



Splunk[®] Enterprise 6.5.0

报表手册

生成时间：2016 年 9 月 26 日下午 10:25

Table of Contents

报表摘要	3
关于报表	3
报表管理	3
创建和编辑报表	3
设置报表权限	9
加速报表	11
计划报表	13
嵌入计划报表	21
已嵌入报表的附加配置	22
配置计划报表的优先级	22
生成报表和仪表板的 PDF	27

报表摘要

关于报表

保存搜索或数据透视表以备后用时会创建报表。创建报表后，您可对它执行许多操作。在本手册中，您将了解如何：

- [手动创建和编辑报表](#)。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](#)，无论在报表创建期间还是稍后时间。
- [设置计划的报表](#)--按固定时间间隔运行并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。查看本功能的例外情况。

报表管理

创建和编辑报表

当创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”端创建报表。

一旦创建报表，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。
- [打开报表并编辑它](#)，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，这取决于它的创建方式。

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，以便它定期运行](#)。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 中创建报表

您可以通过四种方式使用 Splunk Web 创建报表：

- 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。

有关这些报表创建方法的更多信息，请参阅以下小节。

一个报表定义至少包含与搜索相关联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。报表将保留您为原始搜索设置的任何格式，包括图表可视化和事件列表显示选项。

注意：在运行、暂停、确定或完成时，您仅能保存一个搜索。

1. 运行值得保存为报表的搜索，或设计值得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。报表将保留您为原始搜索设置的任何格式，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**。

另存为报表

标题 Food Truck Sales by County

描述 可选

内容 统计表

时间范围挑选器 是 否

取消 保存

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，而不真正编辑报表。

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。请参阅本手册中的[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。

在设置中创建新报表

当希望创建报表时，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”中手动创建新报表。

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 *

sourcetype="access*" action="purchase" | stats count by product name

描述

以...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

取消 保存

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. 给搜索一个对于目标应用唯一的**搜索名称**。
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。

报表加速允许通常缓慢完成的搜索未来运行的速度更快。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，则可以编辑和更新它们。请参阅《[知识管理器手册](#)》中的“管理知识对象权限”。

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	创建方法	优势
通过内联搜索（面板定义中的搜索字符串）备份	<ul style="list-style-type: none">将新搜索或数据透视表另存为仪表板面板。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”）并保存为内联搜索备份的仪表板面板。创建来自仪表板编辑器的面板，选择内联搜索，然后定义搜索字符串。	可以编辑备份面板的搜索，而无需离开仪表板编辑器。
通过报表备份	<ul style="list-style-type: none">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”），然后保存为通过报表备份的仪表板面板。创建来自仪表板面板的面板，选择报表，然后选择报表名称。	<ul style="list-style-type: none">可以利用报表加速的优势，这样面板加载更快。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。

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备份的面板。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创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报表使用一页纸。

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。

转换为报表

报表标题

Top 20 Truck Fleets (Permit Approved)

描述

取消

保存

4. 单击保存。

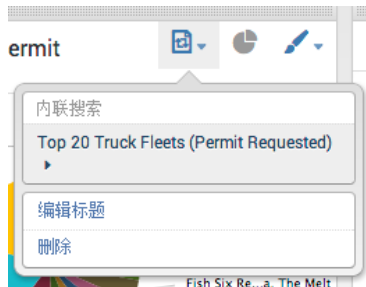
Splunk 软件会把新报表添加到“报表”列表页面。

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，您还将失去通过仪表板更改面板可视化类型的能力。

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，这取决于用于创建报表的工具）。
- **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，这取决于用于创建报表的工具）。

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”中创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创建报表的方式。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 软件命名复制版报表的方式为：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创建的报表。有关为角色授予删除非其所拥有报表的能力的更多信息，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 方法应用创建的报表。但如果您有 Splunk Enterprise 而且更喜欢直接通过配置文件使用报表，当然也毫无疑问。

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

您所创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。

默认情况下只有“管理员”和“超级用户”角色才能更改知识对象（如报表）的权限。请参阅《[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”。

同时，“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。请参阅本主题中的[基于数据透视表的报表权限](#)。

最后，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。请参阅《[搜索手册](#)》中的“在 Splunk Web 中保存和共享任务”。

