldown>
      </table>
    </panel>

    <!-- Hide the html panel when either token is present -->
    <!-- Click in the original table to set either token -->
    <panel>
      <html rejects="$showTable$, $showChart$">
        <h2>Details</h2>
        <div style="padding: 50px; margin: 0 auto; width: 350px;">
          <div class="alert alert-warning">
            <i class="icon-alert"/>
            Click on a row in the table on the left to show details.
          </div>
        </div>
      </html>
    <!-- if showChart token is set, display results here -->
    <chart depends="$showChart$">
      <title>Details for $submitted:sourcetype|s$</title>
      <search>
        <query>
          index=_internal sourcetype=$sourcetype|s$
          | timechart count by sourcetype
        </query>
      </search>
    </chart>
  </row>
</dashboard>
```

```

<earliest>-1h</earliest>
<latest>now</latest>
</search>
</chart>
<!-- if showCTable token is set, display results here --&gt;
&lt;table depends="$showTable$"&gt;
&lt;title&gt;Details for $submitted:sourcetype|$s&lt;/title&gt;
&lt;search&gt;
&lt;query&gt;
index=_internal sourcetype=$sourcetype|$s|
timechart bins=10 count by sourcetype
&lt;/query&gt;
&lt;earliest&gt;-1h&lt;/earliest&gt;
&lt;latest&gt;now&lt;/latest&gt;
&lt;/search&gt;
&lt;option name="wrap"&gt;true&lt;/option&gt;
&lt;option name="rowNumbers"&gt;false&lt;/option&gt;
&lt;option name="dataOverlayMode"&gt;none&lt;/option&gt;
&lt;option name="drilldown"&gt;cell&lt;/option&gt;
&lt;option name="count"&gt;10&lt;/option&gt;
&lt;/table&gt;
&lt;/panel&gt;
&lt;/row&gt;
&lt;/dashboard&gt;
</pre>

```

预定义钻取标记

用户单击不同的可视化元素时，预定义标记捕获信息。根据可视化类型不同，您可以使用不同标记捕获单击位置或相关数据。

chart

标记	描述
\$click.name\$	单击位置的 X 轴字段或类别名称。如果用户单击图表图例，则不可用。
\$click.value\$	单击位置的 X 轴字段或类别值。如果用户单击图表图例，则不可用。
\$click.name2\$	单击位置的 Y 轴字段或系列名称。如果用户单击图表图例，则不可用。
\$click.value2\$	单击位置的 Y 轴字段或系列值。如果用户单击图表图例，则不可用。
\$row.<fieldname>\$	访问对应单击位置 X 轴的 Y 轴的字段值。如果用户单击图表图例，则不可用。
\$row.<x-axis-name>\$	访问对应单击位置的 X 轴字段值。如果用户单击图表图例，则不可用。
\$earliest\$	单击图表分段的最早时间。如果不适用，使用搜索的最早时间。
\$latest\$	单击图表分段的最晚时间。如果不适用，使用搜索的最近时间。

event

标记	描述
\$click.name\$	在事件列表中的单击元素的字段名称。如果单击位置的字段名称不可用，\$click.name\$ 值默认如下。 <ul style="list-style-type: none"> 在事件中单击元素：_raw 单击事件时间戳：_time 单击标签：使用标签名称。例如，如果 host 已加标签，使用 host。
\$click.value\$	事件列表中的单击元素的字段值。
\$click.name2\$	和 \$click.name\$ 一样。
\$click.value2\$	和 \$click.value\$ 一样。
\$row.<fieldname>\$	访问单击事件中的任意字段值。例如，要获取 host 字段值，请使用 \$row.host\$。
\$earliest\$	单击事件的最早时间。等同于 _time 字段值。默认为最早搜索时间。

\$latest\$	单击事件的最晚时间。等同于 <code>_time</code> 字段值后的一秒。默认为最晚搜索时间。
------------	---

map

预定义标记对群集和分级统计地图可用。一些标记只在群集地图中可用。

标记	描述
<code>\$click.name\$</code>	单击位置的字段名称。如果多个字段与位置有关，请使用第一个字段。
<code>\$click.value\$</code>	单击位置的字段值。如果多个字段与位置有关，请使用第一个字段。
<code>\$click.name2\$</code>	相当于 <code>\$click.name\$</code>
<code>\$click.value2\$</code>	相当于 <code>\$click.value\$</code>
<code>\$row.<fieldname>\$</code>	访问与单击位置相关的字段值。查看“统计”选项卡了解可用字段。
<code>\$earliest\$</code>	生成地图的搜索的最早时间。
<code>\$latest\$</code>	生成地图的搜索的最晚时间。
<code>\$click.lat.name\$</code>	群集地图：单击位置的纬度字段名称。
<code>\$click.lat.value\$</code>	群集地图：单击位置的纬度字段值。
<code>\$click.lon.name\$</code>	群集地图：单击位置的经度字段名称。
<code>\$click.lon.value\$</code>	群集地图：单击位置的经度字段值。
<code>\$click.bounds.<orientation>\$</code>	群集地图：单击位置的南、西、北或东外层边界。例如，使用 <code>\$click.bounds.east\$</code> 以获取东外层界限。

single value

标记	描述
<code>\$click.name\$</code>	单值代表的字段名称。 在配置单值钻取的 <code><condition></code> 元素中， <code>field</code> 对应 <code>\$click.name\$</code> 。
<code>\$click.value\$</code>	单值代表的字段值
<code>\$click.name2\$</code>	和 <code>\$click.name\$</code> 的一样。
<code>\$click.value2\$</code>	和 <code>\$click.value\$</code> 的一样。
<code>\$row.<fieldname>\$</code>	访问单值统计表行中的任意字段值。
<code>\$earliest\$</code>	生成单值搜索的最早时间。
<code>\$latest\$</code>	生成单值搜索的最晚时间。

table

标记	描述
<code>\$click.name\$</code>	表中最左边字段（列）名称。通常， <code>_time</code> 位于含此字段且各列按默认排序的表中的最左边。
<code>\$click.value\$</code>	单击表行中的最左字段（列）值。
<code>\$click.name2\$</code>	单击字段（列）名称。在配置表钻取的 <code><condition></code> 元素中， <code>field</code> 对应 <code>\$click.name2\$</code> 。
<code>\$click.value2\$</code>	单击字段（列）值。使用此标记捕获用户单击的特定表格单元值。

\$row.<fieldname>\$	访问来自单击表行的任何字段（列）值。
\$earliest\$	单击图表行的最早时间。如果不适用，使用搜索的最早时间。
\$latest\$	单击表行的最晚时间。如果不适用，使用搜索的最晚时间。

棚架

标记	描述
\$trellis.name\$	拆分字段名称
\$trellis.value\$	拆分字段值

弃用和删除

请参阅《发行说明》中的“弃用功能列表”，了解已弃用或已删除的元素的附加信息。

图表配置参考

图表概述

<chart> 元素是高度可配置的面板可视化。

<chart>	
在图表中显示搜索数据的面板。保存的报表包含图表格式信息。保存的搜索不包含这些信息。有关更多信息，请参阅“保存报表并将其共享给其他人”。当您在图表面板中加载保存的报表时，也会加载保存的报表格式。不过，您可以通过图表选项来内联覆盖图表格式。	
图表使用命名选项来指定图表特定的属性。本参考包含图表的所有可配置属性的部分。	
父元素	
<pre><row> <panel></pre>	
<pre><chart> <title> (0..1) <search> (0..1) <earliest> (0..1) <latest> (0..1) <drilldown> (0..n) <selection> (0..n, for charts of type area, line, and column only) <option name="[property]"> (0..n)</pre>	

常规图表属性

除非另有说明，这些是适用于所有图表的属性。

属性	类型	默认	描述
charting.backgroundColor	十六进制颜色值。		图表背景颜色。
charting.chart	(area bar bubble column fillerGauge line markerGauge pie radialGauge scatter)	柱形图	设置图表类型。
			要检索的结果数。设置为 0 以获取所有结果。

<code>charting.data.count</code>	数字	10000	警告：设置为 0 以检索所有结果可显著影响性能。
<code>charting.data.fieldListMode</code>	(show_hide hide_show)	hide_show	应用 fieldShowList 和 fieldHideList 过滤器的顺序。 此属性不适用于散点图和气泡图。
<code>charting.data.fieldShowList</code>	字段阵列	—	要在结果中明确显示的字段列表。 此属性不适用于散点图和气泡图。
<code>charting.data.fieldHideList</code>	字段阵列	—	要从结果中明确隐藏的字段列表（JSON 数组格式）。 此属性不适用于散点图和气泡图。
<code>charting.drilldown</code>	(all none)	all	<code>all</code> : 启用钻取。 <code>none</code> : 禁用钻取。
<code>charting.fieldColors</code>	十六进制颜色图。 请参阅描述。	—	用于每个字段的十六进制颜色值的映射。 映射是一个以逗号分隔的关键字/值对列表，外加大括号。 关键字通过分号与其值相分隔。 示例： <pre>{"foo\bar": 0xfffff00, foo: 0xff0000, "foobar": 0x000000}</pre> 使用双引号转义键或字符串值中的以下特殊字符： <code>[]{}(),: "</code> 在已有的双引号或反斜线或冒号前面添加反斜线以进行转义。 请参阅“在图表中为字段指定自定义颜色”中的示例。
<code>charting.fieldDashStyles</code>	短划线样式图。	—	用于 JSON 对象格式每个字段的短划线样式图。 例如：{"Field1": "shortDash"}。 可能的短划线样式是：(dash dashDot dot longDash longDashDot longDashDotDot shortDash shortDot shortDashDot shortDashDotDot solid)。
<code>charting.textColor</code>	十六进制颜色值。	—	图表字体颜色。
<code>charting.foregroundColor</code>	十六进制颜色值。	—	图表前景颜色。
<code>charting.legend.labels</code>	标签的 CSV	—	用于预填充图例的标签列表。 此属性不适用于散点图和气泡图。
<code>charting.legend.labelStyle.overflowMode</code>	(ellipsisEnd ellipsisMiddle ellipsisNone ellipsisStart)	ellipsisMiddle	通过使用省略号 (...) 替代删除的文本，确定如何显示溢出边界布局的标签。 <code>ellipsisStart</code> : 删除开头的文本。 <code>ellipsisMiddle</code> : 删除行中间的文本。 <code>ellipsisEnd</code> : 删除布局边界的文本。 <code>ellipsisNone</code> : 完全禁用文本截断。
			如果存在属性，禁用与仪表板中的其他面板的图

<code>charting.legend.masterLegend</code>	n/a		例颜色同步。 注意：唯一的有效值是空标记。如果指定了值，该属性将被忽略。
<code>charting.seriesColors</code>	十六进制颜色列表	请参阅下文*	使用十六进制值阵列定义图表系列的颜色。 注意：要应用静态颜色到指定字段，使用 <code>charting.fieldColors</code> 属性。
<code>height</code>	数字	—	图表的高度（以像素为单位）。 默认值为 250，必须在 100 和 10000 之间。

*`charting.seriesColors` 的默认值：

