Splunk® Enterprise 8.2.0

告警手册

生成时间：2021 年 5 月 24 日，14:15

Table of Contents

告警概述

告警入门

使用告警以监视和响应特定事件。告警使用保存的搜索来实时或按计划查找事件。当搜索结果符合特定条件时会触发告警。在告警触发后，您可以使用告警操作来响应。

此资源包含使用告警和告警操作的信息、说明和场景。要开始了解告警的相关信息，请参阅“告警工作流”。查看告警类型中的告警选项。

告警工作流

告警将保存的搜索、类型和触发条件的配置以及告警操作结合起来。如下将详细介绍告警的各个部分是如何协作。

搜索：您想要跟踪什么？

您可以为想要跟踪的事件启动一个搜索。将此搜索保存为告警。

告警类型：您想以怎样的频率检查事件？

告警使用保存的搜索来检查事件。调整告警类型以配置搜索的运行频率。使用计划告警定期检查事件。您也可以使用实时告警持续监视事件。

告警触发条件和限制：您想以怎样的频率触发告警？

不一定必须在每次产生搜索结果时即触发告警。设置触发条件来管理告警触发的时间。您也可以限制告警，以控制在最初的告警产生后最快可以何时产生下一个告警。

告警操作：告警触发后会怎样？

当触发告警时，它可以初始化一个或多个告警操作。告警操作会将所触发的告警通知您，并协助您响应告警。您可以配置告警操作频率和类型。

选择告警类型

告警类型

有两种告警类型：计划和实时。告警类型的定义是基于告警搜索时间。您可以为任意告警类型配置时间、触发和其他行为，具体取决于实际场景。

告警类型对比

下面列出了计划和实时告警的对比信息。

告警类型	搜索事件的时间	触发选项	限制选项
计划	按计划进行的搜索。从现有时间选项中选择，或使用 cron 表达式定义搜索的执行计划。	指定根据结果或结果字段计数触发告警的条件。当一组搜索结果符合触发条件时，会触发告警一次或每个结果触发一次。	指定抑制的时间周期。
实时	持续搜索。	**按结果**：每次产生搜索结果都触发。	指定抑制的时间周期和可选字段值。
实时	持续搜索。	**滚动时间窗**：根据滚动时间窗口内的结果或结果字段计数，指定触发告警的条件。例如，当 5 分钟的时间窗内产生的结果超过 10 个时，即触发实时告警。	指定抑制的时间周期。

告警类型和触发场景

在选择了计划或实时告警后，您即可以配置结果触发告警的方式。您可能需要配置每个结果都会触发的实时告警，或只有在结果符合特定条件时才会触发的计划告警，具体取决于您所监视的事件。以下场景说明了告警类型和触发的不同使用案例。

计划的告警

采用计划告警来定期搜索事件，并监视他们是否满足特定条件。计划告警适用于立即或实时监视并非优先事项的场景。

场景

- 一个网络零售商的日目标是实现 500 个销售业绩。此零售商的管理员新建了一个计划告警来监视销售业绩。该管理员设定此告警于每天 23:00 搜索销售事件。她进行了告警配置，在搜索结果数低于 500 时触发告警。
- 管理员想监视用户点击链接失败并产生 404 错误页面的频率。该管理员新建了一个计划告警，每小时搜索 404 错误并在搜索结果数超过 100 时触发告警。
- 管理员新建了一个计划告警，检查在过去的几小时中是否有哪个特定主机未发送数据到 Splunk 平台。他设定此告警每三小时对主机的事件进行搜索。该管理员配置此告警在没有搜索结果时触发。

实时告警

实时告警持续搜索事件。他们适用于要求立即监视和响应的场景。您可以使用每个结果都会触发一次的实时告警，或只有在指定滚动时间窗内满足特定条件时才会触发的实时告警。

按结果触发

按结果触发的实时告警有时也称为“按结果告警”。使用这种告警类型和触发条件来持续搜索事件，并在事件发生时接收通知。

> **警告：**在高可用性部署中，必须小心使用按结果触发。如果对等节点不可用，则实时搜索不会警告搜索可能不完整。建议在这种部署中使用计划告警。

场景

以下为使用按结果触发的实时告警示例。

- 一个社交网站的管理员想时时了解登录失败的情况。她设置了一个实时告警来搜索失败的登录操作。她选择了按结果触发的条件以便能跟踪每一个失败的登录操作。
- 管理员想实时监视一组主机的错误。有些错误需要的响应较之其他错误更为迫切。该管理员设置了一个按结果触发的实时告警。他使用了一个字段来限制此告警。此字段指定了迫切性较低的错误码和一个小时的抑制时间周期。每个迫切性较高的错误都会触发此告警，但迫切性较低的错误一小时内最多只能触发此告警一次。

滚动时间窗触发

按滚动时间窗口触发的实时告警有时也称为“滚动窗口告警”。这种告警类型和触发条件适用于特定时间窗对于您实时监视的事件模式来说非常重要的场景。

场景

以下为使用按滚动时间窗触发的实时告警示例。

- 管理员希望在用户于十分钟的时间周期内发生三次登录失败时即产生通知。该管理员设了一个实时告警来搜索登录失败并配置了一个十分钟的滚动时间窗。该管理员限制了此告警，使其对于同一用户一小时内的登录失败只触发一次。
- 管理员想了解 Web 应用程序在一分钟内发生的数据库连接错误超过五个的情况。她配置了一个实时告警来搜索错误事件，并指定了一个一分钟的滚动时间窗口。如果搜索先返回一个结果，五分钟后再返回四个结果，这不会触发告警。但是，如果搜索在一分钟的时间跨度内返回五个结果，则会触发告警。

其他资源

请参阅“限制告警以查看更多限制情况”。

新建告警

新建计划的告警

新建计划告警定期搜索事件。您可以通过配置计划、触发条件和限制来自定义告警。

要对比计划和实时告警，请参阅“告警类型”。要查看告警类型和触发的情况，请参阅“告警类型和触发情况”。

使用 cron 表达式

您可以用 cron 表达式来自定义告警计划。请参阅“使用 cron 表达式进行计划”以了解更多信息。

新建计划告警

前提条件

- 使用 cron 表达式进行计划
- 告警计划提示
- 配置告警触发条件
- 监视触发的告警

步骤

1. 导航到**搜索和报表**应用中的**搜索**页面。
2. 新建一个搜索。
3. 选择**另存为 > 告警**。
4. 输入标题和描述（可选）。
5. 指定权限。
6. 配置告警计划。告警计划有两个选项。

选项	此选项的后续步骤
从可用计划选项中选择一个选项并设置时间。	无。
若需进一步自定义告警，选择**运行 Cron 计划**以使用时间范围和 cron 表达式。	1. 为每个搜索时间范围输入**最早**和**最晚**值。这些值会覆盖原来的搜索时间范围。要避免出现重叠或间隙，执行计划应该与搜索时间范围保持一致。例如，要每 20 分钟运行一次搜索，搜索时间范围也应设置为 20 分钟（-20m）。 2. 输入 cron 表达式来计划此搜索。请参阅以下的 cron 表达式示例：使用 cron 表达式进行计划。

