



# Splunk<sup>®</sup> Enterprise 7.2.0

## 报表手册

生成时间：2018 年 10 月 17 日，上午 8:58

# Table of Contents

<b>报表摘要</b>	<b>3</b>
关于报表	3
<b>报表管理</b>	<b>4</b>
新建和编辑报表	4
设置报表权限	10
加速报表	11
计划报表	13
嵌入计划报表	15
已嵌入报表的附加配置	16
配置计划报表的优先级	16
在 Splunk Web 中优先安排并发计划报表	21
偏移计划的搜索启动时间	22
生成报表和仪表板的 PDF	24

# 报表摘要

## 关于报表

保存搜索或数据透视表之后新建报表，以便日后再次使用。新建报表后，您可对它执行许多操作。在本手册中，您将了解如何：

- 手动新建和编辑报表。从“搜索”或“数据透视表”添加报表到“报表”列表页面。Splunk Enterprise 可在 `savedsearches.conf` 中手动配置报表。将仪表板面板转换为报表。通过更改权限将您的报表共享给其他人。
- 加速缓慢完成的报表，无论在报表新建期间还是未来一个时间点。
- 设置计划的报表--按固定时间间隔运行以及在每次运行时都触发告警操作（例如，发送包含搜索结果的电子邮件）的报表。计划报表还可用于**摘要索引**。
- 配置计划报表的优先级。了解报表计划程序如何管理多个并发报表，并了解如何配置您的报表计划程序选项。
- 了解如何生成报表、仪表板、搜索和数据透视表的 PDF。在 PDF 中启用非拉丁字体。在 Splunk Enterprise 中可通过编辑 `.conf` 文件配置 PDF 生成。查看此功能的例外情况。

# 报表管理

## 新建和编辑报表

当新建希望再次运行或与其他人分享的搜索或数据透视表时，您可以将它保存为报表。这意味着，您可以同时从 Splunk 平台的“搜索”和“数据透视表”端新建报表。

一旦新建报表，您可以：

- 在报表查看页面中**查看报表返回的结果**。您可以通过单击“报表”列表页面上的报表名称转到报表的查看页面。
- **打开报表并进行编辑**，以便返回不同的数据或以其他方式显示其数据。您的报表会在“数据透视表”或“搜索”中打开，这取决于它的新建方式。

此外，如果权限允许的话，您可以：

- **更改报表权限**以与其他 Splunk 用户共享报表。请参阅本手册中的“设置报表权限”。
- **计划报表，以便定期运行**。计划的报表可以在每次运行时执行操作，如通过电子邮件发送报表结果给一组相关方。请参阅本手册中的“计划报表”。
- **加速在搜索中构建的缓慢完成的报表**。请参阅本手册中的“加速报表”。
- **在外部网站中嵌入计划报表**。请参阅本手册中的“嵌入计划报表”。
- **将报表添加到仪表板**作为仪表板面板。请参阅《*仪表板和可视化*》手册中的“添加搜索、报表或数据透视表到仪表板”。

**注意：**用于通过数据透视表构建的报表的权限必须匹配用于构建它们的数据模型。请参阅本手册中的“基于数据透视表的报表权限”。

## 手动在 Splunk Web 中新建报表

您可以通过四种方式使用 Splunk Web 新建报表：

- 从“搜索”，通过保存搜索为报表。
- 从“数据透视表”，通过保存数据透视表为报表。
- 若想添加新的报表，请导航到**设置 > 搜索、报表和告警**并单击**新建**。
- 从仪表板开始，通过将内联搜索操纵的仪表板面板转换为报表。

有关这些报表新建方法的更多信息，请参阅以下小节。

一个报表定义至少包含与搜索相关的搜索字符串和时间范围（用相对时间修饰符表示）。您还可以命名报表，以便在“报表列表”页面和“设置”中的“搜索和报表”页面中进行识别。

### 从“搜索”或“数据透视表”视图中保存搜索或数据透视表为报表

当设计返回有用结果的搜索或数据透视表时，您可将它保存为报表。报表将保留设置原始搜索所用的任何格式，包括图表可视化和事件列表显示选项。

**注意：**您只能在搜索运行、暂停或完成时，将其另存为一个报表。

1. 运行需要保存为报表的搜索，或设计需要保存为报表的数据透视表。
2. 单击**另存为**并选择**报表**，以保存搜索或数据透视表为报表。报表将保留设置原始搜索所用的任何格式，包括图表可视化和事件列表显示选项。
3. 为报表提供唯一的**标题**。支持的标题字符包括 a-z、A-Z、0-9 或 \_。
4. （可选）提供报表的**描述**。
5. （可选）添加时间范围挑选器至报表。时间范围挑选器允许用户可以在没有写入权限的前提下，重新运行不同时间范围的报表，而不用真正地去编辑报表。

如果没有提供时间范围挑选器，则报表始终运行与原始搜索一样的时间范围。要更改时间范围，具备该报表编辑权限的用户必须在“搜索”中将其打开，更新其时间范围，然后保存该编辑内容。

**注意：**对于始终显示最后计划运行返回结果的计划报表，时间范围挑选器选项不可用。如果计划一份具有时间范围挑选器的报表，则时间范围挑选器会消失。请参阅“计划报表”。

6. 单击**保存**以将该搜索保存为报表。

当保存搜索为报表时，可以：

- 查看或运行报表并在报表查看页面上查看它返回的结果。
- 通过更改权限将您的报表共享给其他人。
- 安排报表按计划运行。
- 加速报表，以便在下次运行时完成速度更快。
- 在外部网站中嵌入报表。只能嵌入计划报表。

- 继续编辑报表。
- 添加报表到仪表板。

### 在设置中新建新报表

当希望新建报表时，通常最简单的方式是运行搜索或数据透视表，然后将它保存为报表，如上所示。此方法使您可以在保存前对搜索进行测试。

然而，您还可以“设置”中手动新建新报表。

1. 导航到**设置 > 搜索、报表和告警**，并单击**新建**以定义和添加新报表。

当在“设置”中定义报表时，您将它设置为“保存的搜索”。本搜索会在您完成后作为报表显示在“报表”列表页面上（或如果配置为告警，将显示在“告警”列表页面上）。

**新增**  
搜索、报表和告警 » 新增

目标应用 \*

Search & Reporting (search) ▼

搜索名称 \*

Purchased products, last 24 hrs

搜索 \*

source type="access" action="purchase" | stats count by product name

描述

以如下身份运行

☒ 所有者 ☐ 用户

[了解更多信息](#)

**时间范围**

开始时间 完成时间

-24h

时间说明符: y, mon, d, h, m, s

[了解更多信息](#)

**加速**

☒ 加速此搜索

摘要范围

1个月 ▼

**计划和告警**

☐ 计划此搜索的时间

2. 为搜索提供**目标应用**。此设置默认使用您的当前应用上下文。
3. 给搜索一个**搜索名称**，使其对目标应用具有唯一性。支持的搜索名称字符包括 a-z、A-Z、0-9 或 \_。
4. 在**搜索**字段中，提供字符串。
5. （可选）提供搜索描述。
6. （可选）确定搜索是否应该以**所有者**或**用户**身份运行。

此设置确定是否使用搜索**所有者**（定义搜索的人）的权限或搜索**用户**（正在运行搜索的人）的权限运行搜索。默认情况下，报表以**所有者**身份运行。请参阅本手册中“确定以报表所有者还是报表用户身份运行报表”。

7. 使用**相对时间修饰符**提供搜索**开始时间**和**完成时间**。如果您希望搜索在所有时间运行，则将**开始时间**和**结束时间**留空。
8. （可选）如果权限允许的话，通过选择**加速此搜索**和选择适当**摘要范围**，为搜索设置报表加速。

报表加速启用通常完成时间较慢的搜索，使其在未来运行中完成速度加快。请参阅本手册中的“加速报表”。仅特定搜索类型可用于报表加速。

9. （可选）如果想要定义此搜索为计划报表或告警，并且您的权限允许的话，请选择**计划此搜索**。

有关定义计划报表（定期运行以及通过电子邮件发送搜索结果或在每次运行时都启动脚本的报表）的更多信息，请参阅本手册中的“计划报表”。

有关定义告警的更多信息，请阅读《告警手册》。

10. （可选）为搜索启用摘要索引。

摘要索引是搜索加速的一种方式。请参阅《知识管理器手册》中的“使用摘要索引提高报表效率”。

11. 单击**保存**以保存报表。

如果您对“搜索、报表和告警”页面上列出的搜索具有“写入”权限，则可以进行编辑和更新。请参阅《知识管理器手册》中的“管理知识对象权限”。

### 预览已保存的搜索

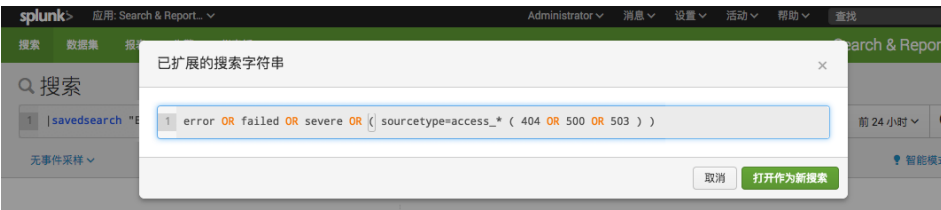
您可以在运行之前使用搜索扩展预览搜索。通过搜索扩展，您可以扩展整个搜索（包括已保存搜索）以预览搜索，无需运行搜索。

### 前提条件

- 新建报表。请参阅“在设置中新建新报表”。

### 步骤

1. 导航至 Splunk 搜索页面。
2. 在搜索栏输入默认报表 `Errors in the last 24 hours`。
3. 使用键盘快捷方式 **Command-Shift-E (Mac OSX)** 或 **Control-Shift-E (Linux 或 Windows)** 打开搜索扩展。  
搜索扩展预览在功能打开的情况下突出显示语法和行数。



4. （可选）复制搜索片段。
5. （可选）单击**在搜索中打开**运行搜索。

随即，扩展搜索窗口打开。

### 将仪表板面板内联搜索转换为报表

如果用的是 Splunk 仪表板，您可能知道可以通过内联搜索或报表“操纵”仪表板面板。这两种面板类型各具优势。

面板类型	新建方法	优势
由内联搜索（面板定义中的搜索字符串）支持	<ul style="list-style-type: none"><li>• 将新搜索或数据透视表另存为仪表板面板。</li><li>• 在“搜索”或“数据透视表”中打开现有报表（请参阅下方“编辑报表”）并保存为由内联搜索支持的仪表板面板。</li><li>• 新建来自仪表板编辑器的面板，选择<b>内联搜索</b>，然后定义搜索字符串。</li></ul>	可以编辑支持面板的搜索，而无需离开仪表板编辑器。
由报表支持	<ul style="list-style-type: none"><li>• 在“搜索”或“数据透视表”中打开现有报表（请参阅下方“编辑报表”），然后保存为由报表支持的仪表板面板。</li><li>• 新建来自仪表板面板的面板，选择<b>报表</b>，然后选择报表名称。</li></ul>	<ul style="list-style-type: none"><li>• 可以利用报表加速的优势，这样面板加载更快。</li><li>• 倘若报表已计划，则可以立即显示来自上次计划报表运行的结果。</li></ul>