```
[0x1e93c6, 0xf2b827, 0xd6563c, 0x6a5c9e, 0x31a35f, 0xed8440, 0x3863a0, 0xa2cc3e, 0xcc5068, 0x73427f, 0x11a88b, 0xea9600, 0x0e776d, 0xffb380, 0xaa3977, 0x91af27, 0x453aa, 0x99712b, 0x553577, 0x97bc71, 0xd35c2d, 0x314d5b, 0x99962b, 0x844539, 0x00b290, 0xe2c188, 0xa34a41, 0x44416d, 0xe29847, 0x8c8910, 0xb416d, 0x774772, 0x3d9988, 0xbdbd5e, 0x5f7396, 0x844539]
```

常规图表属性：选择的示例

```
<dashboard>
  <label>Selected chart examples</label>
  <row>
    <panel>
      <chart>
        <title>A line chart</title>
        <search>
          <query>
            index=_internal source="*metrics.log"
            group=per_sourcetype_thruput
            | timechart sum(kb) by series
          </query>
          <earliest>-1h</earliest>
          <latest>now</latest>
        </search>
        <option name="charting.chart">line</option>
      </chart>
    </panel>

    <panel>
      <chart>
        <title>Show only splunkd_access and splunkd fields</title>
        <search>
          <query>
            index=_internal source="*metrics.log"
            group=per_sourcetype_thruput
            | timechart sum(kb) by series
          </query>
          <earliest>-1h</earliest>
          <latest>now</latest>
        </search>
        <option name="charting.data.fieldShowList">
          ["splunkd_access", "splunkd"]
        </option>
        <option name="charting.chart">line</option>
      </chart>
    </panel>
  </row>

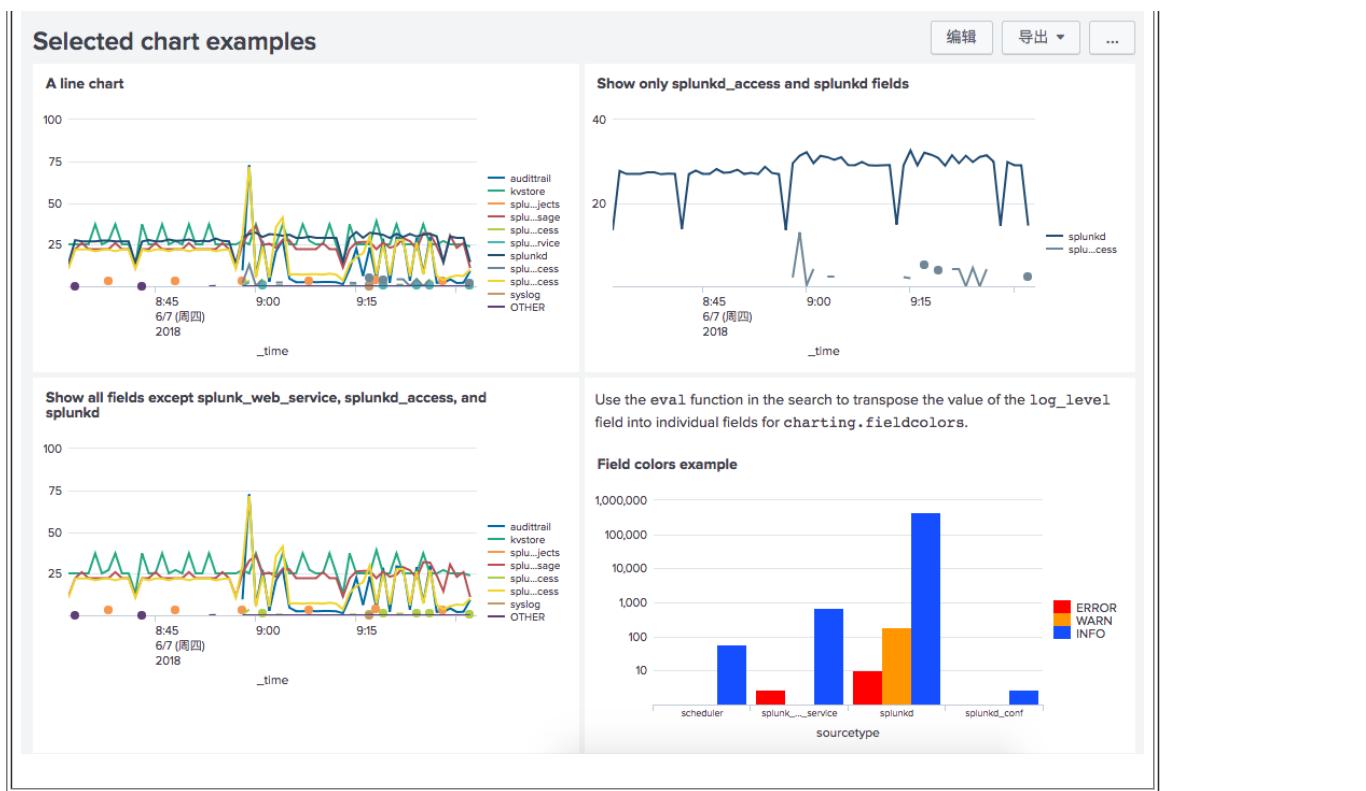
  <row>
    <panel>
      <chart>
        <title>Show all fields except splunk_web_service, splunkd_access, and splunkd</title>
        <search>
```

```

<query>
    index=_internal source="*metrics.log"
    group=per_sourcetype_thruput
    | timechart sum(kb) by series
</query>
<earliest>-1h</earliest>
<latest>now</latest>
</search>
<option name="charting.data.fieldHideList">
    ["splunk_web_service", "splunkd_access", "splunkd"]
</option>
<option name="charting.chart">line</option>
</chart>
</panel>