7. （可选）更改**失效**设置。此设置控制触发的告警记录（显示在**触发的告警**页面中）的寿命。
8. 配置触发条件。
9. （可选）配置触发限制时长。
10. 选择在告警触发时应执行的一个或多个告警操作。
11. 单击**保存**。

其他资源

- 查看告警计划提示中的计划告警的最佳实践。
- 另请参阅“告警示例”。

使用 cron 表达式进行告警计划

您可以使用时间范围和 cron 表达式自定义告警计划。Splunk cron 分析器默认采用配置搜索头时所用的时区。您可以转到**设置 > 搜索、报表和告警 > 计划时间**来确认或更改此设置。

Cron 表达式语法

Cron 表达式是由空格分隔的五个字段的数据字符串。

从左到右，五个 cron 字段有以下按时间顺序排序的值范围：

- 分钟：0-59
- 小时：0-23
- 日期：1-31
- 月份：1-12
- 星期：0 - 6（0 表示周日）。

通常使用的 cron 字段格式

以下 cron 字段格式适用于大多数使用案例。

格式	描述	描述性说明	小时字段示例	示例含义
N	一个值	仅限此值	9	9:00
N,M	多个以逗号分隔的值	仅限列出的值	9,15	上午 9:00 和 下午 3:00
I-J	值范围（含起止值）	此范围内的所有值，包括范围起止值	9-17	上午 9:00 到下午 5:00
*	星号（表示“所有值”）	此字段中的每个值	*	每个小时
*/N	此字段中的每个 N 值	此字段的所有值都以 N 为间隔	*/3	每 3 小时 0, 3, 6, 9, 12, 15, 18, 21

适用于范围和间隔的 cron 字段格式

一些情况中，您可能想要使用多个值范围或在 cron 表达式中将范围和间隔组合起来。以下格式选项可用。

格式	描述	含义	小时字段示例	示例含义
I-J,K-L	多个以逗号分隔的值范围	这些范围内的所有值，包括范围起止值。	例如：9-12,15-17 会显示为 * 9-12,15-17 * * *	从上午 9:00 到中午 12:00 和 下午 3:00 到下午 5:00，每分钟都会发出一次告警。
I-J/N	范围及 /N 间隔	此字段中以 /N 为间隔且在此范围内的每个值	例如： N=2 9-12/2 这会显示为 * 9-12/2 * * *	从上午 9:00 到中午 12:00，每第二个小时过后每分钟都会发出一次告警
I-J/N,K-L/N	多个以逗号分隔的范围和以 /N 为间隔	此字段中以 /N 为间隔且在指定范围内的每个值	例如： N = 1 9-12/1,15-17/1 这会显示为 * 9-12/1,15-17/1 * * *	从上午 9:00 到中午 12:00 和下午 3:00 到下午 5:00 的每小时中，每一分钟都会发出一次告警。

使用 cron 间隔

在具有 /N 间隔的 cron 表达式中，将使用指定范围内以 N 为间隔的所有值。如果范围内的某个数不是 N 的整数倍，值将重置为 0。

例如，*/9 * * * * 表示在一小时内从 0 分开始的“每九分钟”。使用以下分钟字段值：

9, 18, 27, 36, 45, 54

54 之后，值重置为 0。

此语法并非与每个系统都兼容

Cron 值范围和间隔
使用 I-J/N 范围和间隔格式时，间隔 N 将应用于范围内的第一个字段。

例如，分钟字段中的 13-36/10 产生以下所用值：

13, 23, 33

表达式示例

以下为 cron 表达式的一些示例。

```
5 9 * * *       At 9:05 every day.
30 * * * *      At minute 30 of every hour. For example, if you set this CRON job at 11:02, your job will begin running at
11:30,
```

```
                    12:30, 1:30, etc...
* 1 * * *          Every first minute after hour 1. For example: 1:01, 1:02,...,23:59.
0 12 * * *       At 12 PM every day, on the hour.
*/20 * * * 1-5    At every 20 minutes of every hour, beginning at minute zero, Monday through Friday. For example: 11:20,
11:40, 12:00...
0 9 1-7 * *     The first 7 days of every month at 9 AM.
```

告警计划提示

本主题介绍了使用计划告警的最佳实践和建议。

最佳实践

协调告警计划与搜索时间范围

协调告警计划与搜索时间范围可以防止搜索对事件数据评估两次的情况发生。如果搜索时间范围超出搜索计划，则会导致事件数据集重叠。

当搜索时间范围小于计划告警的时间范围时，可能会导致事件一直未被评估。

将告警计划为具有至少一分钟的延迟

对于事件数据可能不会立即到达索引器的分布式搜索部署场景，这种做法很重要。延迟后可以确保您将所有事件都计算在内，而不是仅计算最先建立索引的事件。

最佳实践示例

此示例显示如何配置为搜索计划设置了 30 分钟延迟的告警。搜索时间范围和告警计划的跨度均为一小时，因此不会存在事件数据重叠或间隙。

1. 从“搜索页面”，新建搜索并选择**另存为 > 告警**。
2. 在**另存为告警**对话框中，指定以下选项。
   - **标题**：告警示例（30 分钟延迟）
   - **告警类型**：计划
   - **时间范围**：运行 Cron 计划
   - **最早**：-90m
   - **最晚**：-30m
   - **Cron 表达式**：30 * * * *
3. 继续为告警定义操作。

最早和**最晚**值将搜索时间范围定义为从搜索启动之前的 90 分钟到搜索启动之前的 30 分钟。告警在半点运行且每小时运行一次。它以一小时为时间周期收集事件数据。当计划的搜索在指定时间（如下午 3:30）开始时，它将收集从下午 2:00 到下午 3:00 之间建立索引的事件数据。

管理并发计划搜索的优先级

根据部署情况，可能每次只能运行一个计划搜索。在这种情况下，即使您计划同时运行多个搜索，搜索计划程序仍会确保计划搜索依次运行。

您可能需要修改计划搜索的优先级，以确保搜索获得的是当前数据或防止数据收集中出现间隙。如果有 Splunk Enterprise，则可以通过编辑 `savedsearches.conf` 配置文件配置计划搜索的优先级。更多相关信息，请参阅*报表手册*中的“配置计划的报表优先级”。