您可以轻松地将仪表板面板定义中的内联搜索转换为报表，从而将面板转换成报表支持的面板。进行此操作时，新报表会添加到“报表”列表页面和“设置”中的“搜索、报表和告警”页面。您现在还可以为操纵面板的报表定义加速、计划和权限设置。

有关仪表板面板如何新建及如何以内联搜索结束的更多信息，请参阅《仪表板和可视化》手册中的“添加面板至仪表板”。

基于报表的仪表板面板可以使用与它们关联报表不同的格式。请参阅本主题中的“要使仪表板面板具有其附属报表的格式”。

**要将仪表板面板转换为报表**

1. 找到要转换的仪表板，并单击**编辑**。

图标将显示在仪表板每个面板的右上角。

2. 对于基于搜索或数据透视表的面板，单击“面板属性”并选择**转换为报表**。

“面板属性”图标在之前步骤提到三个面板编辑图标的最左侧。其图标指示面板的文档类型--基于搜索的面板使用放大镜、数据透视表使用数据透视图标，或基于搜索或数据透视表的一张工作表。

将显示**保存面板为报表**对话框。



3. (可选) 可以为报表提供**标题**和**描述**，并且与面板关联的标题和描述不同。

A screenshot of the '转换为报表' (Convert to Report) dialog box. The dialog has a title bar with a close button. Inside, there are two input fields: '报表标题' (Report Title) with the text 'Top 20 Truck Fleets (Permit Approved)' and '描述' (Description) which is empty. At the bottom, there are two buttons: '取消' (Cancel) and '保存' (Save).

4. 单击**保存**。

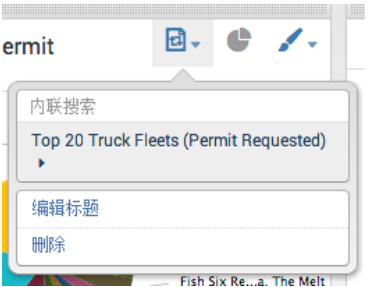
Splunk 软件会把新报表添加到“报表”列表页面。

**使仪表板面板具有其附属报表的格式**

如果您将仪表板面板转换为报表并编辑报表，以便它使用不同的可视化或具有不同的可视化格式，则您的更改将不会自动反映在附属面板中。要将仪表板面板与更新的报表关联，遵照这些步骤：

1. 单击包含希望更新面板仪表板的**编辑**。
2. 单击希望更新面板的“面板属性”图标。
3. 选择面板/报表名称（该名称仅为转换为报表的面板显示）。

显示报表信息屏幕。此处您可在权限允许的情况下编辑报表的各个方面（权限、加速、计划等等）。



#### 4. 单击使用可视化上的报表格式，然后确认希望面板使用报表的格式。

这样，面板将使用您为报表定义的可视化类型和格式。例如，如果面板显示一张饼图，但与面板关联的报表已配置为以柱形图显示其数据，则单击**使用可视化上的报表格式**。这使得面板以柱形图格式显示数据。



通过类似方式，您可以让面板使用完全不同报表的数据和格式。遵照以上步骤，但单击**选择新报表**而不是**使用可视化上的报表格式**。将打开**选择新报表**对话框。选择其他报表，单击保存，面板将更新以显示依照选定报表可视化的数据。

**注意：**如果仪表板面板源自数据透视表，在转换为报表时，您可能无法通过仪表板更改面板可视化类型。

您的权限将决定可以选择和编辑的报表。

### 编辑报表

您可以轻松编辑现有报表。您可以编辑报表的定义（其搜索字符串、数据透视表设置或结果格式）。您还可以编辑其描述、权限、计划和加速设置。

#### 要编辑报表的定义

如果希望编辑报表的定义，这里有两种方式，取决于您是否在“报表”列表页面或查看报表本身。

- 如果您在**报表列表页面**，查找您希望编辑的报表，转到**操作**列，并单击**在搜索中打开**或**在数据透视表中打开**（您将看到其中一个，这取决于用于新建报表的工具）。
- 如果**进入报表以查看其结果**，单击**编辑**并选择**在搜索中打开**或**在数据透视表中打开**（您将看到其中一个，这取决于用于新建报表的工具）。

#### 编辑在搜索中打开的报表定义

在搜索中打开报表后，您可以更改搜索字符串、时间范围或报表格式。在重新运行报表后，将启用报表右上角的**保存**按钮。单击该按钮以保存报表。您还拥有保存已编辑搜索为新报表的选项。

#### 编辑在数据透视表中打开的报表定义

在“数据透视表”中打开报表后，更改数据透视表的定义为您希望的定义。您可以添加、删除或重新定义筛选器、拆分行、拆分列或列值。您还可以更改格式化数据透视表结果的方式（更改可视化类型，或修复显示图表的方式）。完成后，单击页面右上角的**保存**以保存您的报表。您还拥有保存已编辑数据透视表为新报表的选项。

#### 要编辑报表的描述、权限、计划和加速设置

您可从“报表”列表页面或数据透视表查看页面完成。单击**编辑**并选择：

- **编辑描述**以更改报表的名称和描述。
- **编辑权限**以更改报表权限。请参阅本手册中的“设置报表权限”。
- **编辑计划**以计划报表或更改报表计划（如果已经存在）。请参阅本手册中的“计划报表”。
- **编辑加速**以更改加速报表的方式。**注意：**本选项仅对在“搜索”中新建的某些报表类可用。请参阅本手册中的“加速报表”。

**注意：**如果在“搜索”或“数据透视表”中打开了报表，则无法执行这些操作。如果希望编辑报表的这些方面，保存报



表或返回“报表”列表页面。

## 复制报表

报表复制是基于现有报表快速新建报表的方式。然后，您可以给副本设置唯一的名称并编辑它，这样它会返回不同的结果。

**注意：**如果在“搜索”或“数据透视表”中打开了报表，则无法执行该操作。如果希望复制报表，则保存报表或返回“报表”列表页面。

**警告：**切勿给复制的报表设置与原始报表相同的名称和搜索字符串。否则会出现原始报表和复制的报表链接在一起的情况。这意味着原始报表必须存在，这样它的副本才会存在。如果您删除了原始报表，链接的复制报表也会随之消失。

如果您将副本保持专用，您可以给其设置与源报表相同的名称以利用该链接。用户更新原始报表时，Splunk 软件也会更新链接的专用自定义副本。

1. 打开“报表”列表页面。
2. 查找要复制的报表，并单击**编辑**链接。
3. 从出现的列表中选择**复制**。

“复制”窗口会出现。

4. 对于**新标题**，为复制的报表提供一个唯一的名称。

Splunk 软件命名已复制报表的方式为：原始报表的名称加上单词 "Clone"。我们建议您给复制的报表设置唯一的名称，特别是在您计划与其他用户共享的情况下。

5. (可选) 给复制的报表输入**描述**，并设置其**权限**。

如果您不想和其他人共享复制的报表，则保持**权限**设置为**专用**。如果您希望复制的报表拥有与原始报表相同的权限，则选择**复制**。

6. 单击**复制报表**以复制报表。复制的报表现在显示在“报表”列表页面上。

## 禁用报表

如果权限允许，您可以禁用报表。禁用后的报表会继续显示于“报表”列表页面和“搜索、报表和告警”中，但无法运行。

您一般会在禁用计划的报表时使用该功能。这意味着它们会按照计划停止运行，但仍存在于系统中，且计划定义保持不变。如果想让禁用后的报表重新按计划运行，您可以启用遭禁用的报表。

1. 导航到**设置 > 搜索、报表和告警**。
2. 定位要禁用的搜索，并单击其**禁用**链接。

如果试图运行遭禁用的报表，您将会看到一条错误信息。如果权限允许，错误消息中会包含一个**启用报表**按钮（可用其启用遭禁用的报表）和一个**在搜索中打开**按钮（可用其运行报表使用的搜索字符串）。

## 删除报表

您可以从“报表”列表页面或报表查看页面删除报表。只需单击**编辑**并选择**删除**。大部分角色仅能删除他们新建的报表。有关为角色授予删除非其所拥有报表的功能的更多信息，请参阅《*知识管理器手册*》中的“禁用或删除知识对象”。

**注意：**如果在“搜索”或“数据透视表”中打开了报表，则无法执行该操作。如果希望编辑报表的这些方面，保存报表或返回“报表”列表页面。

## 在 savedsearches.conf 中配置报表 (Splunk Enterprise)

通过 Splunk Web 或“设置”保存报表时，Splunk 软件会自动把该报表的一个配置段落添加到 `savedsearches.conf`。UI 将验证您的更改，您无需重新启动系统就可通过 UI 方法应用新建的报表。但如果您有 Splunk Enterprise 而且更喜欢直接通过配置文件使用报表，当然就可以这样操作。

有关在 `savedsearches.conf` 中配置报表和告警的更多信息，请参阅 `savedsearches.conf` 的规范文件和《*告警手册*》中的“在 `savedsearches.conf` 中配置告警”主题。

## 问答

有什么问题吗？请访问 Splunk Answers，查看 Splunk 社区有哪些与报表相关的问题和答案。

## 设置报表权限

您所新建的任何报表最初都是您个人的，只供您使用。如果通过角色授予您的功能允许此操作，则可以更改报表权限以与其他人共享。

### 前提条件

- 《知识管理器手册》中的“管理知识对象权限”。
- 《知识管理器手册》中的“使超级用户和管理员以外的角色能够设置权限和共享对象”。
- 基于数据透视表的报表权限。从“数据透视表”构建的报表权限不得超过报表引用的数据模型的权限。
- 确定以报表所有者还是报表用户身份运行报表。
- 《搜索手册》中的“在 Splunk Web 中保存和共享任务”。修改完现有**计划报表**的权限后，这些新权限仅适用于该计划报表未来生成的任务。如果要修改该计划报表生成的现有任务的权限，您需要使用任务管理器。