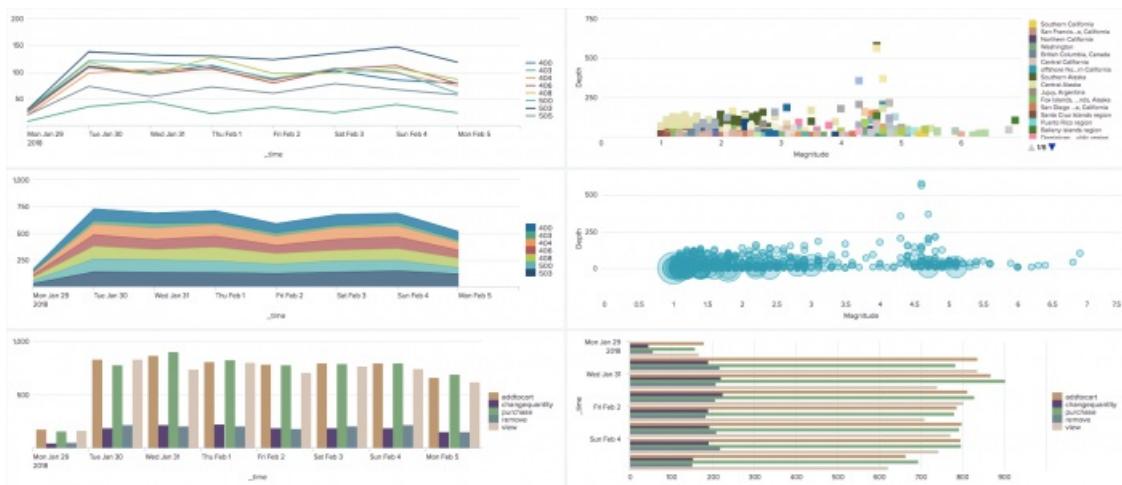
<panel>
<html>
    Use the <tt>eval</tt> function in the search to transpose
    the value of the <tt>log_level</tt> field into individual
    fields for <tt>charting.fieldcolors</tt>.
</html>
<chart>
    <title>Field colors example</title>
    <search>
        <query>
            index = _internal log_level=* | stats
            count(eval(log_level="ERROR")) as ERROR
            count(eval(log_level="WARN")) as WARN
            count(eval(log_level="INFO")) as INFO
            by sourcetype
        </query>
        <earliest>-7d@h</earliest>
        <latest>now</latest>
    </search>
    <option name="charting.axisY.scale">log</option>
    <option name="charting.chart">column</option>
    <option name="charting.fieldColors">
        {"ERROR": 0xFF0000, "WARN": 0xFF9900, "INFO":0x0066FF, "NULL":0xC4C4C0}
    </option>
    <option name="charting.legend.placement">right</option>
    </chart>
</panel>
</row>
</dashboard>

```



面积图、气泡图、条形图、柱形图和散点图

折线图、面积图、柱形图、散点图、气泡图和条形图特定的属性，所有这些都包含 X 轴和 Y 轴。



属性	类型	默认	描述
<code>charting.annotation.categoryColors</code>	HEX 或 RGB 颜色图。 请参阅描述。	—	<p>用于每个事件注释类别的十六进制或 RGB 图。此属性只用于事件注释叠加的图表，<code>annotation_category</code> 字段。</p> <p>映射是一个以逗号分隔的关键字/值对列表。</p> <p>关键字通过分号与其值相分隔。</p> <p>示例：</p> <pre>{"foo\bar": 0xfffff00, foo: 0xfffff00, "foobar": 0x000000}</pre> <p>使用双引号转义键或字符串值中的以下特</p> <pre>["{}()", ":"</pre>

			在已有的双引号或反斜线或冒号前面添加行转义。 要在简单 XML 中查看正在使用的属性示例，可以在简单 XML 中的事件注释。 此属性只应用于面积图、柱形图和折线图
<code>charting.axisLabelsX.axisVisibility</code> <code>charting.axisLabelsY.axisVisibility</code>	(show hide)	取决于轴类型	指示轴线是否可见。对于数字轴，默认为所有其他轴，默认为显示。
<code>charting.axisLabelsY2.axisVisibility</code>	(show hide)	取决于轴类型	仅适用于面积图、条形图、柱形图和折线图。对于数字轴， 默认为隐藏。他轴， 默认为显示。
<code>charting.axisLabelsX.extendsAxisRange</code> <code>charting.axisLabelsY.extendsAxisRange</code>	布尔值	true	指示轴的范围是否延伸以对齐整个主要刻度。
<code>charting.axisLabelsX.integerUnits</code> <code>charting.axisLabelsY.integerUnits</code> <code>charting.axisLabelsY2.integerUnits</code>	布尔值	false	指示主要单位是否应四舍五入取整。 仅条形图和折线图支持 <code>charting.axisLabelsY.integerUnits</code> <code>charting.axisLabelsY2.integerUnits</code>
<code>charting.axisLabelsX.majorLabelStyle.overflowMode</code>	(ellipsisMiddle ellipsisNone)	ellipsisNone	指示轴标签是否省略为刻度间距。 条形图不支持此属性。
<code>charting.axisLabelsX.majorLabelStyle.rotation</code>	(-90 -45 0 45 90)	0	轴标签旋转（以度为单位）。 正值顺时针方向旋转。负值逆时针方向旋转。 条形图不支持此属性。
<code>charting.axisLabelsX.majorLabelVisibility</code> <code>charting.axisLabelsY2.majorLabelVisibility</code> <code>charting.axisLabelsY.majorLabelVisibility</code>	(auto show hide)	auto	控制主要刻度线标签是否可见。 设置为 <code>show</code> 以始终显示标签，即使在促销时。 <code>auto</code> : 显示或隐藏各个主要标签，以便在保持可读性且无重叠。 <code>show</code> : 显示所有主要标签，即使在促销时。 <code>hide</code> : 隐藏所有主要标签。 气泡图或散点图不支持 <code>charting.axisLabelsY2.majorLabelVisibility</code> <code>charting.axisLabelsY.majorLabelVisibility</code> 未用。
<code>charting.axisLabelsX.majorTickSize</code> <code>charting.axisLabelsY.majorTickSize</code>	数字	6	主要刻度线的大小（以像素为单位）。 <code>charting.axisLabelsY.majorTickSize</code>
<code>charting.axisLabelsX.minorTickSize</code> <code>charting.axisLabelsY.minorTickSize</code> <code>charting.axisLabelsY2.minorTickSize</code>	数字	6	次要刻度线的大小（以像素为单位）。 气泡图和散点图不支持 <code>charting.axisLabelsY2.minorTickSize</code>
<code>charting.axisLabelsX.majorTickVisibility</code> <code>charting.axisLabelsY.majorTickVisibility</code>	(auto show hide)	auto	指示主要刻度线是否可见。 <code>auto</code> : 对于数字轴， 默认情况下刻度线是不可见的，仅当对应标签可见时显示主要刻度线。 <code>show</code> : 强制所有主要刻度线可见，无论标签是否可见。 <code>hide</code> : 隐藏所有主要刻度线。
			仅适用于面积图、条形图、柱形图和折线图

<code>charting.axisLabelsY2.majorTickVisibility</code>	(auto show hide)	取决于轴类型	要刻度线是否可见。 <code>auto</code> : 对于数字轴，默认情况下刻度线是可见的，仅当对应标签可见时显示主要刻度线。 <code>show</code> : 强制所有主要刻度线可见，无论标签是否可见。 <code>hide</code> : 隐藏所有主要刻度线。
<code>charting.axisLabelsX.majorUnit</code> <code>charting.axisLabelsY.majorUnit</code> <code>charting.axisLabelsY2.majorUnit</code>	(Positive integer auto)	auto	用于沿数字轴放置主要刻度线的间距单位。 默认情况下，将基于相关轴的刻度自动计算。 气泡图和散点图不支持 <code>charting.axisLabelsY2.majorUnit</code> 。
<code>charting.axisLabelsX.minorTickVisibility</code> <code>charting.axisLabelsY.minorTickVisibility</code> <code>charting.axisLabelsY2.minorTickVisibility</code>	(auto show hide)	auto	指示次要刻度线是否可见。 <code>auto</code> : 仅当对应标签可见时显示次要刻度线。 <code>show</code> : 强制所有次要刻度线可见，无论标签是否可见。 <code>hide</code> : 隐藏所有次要刻度线。
<code>charting.axisLabelsY2.majorTickSize</code>	数字	6	仅适用于面积图、条形图、柱形图和折线图。设置刻度线的大小（以像素为单位）。
<code>charting.axisX.abbreviation</code> <code>charting.axisY.abbreviation</code> <code>charting.axisY2.abbreviation</code>	(none auto)	无	启用大的 X, Y 缩写和离 SI 前缀最近的缩写。 气泡图和散点图不支持 <code>charting.axisY2.abbreviation</code> 。
<code>charting.axisX.includeZero</code> <code>charting.axisY.includeZero</code>	布尔值	false	指示轴范围是否包含零。
<code>charting.axisX.maximumNumber</code> <code>charting.axisY.maximumNumber</code>	数字	auto	设置轴范围的最大数字。
<code>charting.axisX.minimumNumber</code> <code>charting.axisY.minimumNumber</code>	数字	auto	设置轴范围的最小数字。
<code>charting.axisX.scale</code> <code>charting.axisY.scale</code>	(linear log)	linear	使用线性或对数刻度。 仅气泡图和散点图支持 X 轴的对数刻度。
<code>charting.axisTitleX.text</code> <code>charting.axisTitleY.text</code> <code>charting.axisTitleY2.text</code>	文本	—	指定轴的标题。 气泡图和散点图不支持 <code>charting.axisTitleY2.text</code> 。
<code>charting.axisTitleX.visibility</code> <code>charting.axisTitleY.visibility</code>	(visible collapsed)	visible	指示是否显示 X 轴或 Y 轴的标题。
<code>charting.axisTitleY2.visibility</code>	(visible collapsed)	collapsed	仅适用于面积图、条形图、柱形图和折线图。当两个轴有重叠时，指示是否显示第二个轴标题。
<code>charting.chart.resultTruncationLimit</code>	数字	50000	覆盖呈现在图表中的数据点数的默认限制。
<code>charting.gridLinesX.showMajorLines</code>	布尔值	false	指示 X 轴上的主要网格线是否可见。 此属性不适用于散点图或气泡图。
<code>charting.gridLinesY.showMajorLines</code>	布尔值	true	指示 Y 轴上的主要网格线是否可见。
<code>charting.gridLinesY2.showMajorLines</code>	布尔值	false	仅适用于面积图、条形图、柱形图和折线图。当两个 Y 轴上有重叠时，指示是否显示第二个 Y 轴上的主要网格线。
<code>charting.gridLinesX.showMinorLines</code> <code>charting.gridLinesY.showMinorLines</code> <code>charting.gridLinesY2.showMinorLines</code>	布尔值	False	仅适用于面积图、条形图、柱形图和折线图。当两个 Y 轴上有重叠时，指示是否显示次要网格线。

<code>charting.layout.splitSeries</code>	布尔值	<code>False</code>	多系列图表拆分为从上到下堆叠的单独图 列一个图表。
<code>charting.layout.splitSeries.allowIndependentYRanges</code>	布尔值	<code>False</code>	仅适用于面积图、条形图、柱形图和折线 为 <code>True</code> 时，允许每个系列具有其本身 的围。
<code>charting.legend.placement</code>	(<code>top</code> <code>left</code> <code>bottom</code> <code>right</code> <code>none</code>)	<code>right</code>	放置图例的地方。
<code>charting.legend.mode</code>	(<code>standard</code> <code>seriesCompare</code>)	<code>standard</code>	提供可视化和行为设置。 <code>"Standard"</code> 是 系列时（如，此设置更改工具提示的样式 时）， <code>"seriesCompare"</code> 很有用。 您只可以将此属性用于折线图和面积图

面积图属性

属性	类型	默认	描述
<code>charting.areaFillOpacity</code>	0 – 1.0	.75	配置面积图的不透明度。 1.0 表示面积图不透明。0 表示面积图透明。
<code>charting.axisY2.enabled</code>	布尔值	<code>false</code>	为图表叠加启用第二个 Y 轴。
<code>charting.axisY2.fields</code>	逗号分隔列表	—	为图表叠加映射到第二个 Y 轴的字段。
<code>charting.axisY2.includeZero</code>	布尔值	<code>false</code>	指示是否为图表叠加在第二个 Y 轴范围内包含零。