计划报表和告警的差异

计划报表在某些方面有点像计划或实时告警。您可以计划一个报表，并设置一个操作在每次计划报表运行的时候运行。

但是，因为计划报表的操作会在每次运行报表的时候运行，所以计划报表不同于告警。报表操作不会依赖于触发条件。

例如，您可以使用每小时运行一次的搜索来监控酒店客人的入住事件。以下是计划报表与使用电子邮件通知操作的计划告警之间的不同之处。

- **计划报表**：在每次完成报表的时候，即使没有显示入住事件的搜索结果，仍然会运行其操作并发送电子邮件。在这种情况下，您每个小时都会收到电子邮件通知。

- **计划告警**：只有被显示一个或多个入住事件的搜索结果触发的时候，才会运行告警操作。在这种情况下，只有当结果触发告警操作的时候，您才会收到电子邮件通知。

有关更多信息，请参阅*报表手册*中的“计划报表”。

新建实时告警

使用实时告警在事件发生时监视事件或事件模式。您可以新建按结果触发或按滚动时间窗触发的实时告警。从计算资源方面来看，实时告警的成本可能较高，因此应尽量使用计划告警。

要对比计划和实时告警，请参阅“告警类型”。要查看告警类型和触发的情况，请参阅“告警类型和触发情况”。

新建按结果触发的实时告警

按结果触发的实时告警有时也称为“按结果告警”。这种告警类型和触发条件使用持续的实时搜索来查找事件。每个搜索结果都会触发告警。

> **警告：**如果您拥有 Splunk Enterprise 高可用性部署，请小心使用按结果触发。如果对等节点不可用，则实时搜索不会警告搜索可能不完整。若要避免此问题，请使用计划的告警

按以下步骤来新建按结果触发的实时告警。

1. 导航到**搜索和报表**应用中的搜索页面。
2. 新建一个搜索。
3. 选择**另存为** > **告警**。
4. 输入标题和描述（可选）。
5. 指定权限。
6. 选择**实时**告警类型。
7. （可选）更改**失效**设置。此设置控制触发的告警记录（显示在触发的告警页面中）的寿命。
8. 选择**按结果**触发选项。
9. （可选）配置触发限制时长。
10. 至少选择一个在告警触发时执行的告警操作。
11. 单击**保存**。

新建按滚动窗口触发的实时告警

按滚动时间窗口触发的实时告警有时也称为“滚动窗口告警”。滚动时间窗为一个时间间隔或递增值，如 5 分钟，而不是一个计划的时间。由于实时告警持续进行搜索，为事件设定的时间窗也会向前滚动。

当特定时间窗对于您实时监视的事件模式来说非常重要时，使用这种告警类型和触发条件。这种告警类型和触发条件对资源的需求最高。可能时，可考虑使用另一种告警类型。

按以下步骤来新建按滚动窗口触发的实时告警。

1. 导航到**搜索和报表**应用中的搜索页面。
2. 新建一个搜索。
3. 选择**另存为** > **告警**。
4. 输入标题和描述（可选）。
5. 指定权限。
6. 选择**实时**告警类型。
7. （可选）更改**失效**设置。此设置控制触发的告警记录（显示在触发的告警页面中）的寿命。
8. 从基于结果的可用条件中选择一个条件，或输入自定义的触发条件。不要选择按结果触发。
9. 指定一个时间间隔并添加到触发条件中。
10. （可选）配置触发限制时长。
11. 至少选择一个在告警触发时执行的告警操作。
12. 单击**保存**。

其他资源

- 查看“告警权限”以了解告警和告警操作权限的相关信息。
- 按照告警示例中的各个告警示例尝试一下。
- 查看“配置告警触发条件”以了解使用触发条件的相关信息。
- 了解“触发的告警”页面以查看“监视触发的告警”中的触发的告警记录

管理告警触发条件和限制

配置告警触发条件

告警可以按计划或实时搜索事件，但不必每次产生搜索结果时即触发告警。触发条件有助于您监视事件数据的模式或优先处理特定事件。

告警触发和告警限制
限制告警与配置触发条件不同。若已新建触发条件，则会对搜索结果进行评估，判断其是否符合这些条件。如果结果符合触发条件，告警限制会控制是否将触发抑制一段时间。有关限制的更多信息，请参阅“限制告警”。

触发配置工作流

在配置告警触发时，思考以下问题会有所帮助。

告警监视的事件模式是什么？
触发条件评估特定模式的告警搜索结果。此模式将结果字段及其行为结合起来。例如，您可以选择其中一个内置字段计数选项，如**主机数**，以便重点关注 `host` 字段。随后您可以指定要监视的行为，如当该数字下降了 5 的时候。您也可以输入自定义的触发条件。

模式会触发告警一次还是每个结果都会触发？
当出现该事件模式时，告警仅会触发一次或是模式中的每个结果都会触发一次。您可以根据通知或其他所需的告警操作行为来选择一个选项。

告警类型和触发选项

两种告警类型都提供与告警搜索结果协作的触发配置选项。下面是每种类型的可用触发选项对比。

告警类型	触发选项	指定触发条件	匹配的结果触发告警的方式
计划	添加触发条件以对搜索结果进行评估。	内置结果和字段计数选项或自定义触发条件	所有搜索结果每次匹配特定条件时即触发告警一次，或每个匹配的结果都触发一次。
实时	按结果	N/A	默认情况下，每个匹配的结果都会触发一次告警。
实时	包含滚动时间窗的触发条件。	内置结果和字段计数选项或自定义条件。也会指定一个滚动时间窗或间隔。	所有搜索结果每次匹配特定条件时即触发告警一次，或每个匹配的结果都触发一次。

搜索和触发条件的协作方式

触发条件作为辅助搜索用于评估告警的初始搜索结果。如果辅助搜索未返回结果，则不会触发告警。只有当辅助搜索产生结果时，才会触发告警。

取决于所选择的告警操作，您可以访问有关可触发告警的结果的信息。触发条件的辅助搜索不会判断哪些信息可用于通知或其他告警操作。结果字段和其他信息来自于初始基本搜索。

使用不带触发条件的告警基本搜索可以限制可用于通知的信息。以下示例将使用带自定义触发条件的基本搜索和使用不带触发条件的基本搜索这两种情况进行了对比。

示例

紧急 `log_level` 事件数量达到 10 个以上时将触发该计划告警。当告警触发时，它会发送带有搜索结果的电子邮件。

使用带自定义触发条件的搜索

告警使用此搜索，且时间范围挑选器中的**过去 7 天**已勾选。

```
index=_internal (log_level=ERROR OR log_level=FATAL OR log_level=CRITICAL) | stats count by log_level
```

添加了以下自定义触发条件。

```
search count > 10
```

在此场景中，最初的搜索结果包含了所有日志级别的详细计数，但只有当 log_level 计数大于 10 时才会触发告警。这意味着，所有 log_level 计数都可用作告警通知的组成部分。

使用不带触发条件的搜索

以下搜索看起来与前一示例类似。它产生类似的告警触发行为。但是，它会新建不同的结果，并限制 log_level 信息对通知和其他告警操作的可用性。

```
log_level=ERROR OR log_level=FATAL OR log_level=CRITICAL) | stats count by log_level | search count > 10
```