### 步骤

1. 为您的报表打开“编辑权限”对话框。  
有多种方式可以访问“编辑权限”对话框：

访问方式	针对现有报表？	访问步骤
何时首次新建报表	否	1. 运行搜索。 2. 将搜索保存为报表。 3. 在“您的报表已新建”对话框中，单击 <b>权限</b> 。
从“报表”列表页面	是	1. 导航至“报表”列表页面。 2. 查找要为此编辑权限的报表。 3. 单击 <b>编辑</b> 并选择 <b>权限</b> 。
从报表显示视图	是	1. 导航至“报表”列表页面。 2. 查找报表名称并单击以打开报表。 3. 单击 <b>编辑</b> 并选择 <b>编辑权限</b> 。
从设置	是	1. 导航到 <b>设置 &gt; 搜索、报表和告警</b> 。 2. 查找需编辑其权限的报表。 3. 单击其 <b>权限</b> 链接。

2. 选择**应用**或**所有应用**。  
所有报表在特定应用的上下文中新建。
  - 选择**应用**可与该报表所属应用的其他用户共享报表。
  - 选择**所有应用**以与 Splunk 平台实现的所有用户共享报表。选择**应用**或**所有应用**将显示**运行行为**字段和角色权限设置。
3. **（可选）**确定报表以**所有者**还是**用户**身份运行。  
此设置确定是否使用搜索**所有者**（定义搜索的人）的权限或搜索**用户**（正在运行搜索的人）的权限运行搜索。默认情况下，报表以**所有者**身份运行。  
在“设置”中的“搜索、报表和告警”页面中设置权限时，看不到**所有者**和**用户**控件。相反，它们会显示在报表的详细信息页面中。
4. 根据角色设置**读取**和**写入**权限。  
**读取**使所选角色的用户能够查看和运行报表，但无法编辑。**写入**使用户能够根据需要运行和编辑报表。如果没有针对特定角色标记这些设置，则该角色无法看到报表。
5. 单击**保存**以保存权限更改。

### 确定以报表所有者还是报表用户身份运行报表

当与其他用户共享报表时，您可以选择通过报表“所有者”（即报表新建者）的权限或者报表“用户”（即报表运行者）的权限使其运行。使用此设置有两个原因：

- 允许访问报表运行者通过其他方式无法使用的搜索数据。
- 这有助于预防以下情况：过多运行您自己的报表时达到并发搜索的上限。

默认情况下，所有报表以**所有者**身份运行。

**注意：**计划报表**只能**以**所有者**身份运行。报表共享后将以**用户**身份运行；如果您先共享报表然后再计划该报表，则其权限将更改为以**所有者**身份运行。

**所有者**和**用户**设置也能够影响您的用户与带有报表支持面板的仪表板之间的交互。请参阅《仪表板和可视化手册》中的“添加面板至仪表板”。

### 控制报表结果的访问权限

**所有者和用户**设置能够让您控制报表返回数据的访问权限。例如，假设您有一个索引限制为具有“管理员”角色的用户。当具有“管理员”角色的人员写入在此索引中访问事件的搜索，然后共享为以**所有者**身份运行的报表，则角色级别较低的任何用户也能将其运行，并查看来自受限制索引的事件，因为报表会以“管理员”角色所有者运行的方式来运行。如果“管理员”用户想要以其他方式显示受限制数据的某些方面给权限级别较低的用户，这可能就是所需结果。

如果“管理员”共享报表从而以**用户**身份运行，则任何人都能运行，但在此过程中，报表以自身的权限而非报表所有者的权限运行。因此，如果您具备“用户”角色，且运行报表，则报表无法从受限制的索引中返回事件，因为您的权限可能没有报表所有者高。

### 为报表所有者阻止超出并发搜索任务限制

**所有者和用户**控件确定报表任务是否计入报表“所有者”或报表“用户”的并发搜索任务限制。这些限制按角色变化，并在**设置 > 访问控制 > 角色 > <角色名>**中设置。您可能想要以**用户**身份运行共享报表，这样当其他用户同时运行报表时不会达到您的并发搜索限制。

例如，默认情况下，具有“管理员”角色的人员可以同时运行 50 个搜索任务。“管理员”用户同时运行 50 个以上任务的可能性极小，但是万一出现这种情况，则其他任务根据报表计划程序等待队列，以便稍后运行。

现在假设您具有“管理员”角色。您运行搜索、另存为报表然后共享以运行**所有者**。稍后，其他人会建立仪表板并使用您的报表以备份其中一个面板。如果此仪表板特别常用，则可能会出现频繁突破并发搜索限制的现象，这是因为负载或重新负载仪表板的用户过多。要解决此问题，可以编辑报表权限，使其以**用户**身份运行。

## 基于数据透视表的报表权限

“数据透视表”中构建的报表权限无法超过报表引用的数据模型的权限。例如，如果某报表引用的是专用数据模型，则您无法将其共享给所有应用的用户。如果进行此操作，则会得到一个错误讯息。您必须先将报表引用的数据模型共享给所有应用的用户，然后对报表权限进行相应设置。有关共享数据模型的更多信息，请参阅《*知识管理器手册*》中的“管理数据模型”。

这里还有稍微更复杂一点的示例。您的 Splunk 部署已安装了两个应用：搜索和安全性。在“安全性”应用上下文中，您使用它的“外部威胁”数据模型新建名为“Top Firewall Attacks by IP”的基于数据透视表的报表。“外部威胁”数据模型具有“安全性”应用范围内的权限，仅此而已。

首次新建报表时，将其权限设置为**所有者**，这意味着您是唯一可以看到报表并更新的人员。无论应用上下文为何，如果您想让所有人看到“Top Firewall Attacks by IP”报表，请将报表权限更改为**所有应用**。现在，当切换应用上下文为“搜索”应用时，您可能希望从“搜索”应用访问“Top Firewall Attacks by IP”。

然而，您无法从“搜索”应用中查看。这是因为报表无法在没有“外部威胁”数据模型的情况下构建，同时该数据模型的权限仍在“安全性”应用范围内。要从“搜索”应用访问和运行“Top Firewall Threats by IP”报表，请将其权限设置为**所有应用**以全局共享“外部威胁”数据。

## 加速报表

如果您的报表具有大量的事件，并且运行的速度很慢，您可以加速报表，从而您将来再次运行时它的完成速度更快。加速报表时，Splunk 软件会运行一个后台进程；该进程将根据报表返回的结果构建一个数据摘要。下次运行搜索时，Splunk 软件会根据此摘要而非完整的索引来运行搜索。由于此摘要比完整的索引要小，并且包含与搜索相关的预先计算的摘要数据，所以将以比首次运行搜索时快得多的速度完成搜索。

### 报表加速的限制

如果出现以下情况，您将无法加速报表：

- 报表是通过数据透视表新建的。通过数据模型加速来加速数据透视表报表。请参阅《*知识管理器手册*》中的“管理数据模型”。
- 您的权限不允许您加速搜索。如果您的角色不具有 `schedule_search` 和 `accelerate_search` 操作，则无法加速报表。
- 您的角色没有此报表的写入权限。
- 报表所基于的搜索不符合加速条件。请参阅本主题的“报表如何才能符合报表加速的条件”。

此外，如果报表基本搜索包含**标记**、**事件类型**、**搜索宏**和其他知识对象，则加速这些报表时应当格外小心，因为这些知识对象的定义可能会在加速报表后单独进行更改。如果此情况发生，则加速报表可能会返回无效的结果。

如果怀疑您所加速的报表正返回无效结果，则可验证其摘要，确认摘要中包含的数据是否一致。请参阅《*知识管理器手册*》中的“确认摘要”。

### 编辑加速对话框

如果权限允许您加速特定报表，同时报表符合加速条件，则可在新建报表时或新建后的任何时间加速它。

- 当您**将搜索保存为报表**时，您将会看到“您的报表已新建”对话框，请单击**其他设置**并选择**加速**。
- 如果希望**加速现有报表**，导航到“报表”列表页面或报表查看页面。

- 在“报表”列表页面上，要加速报表（或更改其当前加速配置）：
  - 展开报表的行并单击加速的**编辑**。
  - 或者，单击选定报表的**编辑**并选择**编辑加速**。
- 在报表查看页面（您可通过单击“报表”列表页面上的报表名称来访问）上，要加速报表：
  - 单击**编辑**并选择**编辑加速**。
  - 或者，单击**更多信息**并单击加速状态旁边的**编辑**。

**注意：**如果尝试加速不符合加速条件的报表，则将收到错误消息，通知您无法加速报表。

在“编辑加速”对话框上，选择**加速报表**以显示**摘要范围**。

加速报表时，您必须选择一个**摘要范围**值，如 **7 天**、**3 个月**或**所有时间**。此范围表示摘要在构建之后在任何给定时刻始终涵盖的近似时间跨度。在构建了摘要，再次运行此报表时，要获得完整的加速优势，报表的时间范围必须与此摘要的范围一致。有关更多信息，请参阅以下“摘要范围的工作方式”子主题。

**注意：**这里讨论的数据摘要所使用的原理类似于传统**摘要索引**的原理，但其相似处只限于此。数据摘要是为报表加速目的新建的，并不是摘要索引。有关报表加速和摘要索引的更多信息，以及用户为何可能选择一种方法而不选择另一种方法的信息，请参阅《知识管理器手册》中的“关于报表加速和摘要索引”。

### 摘要范围的工作方式

**摘要范围**设置报表的数据摘要将会覆盖的近似时间范围。未来运行报表时，仅该范围内的报表部分受益于加速。

例如，如果您选择的**摘要范围**为 **7 天**，则表示从现在开始，您希望摘要始终覆盖至少过去七天的数据。随着时间的推移，Splunk 软件会从摘要中删除早于七天的数据，同时继续汇总传入的新数据。

在构建了摘要之后，只要您对在最近七天内的时间范围运行，与它关联报表的完成速度要相对快一些。如果您对最近 10 天运行报表，则涵盖最近七天的那部分搜索将受益于加速，而涵盖剩余 3 天的那部分搜索必须针对原始数据运行，因而不会得到加速。

对于其他**摘要范围**设置也是如此。如果您计划对在最近 30 天内的时间范围运行报表，则应选择 **1 个月**。如果您预计您需要对在最近一年内的时间范围运行搜索，则应选择 **1 年**。请记住：摘要越大，第一次生成时花费的时间越长，并且会耗费更多的存储资源。

**注意：**如果您不希望运行搜索的时间上有任何限制，但仍能受益于加速，请选择**所有时间**。

## 搜索模式和报表加速

报表加速仅对**搜索模式**设置为**智能**或**快速**的报表起作用。如果为已加速的报表选择了**详细**搜索模式，则它运行起来就像根本没有加速那样慢。有关**搜索模式**设置的更多信息，请参阅《搜索手册》中的“设置搜索模式以调整搜索体验”。