<code>charting.axisY2.maximumNumber</code>	数字	<code>auto</code>	为图表叠加设置 Y 轴范围的最大数字。
<code>charting.axisY2.minimumNumber</code>	数字	<code>auto</code>	为图表叠加设置 Y 轴范围的最小数字。
<code>charting.axisY2.scale</code>	(<code>inherit</code> <code>linear</code> <code>log</code>)	<code>inherit</code>	为图表叠加映射到第二个 Y 轴的刻度。 从第一个 Y 轴继承，或使用线性或对数刻度。
<code>charting.chart.overlayFields</code>	逗号分隔的列表	—	用于图表叠加的字段列表。
<code>charting.chart.showDataLabels</code>	(<code>all</code> <code>minmax</code> <code>none</code>)	无	指示如何在图表中显示标签： <code>all</code> : 显示全部标签 <code>minmax</code> : 仅为最低和最高数值显示标签。 <code>none</code> : 不显示标签。
<code>charting.chart.nullValueMode</code>	(<code>gaps</code> <code>zero</code> <code>connect</code>)	<code>gaps</code>	确定如何处理空值。
<code>charting.chart.showLines</code>	布尔值	<code>true</code>	指示是否在面积图中显示线条。
<code>charting.chart.stackMode</code>	(<code>default</code> <code>stacked</code> <code>stacked100</code>)	默认	设置堆叠面积图。

条形图属性

属性	类型	默认	描述
<code>charting.chart.barSpacing</code>	数字	1	指定条形图中的条形间距（以像素为单位）。
<code>charting.chart.seriesSpacing</code>	数字	—	指定条形图中的群集系列之间的间距（以像素为单位）。
<code>charting.chart.showDataLabels</code>	(<code>all</code> <code>minmax</code> <code>none</code>)	无	指示如何在图表中显示标签： <code>all</code> : 显示全部标签 <code>minmax</code> : 仅为最低和最高数值显示标签。

			none : 不显示标签。
<code>charting.chart.stackMode</code>	(default stacked stacked100)	默认	设置堆叠条形图。

气泡图属性

属性	类型	默认	描述
<code>charting.chart.bubbleMaximumSize</code>	数字	50	指定每个气泡的最大大小（以像素为单位）。
<code>charting.chart.bubbleMinimumSize</code>	数字	10	指定每个气泡的最小大小（以像素为单位）。
<code>charting.chart.bubbleSizeBy</code>	(area diameter)	area	确定是面积决定气泡大小还是直径决定气泡大小。

柱形图属性

属性	类型	默认	描述
<code>charting.axisY2.enabled</code>	布尔值	false	为图表叠加启用第二个 Y 轴。
<code>charting.axisY2.fields</code>	逗号分隔列表	—	为图表叠加映射到第二个 Y 轴的字段。
<code>charting.axisY2.includeZero</code>	布尔值	false	指示是否为图表叠加在第二个 Y 轴范围内包含零。
<code>charting.axisY2.maximumNumber</code>	数字	auto	为图表叠加设置 Y 轴范围的最大数字。
<code>charting.axisY2.minimumNumber</code>	数字	auto	为图表叠加设置 Y 轴范围的最小数字。
<code>charting.axisY2.scale</code>	(inherit linear log)	inherit	为图表叠加映射到第二个 Y 轴的刻度。 从第一个 Y 轴继承，或使用线性或对数刻度。
<code>charting.chart.columnSpacing</code>	数字	1	指定列之间的间距（以像素为单位）。
<code>charting.chart.overlayFields</code>	逗号分隔的列表	—	用于图表叠加的字段列表。
<code>charting.chart.seriesSpacing</code>	数字	—	指定柱形图中的群集系列之间的间距（以像素为单位）。
<code>charting.chart.showDataLabels</code>	(all minmax none)	无	指示如何在图表中显示标签： all : 显示全部标签 minmax : 仅为最低和最高数值显示标签。 none : 不显示标签。
<code>charting.chart.stackMode</code>	(default stacked stacked100)	默认	设置堆叠柱形图。

折线图属性

属性	类型	默认	描述
<code>charting.axisY2.enabled</code>	布尔值	false	为图表叠加启用第二个 Y 轴。
<code>charting.axisY2.fields</code>	逗号分隔列表	—	为图表叠加映射到第二个 Y 轴的字段。
<code>charting.axisY2.includeZero</code>	布尔值	false	指示是否为图表叠加在第二个 Y 轴范围内包含零。
<code>charting.axisY2.maximumNumber</code>	数字	auto	为图表叠加设置 Y 轴范围的最大数字。

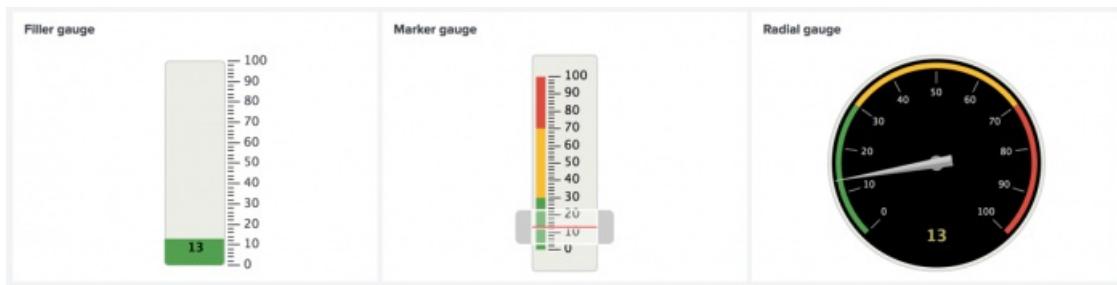
<code>charting.axisY2.minimumNumber</code>	数字	auto	为图表叠加映射到第二个 Y 轴的最小数字。
<code>charting.axisY2.scale</code>	(inherit linear log)	inherit	为图表叠加映射到第二个 Y 轴的刻度。 从第一个 Y 轴继承，或使用线性或对数刻度。
<code>charting.chart.nullValueMode</code>	(gaps zero connect)	gaps	确定如何处理空值。
<code>charting.chart.overlayFields</code>	逗号分隔的列表	—	用于图表叠加的字段列表。
<code>charting.chart.showDataLabels</code>	(all minmax none)	无	指示如何在图表中显示标签： all : 显示全部标签 minmax : 仅为最低和最高数值显示标签。 none : 不显示标签。
<code>charting.chart.showMarkers</code>	布尔值	false	指示是否在折线图中绘制标记。
<code>charting.chart.stackMode</code>	(default stacked stacked100)	默认	设置堆叠折线图。
<code>charting.lineDashStyle</code>	(dash dashDot dot longDash longDashDot longDashDotDot shortDash shortDot shortDashDot shortDashDotDot solid)	solid	指定图表中所有折线系列的短划线样式。
<code>charting.lineWidth</code>	float	2	图表中所有折线系列的线条宽度（以像素表示）。如果需要，您可以提供十进制值。

散点图属性

属性	类型	默认	描述
<code>charting.chart.markerSize</code>	数字	4	指示标记的大小（以像素为单位）。

仪表图表

特定于仪表图表的属性：



属性	类型	默认	描述
<code>charting.gaugeColors</code>	[Hex, ...]	[0x84E900, 0xFFE800, 0xBF3030]	<p>用于生成范围段颜色的十六进制颜色值阵列。 按照数组中指示的顺序来显示颜色。 例如，您可以通过将 <code>gaugeColors</code> 值更改为以下样式来颠倒默认的绿-黄-红顺序：</p> <pre>[0xBF3030, 0xFFE800, 0x84E900]</pre> <p>您可以指定任意数量的颜色。如果仪表的范围间隔的数量大于或小于</p>

			rangeColors 的数量，则会根据需要插入颜色。无论您指定搜索语言中的范围间隔还是 rangeValues 参数，都会出现这种插入情况。
<code>charting.chart.majorUnit</code>	数字	auto	指定主要刻度线的间距（以像素为单位）。
<code>charting.chart.rangeValues</code>	数字阵列	—	<p>该数组代表仪表所表示的整个数字范围，以及在此范围内的着色子范围的相对大小。</p> <p>例如，一系列：</p> <pre>[0,30,70,100]</pre> <p>指示仪表从零开始，结束于 100，并具有三个子范围，分别由其他塞尺颜色来确定。如果搜索返回值 71，塞尺会上移至仪表中的相应值，并呈现分配给顶部范围（71-100）的颜色。</p> <p>注意：当您在简单 XML 中指定范围值时，它们会覆盖通过仪表板面板所基于的搜索所指定的范围值。</p>
<code>charting.chart.showLabels</code>	布尔值	True	指示是否显示标签。
<code>charting.chart.showMajorTicks</code>	布尔值	True	指示是否显示主要刻度线。
<code>charting.chart.showMinorTicks</code>	布尔值	请参阅描述	指示是否显示次要刻度线。对应于径向仪表默认为 False，而对应于塞尺和标记规是 True
<code>charting.chart.style</code>	(minimal shiny)	shiny	<p>指定仪表的显示样式。</p> <p>shiny：仪表的图形化版本，带有镀铬发光、阴影等效果，以模仿现实世界中的形态。</p> <p>minimal：仪表的“基本”版本。</p>
<code>charting.chart.usePercentageRange</code>	布尔值	False	指示是否格式化范围值为百分比。
<code>charting.chart.usePercentageValue</code>	布尔值	False	指示是否格式化仪表值为百分比。

塞尺特定属性

属性	类型	默认	描述
<code>charting.chart.orientation</code>	(x y)	y	<p>设置仪表的方向。</p> <p>x：水平方向 y：垂直方向</p>
<code>charting.chart.showValue</code>	布尔值	True	指示仪表是否显示其值。

标记规特定属性

属性	类型	默认	描述
<code>charting.chart.orientation</code>	(x y)	y	<p>设置仪表的方向。</p> <p>x：水平方向 y：垂直方向</p>
<code>charting.chart.showRangeBand</code>	布尔值	true	指示在标记规左侧是否显示颜色范围段。
<code>charting.chart.showValue</code>	布尔值	False	指示仪表是否显示其值。

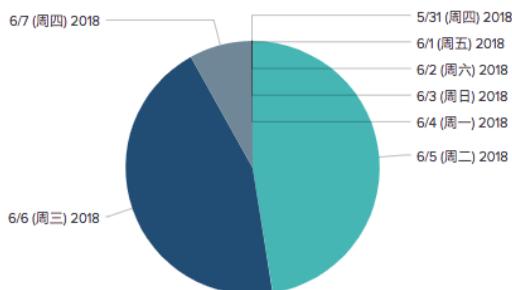
径向仪表特定属性

属性	类型	默认	描述
			范围弧度的长度（以度为单位）。

<code>charting.chart.rangeArcAngle</code>	数字	270	正值为顺时针方向。负值为逆时针方向。
<code>charting.chart.rangeStartAngle</code>	数字	45	绘制范围弧度的起点角度, 以度为单位。范围弧度从仪表底部沿顺时针方向。
<code>charting.chart.showRangeBand</code>	布尔值	true	指示在径向仪表顶部是否显示颜色范围段。
<code>charting.chart.showValue</code>	布尔值	True	指示仪表是否显示其值。

饼图

特定于饼图的属性:



属性	类型	默认	描述
<code>charting.chart.sliceCollapsingLabel</code>	文本	其他	合并扇区的标签。
<code>charting.chart.sliceCollapsingThreshold</code>	数字	0.01	用于使较小扇区折叠为合并扇区的阈值。 有效值在 0 和 1 之间。 0 指示未折叠。1 指示所有扇区折叠为单个饼图。 默认值 (0.01) 使扇区折叠为小于整个饼图的 1%。
<code>charting.chart.showLabels</code>	布尔值	true	指示是否显示标签。
<code>charting.chart.showPercent</code>	布尔值	false	指示是否随标签显示百分比。

事件处理程序参考

使用简单 XML 事件处理程序元素新建响应的仪表板行为。

什么是事件处理程序?

在 web 程序中, 事件处理程序可以侦听状态改变和用户行为 (如鼠标点击或滚动) 并定义响应。这些更改或交互为事件。简单 XML 中的事件处理程序运作与之相似。

事件处理上下文

会发生的和在简单 XML 元素中显示的事件因上下文 (如表单输入或钻取) 而异。处理事件的使用情况也因上下文而异。

例如, 在表单输入中, 您可以使用 `<change>` 元素, 该元素可以侦听用户选择和基于该选择的设置标记值。此标记值更新可以在表单中触发面板显示或隐藏行为, 根据选择自定义内容。

上下文	此上下文中发生的事件	使用案例示例
表单输入	用户选择或输入	根据用户输入值自定义表单内容。
搜索状态	搜索有多个状态事件, 如正在搜索、已取消或已完成。	使用搜索事件处理程序侦听搜索状态变更、捕获数据或在不同状态下新建动态行为。
钻取	用户通过仪表板与数据进行交互。	使用钻取与仪表板用户共享其他数据见解。例如, 您可以打开辅助搜索或链接到外

加载	用户在单页窗口中加载时的优化。	部分 URL。
仪表板页面加载	页面在浏览器窗口中加载，显示仪表板	在页面加载上设置标记以管理初始显示设置，如面板显示、隐藏或搜索可视化结果。

自定义响应的行为

在部分元素中，您可以定义对状态更改作出有条件的响应。例如，搜索完成之后，您可能想要以不同的方式处理特定搜索结果字段值。

标记和事件处理程序

使用预定义标记或自定义标记捕获动态值或帮助实施响应行为。可用的预定义标记因上下文而异。

如果您不熟悉标记，请参阅仪表板中的“[标记使用方法](#)”。

表单输入

以以下任何一种表单输入元素响应用户输入。

- <checkbox>
- <dropdown>
- <link>
- <multiselect>
- <radio>
- <text>
- <time>

事件处理程序元素

使用 <change> 元素以定义对输入中的用户选择的响应。您可以将 <condition> 子元素包含在 <change> 中以有条件地处理用户输入值。

注意：<change> 元素对多选输入不可用。