1. 为您的报表打开“编辑权限”对话。

有多种方式可以访问“编辑权限”对话：

访问方式	针对现有报表？	访问步骤
何时首次创建报表	否	<ol style="list-style-type: none"> 1. 运行搜索。 2. 将搜索保存为报表。 3. 在“您的报表已创建”对话中，单击权限。
从“报表”列表页面	是	<ol style="list-style-type: none"> 1. 导航至“报表”列表页面。 2. 查找要为此编辑权限的报表。 3. 单击编辑并选择权限。
从报表显示视图	是	<ol style="list-style-type: none"> 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. 单击编辑并选择编辑权限。
从设置	是	<ol style="list-style-type: none"> 1. 导航到设置 > 搜索、报表和告警。 2. 查找需编辑其权限的报表。 3. 单击其权限链接。

2. 选择**应用**或**所有应用**。

所有报表在特定应用的上下文中创建。

- 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**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。请参阅本主题中的[确定以报表所有者还是报表用户身份运行报表](#)。

编辑权限

×

报表

Messages by minute last 3 hours

所有者

nobody

应用

search

显示

所有者

应用

所有应用

以...身份运行

所有者

用户

了解更多信息

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

取消

保存

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。

请参阅《[知识管理器手册](#)》中的“管理知识对象权限”。

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”（即报表创建者）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备份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。要解决这个问题，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”数据模型创建名为“Top Firewall Attacks by IP”的基于数据透视表的报表。“外部威胁”数据模型拥有限于“安全性”应用的权限，仅此而已。

首次创建报表时，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：

- 通过“数据透视表”创建。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，您就不能加速搜索。
- 您的角色没有报表的写入权限。
- 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，且这些知识对象的定义可在报表加速后独立于报表进行修改，则加速这类报表时应格外小心。如果此情况发生，则加速报表可能会返回无效的结果。

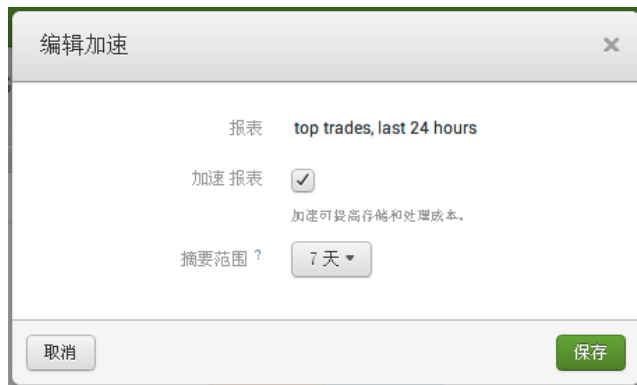
如果您怀疑加速后的报表返回无效的结果，可以对结果摘要进行确认，以查看摘要内包含的数据是否一致。请参阅《*知识管理器手册*》中的“确认摘要”。

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，则可在创建报表时或创建后的任何时间加速它。

- 当保存搜索为报表时**，您将被转到“您的报表已创建”对话框，其中您可以从三个可选“其他设置”选项中选择。单击**加速**选项打开“编辑加速”对话框。
- 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创建的，**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，请参见《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。计划的报表可以触发两种操作：**发送电子邮件和运行脚本**。

有两种方法可以计划报表并定义报表操作：

- 可以使用“编辑计划”对话框
- 可以在“设置”中打开报表并为其定义计划

报表计划的限制

仅当您的角色中包含 `schedule_search` 操作时才能创建计划的报表。请参阅《确保 Splunk Enterprise 安全手册》中的“关于使用功能定义角色”。

打开“编辑计划”对话框

可通过三种方式打开“编辑计划”对话框。

“编辑计划”对话框分为两部分。在第一部分中，计划一个报表。在第二部分中，定义计划报表的操作。

要在“设置”中创建或更新计划报表，请导航到**设置 > 搜索、报表和告警**。请参阅本主题中的[“在设置中计划报表”](#)。

将搜索保存为报表后

创建完报表后马上用此方法计划该报表。

1. 创建并运行搜索。
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。

请参阅本手册中的[创建和编辑报表](#)。

3. 在“您的报表已创建”对话框中，单击**计划**。

从“报表”列表页面

使用该方法计划现有报表。

1. 导航至报表列表页面。
2. 定位您想要计划的报表并对其进行扩展。
3. 在**计划**行上单击**编辑**。

替代方法：

1. 导航至报表列表页面。
2. 定位您想要计划的报表
3. 单击报表的**编辑**并选择**编辑计划**。

使用“编辑计划”对话框计划报表

本步骤将向您显示如何使用“编辑计划”对话框为新的或现有报表定义报表计划。

注意：计划现有报表时，请注意：

- **计划的报表不能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。
- **计划的报表只能以所有者的身份运行。**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。请参阅本手册中[“确定以报表所有者还是报表用户身份运行报表”](#)。