## 报表如何才能符合报表加速的条件

要符合加速条件，报表基于的搜索必须具有以下特征：

- 基本搜索必须使用**转换命令**（如 `chart`、`timechart`、`stats` 和 `top`）。
- 如果基本搜索在转换命令之前已具有命令，则必须为**流命令**。在第一个转换命令之后允许使用**非流命令**。
- 基本搜索必须在**智能**或**快速搜索模式**中运行。如果您以**详细模式**保存报表，然后再进行加速，Splunk 软件会自动将搜索模式更改为**智能**或**快速**。已加速报表的搜索模式无法再更改为**详细**。
- 基本搜索无法使用事件示例。

有关子事件示例的更多信息，请参阅《搜索手册》中的“事件集示例”。

《知识管理器手册》的“管理报表加速”中提供了多个示例，包括符合条件的和不符合条件的搜索。

## 管理报表加速摘要

Splunk Web 在**管理器 > 报表加速摘要**位置针对此功能提供了一个“管理器”页面。在此页面上，您可以查看您有权限访问的报表摘要。您可以查看应用于报表摘要的报表、查看摘要的构建进度、确认摘要的一致性、重新构建损坏的摘要、删除过时或占用了所需空间的摘要，还可执行其他操作。

**注意：**如果您的角色允许您加速报表（此角色必须具有 `schedule_search` 操作），则您只能访问管理器中的“报表加速摘要”页面。

注意，随着实现所用的摘要数量的增加，您可能会遇到存储和性能方面的影响，这很重要。这是因为搜索加速摘要需要存储空间，Splunk 软件必须每隔 10 分钟在后台搜索一次数据，才能确保将数据更新至最新状态。使用“报表加速摘要”页面，可以快速识别在给定使用频率下占用的空间量过多，高于其价值的摘要。

有关报表加速的更多信息，包括后台处理方式的说明、摘要存储和性能注意事项的论述以及有关使用“报表加速摘要”页面的摘要管理的更多提示，请参阅《知识管理器手册》中的“管理报表加速”。

## 计划报表

计划的报表是以计划的时间间隔运行的报表，每次运行时都将触发一个操作。对于一个计划的报表，您最多可以定义 4 个操作：

- 通过电子邮件发送报表摘要
- 将报表结果写入 CSV 查找文件
- 设置可将消息发送到外部 Web 资源（如聊天室）的 webhook
- 记录并索引可搜索事件

只当您的角色中包含 `schedule_search` 功能时才能新建计划的报表。请参阅《确保 Splunk Enterprise 安全》中的“关于定义带功能的角色”。

### 打开“编辑计划”对话框

打开“编辑计划”对话框为现有的报表定义计划，选择性地设置每次报表按计划运行时触发的操作。

可通过三种方式打开“编辑计划”对话框：

- 将搜索保存为报表后
- 当您拓展数据集为计划报表时
- 当您管理现有的报表时

#### 将搜索保存为报表后

新建完报表后马上用此方法计划该报表。

1. 新建并运行搜索。
2. 将搜索保存为报表。  
请勿启用时间范围挑选器。计划报表无法包含时间范围挑选器，因为它们始终在设置的计划中运行。
3. 单击**计划**。

请参阅新建和编辑报表。

#### 当您拓展数据集为计划报表时

使用此方法拓展数据集为计划报表。

1. 在应用栏中，单击**数据集**。
2. 为想要计划为报表的数据集选择**管理 > 计划报表**。

请参阅《知识管理器手册》中的“数据集类型和使用方法”。

#### 当您管理现有的报表时

使用设置中的“报表”列表页面或“搜索、报表和告警页面”管理报表。

1. 转到您用来管理报表的页面。

页面	导航
“报表”列表页面	在应用栏中，单击 <b>报表</b> 。
搜索、报表和告警	选择 <b>设置 &gt; 搜索、报表和告警</b>

2. 针对您想要计划的报表，选择**编辑 > 编辑计划**。

另外，在“报表”列表页面上，您可以拓展报表行以获取计划控制。

1. 前往“报表列表”页面。

2. 为您想要计划的报表展开行。
3. 在**计划**行上单击**编辑**。

## 计划报表

计划的报表无法包含时间范围挑选器。计划含时间范围挑选器的报表时，Splunk 软件会从报表中删除挑选器。

计划报表只能以所有者身份运行。报表共享后将以用户的身份运行，计划这类报表时，Splunk 软件将更新报表设置，使其以所有者的身份运行。请参阅“确定以报表所有者还是报表用户身份运行报表”。

### 前提条件

请参阅以下主题：

- 打开“编辑计划”对话框
- 《告警手册》中的“将 cron 表达式用于计划”。
- 在 Splunk Web 中优先安排并发计划报表

### 步骤

1. 打开“编辑计划”对话框。
2. 选择**计划报表**。
3. 为报表选择**计划**。  
您可以选择如**每小时运行**的预定义计划或选择在 **Cron 计划**上运行，然后使用 **Cron 表达式** 定义自定义计划。
4. 选择报表的**时间范围**。  
**时间范围**指报表收集数据的时间范围。默认为报表已设置好的时间范围。指定一个新时间范围以覆盖此默认设置。
5. （可选）为报表选择**计划优先顺序**。  
使用**计划优先顺序**来提高此搜索的计划优先顺序。只有带有 `edit_search_schedule_priority` 功能的角色可以查看**计划优先顺序**或将其设置为**默认值**以外的值。  
  
小心使用**计划优先顺序**。只有在相对少量计划报表提高了优先顺序时有效。
6. （可选）为报表选择要在其中运行的**计划窗口**。  
当有许多计划报表设置为并发运行时，您可以设置**计划窗口**以指定报告计划程序可以将报表推迟多长时间，并使其让位于更高优先级的报表。只有带有 `edit_search_schedule_window` 功能的角色可以查看**计划窗口**或将其设置为**无窗口**以外的值。
7. （可选）单击**添加操作**以为您的计划报表定义操作。
8. 单击**保存**以保存计划设置。

请参阅“为您的计划报表定义操作。”

## 为计划报表定义操作

计划报表时，您可以选择性地定义每次报表按计划运行时触发的操作。例如，如果您添加电子邮件通知操作到一个计划报表中，报表每次运行 Splunk 软件时将通过电子邮件发送报表结果至一组相关方。

- 要添加操作到计划报表，打开“编辑计划”对话并选择**添加操作**菜单中的选项。

计划报表操作记载在 *告警手册*中。

如欲了解	请参阅
记录并索引可搜索事件	日志事件
将触发告警的结果或计划报表写入 CSV 查找文件	输出结果到 CSV 查找
通过电子邮件发送报表摘要	电子邮件通知操作
显示消息或更新其他的 web 资源	使用 webhook 告警操作

弃用**运行脚本**操作。您也可以定义包括脚本的自定义操作。

请参阅《告警手册》中的“关于自定义告警操作”。

所有这些计划报表操作可帮您导出计划报表的结果。有关其他搜索结果导出方法的摘要信息，请参阅《搜索手册》中的“导出搜索结果”。

## 允许其他人访问计划报表

如果您拥有一个**角色**，该角色授予您对应用中的**知识对象**的写入权限，如高级用户或管理员角色，则可设置或更改报表权限，以便它对其他 Splunk 用户可用，无论应用还是全局级别。请参阅“设置报表权限”。

有关管理 Splunk 知识对象的权限的更多信息，请参阅《[知识管理器手册](#)》中的“管理知识对象权限”。

## 管理并发计划报表的优先级

根据您配置 Splunk 部署的方式，可能每次只能运行一个计划报表。在此限制条件下，当您计划多个报表在几乎同一时间运行时，Splunk 的搜索计划程序将确保在收集数据的时间周期内，所有计划的报表依次运行。但是，在某些情况下您可能需要让某些报表在其他报表之前运行，以确保能够获取当前数据或者确保数据收集集中不会出现间隙。

您可以使用**计划窗口**和**计划优先顺序**设置配置计划报表的优先顺序。请参阅 Splunk Web 中的“优先安排计划并发报表”。

## 嵌入计划报表

报表嵌入允许您将报表结果带入大量报表相关方。使用报表嵌入，您可将计划报表嵌入外部（非 Splunk）网站、仪表板和门户。嵌入式报表可以事件视图、表格、图表、映射、单个值或任何可视化类型方式显示结果。它们与原始报表使用相同的格式。

在计划报表定期运行前，您不可嵌入该报表。嵌入式报表始终显示最后计划运行的结果。因此，如果某个嵌入式报表设置为在过去 24 小时内每四小时运行一次，则它将始终显示在最后四小时内获取的先前 24 小时期间的结果。此设计减少了您 Splunk 部署的负载。这也意味着，新嵌入式报表在首次计划运行前为空。

避免嵌入在较短计划上运行且通常需要很长时间完成的报表。报表返回结果前，无法查看嵌入的报表。比如，如果您有每半小时运行一次，但是需要 25 分钟返回结果的报表，报表将每小时显示五分钟结果。优化搜索以运行得更快或以更长的间隔计划报表。

嵌入式报表不具备 Splunk Web 中所查看的报表的所有功能。例如，嵌入式报表不具有钻取功能、不支持工作流动作、表格排序或字段扩展。嵌入报表显示表格可视化时，表格限制为 10 行。嵌入式报表也不支持实时搜索。

`embed_report` 功能控制着您插入计划报表的能力。默认情况下，此功能限制在高级用户角色和任何继承它的角色，如管理员角色。不具有此功能的用户不可以启用或禁用计划报表的嵌入。