```
<change>
  <condition [label="foo" | value="foo" | match="(dashboard eval expression)"]>(0..n)
    (<eval> | <link> | <set> | <unset>) (1..n)
```

有关更多详细信息，请参阅“[简单 XML 参考](#)”中的 change。

表单输入事件标记

响应表单输入中的用户选择。使用预定义标记访问已选 <choice> 元素标签或值。

标记	描述
label	选择的 <choice> 元素标签。
value	选择的 <choice> 元素值。

|示例使用 <change> 元素捕获来自输入的所选标签和值。

```
<form>
  <label>Use tokens with input choices to capture input labels and values</label>
  <fieldset submitButton="false">
    <input type="radio" token="period_tok">
      <label>Select a time range</label>
      <choice value="-24h@h">Last 24 Hours</choice>
      <choice value="-7d@d">Last 7 Days</choice>
      <choice value="-30d@d">Last 30 Days</choice>
    <default>Last 24 Hours</default>
```

```

<change>
    <!-- use predefined input tokens to set -->
    <!-- tokens for the selected label and value -->
    <set token="date_label">$label$</set>
    <set token="earliest_tok">$value$</set>
</change>

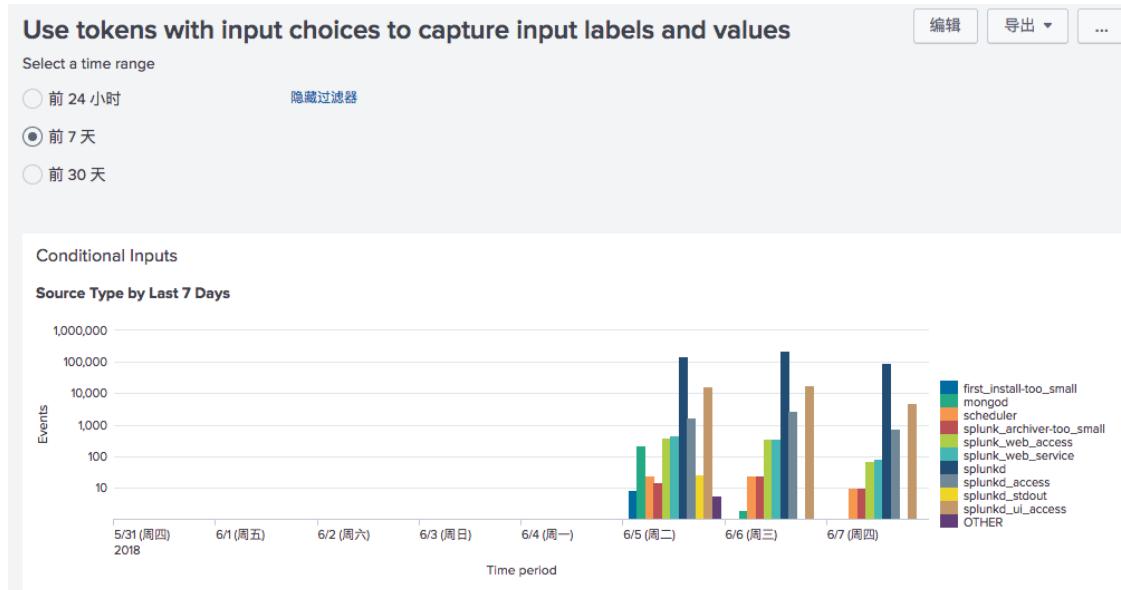
</input>
</fieldset>

<row>
<panel>
    <title>Conditional Inputs</title>
    <chart>
        <!-- Display selected label in the title -->
        <title>Source Type by $date_label$</title>

        <search>
            <query>index = _internal | timechart count by sourcetype</query>
            <!-- use the value of earliest_tok -->
            <!-- to set the time range -->
            <earliest>$earliest_tok$</earliest>
            <latest>now</latest>
        </search>

        <option name="charting.axisY.scale">log</option>
        <option name="charting.axisTitleX.text">Time period</option>
        <option name="charting.axisTitleY.text">Events</option>
    </chart>
</panel>
</row>
</form>

```



搜索事件处理程序

搜索事件处理程序能够让您基于搜索结果或搜索属性启用事件操作。操作包括链接到某页面、设置或取消设置标记，以及执行 `EVAL` 函数。

搜索事件标记

搜索事件处理程序使用预定义标记访问搜索结果和搜索属性。用于每个处理程序的标记可能会有所不同。在一些情况下，事件处理程序不访问启用操作的预定义标记。

标记	描述
----	----

job.property	访问已命名的任务属性值或其辅助属性之一。例如，使用 \$job.request.earliest_time\$ 和 \$job.request.latest_time\$ 访问关于搜索时间范围的信息。 您还可以查看来自“搜索任务查看器”的搜索属性。从“搜索页面”中，运行搜索之后再选择任务 > 检查任务。 请参阅《搜索手册》中的“查看搜索任务属性”，了解可用的属性列表。
result.field	访问已命名的字段值。标记访问来自返回结果第一行的数值。

搜索元素语法

```
<done | error | fail | cancelled | progress>
<condition match="(dashboard eval expression)">(0..n)
(<eval> | <link> | <set> | <unset>) (1..n)
```

关于搜索事件标记的详细信息，请参阅“定义搜索标记”。

已取消

<cancelled>

当搜索取消时执行操作。

父元素

<search>

```
<cancelled>
<condition match="(dashboard eval expression)">(0..n)
(<eval> | <link> | <set> | <unset>) (1..n)
```

可用标记

本元素无标记。

示例

```
<cancelled>
<unset token="sourcetype_count" />
</cancelled>
```

错误

<error>

当出现搜索错误事件，如无效查询时，请执行操作。

父元素

<search>

```
<error>
<condition match="(dashboard eval expression)">(0..n)
(<eval> | <link> | <set> | <unset>) (1..n)
```

可用标记

本元素无标记。

示例

<search>

```
<error>
  <set token="error_message">$message$</set>
</error>
</search>
```

失败

<fail>

在运行过程中，当搜索失败时执行操作。

父元素

```
<search>
```

```
<fail>
  <condition match="(dashboard eval expression)">(0..n)
    (<eval> | <link> | <set> | <unset>) (1..n)
```

可用标记

本元素无标记。仅失败消息可用。

示例

```
<search>
  <fail>
    <set token="fail_message">$message$</set>
  </fail>
</search>
```

进度

<progress>

执行搜索进度事件的操作。访问任务属性和第一个结果行。

父元素

```
<search>
```

```
<progress>
  <condition match="(dashboard eval expression)">(0..n)
    (<eval> | <link> | <set> | <unset>) (1..n)
```

可用标记

job.property
result.field

示例