1. 根据上一个部分中列出的步骤，为新的或现有报表打开“编辑计划”对话框。
2. 选择**计划报表**。
3. 输入**计划和时间范围**。

如果您选择运行 Cron 计划，请参阅本主题中的[“指定报表交付的 cron 计划”](#)。

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。

4. **(可选)** 为报表选择要在其中运行的**计划窗口**。



仅为报表提供一个计划窗口，前提是：

- 报表无需始终在计划好的运行时间开始运行。
- 您觉得该报表可能导致其他报表错过计划好的运行。由于资源约束，如最大并发报表限制，这种情况可能会发生。

计划窗口指定报表计划程序可以将报表推迟多长时间，并使其在资源受限的时间内让位于更高优先级的报表。

当报表计划要运行时，计划窗口将打开。最初它允许其他更高优先级的报表在它之前运行。当计划窗口接近关闭时，报表运行的机会将增加。完成缓慢和在罕见的基础上运行的报表，往往是计划窗口很好的候选者。

窗口的宽度以分钟为单位进行定义。它可以是从 0 到 44,640（一个月 31 天对应的分钟数）中任意数字的分钟数。窗口宽度不应超过报表的时长。例如，如果您有一个每小时运行的计划报表，您不要为该报表定义两小时宽度的计划窗口，因为这会导致报表错过计划运行。

5. 单击**下一步**为计划报表设置一个操作。

请参阅本主题中的[“为计划的报表设置操作”](#)。

有关**计划窗口**设置、报表计划程序使用来减少跳过计划报表运行事件的方法，以及最大并发报表限制的更多信息，请参阅本手册中的[“配置计划报表的优先级”](#)。

要在“设置”中创建或更新报表计划，单击**搜索、报表和告警**以转到包含该名称的页面。打开新的或现有报表的详细信息页面。请参阅本主题中的[“在设置中计划报表”](#)。

指定报表交付的 cron 计划

您可以使用标准 cron 符号定义自定义交付计划。当您选择 **Cron** 选项时，将出现一个字段，您可以从中输入 cron 计划。

注意：Splunk 软件使用 cron 符号的五个参数，而不是六个。Splunk 软件不使用 `year` 的第六个参数，该参数在其他 cron 符号形式中较为常见。