在这种情况下，搜索结果仅包含大于 10 的 log_level 值。通过对比可知，前一示例中使用带触发条件的搜索意味着其结果会包含所有 log level 字段的计数。

没有告警事件时使用搜索触发

如果您希望在没有事件触发告警时得到通知，可以使用以下搜索或类似搜索做到这一点：

```
<your search for events for this data> earliest=0 latest=now | stats count
```

将此搜索保存为告警时，将其设置为在 count=0 或 count < 0 时触发。

限制告警

使用限制来将告警触发抑制一段时间。类似的搜索结果或计划可能会导致告警的频繁触发。

限制告警与配置告警触发条件不同。触发条件评估告警的初始搜索结果，以检查特定字段计数、事件时间或其他模式。要查看告警触发信息，请参阅“配置告警触发条件”。

限制配置

新建或编辑告警之后，您可以启用并配置告警限制，也称为抑制。

告警类型	触发选项	如何配置限制
计划	一次	用时间值字段和下拉递增值表示抑制时间周期。时间值必须大于 0。
计划	按结果	1. 键入一个或多个以逗号分隔的字段来检查事件匹配值。抑制这些字段中具有相同值的事件。 作为示例，您可在字段 product_category 和字段 best_sellers 上配置抑制。在对 product_category 字段**和** best_sellers 都具有值 arcade 的位置上的事件发出告警之后，将在限制期间抑制 product_category 和 best_sellers 字段中具有值 arcade 的后续事件。 2. 用时间值字段和下拉递增值表示抑制时间周期。时间值必须大于 0。
实时	滚动时间窗	用时间值字段和下拉递增值表示抑制时间周期。时间值必须大于 0。
实时	按结果	1. 键入一个或多个以逗号分隔的字段来检查事件匹配值。抑制这些字段中具有相同值的事件。 作为示例，您可以对 product_category 字段配置抑制。product_category 值为 arcade 的一个事件上发出告警之后，将在限制期间抑制 product_category 字段值为 arcade 的后续事件。 2. 用时间值字段和下拉递增值表示抑制时间周期。时间值必须大于 0。

如果为现有的告警操作设置限制，编辑警报的详细信息会导致限制被忽略。警报更改会导致删除限制文件，该文件记录忽略事件的时间。因此，在触发下一个事件之前，不会进行限制。

限制场景

- 管理员用按结果触发的实时告警来监视系统事件，包括错误。系统事件每分钟会发生 20 次或以上。考虑到通知的产生，

可以将告警触发抑制一小时。该管理员使用字段值和一小时的抑制时间周期来限制事件。

- 按结果触发的实时告警监视磁盘错误。告警搜索结果中的部分事件具有相同的 `clientip` 或 `host` 值，但可能会在短时间内触发多个告警。管理员限制了告警，以便在触发最初告警后将后续的触发抑制 10 分钟。
- 计划告警每小时搜索一次销售事件。当结果数增加了 100 时会触发告警，且根据配置会发送一封电子邮件通知给销售团队。销售团队想限制电子邮件通知。管理员限制了告警，以便在最初告警触发后抑制触发三个小时，并初始化电子邮件通知。

如果您有一组运行于相似数据集上的告警，则它们可以同时对相同数据分别发出告警。这意味着即使您为所有告警设置了限制规则，它们总的通知频率仍然可能很高。您可以为这些告警创建抑制组，以便当其中一个告警发出时，整个告警组都会受到抑制。

请参阅“定义告警抑制组以限制类似告警的设置”。

限制计划的搜索和实时搜索

限制告警与限制计划和实时搜索的原理类似。

如果您有频繁运行的计划的搜索且您不希望每次生成结果时都收到通知，设置限制控制以将告警抑制到更长时间。

对于实时搜索，如果您将告警配置为满足特定触发条件时触发一次，则您无需配置限制。如果每个结果都会触发告警，您可能需要配置限制，以抑制其他告警。

在为实时搜索配置限制时，从采用与基本搜索时间范围长度匹配的限制时长开始。在必要时扩展此限制时长。这可以防止您收到给定事件的多个通知。

定义告警抑制组以限制类似告警的设置

如果您的组织依赖大量告警，则可能会发现您有运行在相同或非常相似的数据集上的类似告警集合。这可能导致以下情况：同一组数据频繁触发多个告警，即使您为每个告警设置了限制规则，也会导致很高频率的通知。

为管理这种情况，您可以将这类告警组合成一个大型告警并对其应用限制规则。这种方法可以降低告警通知的频率。但与被替换的那些告警相比，这个组合告警的搜索性能也可能较差。

相反，您可以为这些告警集设置告警抑制组。如果一组告警属于同一个抑制组，则当其中一个告警进入某个触发的告警的抑制期时，所有告警都会受到限制。该触发的告警会执行其告警操作（如果有）。该组中的其他告警不会执行其告警操作。

例如：您有一个包含五个告警的告警抑制组。其中每一个告警都有不同的抑制周期和不同的告警操作。如果组内某个告警进入为期 5 分钟的告警抑制期，并且触发了电子邮件告警操作，则该组中的所有告警都将被抑制 5 分钟。然而，唯有一种告警操作会发生：触发告警的电子邮件。

属于不同用户的告警不能包含在同一抑制组中。

告警抑制组的最佳做法

当告警抑制组由具有相同告警抑制周期和告警操作集的告警组成时，其性能最佳。如果他们使用抑制字段，则应该共用同一组告警抑制字段。告警属性的这种共用有助于确保行为可预测。您知道，只要触发了该组的某个告警，其余告警就会进入相同时长的抑制期，会执行的操作也始终相同，并且当一个告警被触发时，所有告警都会被触发。

当抑制组中的告警具有不同的抑制字段集时，您可能会发现，该组中的多个告警是由不同的数据集触发的。

创建一个抑制组

前提条件

- 阅读“配置告警触发条件”。
- 阅读“限制告警”以了解如何为单个告警设置告警限制。

步骤

1. 选择**设置** > **搜索、报表和告警**，前往“搜索、报表和告警”列表页面。
2. 找到要添加到告警抑制组的告警，然后选择**编辑** > **高级编辑**。
   类型列指示列表中哪些已保存的搜索被配置为告警。选择会利用限制来抑制频繁告警通知的告警。
3. 在告警的“高级编辑”页面上，找到 `alert.suppress.group_name` 字段，然后输入此告警所属的抑制组的名称。单击**保存**。
4. 对第一个告警所属抑制组中的所有其他告警重复步骤 2-3。

配置告警操作

设置告警操作

告警操作有助于您响应触发的告警。可启用一个或多个告警操作。了解可用选项的相关信息。

如欲了解	请参阅
当告警触发时，发送电子邮件通知	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
将触发的告警或计划报表的结果写入 CSV 查找文件	将结果输出到 CSV 查找
为可搜索的告警事件建立日志和索引	日志事件
在最近触发的告警列表中添加一个告警，以进行监视	监视触发的告警