```
<progress>
  <condition match=" 'job.resultCount' == 0">
    <set token="show_html">true</set>
  </condition>
  <condition>
    <unset token="show_html"/>
  </condition>
</progress>
```

完毕

<done>

基于已完成的搜索事件执行操作。

父元素

```
<search>

<done>
<condition match="(dashboard eval expression)">>(0..n)
(<eval> | <link> | <set> | <unset>) (1..n)
```

可用标记

```
job.property
result.field
```

示例

```
<done>
<condition match=" 'job.resultCount' == 0">
    <set token="show_html">true</set>
</condition>
<condition>
    <unset token="show_html"/>
</condition>
</done>
```

可视化事件处理程序

<[Visualization]>

事件处理程序应用于以下可视化类型：

- chart
- event
- map
- single
- table

```
<[Visualization]>
<drilldown> (0..n)
<condition [label="foo" | value="foo" | match=(dashboard eval expression)]>(0..n)
(<eval> | <link> | <set> | <unset>) (1..n)
<selection> (0..n, for charts of type area, line, and column only)
(<eval> | <link> | <set> | <unset>) (1..n)
```

子元素

元素	类型	默认	描述
<drilldown>	事件操作	—	用于钻取行为的操作。
<selection>	<set>	—	适用于面积图、柱形图或折线图。 使用 <set> 元素为图表的平移和缩放功能定义时间窗口标记。

示例

使用内联搜索的折线图面板示例。它将结果限制在指定的时窗内，并提供 X 轴和 Y 轴的标签：

```
<dashboard>
<label>Top source types in the last week</label>
<row>
<panel>
<title>Chart example</title>
<chart>
<title>Top sourcetypes in the last week</title>
<search>
<query>
index=_internal source="*metrics.log" group=per_sourcetype_thruput
| timechart sum(kb) by series
</query>
<earliest>-1w</earliest>
<latest>now</latest>
```

```

</search>
<option name="height">200px</option>
<option name="charting.chart">line</option>
<option name="charting.axisY.scale">log</option>
<option name="charting.chart.nullValueMode">connect</option>
</chart>
</panel>
...
</row>
</dashboard>

```



钻取事件标记

对于动态钻取，每个可视化类型都有可用的预定义标记。预定义标记数值可能会有所变化，具体取决于可视化。

- [图表事件标记](#)
- [事件事件标记](#)
- [地图事件标记](#)
- [单个事件标记](#)
- [表格事件标记](#)

图表（事件标记）

单击的字段名称是 Y 轴（若存在）的字段或系列的名称（和 click.name2 类似）。如果字段或系列的名称不可用，则会使用 X 轴的字段或类别（click.name）。

数据属性	描述
click.name	X 轴的字段或类别名称。单击图例时不可用。
click.value	X 轴的字段或类别值。单击图例时不可用。
click.name2	Y 轴的字段或系列名称。
click.value2	Y 轴的字段或系列值。单击图例时不可用。
row.<fieldname>	单击 X 轴时，此点沿 Y 轴的所有字段。单击图例时不可用。
row.<x-axis-name>	X 轴的值。单击图例时不可用。
earliest/latest	点击过的图表区段的时间范围，如果不适用，则指搜索的时间范围。

事件（事件标记）

click.name 的值取决于单击的上下文，如下所述：

数据属性	描述
click.name	和单击关联的字段名称。 事件查看器中字段名称有歧义的情况： <ul style="list-style-type: none"> 在原始事件中单击一个术语：设置 _raw 为字段名称。 单击事件时间戳：设置 _time 为字段名称。

	<ul style="list-style-type: none"> 单击一个标记：根据标记名称，设置一个字段名称，如下所示： <code>tag::<field></code> (例如，当主机设有标记时，<code>tag::host</code>)
<code>click.value</code>	与单击关联的值。
<code>click.name2</code>	和 <code>click.name</code> 一样。
<code>click.value2</code>	和 <code>click.value</code> 一样。
<code>row.<fieldname></code>	按行显示每个字段值 <code>row.<fieldname></code> 。
<code>earliest/latest</code>	单击的事件的时间范围，即： <code>最早: _time</code> <code>最晚: (_time + 1 second)</code>

地图（事件标记）

动态钻取中的 `<condition>` 标记的字段始终对应 `click.name`。

数据属性	描述
<code>click.name</code>	第一个或唯一一个显示标记的字段的名称。
<code>click.value</code>	第一个或唯一一个显示标记的字段的值。
<code>click.name2</code>	与 <code>click.name</code> 相同。
<code>click.value2</code>	与 <code>click.value</code> 相同
<code>click.lat.name</code>	确定标记位置的纬度字段的名称。
<code>click.lat.value</code>	标记的地理位置的维度值。
<code>click.lon.name</code>	确定标记位置的经度字段的名称。
<code>click.lon.value</code>	标记的地理位置的经度值。
<code>click.bounds.<orientation></code>	标记表示的所有群集位置的外部边界。 方向：南、西、北、东
<code>row.<fieldname></code>	单击的标记的每个字段值都显示在此表单中。
<code>earliest/latest</code>	生成地图可视化的搜索的时间范围。

单个（事件标记）

动态钻取中的 `<condition>` 标记的字段始终对应 `click.name`。

数据属性	描述
<code>click.name</code>	通过单个值可视化显示的字段名称。
<code>click.value</code>	通过单个值可视化显示的值。
<code>click.name2</code>	与 <code>click.name</code> 相同。
<code>click.value2</code>	与 <code>click.value</code> 相同。
<code>row.<fieldname></code>	在同一结果行中（获取单个值的地方）显示每个字段。
<code>earliest/latest</code>	生成单个值可视化的搜索的时间范围。

表格（事件标记）

动态钻取中的 <condition> 标记的字段始终对应 click.name2。

数据属性	描述
click.name	显示在表格最左端的字段的名称。如果存在，始终是 _time。
click.value	点击行最左边一列的值。
click.name2	所单击列的名称。
click.value2	所单击列的值。
row.<fieldname>	所单击表格行的所有字段值，包括未显示字段。
earliest/latest	点击过的表格行的时间范围，如果不适用，则是搜索的时间范围。

钻取

<drilldown>

定义用户单击仪表板或表单中的字段时要链接的自定义目标。

使用 <link> 标记指定到目标的路径。

使用 <set> 或 <unset> 标记来设置或取消设置标记。
为设置或取消设置标记指定一个条件以指定字段。

注意：您可直接在 <drilldown> 中指定一个或多个操作 (<eval>、<link>、<set>、<unset>) 或条件 (<condition>)，但是不能同时指定操作和条件。

属性

名称	类型	默认	描述
target	文本	—	对应于 <a> HTTP 标记的 target 属性。 指定 "_blank" 以在新窗口中打开钻取。 指定 "_self" 以在同一窗口中打开钻取。 指定一个任意字符串，以在新窗口中打开钻取。对这个目标的后续引用在本窗口中打开。

父元素

<chart> <event> <map> <single> <table>

<drilldown>
(<eval> | <link> | <set> | <unset>) (1..n) | <condition> (1..n)

示例 1：将值传递给表单

```
<table>
<search>
    <query>index=_internal </query>
</search>

<!-- Pass the clicked row's 'count'-column value -->
<!-- to populate a destination form's 'foo' token. -->
<drilldown>
    <link>
        /app/search/simple_xml_form?form.foo=$row.count$
    </link>
</drilldown>
</table>
```

示例 2：将参数传递给表单

```
<table>
<search>
    <query>index=_internal</query>
</search>
```

```

<!-- Pass the clicked cell's value, earliest time, -->
<!-- and latest time to a destination form's      -->
<!-- token ('foo') and search parameters          -->
<drilldown>
  <link>
    <![CDATA[
/app/search/simple_xml_form?form.foo=$click.value2$&earliest=$earliest$&latest=$latest$
  ]]>
  </link>
</drilldown>
</table>

```

示例 3：将来自图表的值传递给网站

```

<chart>
  <search>
    <query>index=_internal | chart count by sourcetype</query>
  </search>
  <option name="charting.chart">column</option>

  <!-- $click.value$ captures the value clicked by the user -->
  <!-- From the x-axis of a column chart and passes      -->
  <!-- it to the website as a query parameter          -->
  <drilldown>
    <link>
      http://splunk-base.splunk.com/integrated_search/?q=$click.value$</link>
    </drilldown>
  </chart>

```

selection

<selection>

为图表的平移和缩放功能设置时间窗口。也可使用标记来设置其他值，例如：图表中 X 轴的数字值。

仅适用于面积图、柱形图或折线图。

关于图表的平移和缩放功能，请参阅“图表控制”了解详细信息。

父元素

```

<chart>
  <option name="charting.chart">area</option>
  | <option name="charting.chart">column</option>
  | <option name="charting.chart">line</option>

```

使用预定义的标记来捕获时间窗口的最早和最晚时间，以及为字段捕获该时间窗口内的最早和最晚值。

例如：

```

<selection>
  <set token="selection.earliest">$start$</set>
  <set token="selection.latest">$end$</set>
  <set token="start.[fieldname]">$start.[fieldname]$</set>
  <set token="end.[fieldname]">$end.[fieldname]$</set>
</selection>

```

也能用于设置钻取链接。