以下参数：

`(* * * * *)`

对应于：

`minute hour day month day-of-week`

以下是一些 cron 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.
```

使用“编辑计划”对话框为计划的报表定义操作

计划的报表每次运行时都能执行以下操作：

- **发送带结果的电子邮件给一组收件人。**这些电子邮件可以提供文本格式的报表结果，或者包含 CSV 或 PDF 附件形式的报表结果。
- **运行访问报表结果的脚本。**您的脚本将报表结果发布到外部系统以进一步处理，或者按定期计划进行归档。

注意：您可以使用这些计划报表的操作导出搜索结果。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”。

定义“发送电子邮件”操作

本过程显示如何使用“编辑计划”对话框来设置计划报表的“发送电子邮件”操作。

如果未先在“设置”中为您的 Splunk 部署配置电子邮件通知，则无法设置这类操作。请参阅《*告警手册*》中的“电子邮件通知操作”。

1. 进入“编辑计划”对话框，如果需要的话定义报表计划，然后单击**下一步**。

请参阅本主题中的“计划报表”。

2. 选择**发送电子邮件**以创建电子邮件操作。

编辑电子邮件选项对话框打开。

3. 提供用逗号分隔的**收件人**电子邮件收件人的列表。

4. (可选) 提供用逗号分隔的**抄送**和**密送**电子邮件收件人的列表。

单击**显示抄送和密送**以查看**抄送**和**密送**字段。

5. 设置电子邮件**优先级**。

优先级是否强制执行取决于您的电子邮件客户端。

6. (可选) 提供电子邮件**主题**和**消息**。

您可以在电子邮件主题和消息文本中使用令牌，来给您的用户提供各种信息。请参阅本主题中的[“在计划报表电子邮件主题和正文中使用令牌”](#)。

7. (可选) 对于所**包括**的范围，请选择选项来包括或附加有关搜索和其结果的信息。

在电子邮件中，可以包括：

- 相关报表的链接。
- 电子邮件代表的报表运行结果的链接。
- 计划报表的搜索字符串。
- 报表运行的结果，以内联表、CSV 文件或原始事件列表的格式显示。

您也可以使用 CSV 文件或 PDF 的格式附加报表运行的结果。请参阅本主题中的[“在计划报表电子邮件中包含结果”](#)。

8. (可选) 将电子邮件**类型**更改为**纯文本**。

默认情况下，**类型**设为 **HTML 和纯文本**。

9. 单击**保存**以保存您的电子邮件操作设置。

有关配置脚本的详细信息，请参阅本主题中的[运行脚本](#)。

如果有 Splunk Enterprise，您还可在 `alert_actions.conf` 或 `savedsearches.conf` 配置文件中配置报表电子邮件操作。使用 `alert_actions.conf` 配置全局属性。使用 `savedsearches.conf` 配置单个报表。请参阅《告警手册》中的“在 `savedsearches.conf` 中配置告警”。

更多有关生成并邮寄报表结果 PDF 文件的信息，请参阅本手册中的[“生成报表和仪表板的 PDF”](#)。

以下数字显示作为文本（在电子邮件正文中）交付的结果的计划报表电子邮件：



Splunka Testerman <splunk250@gmail.com>

Splunk Report: Source type count for past 7 days

1 message

splunk <splunk>

To: splunk250@gmail.com

Wed, Apr 23, 2014 at 11:00 AM

The scheduled report 'Source type count for past 7 days' has run.

Report: [Source type count for past 7 days](#)[View results in Splunk](#)

_time	scheduler	splunk_python	splunk_web_access	splunk_web_service	splunkd	splunkd_access
Wed Apr 16 00:00:00 2014	1	1	2634	15	84361	2653
Thu Apr 17 00:00:00 2014	1	1	11441	217	155955	11747
Fri Apr 18 00:00:00 2014	1	1	0	0	151517	9
Sat Apr 19 00:00:00 2014	1	1	0	0	151515	9
Sun Apr 20 00:00:00 2014	1	1	0	0	151520	9
Mon Apr 21 00:00:00 2014	1	0	6204	58	154622	6245
Tue Apr 22 00:00:00 2014	1	0	3147	235	153378	3705
Wed Apr 23 00:00:00 2014	0	0	3412	148	71503	3541

If you believe you've received this email in error, please see your Splunk administrator.

splunk > the engine for machine data

定义“运行脚本”操作

您可以指定一个脚本，每次运行计划的报表时都运行该脚本。本过程显示如何使用“编辑计划”对话框来设置计划报表的“运行脚本”操作。

1. 进入“编辑计划”对话框，如果需要的话定义报表计划，然后单击**下一步**。

请参阅本主题中的“计划报表”。

2. 选择**运行脚本**以创建电子邮件操作。

文件名字段会出现。

3. 提供脚本的**文件名**。

此脚本必须在 Splunk Enterprise 实例中位于以下位置：`$SPLUNK_HOME/bin/scripts`

4. 单击**保存**以保存您的脚本操作设置。