报表嵌入之后，便不能再对其进行编辑。要编辑某个报表，您必须禁用该报表的嵌入。有关更多信息，请参阅下文中的“嵌入报表”。

## 嵌入报表

如果可以嵌入报表，则可以嵌入任何您在“报表”列表页面上看到的报表。

### 1. 转到“报表”列表页面并找到您要嵌入的报表。

**注意：**必须先运行报表然后才能嵌入，如有必要，还需调整其结果格式。您在此定义的任何内容将指定报表显示结果的方式（在您将它嵌入到外部站点后）。您不可以编辑已启用嵌入的报表。

### 2. 要嵌入报表，单击**编辑**并选择**嵌入**。

如果还未计划报表，则将显示“必须计划报表”对话框。单击**计划报表**以计划报表。有关更多信息，请参阅本手册中的“计划报表”。

如果报表已计划好，Splunk Web 会打开“启用报表嵌入”对话框。当您在遇到“必须计划报表”对话框后计划报表时，它还将打开此对话框。

### 3. 在“启用报表嵌入”对话框中，单击**启用嵌入**以嵌入报表。

将显示带有几行代码的“嵌入”对话框，您可将这些代码粘贴到基于 HTML 的网页。

### 4. 将代码从“嵌入”对话框复制出来并粘贴到您想要嵌入报表的基于 HTML 的网页。

### 5. 单击**完成**以关闭“嵌入”对话框。

**注意：**新嵌入式报表在首次计划运行前将不会显示数据或可视化。因此，如果您将报表计划为每四小时运行一次且在中途一小时将报表嵌入，则您必须等待大约 30 分钟，它才会显示内容。

在您嵌入报表后，您可在需要时随时从“嵌入”对话框获取它的嵌入代码。只需转到“报表”列表页面，单击已启用嵌入的报表的**编辑**，并选择**嵌入**。

您可在多个页面嵌入单个报表。无论它在什么情况下显示，它都会使用和原始报表相同的显示格式。

## 禁用报表嵌入

想要禁用报表的嵌入通常有两个原因：

- 您想要编辑报表（更新它的搜索字符串或显示格式）。不可以编辑嵌入的报表。
  - 如果禁用报表的嵌入，则需要编辑，然后再次启用该报表的嵌入，则您将必须等待，直到报表按计划运行时才可以看到更改反映在该报表嵌入的外部网站上。

- 您想要取消通过报表所嵌入的外部网站访问报表的权限。

要禁用报表，打开报表的“嵌入”对话框，并单击**禁用嵌入**。

## 已嵌入报表的附加配置

报表嵌入适用于具有与他们的角色关联的 `embed_reports` 操作的、无需任何其他 `.conf` 文件配置的用户。但是，有几个 Splunk 管理员应该注意的配置属性。

### 如果使用搜索头群集，请设置 `embedSecret` 属性

嵌入报表时，Splunk 软件会生成指向您 Splunk 部署中报表的 URL。这些 URL 通常可能只用于生成它们的搜索头中。如果您在 `server.conf` 中为 `embedSecret` 参数设置字符串值，则搜索头池中的所有搜索头都可使用相同的 URL。

您可为 `embedSecret` 设置任何字符串值。将它理解为一种密码。默认情况下，`embedSecret` 参数没有值。

### 如有必要，绕过 SSO 验证

Splunk 软件在外部网页中嵌入报表时，会向多个资源发送数个 HTTP 请求，一些情况下可能会调用 SSO 验证系统。要解决此问题，请使用替换 URI IP 地址、主机或端口前缀来更新 `embed_uri` 属性（位于 `web.conf` 中）。这会对路径进行硬编码，使它始终历经外部可访问 IP 地址或主机名称。

#### 若您已设置了 `root_endpoint` 属性

如果您已为 `root_endpoint` 属性（位于 `web.conf` 中）设置了显式值，请将该值附加到您为 `embed_uri` 定义的任何内容上。

例如，如果您已设置

```
root_endpoint = /splunkui
```

且想要把 `embed_uri` 设置为 `http://foobar:8088`，则需要将 `root_endpoint` 值附加到您的 `embed_uri` 值上，如下所示：

```
embed_uri = http://foobar:8088/splunkui
```

默认情况下，`embed_uri` 参数为空。它会解析到客户端浏览器 `window.location.protocol + "://" + window.location.host`。

### 更改嵌入式报表之下的页脚

默认情况下，嵌入式报表会显示一个包含 Splunk 徽标的页脚。您可以选择将徽标更改为文本字符串。转到 `embed_footer` 属性（位于 `web.conf` 中）并使用不同的字符串。您不可以使用 HTML 标记。

尽管 `embed_footer = splunk>` 的默认设置会把 Splunk 徽标显示为页脚，您不可以使用此参数插入替代图标或图像。

### 全局禁用报表嵌入

您可以选择为特定 Splunk Enterprise 部署的所有用户禁用报表嵌入。在 `server.conf` 中，将 `allowEmbedTokenAuth` 参数的值从 `true` 更改为 `false`。

### `embed.enabled` 参数

当嵌入这些报表时，已保存搜索端点将 `embed.enabled` 参数添加到 `savedsearches.conf` 中的计划报表段落。 `embed.enabled` 参数决定是否启用给定报表以用于嵌入。如果启用，它设置为 `1`。

## 配置计划报表的优先级

Splunk 软件的报表计划程序负责管理计划的报表和告警。基于您的系统配置，报表计划程序设置并发运行的报表数量限制。当计划要运行的报表数超过能并发运行的报表数时，它对于超出的报表进行优先级排序并尝试按优先级顺序来运行它们。

报表计划程序设置限制来确保几乎没有报表跳过的比例多于其他报表。当缓慢完成的计划报表挤掉了快速完成的报表，并导致它们错过了计划运行时间时，会跳过报表。

### 为何阅读本主题？

阅读本主题，当您：

- 有几个计划同时运行的报表，并且您发现其中一些报表一直在跳过它们的计划运行。
- 需要详细了解如何管理并发报表的计划。
- 需要禁用报表计划程序。



有关如何手动设置计划报表的信息，请参阅本手册中的“计划报表”。

## 不同搜索类型的优先级顺序

报表计划程序确定了您的计划报表和告警的运行优先级。当您的资源有限，只有几个报表可以同时运行时，运行优先级便显得格外重要。报表计划程序运行可以在当前时间运行的报表，并安排余下的报表按优先级顺序运行。

该表显示了不同类型的搜索和报表运行的高级别优先级。

优先级	搜索或报表类型	描述
第一优先级	临时历史搜索	总是首先运行您手动运行的历史搜索。如果您在一些报表计划运行的同一时间启动若干个临时搜索，则其中一些报表可能会脱离它们的计划，为临时搜索任务腾出空间。  例如，您的系统仅能同时运行三个计划报表。现在是中午 12 点，并且您有三个每小时运行一次的计划报表。在中午前几秒钟，您手动运行了三个历史搜索。报表计划程序允许您的临时搜索同时运行，然后将三个计划报表排入队列，当临时搜索完成之后，在报表的计划时间周期中运行这些报表。
第二优先级	使用实时计划手动计划的报表和告警	手动计划的报表默认使用实时计划模式。请参阅本主题中的“实时计划和连续计划”。  在该搜索和报表类别中，应用附加优先级规则来减少跳过了运行有手动计划报表和告警的实例的情况。请参阅本主题中的“报表计划程序如何防止跳过报表运行”。
第三优先级	使用连续计划手动计划的报表	连续计划模式用于填充了摘要索引的计划报表，以及在报表数据的收集集中不能有间断的其他计划报表。请参阅本主题中的“实时计划和连续计划”。
最低优先级	自动计划报表	<b>报表加速和数据模型加速</b> 后台的进程使用计划报表。为一个报表或数据模型设置加速时会计划这些报表。它们生成和更新加速摘要。  如果这些“自动摘要”报表的计划与临时搜索、告警以及手动计划报表相冲突，则始终最后运行自动摘要报表。这意味着您可能会遇到以下情况：因其他优先级更高的报表正在运行而导致无法新建或更新摘要。  请参阅本主题中的“并发计划报表的限制”。

## 报表计划程序如何确定并发计划报表限制

如果有 Splunk Cloud，您的部署将针对搜索和报表性能进行优化；为取得所需结果，您也可以根据要求使用 Splunk 支持。在 Splunk Enterprise 中可以手动优化性能，为执行此操作，您需要了解本部分中介绍的计划逻辑。

Splunk 报表计划程序限制了可以并发运行的计划报表数量。没有这些限制，您的报表性能会受到影响。要确定该限制值应为多少，报表计划程序首先从并发的临时历史搜索的系统范围内的限制开始。

有关并发搜索对于搜索性能的影响的信息，请参阅《容量规划手册》中的“容纳许多同时进行的搜索”。

**警告：**如果有 Splunk Enterprise，切勿更改 `limits.conf` 设置，除非您清楚自己在做什么。

通过一种主要变量为部署中 CPU 数量的计算，Splunk 软件可以确定系统范围内的并发历史搜索限制。计算包括《管理员手册》中“`limits.conf`”里定义的两个参数：

- `max_searches_per_cpu` 为每 CPU 允许的最大并发历史搜索数。默认为 1。
- `base_max_searches` 为不断添加到最大搜索数的基线，作为 CPU 的乘数进行计算。默认为 6。

计算如下：

$$\text{并发历史搜索的系统范围最大数量} = (\text{max\_searches\_per\_cpu} \times \text{CPU 的数量}) + \text{base\_max\_searches}$$

如果您的系统有一个 CPU，您可以并发运行最多 7 个历史搜索  $((1 \times 1) + 6 = 7)$ 。

报表计划程序向另一个 `limits.conf` 参数提供历史搜索的系统范围内限制：`max_searches_perc`。`max_searches_perc` 参数将报表计划程序可并发运行的计划报表最大值设置为并发历史搜索系统范围内限制的 50%。

如果您的系统有一个 CPU，报表计划程序可以安全地一次仅运行三个计划报表（7 的 50% 等于 3.5）。

可设置 `max_searches_perc` 参数，以便在一天或一周的时间内允许运行更多或更少的并发计划报表。请参阅接下来

的“随时间变化的最大并发计划报表限制”。

### 随时间变化的最大并发计划报表限制

您可以配置 `limits.conf` 中的 `max_searches_perc.n` 参数，在固定的周期内允许运行更多或更少的并发计划报表。您可以使用 `max_searches_perc.n` 和 `max_searches_perc.n.when` 来为特定的 cron 周期设置替代百分比。

例如：

```
# The default limit, used when the periods defined below are not in effect.
max_searches_perc = 50

# Increase the value between midnight-5AM.
max_searches_perc.0 = 75
max_searches_perc.0.when = * 0-5 * * *

# More specifically, increase it even more on weekends.
max_searches_perc.1 = 90
max_searches_perc.1.when = * 0-5 * * 0,6
```

`n` 符号可以是任何非负数字，最大为 255。计划程序按第一次匹配的反向 `n` 顺序查看。如果未提供 `n` 设置或者在当前时间未匹配 `when`，则该值回退到 `max_searches_perc` 的默认值。

### 填充加速摘要的并发计划报表限制

`auto_summary_perc` 设置用于自动计划的报表，`max_searches_perc` 设置则用于手动计划的报表。默认情况下，将报表计划程序可并发运行的自动计划报表最大值设置为并发历史搜索系统范围内限制的 50%。