已弃用脚本告警操作。您还可以定义可以包括脚本的自定义操作。

请参阅“关于自定义告警操作”。

电子邮件通知操作

当告警触发时，向指定收件人发送一封电子邮件通知。电子邮件通知可以包括来自搜索结果、搜索任务和告警触发的信息。您可以通过**搜索**页面、**告警**页面或直接在搜索命令中设置电子邮件通知操作。

除了提供告警之外，电子邮件通知中还可以包含其他内容。有关报表的电子邮件通知信息，请参阅*报表手册*中的“计划报表”。有关仪表板 PDF 电子邮件交付的信息，请参阅*仪表板和可视化*中的“生成仪表板 PDF”。

为 Splunk 实例配置电子邮件通知

在您可以设计电子邮件通知操作之前，必须为 Splunk 实现配置电子邮件通知设置。

如果您已配置了电子邮件通知设置，可以跳过此任务。

前提条件

PDF 交付需要额外的用户角色配置。请参阅“配置用户角色以实现 PDF 交付”。

Splunk Cloud 中的步骤

1. 从**搜索和报表**应用的主页，选择**设置** > **服务器设置** > **电子邮件设置**。
2. 在**邮件服务器设置**部分中选择一个可用的**电子邮件安全**选项。
   邮件主机默认为 **localhost**。该值由您的 Splunk Cloud 实施管理员设置，不可编辑。
3. （可选）指定一个逗号分隔的允许的**电子邮件域**列表。不要在此列表中的项目之间输入回车（新行）。此设置将电子邮件域限制为告警邮件可以发送的网域。将该字段留空则表示无域限制。

   如果您在**电子邮件域**中输入了值，则用户无法通过“高级编辑”页面中的 **action.email.mailserver** 设置为单个保存的搜索设置邮件服务器。Splunk 软件将改用**电子邮件设置**页面中的**邮件主机**。在**设置**的“搜索、报表和告警”页面中，用户可以针对某个搜索选择**编辑** > **高级编辑**，从而进入“高级编辑”。

4. 指定**电子邮件格式**设置。

电子邮件格式设置	定义
电子邮件页脚	所有邮件的页脚。使用文本和/或标记。

   链接主机名是传出结果 URL 的主机名。该值由您的 Splunk Cloud 实施管理员设置，不可编辑。

5. 单击**保存**。

Splunk Enterprise 中的步骤

1. 从**搜索和报表**应用的主页，选择**设置** > **服务器设置** > **电子邮件设置**。
2. 指定以下**邮件服务器设置**值。

设置	定义
邮件主机	默认值为 `localhost`。
电子邮件安全	从可用选项中选择一个。
用户名	（可选）SMTP 服务器验证需要用户名。
密码	（可选）SMTP 服务器验证需要密码。如果您有输入密码，则必须在**确认密码**中再次输入。

3. （可选）指定一个逗号分隔的允许的**电子邮件域**列表。此设置将电子邮件域限制为告警邮件可以发送的网域。将该字段留空则表示无域限制。

   如果您在**电子邮件域**中输入了值，则用户无法通过“高级编辑”页面中的 `action.email.mailserver` 设置为单个保存的搜索设置邮件服务器。Splunk 软件将改用**电子邮件设置**页面中的**邮件主机**。在**设置**的“搜索、报表和告警”页面中，用户可以针对某个搜索选择**编辑** > **高级编辑**，从而进入“高级编辑”页面。

4. 指定**电子邮件格式**设置。

电子邮件格式设置	定义
链接主机名	传出结果 URL 的主机名。用方括号括起的 IPv6 地址。示例：`[2001:db8:0:1]`
电子邮件发件人	（可选）指定用于电子邮件标头字段**发件人**里的发件人身份。使用电子邮件地址或字符串。字符串不能包含空格。在字符串后连接 `@<hostname>`，使用电子邮件通知发送机器的主机名称（在 alert_actions.conf 中指定）；如果未指定主机名称，则使用 `@localhost`。如果未指定主机名称，默认为 `splunk@<hostname>` 或 `splunk@localhost`。
电子邮件页脚	所有邮件的页脚。使用文本和/或标记。

5. 单击**保存**。

为告警或计划报表定义电子邮件通知操作

前提条件

- 在**电子邮件设置**页面中配置电子邮件通知设置。请参阅“为 Splunk 实例配置电子邮件通知”
  - （可选）将电子邮件通知限制为一组特定的电子邮件域。如果在**允许的域**字段中列出了电子邮件域，则电子邮件通知只能发送给使用这些域的收件人。
  - 定义电子邮件页脚和 PDF 格式。
- 有些电子邮件通知功能需要特定的角色和功能。有关角色和功能的更多信息，请参阅*《确保 Splunk 平台安全》*手册中的“关于使用功能定义角色”。
  - 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，您必须拥有 `admin` 角色。
  - 要在搜索中向不需要 SMTP 验证的邮件服务器发送电子邮件通知，您的角色必须拥有 `list_settings` 功能。默认情况下，只有 `admin`、`splunk-system-role` 和 `can_delete` 角色拥有 `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` 和 `schedule_search` 功能。
- PDF 交付需要额外的用户角色配置。请参阅“配置用户角色以实现 PDF 交付”。
- 有关标记使用的更多信息，请参阅“在电子邮件通知中使用标记”。

步骤

1. 当您新建告警、为现有告警编辑操作、定义或编辑报表计划时，可以配置电子邮件通知操作。选用下面其中一个选项。

选项	步骤
新建告警	从**搜索和报表**应用中的**搜索**页面，选择**另存为** > **告警**。输入告警详细信息，并根据需要配置触发和限制。
编辑已有告警	从**搜索和报表**应用中的**告警**页面，为现有告警选择**编辑** > **编辑操作**。
定义或编辑报表计划	从**搜索和报表**应用中的**报表**页面，为报表选择**编辑** > **编辑计划**。

2. 单击**添加操作**并选择**发送电子邮件**。
3. 键入用逗号分隔的电子邮件**收件人**列表。
4. （可选）单击**显示抄送和密送**以键入以逗号分隔的抄送和密送电子邮件收件人列表。

5. （可选）设置电子邮件**优先级**。电子邮件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**。
   您可选择性地在主题和消息文本中使用标记。
7. （可选）选择一个或多个下列选项，以在邮件中包含内容。

选项	添加到电子邮件
告警链接或**报表链接**	与电子邮件关联的告警连接或报表链接。
结果链接	相关搜索任务的结果链接。
搜索字符串	告警或计划报表使用的搜索字符串。
内联…	以内联的表格、原始事件清单或 CSV 文件格式显示结果。
触发条件（仅限告警）	触发告警的条件
触发时间（仅限告警）	告警时间戳。
附加 CSV	提供 CSV 格式的结果的文件附件。
附加 PDF	提供 PDF 格式的结果的文件附件。
允许空附件	即使相关搜索未返回结果，也允许 Splunk 平台在电子邮件中包含 CSV 或 PDF 附件。