请参阅本主题中的[运行脚本操作示例](#)。

在计划报表电子邮件主题和正文中使用令牌

令牌是一种变量类型，代表搜索任务生成的数据。Splunk Enterprise 提供多种令牌，可用于包含由电子邮件字段中搜索生成的信息。对于计划报表交付，您可将令牌用于以下电子邮件字段：

- 主题
- Message
- 页脚

使用以下语法访问令牌的值：

`$<token-name>$`

例如，将以下令牌放在计划报表交付的主题字段中，以引用包含报表的应用。

从 `app` 中搜索结果

可用于电子邮件通知的令牌

本部分列出常用的用于报表的计划电子邮件交付的令牌。访问从搜索生成的数据的令牌有四种类别。使用令牌的上下文有所不同。

以下表格列出令牌的所有类别。来自所有类别的令牌都可用于计划报表交付。

类别	描述	上下文
----	----	-----

仪表板的计划 PDF 交付

搜索元数据	有关搜索的信息。	来自搜索的告警操作 计划报表
服务器信息	有关 Splunk Enterprise 服务器的信息	仪表板的计划 PDF 交付 来自搜索的告警操作 计划报表
搜索结果	访问搜索结果	来自搜索 计划报表的告警操作
任务信息	特定于搜索任务的数据	来自搜索的告警操作 计划报表

除了本主题列出的常用令牌之外，`savedsearches.conf` 和 `alert_actions.conf` 文件列出属性，该属性值从令牌可用。要访问这些附加属性值，可在 `$` 标记分隔符之间放入属性。

访问搜索元数据的令牌

访问有关搜索信息的常用令牌。这些令牌由以下上下文提供：

- 告警操作
- 计划报表
- 仪表板的计划 PDF 交付

以下是一些可用的常见令牌。

令牌	描述
<code>\$action.email.hostname\$</code>	电子邮件服务器的主机名。
<code>\$action.email.priority\$</code>	搜索的优先级。
<code>\$app\$</code>	包含搜索的应用名称。
<code>\$cron_schedule\$</code>	应用的 Cron 计划。
<code>\$description\$</code>	搜索的描述。
<code>\$name\$</code>	搜索的名称。
<code>\$next_scheduled_time\$</code>	搜索下次运行的时间。
<code>\$owner\$</code>	搜索所有者。
<code>\$results_link\$</code>	(仅限告警操作和计划报表) 搜索结果的链接。
<code>\$search\$</code>	实际搜索。
<code>\$trigger_date\$</code>	(仅限告警操作) 触发告警的日期。
<code>\$trigger_time\$</code>	(仅限告警操作) 告警运行的计划时间。
<code>\$type\$</code>	指示搜索是否来自告警、报表、视图或搜索命令。
<code>\$view_link\$</code>	查看已保存报表的链接。
<code>\$alert.severity\$</code>	告警的严重性级别。
<code>\$alert.expires\$</code>	告警到期的时间。

结果提供的令牌

从结果中，您可使用 `result.<fieldname>` 标记来访问搜索结果中特定字段的第一个值。这些令牌由以下上下文提供：

- 告警操作
- 计划报表

Token	描述
<code>\$result.fieldname\$</code>	从搜索的第一个结果返回特定字段名称的第一个值。字段名称必须在搜索中显示。

访问任务信息的令牌

访问特定于搜索任务的数据的常见令牌，如搜索 ID 或由搜索任务生成的消息。这些令牌由以下上下文提供：

- 告警操作
- 计划报表

Token	描述
\$job.earliestTime\$	搜索任务开始的初始时间。
\$job.eventSearch\$	包含任意转换命令前部分搜索的搜索的子集
\$job.latestTime\$	搜索任务的最晚时间记录。
\$job.messages\$	搜索任务生成的错误和调试消息列表。
\$job.resultCount\$	搜索任务返回的结果的数量。
\$job.runDuration\$	完成搜索需要的时间（以秒为单位）。
\$job.sid\$	搜索 ID。
\$job.label\$	搜索任务的命名名称。

服务器提供的令牌

提供 Splunk Enterprise 服务器可用的详细信息的常见令牌。这些令牌可用于仪表板的计划 PDF 交付。

以下表格列出某些可用的常见令牌。

令牌	描述
\$server.build\$	Splunk Enterprise 实例的内部版本号。
\$server.serverName\$	托管 Splunk Enterprise 实例的服务器名称。
\$server.version\$	Splunk Enterprise 实例的版本号。

已弃用电子邮件通知令牌

弃用以下来自 Splunk Enterprise 先前版本的令牌。

令牌	描述
\$results.count\$	（已弃用）Use \$job.resultCount\$。
\$results.url\$	（已弃用）Use \$results_link\$。
\$results.file\$	（已弃用）无可用的当量。
\$search_id\$	（已弃用）Use \$job.id\$。

运行脚本操作示例

您可以设置“运行脚本”操作，在每次报表运行时将报表结果发送到外部系统。这是通过运行脚本调用 API 将报表结果发送到外部系统来实现的。

出于安全原因考虑，将所有脚本放到您 Splunk Enterprise 实例的下列路径下：

\$SPLUNK_HOME/bin/scripts

\$SPLUNK_HOME/etc/<AppName>/bin/scripts

您还可使用 shell 脚本或批处理文件配置运行计划报表脚本。在 `savedsearches.conf` 配置文件中做出此配置。请参阅《告警手册》中的“配置脚本式告警”。