使用 `auto_summary_perc.n` 参数来设置时间间隔内允许运行更多或更少的并发自动计划报表。它与“随时间变化的最大并发计划报表限制”中介绍的 `max_searches_perc.n` 参数遵循相同的逻辑。

请参阅《知识管理器手册》中的“管理报表加速”和“加速数据模型”。

## 实时计划和连续计划

每个手动计划报表都有一种计划模式。有两种可能的计划模式：实时计划或连续计划。

实时计划确保最新运行的报表返回当前的数据。使用实时计划的计划报表在其计划运行时间运行，或者根本不运行。因为较长运行时间的报表还没有完成，或者因为使用实时计划的多个报表设置为在同一时间运行，并且它们的数量高于并发计划报表限制，所以会跳过实时计划报表。

与使用连续计划的报表相比，报表计划程序总是优先考虑使用实时计划的报表。

连续计划用于在报表数据的收集中断不能有间断的情况。连续计划确保报表的每次计划运行最终都会执行。如果使用连续计划的报表现在不能运行，则它将在未来运行，在其他报表完成之后运行。

报表计划程序默认情况下为所有计划报表提供实时计划模式，除非计划报表是为摘要索引启用的，在这种情况下它们的计划模式会更改为连续。这样做是因为，当跳过填充摘要索引的计划报表时，摘要索引并不可靠。请参阅《知识管理器手册》中的“使用摘要索引提高报表效率”。

### Splunk Enterprise 中断和继续运行计划报表

当您关闭 Splunk Enterprise 时，计划报表会错过计划运行时间。对于使用实时计划的报表这通常不成问题，但是对于使用连续计划的报表这却是一个大问题，因为它们不能错过任何一次计划运行。

在 Splunk Enterprise 恢复联机之后，报表计划程序会替换错过的连续计划报表的运行。只要在 Splunk Enterprise 实例关闭之前报表至少在其计划时间内运行过一次，则报表计划程序会替换错过的报表运行。报表计划程序使用报表上一次运行时的记录来确定错过了哪些运行。默认情况下，对于错过的报表回溯不超过 24 小时。该限制由 `limits.conf` 中的 `max_continuous_scheduled_search_lookback` 参数控制。

如果 Splunk Enterprise 在连续计划报表的首次计划运行之前关闭，当服务恢复时，报表计划程序不会对于错过的运行进行弥补，因为它没有报表上一次运行时的记录。

### 计划模式示例

实时计划模式与连续计划模式的不同之处，以及在什么情况下您更希望选择某种模式，而非另一种模式？

在该示例中，您有称为 **A** 和 **B** 的两个计划报表：

- 报表 **A** 每分钟运行一次，需花费 30 秒的时间来完成。
- 报表 **B** 每 5 分钟运行一次，需花费 2 分钟的时间来完成。

在您的 Splunk Enterprise 配置中将报表计划程序设置为每次只运行一个报表。

两个报表按计划在下午 1:05 运行。

时间	计划程序的操作
1:05:00 P.M.	计划程序在 1:04 到 1:05 期间运行报表 A，并计划在下午 1:06 再次运行它。当报表 A 完成时，时间为下午 1:05:30。
1:05:30 P.M.	计划程序运行报表 B。由于将花费 2 分钟的时间来运行，所以报表 B 将在 1:07:30 完成。
1:06:00 P.M.	计划程序被唤醒，它尝试运行报表 A，但报表 A 不能运行，因为报表 B 仍在进行中。
1:06:59 P.M.	计划程序继续尝试运行报表 A 直到 1:06:59。这时接下来会发生什么取决于报表 A 使用的是实时计划还是连续计划（请参见下面的部分）。

如果报表 A 配置为使用：

- **实时计划**，计划程序会跳过报表在 1:05-1:06 期间的运行，并将报表 A 的下次运行排定在下午 1:07:00（1:06 到 1:07 期间）。新的报表运行时间基于当前的计划运行时间（下午 1:06:00）。
- **连续计划**，计划程序不会按计划执行，它会无限期地尝试运行下午 1:05 到 1:06 期间的报表。无论最终报表运行时间是什么，报表 A 将覆盖的下一个时间期间是下午 1:06 到 1:07。

### 为单个报表配置计划模式

在 `savedsearches.conf` 中的单个报表级别上定义报表计划模式。请参阅《管理员手册》。使用 `realtime_schedule` 参数为计划报表手动更改计划模式。

```
realtime_schedule= 0 | 1
```

- 设置 `realtime_schedule` 为 1 时将使用实时计划模式。该模式强制计划报表在其计划的开始时间运行。如果它不能运行，则跳过此次计划的运行。这是新计划报表的默认计划模式。
- 设置 `realtime_schedule` 为 0 时将使用连续计划模式。该模式确保计划报表从未跳过任一次计划运行。如果它不能准时运行，则将在稍后运行。为计划的报表启用摘要索引时，Splunk 软件会将 `realtime_schedule` 值设置为 0。

报表计划程序给予使用实时计划的报表比使用连续计划的报表更高的优先级。

### 计划程序如何防止跳过报表运行

实时计划模式会导致跳过报表。为减轻该问题，报表计划程序对于计划模式应用了一组规则。这些规则会减少跳过的报表运行次数。

默认情况下，报表计划程序对于所有的计划报表应用这些规则中的三个规则。您可以手动将第四个规则（计划窗口）应用到不需要在其计划开始时间运行的已选择报表。这便于报表计划程序更灵活地计划需要更高精度的报表。

规则	描述	结果	默认用于所有计划报表？
应用计划报表优先级分数	报表计划程序基于平均运行时间给予每个计划报表一个优先级分数。与分数更高（更长的平均运行时间）的报表相比，它会优先考虑分数更低（更短的平均运行时间）的报表。	当两个或多个报表计划在同一时间运行时，报表计划程序会首先运行平均完成时间最快的报表。不会经常跳过快速完成的报表，但是会更常跳过缓慢完成的报表。	是。
与连续计划相比，优先考虑实时计划	报表计划程序确保使用实时计划的计划报表，具有比使用连续计划的计划报表更好的优先级分数。	使用实时计划的报表仅与其他使用实时计划的计划报表进行优先级竞争。使用连续计划的报表始终在使用实时计划的报表之后运行，并且它们仅与其他使用连续计划的计划报表进行优先级竞争。	是。
改善已被跳过的报表的优先	报表计划程序会降低跳过报表的优先级分数，并优化计划不频繁的报表，因此它们的分数会比跳过相同次数的计划频繁的报表降低地更多。	因为第一条规则，计划不频繁和完成缓慢的报表处于不利地位，该条规则给予它们运行的机会。每次强制计划报表跳过计划的运行时，报表的优先级分数会略有改善。在跳过几次之后，它的优先级分数会允许它在强制它跳过运行的报表之前运	是。

级分数		行。	
将计划窗口应用到已选择的报表	要给予报表计划程序更多的灵活性，您可以为不需要精确开始时间的计划报表定义一个计划窗口。报表计划程序将计划窗口时间间隔添加到报表的优先级分数，而该分数是临时增加的。窗口在报表的计划运行时间打开。	具有更高优先级分数的计划报表允许分数更低的报表在其之前运行。随着时间的推移和计划窗口变窄，会改善报表的优先级分数，直到允许报表运行。	否。您为计划报表手动定义计划窗口。报表计划程序不会将“改善已被跳过的报表的优先级分数”规则应用于使用计划窗口的报表。

### 报表计划程序如何确定计划报表的基本优先级分数

报表计划程序为所有的计划报表派生一个基本优先级分数，然后根据报表是否为连续计划、被跳过或有计划窗口，为每个计划报表调整分数。基本优先级分数是计划报表的平均运行时间。平均运行时间基于计划报表之前运行时间的存储历史。使用每次新的报表运行时间更新平均运行时间。

要获得基本优先级分数，Splunk 软件使用默认因子 100 来延长每个计划报表的平均运行时间。如此做是为了区分平均运行时间以秒为单位变化的报表。

计划报表历史存储在 **KV 存储** 中，因此当 Splunk Enterprise 关闭和重新启动时也不会丢失。

### 向问题报表手动分配计划优先级或计划窗口

如果在应用默认报表计划程序规则后，跳过的计划报表仍有问题，可以使用**计划优先级**或**计划窗口**设置，通过改变计划程序优先安排特定计划报表的方式解决这些问题。

使用**计划优先级**提高特定高值计划报表的运行优先级。使用**计划窗口**使其他报表在低重要度计划报表之前运行。

要了解这些设置的深度说明，请参阅“在 Splunk Web 中优先安排并发计划报表”。

请参阅“计划报表”以了解这些设置是如何适用于报表计划工作流中的。

### 通过 .conf 文件配置计划报表的优先顺序。

管理计划报表优先顺序的规则默认设置应该保持跳过报表的事件次数降低到一个低级别上，特别是如果您将计划窗口应用到似乎是导致定期跳过其他报表的报表上。然而，如果您有 Splunk Enterprise 且跳过的报表数量已超出接受范围，请调整与计划的搜索优先顺序相关的 `limits.conf` 参数。

**警告**切勿更改 `limits.conf` 设置，除非您知道您正在做什么。

- `search_history_max_runtimes`：设置用于计算计划报表的平均运行时间的之前运行时间的数量。当该平均运行时间通过 `priority_runtime_factor` 扩展时，它就成为该报表的优先级。默认为 10。
- `priority_runtime_factor`：设置报表平均运行时间的扩展因子来获得它的优先级值。默认为 10。请参阅本主题中的“报表计划程序如何确定计划报表的基本优先级分数”。
- `priority_skipped_factor`：应用于“改善报表的优先级分数”规则。它设置当跳过报表时报表的优先级降低的因子。默认为 1。设置该值更高会导致当跳过报表时报表的优先级分数下降更快，或者设置该值更低，以减缓跳过报表后优先级分数的下降速度。

### 禁用报表计划程序

仅在必要时禁用报表计划程序。当禁用报表计划程序时，计划报表、告警和摘要索引填充搜索将不会运行。触发告警和计划报表的相关操作将不会执行。

**警告**如果您的 Splunk Enterprise 实现包含**搜索头群集**，通过发出 `splunk disable scheduler` 命令您可以在**群集管理员**上禁用计划程序，无论您是在哪个**群集成员**上发出的命令。群集管理员管理整个群集中的搜索计划和分发。当您在群集管理员上禁用报表群集化时，您禁用了整个群集中的报表计划。

请参阅《分布式搜索》手册中的“搜索头群集化架构”。

您可以禁用报表计划程序来解决您的 Splunk Enterprise 部署中遇到的问题，如沉重的处理负载或网络或硬件相关的问题。您不必重新启动 `splunkd` 就可以实现此目的。