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**。

如果有 Splunk Enterprise，则可以通过编辑 alert_actions.conf 配置文件配置电子邮件告警设置。详细信息请参阅 alert_actions.conf。

使用搜索命令发送电子邮件通知

您可通过 sendemail 搜索命令直接发送电子邮件通知。以下是一个示例：

```
index=main | head 5 | sendemail to=<email address> server=<server info> subject="Here is an email notification" message="This is an example message" sendresults=true inline=true format=raw sendpdf=true
```

如果您向需要 SMTP 身份验证的服务器发送电子邮件通知，您必须分配到管理员角色。

请参阅*搜索参考*中所列的 sendemail 命令，了解详细信息。

示例 - 根据搜索结果发送电子邮件给不同的收件人

此示例显示了您可以如何使用 $result.recipient$ 标记使 Splunk 软件根据搜索返回的结果数，发送通知电子邮件给不同的收件人。

$result.recipient$ 标记与搜索中的 eval 语句结合使用。该 eval 语句设置发送电子邮件给特定地址的条件。

此处是一个设计为和 $result.recipient$ 结合使用的搜索示例。

```
"error" | stats count | eval recipient=case(count > 3500, "recipient1@domain.com", count >= 500, "recipient2@domain.com", 1==1, null()) | where isnotnull(recipient)
```

此搜索保存为告警或计划报表之后，您可以为其设计电子邮件通知操作，这样您可以在**收件人**字段键入 $result.recipient$。

触发告警或计划报表按计划运行时，如果结果数超过 3500，则会发送通知给 recipient1。如果结果数低于 500，则会发送通知给 recipient2。如果两个条件都不满足，则不发送通知。

有关标记使用的更多信息，请参阅“在电子邮件通知中使用标记”。

配置用户角色以实现 PDF 交付

PDF 交付计划要求以下功能。

- schedule_search
- admin_all_objects。当邮件主机需要登录凭据时需要此功能。

- list_settings

有关更多信息，请参阅*安全性手册*中的“关于使用功能定义角色”。

在电子邮件通知中使用标记

标记代表搜索所产生的数据。他们在搜索结束时作为数据值填充的占位符或变量使用。

您可在下面的电子邮件通知字段中使用标记。

- 发送
- 抄送
- 密送
- 主题
- 消息
- 页脚

如果有 Splunk Enterprise，则可以通过编辑 alert_actions.conf 更改页脚文本。

使用此标记语法引用搜索中的值： $<token>$

例如，将下面的文本和标记放入电子邮件通知的主题字段中，以引用搜索任务的搜索 ID：

```
Search results from $job.sid$
```

可用于电子邮件通知的标记

有四种类别的标记可访问搜索生成的数据。标记的可用性会因上下文而有所不同。

类别	上下文：告警操作	上下文：计划报表	上下文：计划 PDF 交付
搜索元数据	是	是	是
搜索结果	是	是	否
任务信息	是	是	否
服务器信息	是	是	是
仪表板信息	否	否	是

如果有 Splunk Enterprise，则可以使用标记访问列于 savedsearches.conf 和 alert_actions.conf 中的各属性的值。根据标准标记语法使用属性名。例如，要访问电子邮件通知的主题，使用 $action.email.subject$。

搜索元数据标记

常见的访问搜索信息的标记。

标记	描述
$action.email.hostname$	电子邮件服务器主机名
$action.email.priority$	搜索的优先级
$alert.expires$	告警过期时间
$alert.severity$	告警严重性级别
app	搜索的应用上下文
$cron_schedule$	搜索 cron 计划
$description$	易于理解的搜索描述
$name$	搜索名称

$next_scheduled_time$	搜索下次运行的时间
$owner$	搜索所有者
$results_link$	（仅限告警操作和计划报表）搜索结果的链接
$search$	搜索字符串
$trigger_date$	（仅限告警操作）告警触发的日期，格式为 Month(string) Day, Year
$trigger_time$	（仅限告警操作）告警触发的时间，格式为 epoch 时间
$type$	指示搜索是否来自告警、报表、视图或搜索命令
$view_link$	查看保存的搜索的链接

结果标记

您可从搜索返回的第一个结果行访问字段值。标记的字段可用性取决于搜索结果中有哪些字段。

标记	描述
$result.*fieldname*$	来自第一个搜索结果行的特定字段名称的第一个值。验证搜索生成了所访问的字段。

要在结果中包含或排除特定的字段，可在告警的基本搜索中使用 `fields` 命令。有关更多信息，请参阅*搜索参考*中的字段。

任务信息标记

访问特定于搜索任务的数据的常见标记，如搜索 ID 或由搜索任务生成的消息。

标记	描述
$job.earliestTime$	初始任务开始时间
$job.eventSearch$	在任何转换命令之前出现的搜索子集
$job.latestTime$	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
$job.resultCount$	搜索任务结果计数
$job.runDuration$	搜索任务完成所需的时间（单位为秒）
$job.sid$	搜索 ID
$job.label$	搜索任务名称

服务器标记

提供有关 Splunk 部署的详细信息。

标记	描述
$server.build$	Splunk 部署的内部版本号。
$server.serverName$	承载 Splunk 部署的服务器名称。
$server.version$	Splunk 部署的版本号。

仪表板元数据标记

访问仪表板元数据并将其包括在仪表板交付电子邮件中。

标记	描述

$dashboard.label$	仪表板标签
$dashboard.title$	相当于 $dashboard.label$
$dashboard.description$	仪表板描述
$dashboard.id$	仪表板 ID

已弃用电子邮件通知标记

以下标记已弃用。

标记	替代选项
$results.count$	（已弃用）Use $job.resultCount$。
$results.file$	（已弃用）无可用的当量。
$results.url$	（已弃用）Use $results_link$。
$search_id$	（已弃用）Use $job.id$。

使用 webhook 告警操作

Webhook 允许您在特定的 web 资源上定义自定义回调。例如，您可以设置 webhook 使告警消息在聊天室里弹出或在网页上发布通知。当触发告警时，webhook 将在 URL 上发起 HTTP POST 请求。webhook 在 POST 请求的正文中传递关于告警的 JSON 格式的信息。

设置 Webhook 告警时，必须从目标源获取 hook URL。例如，如果要将 Webhook 告警发布到 Slack 房间，则必须遵循 Slack 的 Webhook 指示以获取正确的 URL 才能使用。您可以使用诸如 https://webhook.site 之类的 webhook 测试站点来测试是否触发了 webhook。