如果您在计划的报表脚本方面遇到问题，可查看 Splunk 社区 Wiki 上这个优秀的关于告警脚本疑难解答的主题。

有关运行脚本告警操作的更多信息，请参阅《告警手册》中的“设置告警操作”。

在设置中计划报表

在“设置”中，您可以让已保存报表的行为与使用“编辑计划”对话框所计划的报表类似。

1. 导航到设置 > 搜索和报表。

2. 打开报表的详细信息页面。

3. 选择**计划此搜索的时间**以打开报表的计划和告警选项。

4. 设置报表计划。

您可以选择**基本计划类型**（允许您从一定范围的预设选项中进行选择）和 **Cron**（允许您使用标准 cron 符号设置计划）。请参阅本主题中的[“指定报表交付的 cron 计划”](#)。

5. （可选）当有多个并发计划报表时，为不需要在计划运行时间运行的报表提供一个**计划窗口**。

报表将在该窗口内的某个时间点运行。与此同时，其他报表会在它之前运行。请参阅本主题中的[“计划报表”](#)。

6. 为使该报表的行为与使用“编辑计划”对话框所创建的报表类似，请将告警**条件**设置为**始终**。

这可以确保 Splunk Enterprise 在每次运行报表时都执行您所定义的告警操作。

7. 将告警模式设置为**每次搜索一次**。

无需为计划报表激活**限制**，对于计划报表，**过期时间**和**严重性**设置也并不重要。

8. （可选）为计划报表设置所需的告警操作。

请参阅本主题中的[“为您的计划报表定义操作”](#)。

切勿为计划的实时报表定义告警操作。请参阅本主题中的[“为仪表板创建实时的计划报表”](#)。

9. （可选）通过**摘要索引**设置后启用摘要索引。

仅当您打算为此计划的报表填入摘要索引时才需要此设置。请参阅[“启用摘要索引”](#)。

10. 单击**保存**以保存更改。

为仪表板创建实时的计划报表

当您为仪表板面板使用非计划的实时搜索时，每次用户加载仪表板时会重新启动它们。这会导致出现实时搜索的并发搜索限制达到极限的情况。

在“设置”中，您可以创建实时计划报表--计划为“始终”告警的实时报表--无告警操作。这种类型的计划报表可用于备份保存的搜索仪表板面板。这会设置一个由不断运行的单个实时搜索备份的仪表板面板，即使在多个用户同时查看仪表板的时候。

如果您想要使用计划实时报表备份仪表板面板，则面板必须按名称引用报表。

如果您向计划实时报表添加一个告警操作，则它会变成一个告警。如果实时搜索在短时间内收到大量的结果，您可能需要向告警添加限制规则。请参阅《告警手册》中的“告警入门”。

启用摘要索引

摘要索引是您可以通过**设置 > 搜索、报表和告警**为任何计划的报表配置的操作。对较长时间跨度内的大量数据执行分析/报告时，如果多个用户定期运行相似的报表，这通常会相当耗时并会导致性能大幅降低，此时可以利用摘要索引。

通过摘要索引，您的计划的报表可以基于为涵盖某一时间段的事件计算足够统计数据（摘要）的报表。此报表会设置为每次按计划运行时，其结果都将保存到您指定的摘要索引中。之后，您就可以根据这一较小（因此速度也会较快）的摘要索引运行报表，而不必使用来自摘要索引接收其事件的相对较大的数据集。

注意：您不必将摘要索引用于已经利用了报表加速的报表。有关更多信息以及对运行速度较慢的报表进行加速的这两种方法的区别，请参阅《知识管理器》手册中的“关于报表加速和摘要索引”。

要设置计划报表的摘要索引：

1. 导航到**设置 > 搜索、报表和告警**。

2. 打开将填充摘要索引的报表的详细信息页面。

3. 单击**摘要索引**下的**启用**。

要使摘要索引定期收集数据，该报表的**告警条件**必须为**始终**。

4. 单击**保存**以保存更改。

注意：注意正确构建用来填充摘要索引的搜索。在多数情况下，应使用特殊的转换命令。请在阅读并理解《知识管理器》手册中的“使用摘要索引提高报表效率”后，再尝试设置摘要索引。

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**的写入访问权限（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 Splunk Enterprise 实现的其他用户可用，无论在应用还是全局级别。请参阅本手册中的[“设置报表权限”](#)。

有关管理 Splunk Enterprise 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 Splunk Enterprise 实现的设置方式，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 Enterprise 的搜索计划程序将确保在收集数据的时间段内，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特定的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（视您的需要而定）。

您可以通过编辑 `savedsearches.conf` 来配置计划报表的优先级。有关此功能的更多信息，请参阅本手册中的[“配置计划报表的优先级”](#)。

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。嵌入的报表可以事件视图、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。

注意：在计划报表定期运行前，您不可嵌入该报表。嵌入的报表始终显示最后计划运行的结果。因此，如果某个嵌入的报表设置为在过去 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，新嵌入的报表在首次计划运行前为空。

嵌入的报表不具备 Splunk Web 中所查看的报表的所有功能。例如，嵌入的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。嵌入的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：新嵌入的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中。