#### 1. 访问 CLI。

请参阅《管理员手册》中的“关于 CLI”。

#### 2. 在 CLI 中输入 `splunk disable scheduler` 命令。

在禁用报表计划程序之后要启用它，请访问 CLI 并输入 `splunk enable scheduler` 命令。

### 查看报表计划程序状态

如果您不确定报表计划程序是处于启用或禁用状态，请访问 CLI 并输入 `show scheduler-status` 命令。该操作会返回报表计划程序状态。

## 在 Splunk Web 中优先安排并发计划报表

计划报表不在下次计划开始时间运行前运行时，计划程序跳过报表运行并继续下一步骤。使用**计划优先顺序**和**计划窗口**设置确保不跳过重要报表。

**计划窗口**和**计划优先顺序**设置更改 Splunk 部署达到并发计划报表系统范围限制时，**搜索计划程序**安排计划报表优先级的方式。

达到系统范围并发报表限制后，搜索计划程序在并发运行的计划报表跌破并发计划的搜索限制时优先安排超出的并发计划报表。这意味着这些报表不会严格按计划运行时间运行。但是运行时，它们仍然收集准时运行时本应覆盖的时间范围的数据。在一些情形下搜索计划程序可能需要在处理其他报表前优先处理特定报表以确保它包含当前数据或防止数据收集过程中出现中断。

使用**计划优先顺序**提高值较高的计划报表的运行优先顺序。使用**计划窗口**使其他报表在低重要度计划报表之前运行。

计划优先顺序和计划窗口设置是相互排斥的。如果计划报表同时有更高或最高的计划优先顺序和定义的计划窗口，搜索计划程序根据计划优先顺序值优先安排报表，忽略计划窗口定义。

要了解**计划窗口**和**计划优先顺序**如何适合计划报表定义的 Splunk Web 程序，请参阅“计划报表”。

关于并发计划报表和搜索计划程序的更多信息，请参阅“配置计划报表的优先顺序”。本主题讨论只有通过配置文件编辑才能获得的其他并发报表管理方式。

监视控制台有显示搜索计划程序如何对您的计划搜索进行管理的仪表板。如果您使用 Splunk Enterprise，计划程序活动仪表板显示历史和实时报表的系统范围并发搜索限制。他们还显示您在此时运行的并发搜索总数。请参阅《*监视 Splunk Enterprise*》中的“计划程序活动”。

### 搜索计划程序示例

如果您计划并发运行七个报表，而计划搜索的并发限制为三，那么其中四个报表将由搜索计划程序延迟并安排优先顺序。只要并发运行的报表中有一个完成，在优先顺序中排第一的报表就会运行，随着更多报表完成运行，其他延迟的报表将运行。

由搜索计划程序延迟的计划报表不会按其计划运行。实际运行时，它会搜索原先计划搜索的时间范围。

比如，您在过去几个小时有按小时运行的计划报表。现在假如搜索计划程序延迟报表 2 a.m. 的运行，使其在 2:07 a.m. 运行。当报表在 2:07 a.m. 运行时，将仍搜索为报表计划运行设置的原始时间范围 1 a.m. 到 1:59 a.m.。

### 使用计划优先顺序来提高计划报表的优先顺序。

**计划优先顺序**使您可以提高延迟的计划报表的运行优先顺序。这意味着它可能先于其他报表运行，可能更有机会在计划运行时间或靠近计划运行时间运行。

小心使用**计划优先顺序**设置。此设置只在您的一小部分报表的**计划优先顺序**值为**更高**或**最高**时最适用。

为报表赋上**更高的计划优先顺序**，可使它在相同的计划模式下先于其他报表运行。为报表赋上**最高的计划优先顺序**报表，可它先于优先顺序较后的报表运行，无论计划模式如何。

只有您至少一个角色有 `edit_search_schedule_priority` 功能时，您才能看到**计划优先顺序**字段，并将它设置为**默认值**以外的值。您还需要 `schedule_search` 功能以计划报表。

### 搜索计划程序如何安排计划优先顺序和计划模式组合

所有手动计划报表都有计划模式。有两种可用的计划模式：实时和连续。计划报表默认情况下是实时计划模式，除非计划报表是为**摘要索引**启用的，在这种情况下它们的计划模式会更改为连续。

如果有足够多的其他计划报表优先于实时计划模式的计划报表，实时计划模式计划报表可能会跳过计划运行，而连续计划模式的报表将持续运行。

计划报表的实时计划模式不与实时搜索直接相关，也和搜索是否“实时运行”无关。历史计划报表和实时计划报表都可以使用实时计划模式。

请参阅“实时计划和连续计划”。

这里是关于**计划优先顺序**设置在计划模式方面是如何运作的更加详细的说明。

- 在**默认**和**更高的**优先顺序下，搜索计划程序将实时计划模式的计划报表安排在并发计划模式报表之前。他们的优先顺序位于**最高**计划模式的计划报表之后。
- 在具有连续计划模式的计划报表中，搜索计划程序总是使具有**更高**优先顺序的报表位于具有**默认**优先顺序的报表之前。

- 在具有实时计划模式的计划报表中，搜索计划程序总是使具有**更高**优先顺序的报表位于具有**默认**优先顺序的报表之前。
- 搜索计划程序总是使具有**最高**优先顺序的计划报表优先于具有**默认**和**更高**优先顺序的计划报表。
- 在优先级为**最高**的计划报表组中，实时模式的报表优先于连续模式的报表。

此表格显示搜索计划程序如何安排具有不同**计划优先级**和计划模式组合的计划报表的优先顺序。以升序优先级顺序列出。

计划优先级	计划模式	整体优先级顺序
默认	连续	第六
更高	连续	第五
默认	实时	第四
更高	实时	第三
最高	连续	第二
最高	实时	第一

考虑每个**计划优先级**和计划模式组合应有多少报表时，可以把它想象成是一个金字塔，底部有着大多数计划报表，顶部只有少量计划报表。在这个金字塔中，最低的优先级组合（如**默认/连续**和**更高/连续**）会在底部。最高优先级组合（如**最高/连续**和**最高/实时**）会在顶部。

## 使用计划窗口以降低计划报表的优先级

**计划窗口**指定报表计划程序可以使报表延迟运行的时间，允许更高优先级报表提前运行的时间。设置报表的**计划窗口**，如果：

- 报表是低优先级，不总是需要在计划运行时间运行。
- 您有与此报表并发运行的其他计划报表，且报表的优先级高于此报表，您想要这些报表能够更加有机会准时或者比较准时地运行。

完成缓慢和不经常运行的报表，往往比较适合使用计划窗口。

### 规范计划窗口使用的功能

计划报表时，只有您的一个角色在 `schedule_search` 功能以外有 `edit_search_schedule_window` 功能时，才可以看到**计划窗口**字段。**计划窗口**字段默认为**无窗口**。

如果您有 `schedule_search` 功能，但您没有 `edit_search_schedule_window` 功能，计划报表时，您无法看到**计划窗口**字段。没有 `edit_search_schedule_window` 功能时，您新建的计划报表会像**计划窗口**设置为**自动**时一样。

### 计划窗口设置

设置计划报表的**计划窗口**时，您可以：

- 选择预设时间窗口，比如 **5 分钟**、**30 分钟** 或 **4 小时**。
- 选择**自定义**，并通过输入分钟数定义计划窗口的宽度。您可以输入从 0 到 44,640（一个月 31 天对应的分钟数）中的任意数字。
- 选择**自动**以使搜索计划程序依据时间周期和报表的平均运行时间计算报表的最优计划窗口宽度。

当报表计划要运行时，计划窗口将打开。最初，窗口允许其他更重要的报表在此报表之前运行。当计划窗口接近关闭时，报表运行的可能性将增加。

不要给报表赋等于或超出期间的**计划窗口**。比如，如果您的报表期间为 1 小时，给报表赋小于 1 小时的**计划窗口**值。如果您赋的值超出 1 个小时，报表可能会错过计划运行。

如果您想要验证计划窗口是否应用到特定报表，在 `scheduler.log` 中搜索报表。如果它有计划窗口，就会有非零的 `window_time` 值。

## 偏移计划的搜索启动时间

如果您的组织有在同一时间运行的大量**计划的搜索**，如每分钟或每五分钟运行，**搜索计划程序**会导致网络硬件或索引器超载。在 `savedsearches.conf` 中使用 `allow_skew` 设置以减少这些干扰。

Splunk 实现有大量设置为在某一分钟运行的计划的搜索时，计划程序尝试在那一分钟的第 0 秒后尽快运行。这么多搜索都会在几乎同一时间启动，这会导致有关的硬件 CPU 很快以 100% 容量运行，最多几秒钟。这些 CPU 峰值对运行 Splunk 的硬件不一定是个问题，但是可能导致内部网络流量过大，使网络交换机过载。

`allow_skew` 设置使计划的搜索的实际开始时间从计划运行时间随机偏移。比如说，如果您有一个计划每分钟运行的搜

索，allow\_skew 可使此搜索偏移，所以实际上搜索每次都在每分钟的 23 秒后开始运行。计划程序将 allow\_skew 应用于按类似计划运行的大量搜索时，每个搜索的偏移随机性形成实际开始时间的平均分布。

如果您有 Splunk Cloud，您必须提交支持请求将 allow\_skew 应用于计划的搜索。

### allow\_skew 方式

您提供给 allow\_skew 的值提供搜索可以在启动时间偏移的最大时间范围，从而约束搜索计划程序。您可以按最大时间范围或时间周期百分比设置 allow\_skew。

方法	定义	示例
最大偏移时间范围	使用 <int><time_unit> 结构提供搜索可以偏移的最大时间范围。	40s 针对 1 分钟时间周期的搜索
		3m 针对 5 分钟时间周期的搜索
时间周期百分比	以计划的搜索时间周期百分比的形式，提供指定搜索可偏移最大时间的百分比。	50% 针对 1 分钟的搜索，将偏移限制为最多 30 秒
		100% 针对 5 分钟的搜索，允许偏移到 5 分钟以内的任意时间

您可能在将 allow\_skew 应用到单个搜索时想要提供最大偏移时间，在将 allow\_skew 应用到多个搜索时想要通过一个设置提供时间周期百分比。请参阅“在应用或全局级别设置 allow\_skew”。

由搜索计划程序决定的偏移时间在搜索不断运行时保持不变。比如，如果您为每 5 分钟运行的搜索设置 allow\_skew，计划程序将它偏移至计划开始时间之后 2 分钟时运行，那么之后搜索每次运行时都使用相同的偏移量。编辑搜索前，搜索的偏移量不变，编辑搜索后，计划程序重新为搜索计算偏移量。