Webhook 数据负载

webhook POST 请求的 JSON 数据负载包括以下信息。

- 触发告警的保存的搜索的搜索 ID 或 SID
- 搜索结果链接
- 搜索所有者和应用
- 来自触发搜索结果的结果首行

示例

```
{

        "result": {
                "sourcetype" : "mongod",
                "count" : "8"
        },
        "sid" : "scheduler_admin_search_W2_at_14232356_132",
        "results_link" : "http://web.example.local:8000/app/search/@go?sid=scheduler_admin_search_W2_at_14232356_132",
        "search_name" : null,
        "owner" : "admin",
        "app" : "search"
}
```

根据 webhook 情况，您可以在接收 POST 的资源上配置数据负载。

配置 webhook 告警操作

在为告警选择告警操作时设置 webhook。

1. 新建告警或编辑现有告警的操作时，您可以配置 webhook 操作。选用下面其中一个选项。

选项	步骤
新建告警	从**搜索和报表**应用中的**搜索**页面，选择**另存为** > **告警**。输入告警详细信息，并根据需要配置触发和限制。
编辑已有告警	从**搜索和报表**应用中的**告警**页面，为所需告警选择**编辑** > **编辑操作**。

2. 从**添加操作**菜单中选择 **Webhook**。
3. 为 webhook 键入 URL。
4. 单击**保存**。

将结果输出到 CSV 查找

此操作将触发的告警结果或计划的报表运行的结果写入到您指定的 CSV **查找**文件。结果可以替代现有的文件内容，也可以附加到现有的文件内容。

Splunk 软件使用 `outputlookup` 命令将搜索结果写入到 CSV 查找文件。

前提条件

- 了解如何上载 CSV 查找文件并新建 CSV 查找定义。请参阅*《知识管理器手册》*中的“在 Splunk Web 中定义 CSV 查找”。

步骤

1. 当您新建告警、为现有告警编辑操作、定义或编辑报表计划时，可以将输出结果配置到查找操作。选用下面其中一个选项。

选项	步骤
新建告警	从**搜索和报表**应用中的**搜索**页面，选择**另存为** > **告警**。输入告警详细信息，并根据需要配置触发和限制。
编辑已有告警	从**搜索和报表**应用中的**告警**页面，为现有告警选择**编辑** > **编辑告警**。
定义或编辑报表计划	从**搜索和报表**应用中的**报表**页面，为报表选择**编辑** > **编辑计划**。

2. 单击**添加操作**，然后选择**将结果输出到查找**。
3. 提供 CSV 查找文件的**文件名**。您可以提供一个已上载到 Splunk 实现的 CSV 查找文件名，或提供一个当前未上载的 CSV 查找文件名。
   如果您提供一个未上载到 Splunk 实现的 CSV 查找文件名，Splunk 平台会用您提供的文件名新建一个 CSV 文件。之后，Splunk 平台会用最先触发的搜索任务填充新的 CSV 文件。
   要查看当前已上载到 Splunk 实现中的 CSV 查找文件列表，请选择**设置** > **查找** > **查找表文件**。
4. 确定您想要如何将**结果**写入 CSV 查找文件。

选项	描述
附加	将由搜索运行返回的结果附加到 CSV 文件的内容中。此为默认设置。
替换	用搜索运行返回的结果替换 CSV 文件的内容。

5. 单击**保存**。

日志事件

构建自定义日志事件来索引和搜索元数据。日志事件会发送至您的 Splunk 部署，以为其建立索引。对于某个告警，日志事件可单独使用，也可与其他告警操作一起使用。

授权要求

使用日志事件告警操作需要具有 `edit_tcp` 功能（针对无 `admin` 角色的用户）。

日志事件的令牌

当您设置日志事件的告警操作时，用代表搜索、任务或服务器元数据的纯文本或令牌填充事件字段。也可以用令牌访问第一个搜索结果集。

可用于电子邮件通知的令牌也可用于日志事件。有关使用带告警操作的标记的更多信息，请参阅本手册中的“在电子邮件通知中使用标记”。

设置日志事件告警操作

以下为在建立搜索之后设置自定义日志事件告警操作的步骤。

前提条件
要查看标记使用情况的信息，请参阅本手册中的“在电子邮件通知中使用标记”。

步骤

1. 可以在新建告警或编辑已有告警的操作时配置日志事件操作。选用下面其中一个选项。

选项	步骤
新建告警	从**搜索和报表**应用中的**搜索**页面，选择**另存为** > **告警**。输入告警详细信息，并根据需要配置触发和限制。
编辑已有告警	从**搜索和报表**应用中的**告警**页面，为所需告警选择**编辑** > **编辑操作**。

   以下步骤对于保存新告警和编辑已有告警是一样的。

2. 从**添加操作**菜单中选择**日志事件**。
3. 添加以下事件信息来配置告警操作。使用代表搜索、任务或服务器元数据的纯文本或令牌。
   - **事件文本**
   - **Source 与 sourcetype**
   - **Host**
   - **日志事件的目标索引。** `main` 索引是默认目标。也可以指定另一个现有索引。

   在分布式环境中，请确保已正确配置 `outputs.conf` 文件，例如：

```
[tcpout]
defaultGroup = your_target_indexer
indexAndForward = false
and
[indexAndForward]
index=false
```

   您还必须在搜索头和索引器上定义目标索引。有关在 `outputs.conf` 中配置转发的更多信息，请参阅*《Splunk 通用转发器手册》*中的“使用 `outputs.conf` 配置转发”。

4. 单击**保存**。

监视触发的告警

在触发的告警列表中添加一个告警。按应用上下文、所有者和严重性级别查看触发的告警。

在触发的告警列表中添加告警

1. 根据您在新建告警还是在编辑现有告警，使用以下一种选项。

选项	步骤
新建告警	从**搜索和报表**应用中的**搜索**页面，选择**另存为** > **告警**。输入告警详细信息，并根据需要配置触发和限制。
编辑已有告警	从**搜索和报表**应用中的**告警**页面，为所需告警选择**编辑** > **编辑操作**。

2. 从**添加操作**菜单中选择**添加至触发的告警**。
3. 选择告警**严重**程度。
   严重性级别仅做参考信息。用于将告警分组显示在**触发的告警**列表中。默认级别为“中”。
4. 单击**保存**。

查看最近触发的告警

您可以从“触发的告警”页面或从“告警详细信息”页面查看最近触发的告警的记录。“触发的告警”页面显示触发的告警的所有实例。请参阅“查看触发的告警”，以了解有关查看和解释触发的告警的更多信息。

默认情况下，触发的告警详情记录二十四小时内可用。请参阅“更新触发的告警寿命”了解有关更改各告警的失效设置的相关信息。

运行告警操作脚本

正式弃用运行脚本告警操作。它已被自定义告警操作替换为整合自定义操作的更具可扩展性和更强大的框架。请参阅“关于自定义告警操作”，了解执行和迁移信息。

如果有 Splunk Enterprise，您可以在告警触发时运行告警脚本。从**添加操作**菜单中选择**运行脚本**。输入要运行的脚本的文件名。

例如，您可以配置告警来运行脚本，生成简单网络管理协议（SNMP）陷阱通知。脚本向另一个系统（例如网络系统管理控制台）发送通知。您还可配置另一告警，此告警运行一个调用 API 的脚本，调用的 API 进而将触发事件发送到另一系统。