```

<selection>
  <link>

```

属性

本元素无属性。

示例

左边图表的选择部分放大为右边的图表，并包括选择区域的详细信息。

```

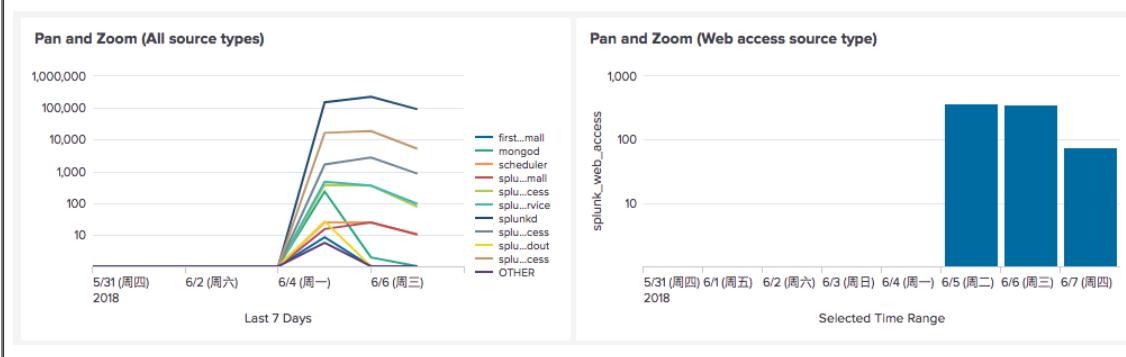
<dashboard>
  <label>Pan and Zoom</label>
  <row>
    <panel>
      <chart>
        <title>Pan and Zoom (All source types)</title>
        <search>
          <query>
            index=_internal | timechart count by sourcetype
          </query>
          <earliest>-7d@h</earliest>
          <latest>now</latest>
        </search>
        <option name="charting.axisX.scale">linear</option>
        <option name="charting.axisY.scale">log</option>
        <option name="charting.chart">line</option>
        <selection>
          <set token="selection.earliest">$start$</set>
          <set token="selection.latest">$end$</set>
          <set token="start.splunk_web_access">$start.splunk_web_access$</set>
          <set token="end.splunk_web_access">$end.splunk_web_access$</set>
        </selection>
        <option name="charting.axisTitleX.text">Last 7 Days</option>
      </chart>
    </panel>
    <panel>
      <chart>
        <title>Pan and Zoom (Web access source type)</title>
        <search>
          <query>
            index=_internal sourcetype=splunk_web_access
            | timechart count by sourcetype
          </query>
          <earliest>$selection.earliest$</earliest>
          <latest>$selection.latest$</latest>
        </search>
        <option name="charting.chart">column</option>
        <option name="charting.legend.placement">none</option>
        <option name="charting.legend.masterLegend">null</option>
        <option name="charting.axisX.scale">linear</option>
        <option name="charting.axisY.scale">log</option>
        <option name="charting.axisTitleX.text">Selected Time Range</option>
      </chart>
    </panel>
  </row>
  <row>
    <panel>
      <html>
        <h3>Token values for the splunk_web_access selection</h3>
        <table border="0" cellpadding="12" cellspacing="0">
          <tr>
            <td>
              <p><b>Time range (epoch time)</b></p>
              <p>
                <b>$selection.earliest$</b>: $selection.earliest$<br/>
                <b>$selection.latest$</b>: $selection.latest$<br/>
              </p>
            </td>
            <td>
              <p><b>Count at the begining and end of time range.</b></p>
              <p>
                <b>$start.splunk_web_access$</b>: $start.splunk_web_access$<br/>
                <b>$end.splunk_web_access$</b>: $end.splunk_web_access$<br/>
              </p>
            </td>
          </tr>
        </table>
      </html>
    </panel>
  </row>

```

```

</panel>
</row>
</dashboard>

```



条件元素

`<condition>` 元素基于多个条件指定操作的范围。操作所基于的可用条件会根据父元素的不同而有所差异。用于条件元素的属性会因父元素的不同而有所差异。

- `condition`（输入）
- 条件（搜索）
- `condition`（钻取）

`condition`（输入）

`<condition>`

基于输入选项指定操作的范围。如果父元素 `<change>` 不存在，则此操作应用到所有选项。`<condition>` 元素对多选输入不可用。

父元素

```

<input>
  <change>

```

```

<condition>
  (<eval> | <link> | <set> | <unset>) (1..n)

```

属性

名称	类型	默认	描述
标签	文本	*	将输入 <code><label></code> 元素指定到条件应用的内容。 '*' 将条件应用到所有输入 <code><label></code> 元素。
match	Eval 表达式	—	为要执行的操作定义所需条件的 Eval 表达式。
值	文本	*	将输入 <code><value></code> 元素指定到条件应用的内容。 '*' 将条件应用到所有输入 <code><value></code> 元素。

示例

使用条件式输入选择搜索的预设时间范围。

所选选项的标记在图表的标题中显示。所选值的条件式标记驱动图表的数据。

```

<form>
  <label>Use tokens with conditional input choices</label>
  <fieldset submitButton="false">
    <input type="radio" token="period Tok">

```

```

<label>Select a time range</label>
<choice value="-24h@h">Last 24 Hours</choice>
<choice value="-7d@h">Last 7 Days</choice>
<choice value="-30d@h">Last 30 Days</choice>
<default>Last 24 Hours</default>

<!-- set condition based on the label defined by <choice> -->
<!-- Within each condition, specify a custom label for display -->
<!-- Capture the selected value in the token, earliest_tok -->
<change>
  <condition label="Last 24 Hours">
    <set token="date_label">Yesterday</set>
    <set token="earliest_tok">$value$</set>
  </condition>
  <condition label="Last 7 Days">
    <set token="date_label">Last week</set>
    <set token="earliest_tok">$value$</set>
  </condition>
  <condition label="Last 30 Days">
    <set token="date_label">Last month</set>
    <set token="earliest_tok">$value$</set>
  </condition>
</change>
</input>
</fieldset>
<row>
<panel>
  <title>Conditional Inputs</title>
  <chart>

    <!-- Display selected label in the title -->
    <title>$date_label$</title>

    <search>
      <query>index = _internal | timchart count by sourcetype</query>
      <!-- use the value of earliest_tok -->
      <!-- to set the time range -->
      <earliest>$earliest_tok$</earliest>
      <latest>now</latest>
    </search>

    <option name="charting.axisY.scale">log</option>
    <option name="charting.axisTitleX.text">Time periods</option>
    <option name="charting.axisTitleY.text">Events</option>
  </chart>
</panel>
</row>
</form>

```



条件 (搜索)

<condition>

为满足条件的时间指定条件和行为。

父元素

<cancelled> | <done> | <error> | <fail> | <progress>

<condition [match=[eval statement]]>
(<eval> | <link> | <set> | <unset>) (1..n)

属性

名称	类型	默认	描述
match	Eval 表达式	—	为要执行的操作定义所需条件的 Eval 表达式。

示例

```
<condition match=" 'job.resultCount' == 0">
<set token="show_table_query">true</set>
</condition>
```

condition (钻取)

<condition>

限制钻取操作的范围，以单击特定字段。如果 <condition> 元素不存在，则钻取操作应用到所有字段。

注意：<condition> 元素应用于输入元素和钻取元素。有关详细信息，请参阅 <condition> (输入)。

父元素

<drilldown>

<condition>
(<eval> | <link> | <set> | <unset>) (1..n)

属性

名称	类型	默认	描述
field	文本	*	在实现钻取、或设置或取消设置标记的地方指定搜索字段。

示例

请参阅 `<set>` 示例，了解使用 `<condition>` 标记为页面内钻取设置标记。

请参阅 `<unset>` 示例，了解使用多个 `<condition>` 标记相关内容。

事件操作

Eval

`<eval>`

执行 Eval 语句。Eval 语句评估表达式且将结果置于某字段。仪表板的 `<eval>` 的工作方式类似于 SPL eval 命令，但有一些例外。更多详细信息，请参阅《[搜索引用](#)》中的 eval。

父元素

```
<drilldown><condition>
<search><condition>
<change><condition>
```

```
<drilldown>
  <eval token="[token_name]">

<drilldown>
  <condition>
    <eval token="[token_name]">

<change>
  <eval token="[token_name]">

<change>
  <condition>
    <eval token="[token_name]">

<search>
  <condition>
    <eval token="[token_name]">

<search>
  <eval token="[token_name]">
```

属性

名称	类型	默认	描述
标记	文本		值为 eval 表达式结果的标记。在 <code><eval></code> 表达式中，您可以为标记使用 <code>\$...\$</code> 分隔符或单引号分隔符。例如，以下这两种选项都是有效的。 <code>\$my_token\$</code> <code>'my_token'</code>

示例

```
<eval token="new_token">[eval expression]</eval>
```

Link

`<link>`

指定到钻取或所选输入选项的目标的链接。

<link> 可以是 <change>、<drilldown>、<search> 或 <condition> 的子标记。

当您想要为特定字段或输入配置不同的钻取操作时，使用 <link> 作为 <condition> 的子标记。否则，使用 <link> 作为 <change> 或 <drilldown> 的子标记。

这里有各种方式使用相对路径或 URL 指定钻取目标，如下所示。

父元素

```
<drilldown><condition>
<search><condition>
<change><condition>
```

```
<drilldown>
  <link>
```

```
<drilldown>
  <condition>
    <link>
```

```
<change>
  <link>
```

```
<change>
  <condition>
    <link>
```

```
<search>
  <condition>
    <link>
```

```
<search>
  <link>
```

属性

名称	类型	默认	描述
field	字段名称		已弃用。使用 <condition field="[field]"...> (仅用于 <drilldown>) 指定从指定列或行捕获的表格中的值。不能同时用 series 属性指定。 尽管支持字段属性，Splunk 仍然建议您用 <condition> 标记指定字段。
series	系列名		已弃用。使用 <condition field="[field]"...> (仅用于 <drilldown>) 指定从特定系列捕获的表格中的值。不能同时用 field 属性指定。 尽管支持系列属性，Splunk 仍然建议您用 <condition> 标记指定系列。
target	文本	—	对应于 <a> HTTP 标记的 target 属性。指定 <link> 元素的目标覆盖 <drilldown> 元素中指定目标的值。 指定 "_blank" 以在新窗口中打开钻取。 指定 "_self" 以在同一窗口中打开钻取。 指定一个任意字符串，以在新窗口中打开钻取。对这个目标的后续引用在本窗口中打开。

父元素