- 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。

如果使用搜索头集群化，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）。这会硬编码路径，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`。

更改嵌入的报表之下的页脚

默认情况下，嵌入的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，在报表的计划时间段中运行它们。
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	报表加速和数据模型加速 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创建或更新摘要。 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中断的情况。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后用的，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，摘要索引是不可靠的。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 的下一次运行排定在下午 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	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	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	是。

优先级分数	计划频繁的报表降低地更多。	允许它在强制它跳过运行的报表之前运行。	
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。

将计划窗口手动分配给问题报表

如果在应用了默认报表计划程序规则之后仍然存在跳过计划报表的问题，您可以为不需要在计划开始时间运行的计划报表提供若干个计划窗口。当您计划一个报表时，可通过在**计划窗口**字段中输入一个数字值来执行此操作。

窗口的宽度以分钟为单位进行定义。它可以是从 0 到 44,640（一个月 31 天对应的分钟数）中的任意数字。

当报表计划要运行时，计划窗口将打开。报表会在该窗口内的任意时间运行。报表计划程序将窗口时间范围添加到计划报表的优先级分数上，使其优先级分数暂时变得更差。这给予其他报表一个机会，使其能优先于具有计划窗口的报表运行。

随着时间的推移和窗口变窄，计划报表的优先级分数会降低，在窗口关闭之前给予其运行的机会。在报表的下次计划运行时，会重复该事件序列。

请参阅本手册中的[“计划报表”](#)。

管理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。

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“创建计划的搜索”对话框。单击**创建**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，您可以设置以 PDF 形式呈现的搜索结果的单个电子邮件交付。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。

发送带告警电子邮件的 PDF

您可以设计告警，该告警在触发后会发送带 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。

在 PDF 中启用非拉丁字体

Splunk 软件预打包有一系列拉丁字体和一组 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，请创建 `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` 中更改文件名称以便先使用 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 `` 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 下列信息的令牌。

Token	受支持的值	描述
\$type\$	<ul style="list-style-type: none"> • dashboard • report • alert 	该 PDF 的知识对象类型
\$app\$	app_id	应用文件夹名称，如 <code>search</code>
\$owner\$	owner	正计划 PDF 的用户
\$name\$	仪表板、报表或告警的 ID	使用 ID 而非标签
\$time\$	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

支持的操作系统：

- Solaris（仅 x86，不是 SPARC）
- Linux Kernel 2.6.x 和更高版本
- Windows Server 2003/2003 R2（64 位），2008/2008 R2（64 位）
- Windows Vista（64 位），XP，7（64 位）
- Intel Macs 上的 Mac OS X 10.5 和 10.6

所有支持 Splunk Web 的浏览器都支持集成的 PDF 生成。然而，如果您使用 Internet Explorer，则在您还安装了 Adobe Acrobat 的情况下将较少遇到问题。

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。