按照 allow\_skew 的搜索偏移总是在计划时间范围内运行。例如，如果一个搜索的运行时间范围是过去的 5 分钟，在每个 5 分钟内计划在 2:05pm 运行，但偏移后实际运行时间为 2:07pm，它将仍然在 2:00:00pm 到 2:04:59pm 这段时间内进行搜索。

### 搜索计划如何影响潜在的计划偏移

设置计划的搜索的 allow\_skew 时，计划的搜索的时间周期决定了搜索计划程序可以将搜索从计划偏移的程度。

对于计划符合下列 cron 表达式模式的计划的搜索，搜索计划程序偏移此类计划的搜索的自由程度最高。

Cron 表达式模式	定义
* * * * *	每分钟
*/M * * * *	每 M 分钟，其中 M > 0
0 * * * *	每小时
0 */H * * *	每 H 个小时，其中 H > 0
0 0 * * *	每天午夜

如果您为具有此类 cron 表达式模式的搜索设置 allow\_skew，根据您使用 allow\_skew 值设置的约束，搜索计划程序可以最多偏移 1 倍时间。

计划不符合这些模式的搜索最多能偏移 60 秒，无论其计划时间周期是多久。这些搜索更有可能需要在您定义的计划时间或比较接近您定义的计划时间运行。

请参阅《告警手册》中的“将 cron 表达式用于计划”。

### 在应用或全局级别设置 allow\_skew

因为 allow\_skew 设计用于大量并发计划的搜索出现冲突的情况，您可能想要将一个 allow\_skew 设置应用于多个搜索。您可以在应用级别或在全局级别应用设置。

应用程序级别	定义	方法
应用	将 allow_skew 设置应用到属于特定应用的所有计划的搜索。	将 allow_skew 设置添加到该应用的 local/savedsearches.conf 文件的 [default] 段落中。
全局	将 allow_skew 设置全局应用到 Splunk 部署中的所有计划的搜索。	将 allow_skew 设置添加到 \$ETC/system/local/savedsearches.conf 中的 [default] 段

当您为 `allow_skew` 应用到多个搜索时，您可以通过为它们提供各自的 `allow_skew` 设置覆盖特定搜索的设置。如果您想要搜索退出应用或全局级别 `allow_skew` 设置，将 `allow_skew=0` 添加到该搜索的 `savedsearches.conf` 段落。

## Allow\_skew 和其他搜索计划程序设置

`allow_skew` 设置不直接和计划窗口和计划优先级设置相关，后两种设置可帮助管理跳过、并发计划报告。不要将 `allow_skew` 用作该使用案例的解决方案。

请参阅 Splunk Web 中的“优先安排计划并发报表”。

## 生成报表和仪表板的 PDF

### 生成报表和仪表板 PDF

要生成仪表板 PDF，您可以单击仪表板上的**生成 PDF**。关于此功能的更多信息，请参阅《仪表板和可视化》中的“生成仪表板 PDF”。

您可以在 Internet 浏览器中或使用一个单独的 PDF 查看应用程序来查看 PDF。

### 计划 PDF 电子邮件交付

您可以为报表和仪表板计划电子邮件 PDF 交付。您可以配置计划按固定时间间隔运行。

要计划报表的 PDF 电子邮件，可使用“新建计划的搜索”对话框。单击**新建**并选择*计划的搜索...*有关更多信息，请参阅本手册中的“计划报表”。

要计划仪表板的 PDF 电子邮件，可导航到仪表板并单击**计划 PDF 交付**来打开“计划 PDF 交付”对话框。有关更多信息，请参阅《数据可视化手册》中的“生成仪表板 PDF”。

通过使用 `sendemail` 搜索命令，您可以设置通过单封电子邮件交付 PDF 形式的搜索结果有关详细信息，请参阅《搜索参考》中的 `sendemail` 主题。

- 注意：`sendemail` 命令不允许您为您的结果设置计划的电子邮件。

### 通过告警电子邮件发送 PDF

您可以设计告警，使告警在触发后发送带 PDF 附件的电子邮件，以显示触发搜索的结果。

有关您可以设计的不同告警类型的更多信息，请阅读《告警手册》。

### 实时搜索和集成的 PDF 生成

使用集成的 PDF 生成为实时运行的搜索、报表或仪表板生成 PDF 时，Splunk 软件会把搜索转换为历史搜索（主要是从时间范围中删除 "rt"）。因此，如果您拥有 5 分钟窗口的实时搜索，则 PDF 将显示该搜索的结果，如同它仅在相对于生成 PDF 时间的过去 5 分钟运行一样。

如果仪表板的板面可显示“所有时间实时”时间范围搜索的结果，该仪表板的 PDF 将显示所有时间内同一搜索的结果。

### 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。如果您有 Splunk Cloud 且需要其他字体，请向 Splunk 支持提交问题。

如果您有 Splunk Enterprise，可以通过更改 `reportCIDFontList` 参数（位于 `alert_actions.conf` 中）控制 CID 字体的加载方式。如果多个字体为给定字符代码提供了字形，则使用来自列表指定第一个字体的字形。默认情况下，`reportCIDFontList = gb cns jp kor` 分别指简体中文、繁体中文、日文和韩文。

如果多个字体为给定字符代码提供了字形，则使用来自列表指定第一个字体的字形。要跳过加载任何 CID 字体，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），要求您的 Splunk Enterprise 管理员添加 Unicode 字体到 `$SPLUNK_HOME/share/splunk/fonts`。如果尚不存在，请新建 `fonts` 目录。

**注意：**安装多种字体时，Splunk 软件会按字母顺序进行排序。这意味着，如果您安装了 Cyrillic 和 Greek，它将始终选择 Cyrillic，除非您在 `$SPLUNK_HOME/share/splunk/fonts` 中更改文件名以便先使用 Greek。

### 集成的 PDF 生成的其他配置选项

有几个用于计划的 PDF 的自定义选项。它们包括下列项目的设置。



- **页眉和页脚显示。**您可以选择是否在您的 PDF 中包括页眉和页脚。您还可以配置页眉或页脚中元素的位置，在左侧、右侧或正中显示它们。
- **HTML 图像支持。**您可以选择呈现带有 HTML `<img>` 标记的 PNG 或 JPEG 图像。HTML 图像呈现可能会导致 PDF 的生成出现问题。如果您在生成 PDF 时遇到问题，则不要选择图像呈现。
- **可选的徽标文件位置。**您可以替代出现在 PDF 的页眉或页脚上默认 Splunk 徽标位置上的徽标图像。您可以指定图像文件的路径并调整徽标位置到左侧、右侧或正中。

您可以使用“邮件服务器”设置管理器来配置这些选项。选择**设置 > 服务器设置 > 电子邮件设置**来查找**邮件服务器设置**页面。滚动到该页面底部来找到 **PDF 报表设置**。

如果您有 Splunk Enterprise，您还可以在 `limits.conf` 和 `alert_actions.conf` 中配置集成的 PDF 生成的某些方面。

### 在应用的本地目录中的文件名配置

您可以调整 `etc/apps/<app_name>/local` 目录内 `alert_actions.conf` 文件中的计划 PDF 文件命名语法。这会更改计划交付的电子邮件中附带的 PDF 文件名称。例如，您可以通过编辑 `etc/apps/search/local/alert_actions.conf` 来调整“搜索和报表”应用的 PDF 设置。

默认情况下，计划 PDF 的文件名遵循此约定：`$type$-$name$-$time:%Y-%m-%d$`。

例如，默认 PDF 文件名是 **dashboard-test-2015-01-15.pdf**。

要更改默认设置，您可以指定表示关于 PDF 下列信息的标记。

标记	受支持的值	描述
<b>\$type\$</b>	<ul style="list-style-type: none"> <li>• dashboard</li> <li>• report</li> <li>• alert</li> </ul>	该 PDF 的知识对象类型
<b>\$app\$</b>	app_id	应用文件夹名称，如 <code>search</code>
<b>\$owner\$</b>	owner	正计划 PDF 的用户
<b>\$name\$</b>	仪表板、报表或告警的 ID	使用 ID 而非标签
<b>\$time\$</b>	计划 PDF 的触发时间	按照 Python 的 <code>strftime</code> 库的格式。

`alert_actions.conf` 中的示例配置设置的外观会如下所示。

```
[email]
reportFileName = $type$-$name$-$time:%Y-%m-%d$
```

- 注意：在 `etc/apps/<app_name>/local/alert_actions.conf` 中进行此更改很重要。

### limits.conf

您可以在 `[pdf]` 段落中把 `max_rows_per_table` 设置为 Splunk 软件以 PDF 格式打印简化结果表格的最大表格行数。默认值为 1000。

**注意：**如果您的表格具有大量行，这会导致多页报告。如果您希望限制表格为仪表板的 PDF 版本生成的页数，请减少该数量。

在同一段落中，您可以将 `render_endpoint_timeout` 更改为默认 3,600 秒（1 小时）之外的数字。这样就能控制 Splunk 软件等待生成缓慢完成搜索 PDF 的时长。

### alert\_actions.conf

`alert_actions.conf` 的 `reportIncludeSplunkLogo` 参数控制 Splunk Enterprise 徽标是否显示在 PDF 页脚中。默认情况下，这将设置为 1 (true)。如果您不希望看到 Splunk Enterprise 徽标，将该值设置为 0 (false)。

### 打印搜索结果或格式报表

如果您正在打印一组搜索结果或一份带格式的报表（显示表格或可视化），Splunk 软件将使用集成的 PDF 生成进行打印。

如果需要计划通过电子邮件交付 PDF 或使用 `sendemail` 命令，您仍需要在**设置 > 搜索、报表和告警**中配置设

置。

## **集成 PDF 生成的例外情况**

这里是集成 PDF 生成期间的一些限制。

### ***使用简单 XML 来设计打印的仪表板***

仅可打印简单 XML 仪表板。简单 XML 支持各种图表功能、具有动态钻取功能，并支持仪表板和表单中搜索的后期处理。有关使用简单 XML 构建仪表板的完整说明，请参阅《*仪表板和可视化*》手册。

### ***无法打印计划的表单***

集成 PDF 生成无法打印计划的表单。您只能打印一次性表单（使用简化 XML 构建）。

## **系统要求**

Splunk Enterprise 支持的所有操作系统均支持生成 PDF。请参阅“本地使用 Splunk Enterprise 的系统要求”了解完整列表

## **问答**

有什么问题吗？请访问 Splunk Answers，查看 Splunk 社区有哪些与 PDF 生成相关的问题和答案。