```
<drilldown><condition>
```

- 1) <link> [viewname] </link>
- 2) <link> [path/viewname] </link>
- 3) <link> [path/viewname?form.token=\$dest_value\$] </link>
- 4) <link> [path/viewname?form.token=\$dest_value\$&earliest=\$earliest\$&latest=\$latest\$] </link>
- 5) <link> [URL?q=\$dest_value\$] </link>

1. 使用指定的视图，它必须和当前的仪表板在同一路径下。
2. 连接到仪表板的相对路径。

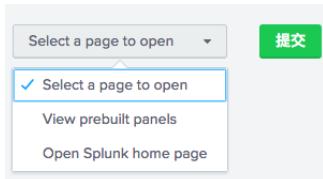
3. 连接到表单，并传入某个标记以填充表单的相对路径。
4. 传入原始搜索的最早时间和最晚时间范围。
(需要使用 CDATA 来转义特殊字符。)
5. 将值传递给目标页面的 URL 和查询参数。

路径值	描述
path	从当前视图到目标视图的路径。通常，您可以将路径指定为：/app/app_name/ 不过，您还可以根据来源和目标视图的应用上下文来指定相对路径。
viewname	您要用于目标的 Splunk 视图的名称。
\$dest_value\$	指定如何从可视化中捕获值。关于每个可视化的详细信息，请参阅“钻取事件标记”。
URL	指定网页的 URL。使用完整的地址，包括协议。例如：http://。
q	当指定 URL 时，使用 q 来指定 web 资源查询字符串中的 dest_value 的值。

示例

使用具有条件式输入的 <link> 打开新页面。

```
<form>
. . .
<fieldset>
<input type="dropdown" token="openNewPageToken">
<label></label>
<default>Select a page to open</default>
<choice value="">Select a page to open</choice>
<choice value="manager_page">View prebuilt panels</choice>
<choice value="splk_page">Open Splunk home page</choice>
<change>
<condition value="manager_page">
<link target="_blank">
<![CDATA[ /manager/search/data/ui/panels?ns=-&pwnr=-&search=&count=25 ]]>
</link>
</condition>
<condition value="splk_page">
<link target="_blank">
http://splunk.com
</link>
</condition>
</change>
</input>
</fieldset>
. .
</form>
```



预建面板

[新建预建面板](#)

用户界面 > 预建面板
预建面板是可轻松添加到多个仪表板中的可循环使用仪表板内容。这些面板由一个或多个可视化及相关表格输入组成。 [了解更多信息](#)

名称	操作	所有者	应用	共享	状态
! 未找到 预建面板。					

设置

<set>

您可发布新的全局标记，此标记可被仪表板内的任何其他元素或搜索使用。通常在使用表单输入或使用钻取时发布标记。

对于表单输入，为特定输入指定要进行操作的标记。

对于钻取，指定单击时要捕获的值。可使用标记动态设置该值。

对于表单输入，`<set>` 可以是 `<change>` 或 `<condition>` 的一个子标记。
 对于钻取，`<set>` 可以是 `<drilldown>` 或 `<condition>` 的一个子标记。

当您想要为特定输入或字段配置不同的钻取操作时，使用 `<set>` 作为 `<condition>` 的子标记。否则，使用 `<set>` 作为 `<change>` 或 `<drilldown>` 的子标记以指定所有输入或所有字段的操作。

父元素

```
<change>
  <condition>

<drilldown>
  <condition>

<change>
<drilldown>
```

这里有两种方式设置标记的值。

1. 使用模板合并输入标记和静态部分，以形成新的标记值。当设置值的时候，模板允许您引用多个标记，并且使用 `|s` 标记过滤器为标记值指定引号。

```
<set token="Token Name">sourcetype=$click.value|s$</set>
```

2. 使用前缀和后缀属性，为输入标记指定静态部分。下面的示例和上面的模板示例是等效的。

```
<set token="Token Name" prefix="sourcetype="" suffix=""">$click.value$</set>
```

属性

名称	类型	默认	描述
标记	标记名称		必填 用于同一页面上的目标可视化的标记。
prefix	文本		放在标记值前面的字符串。
suffix	文本		附加到标记值的字符串。

示例

单击表格，会设置一个标记，用于图表可视化的搜索。

```

<dashboard>
  <label>In-page Drilldown</label>
  <row>
    <panel>
      <table>
        <title>Set sourcetype token on click</title>
        <search>
          <query>
            index=_internal | stats count by sourcetype
          </query>
        <earliest>-1h</earliest>
        <latest>now</latest>
      </search>
      <drilldown>
        <condition field="sourcetype">
          <set token="sourcetype">$click.value2$</set>
        </condition>
      </drilldown>
    </table>
    <chart>
      <title>Chart for $sourcetype$</title>
      <search>
        <query>
          index=_internal sourcetype=$sourcetype$ | timechart count by sourcetype
        </query>
        <earliest>-1h</earliest>
        <latest>now</latest>
      </search>
    </chart>
  </panel>
</row>
</dashboard>

```

unset

<unset>

使用 <unset> 删除之前设置的标记。

父元素

```

<change>
  <condition>

<drilldown>
  <condition>

<change>
<drilldown>

```

<unset token="Token Name">

属性

名称	类型	默认	描述
标记	标记名称		必填 之前设置的标记名称，但是将会忽略。

示例

使用 <set> 和 <unset> 来定义要使用的可视化。

使用标记定义来隐藏面板。

```

<dashboard>
  <label>Example for <set> and <unset></label>
  <row>

```

```

<panel>
  <table>
    <title>Set sourcetype token</title>
    <search>
      <query>
        index=_internal | stats count by sourcetype
      </query>
    <earliest>-1h</earliest>
    <latest>now</latest>
    </search>
    <drilldown>
      <!-- For the sourcetype field clicked: -->
      <!-- Set token to display a chart -->
      <!-- Unset token to display a table -->
      <condition field="sourcetype">
        <set token="sourcetype">$row.sourcetype$</set>
        <set token="showChart">foo</set>
        <unset token="showTable"></unset>
      </condition>
      <!-- For any other field clicked: -->
      <!-- Set token to display a table -->
      <!-- Unset token to display a chart -->
      <condition field="*>
        <set token="sourcetype">$row.sourcetype$</set>
        <set token="showTable">foo</set>
        <unset token="showChart"></unset>
      </condition>
    </drilldown>
  </table>
</panel>

<!-- Hide the html panel when either token is present -->
<!-- Click in the original table to set either token -->
<panel>
  <html rejects="$showTable$, $showChart$">
    <h2>Details</h2>
    <div style="padding: 50px; margin: 0 auto; width: 350px;">
      <div class="alert alert-warning">
        <i class="icon-alert"/>
        Click on a row in the table on the left to show details.
      </div>
    </div>
  </html>
<!-- if showChart token is set, display results here -->
<chart depends="$showChart$">
  <title>Details for $submitted:sourcetype|s$</title>
  <search>
    <query>
      index=_internal sourcetype=$sourcetype|s$
      | timechart count by sourcetype
    </query>
    <earliest>-1h</earliest>
    <latest>now</latest>
  </search>
</chart>
<!-- if showCTable token is set, display results here -->
<table depends="$showTable$">
  <title>Details for $submitted:sourcetype|s$</title>
  <search>
    <query>
      index=_internal sourcetype=$sourcetype|s$
      | timechart bins=10 count by sourcetype
    </query>
    <earliest>-1h</earliest>
    <latest>now</latest>
  </search>
  <option name="wrap">true</option>
  <option name="rowNumbers">false</option>
  <option name="dataOverlayMode">none</option>
  <option name="drilldown">cell</option>
  <option name="count">10</option>
</table>
</panel>
</row>
</dashboard>

```

标记参考

标记为可用于传递简单 XML 仪表板中值的变量的类型。此参考列出对不同的情况可用的标记的类型。

有关标记用法的详细信息，请参阅“仪表板中的标记用法”。

标记类型	元素	描述
表单输入	<input>	用于引用从输入选择的值的用户定义输入。 请参阅“定义表单输入的标记”。 表单输入示例
时间挑选器输入	<input type="time">	仪表板中将两个或多个时间挑选器关联到多个面板的可选用户定义的输入标记。 包含 earliest 和 latest 修饰符以捕获时间范围。 请参阅“定义表单输入的标记”。 时间输入示例
钻取事件	<drilldown>	在图表中单击时可捕获值的预定义标记。动态钻取操作在访问钻取目标时使用来自来源图表的捕获的值。 请参阅“钻取事件标记”，获取预定义钻取标记的列表。
平移和缩放事件	<selection>	为平移和缩放操作获取值范围的预定义标记。图表中应用于用户选择的标记值。标记的上下文仅用于图表。将标记值复制到用户定义的标记以访问仪表板中的值。 start 和 end 为所选区域的起始点和终点捕获图表的 X 轴的值。例如，时间图表中的选择捕获该选择的起始和结束时间。 start.<field> 和 end.<field> 在所选区域的起始点和终点捕获图表的 Y 轴的值。例如，时间图表中的选择捕获由 <field> 指定的系列的事件数量。 请参阅“定义平移和缩放图表控制的标记”。 “定义平移和缩放图表控制的标记”中包括使用时间图表的示例。
条件式钻取操作	<drilldown> <condition> <link> <set> <unset>	配置条件式操作的条件元素内的用户定义的标记。条件式操作包括： <ul style="list-style-type: none">基于条件设置标记值。在可视化中，为多值字段选择一个值。基于标记值选择要打开的视图。基于条件隐藏或显示面板。 请参阅“使用 <drilldown> 元素定义条件式操作的标记”。
条件式表单输入操作	<input> <change> <condition> <link> <set> <unset>	在条件元素内用户定义的标记，以基于标记的条件值修改搜索或选择要显示的可视化。 请参阅“定义具有表单输入的条件式操作的标记”。 具有表单输入示例的条件式操作
设置目标操作	<input> <drilldown> <condition> <link> <set> <unset>	设置和取消设置标记以指定要打开的目标页面。 可与 <input> 元素或 <drilldown> 元素一起使用。<condition> 元素定义操作的条件。<link> 元素获取标记以打开目标。

自定义简单 XML

Splunk Enterprise 用户可以扩展简单 XML 来将自定义 CSS 和 JavaScript 结合到仪表板中。

有关更多信息，请参阅 Splunk 开发人员门户中的“使用简单 XML 修改仪表板”。