注意：出于安全原因，将所有告警脚本放置在以下位置之一：

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

有关用于您新建的 shell 脚本或批处理文件的 savedsearches.conf 里的告警脚本配置的详细信息，请参阅本手册中的“配置脚本式告警”。

自定义告警操作

使用自定义告警操作

应用开发人员可以在他们的应用内构建自定义的、用户可配置的告警操作。用户可以在告警操作管理器页面上找到带有内置自定义告警操作的应用。

若要尝试自定义告警操作，您可以使用内置 webhook 告警操作来向 web 资源（像聊天室或博客）发送通知。有关更多信息，请参阅“使用 webhook 告警操作”。

要了解如何找到带有内置告警操作的应用，请参阅“使用告警操作管理器”。

有关开发人员信息，请参阅以下*开发用于 Splunk Web 的视图和应用*中的主题。

- 自定义告警操作概述
- 将脚本告警操作转换为自定义告警操作

管理告警和告警操作权限

告警权限

告警是具有明确权限的知识对象。用户角色和功能决定了告警新建、使用、编辑和其他权限。

默认情况下，只有“管理员”或“高级用户”角色的用户可以执行以下操作。

- 新建告警。
- 运行实时搜索。
- 计划搜索。
- 保存搜索。
- 共享告警。

获得授权的用户可通过编辑告警权限与其他的应用用户共享告警。当与其他非“管理员”或“高级用户”角色的用户共享告警时，该用户必须具有访问此告警功能的权限。例如，用户要能运行实时搜索以便能访问实时告警。

管理员可以配置告警操作权限来更改特定应用中用户可用的告警操作。有关更多信息，请参阅“告警操作权限”。

和非计划的报表不同，非计划的报表既可以通过所有者权限也可以通过用户权限运行，告警只能通过所有者权限运行。

请参阅*《报表手册》*中的“确定以报表所有者还是报表用户身份运行报表”。

共享告警

您可以在新建告警或后续编辑告警权限时配置分享首选项。以下为编辑告警权限的步骤。

1. 导航到**搜索和报表**应用中的**告警**页面。
2. 找到要共享的告警，并选择**编辑** > **编辑权限**。
3. 通过配置哪些用户可以访问该告警来实现告警分享。选项如下。

选项	分享描述
所有者	使告警对该告警的新建者专用。
应用	为应用的所有用户显示告警。
所有应用	为该 Splunk 部署的所有用户显示告警。

4. 为列出的用户角色选择读取和写入权限。
    - **读取**：用户可在**告警**页面查看告警，并在应用中运行告警。
    - **写入**：拥有适当权限的用户可修改、启用和禁用告警。

告警操作权限

根据您的用户**角色**，您可以为可用的告警配置告警操作权限。

例如，管理员可以为**搜索和报表**应用调整告警操作权限。管理员可以更改在该应用中新建告警的用户可用的告警操作。

要查看和更改告警操作权限，请使用**告警操作**管理器页面。有关更多信息，请参阅“使用告警操作管理器”。

告警操作为**知识对象**。要了解有关管理知识对象权限的更多信息，请参阅*知识管理器*手册中的“管理知识对象权限”。

查看和更新告警

访问和更新告警

有几种方式可以访问和编辑告警。以下为典型告警管理任务的对比以及在 Splunk Web 完成这些任务的位置。

任务	位置
查看当前应用上下文中的所有告警。	**告警**页面
选择一个告警进行查看或更新。	**告警**页面
查看和编辑告警详细信息。	在**告警**页面上，选择一个告警并打开其详细信息页面。
查看可用的告警操作并浏览更多操作。	**告警操作**管理器页面。
查看最近触发的告警。	**触发的告警**列表页面。

使用“告警”页面

告警页面列出了应用的所有告警。它位于应用的顶层导航菜单中。从**告警**页面上，您可以使用以下选项。

选项	描述
为显示的告警选择筛选选项。	• **全部**。查看您有查看权限的所有告警。 • **您的**。查看您自己的告警。 • **此应用的**。查看当前应用的告警。只有您有查看权限的告警在列表中显示。
选择一个显示的告警	打开一个告警的详细信息页面。您可以在此页面查看和编辑此告警。
在搜索中打开	在**搜索**页面中查看或修改此告警的搜索字符串。不支持在 Splunk Web 中更新时间范围。
编辑	打开一个告警的详细信息页面。您可以在此页面查看和编辑此告警。

修改告警搜索

1. 从**告警**页面中找到告警并单击**在搜索中打开**。此告警搜索会在**搜索**页面中打开。
2. 根据需要编辑搜索字符串。
3. 运行编辑的搜索。
4. 单击**保存**以更新告警。如果再次提示，单击**保存**。
5. 请从以下选项中选择。

选项	描述
“查看告警”	打开告警详细信息页面。
“继续编辑”	返回**搜索**页面。
“权限”	查看和编辑告警权限。

访问告警详细信息

在**告警**页面上，选择一个告警查看并更新其设置。获得授权的用户可以更改以下告警设置。

- 启用或禁用告警
- 应用上下文
- 权限
- 告警类型和时间
- 触发条件

- 告警操作

告警页面

告警页面列出了应用的所有告警。它位于应用的顶层导航菜单中。从**告警**页面上，您可以使用以下选项。

选项	描述
为显示的告警选择筛选选项。	• **全部**。查看您有查看权限的所有告警。 • **您的**。查看您自己的告警。 • **此应用的**。查看当前应用的告警。只有您有查看权限的告警在列表中显示。
选择一个显示的告警	打开一个告警的详细信息页面。您可以在此页面查看和编辑此告警。
在搜索中打开	在**搜索**页面中查看或修改此告警的搜索。
编辑	打开一个告警的详细信息页面。您可以在此页面查看和编辑此告警。

修改告警搜索

1. 从**告警**页面中找到告警并单击**在搜索中打开**。此告警搜索会在**搜索**页面中打开。
2. 根据需要编辑此搜索。
3. 运行编辑的搜索。
4. 单击**保存**以更新告警。如果再次提示，单击**保存**。
5. 请从以下选项中选择。

选项	描述
“查看告警”	打开告警详细信息页面。
“继续编辑”	返回**搜索**页面。
“权限”	查看和编辑告警权限。

使用告警操作管理器

在告警操作管理器页面上，您可以为可用的告警操作查看和配置设置。

前提条件
（可选）审阅告警操作权限。

步骤

1. 从顶层导航栏中选择**设置** > **告警操作**。
2. 您可以为告警操作执行以下步骤，具体取决于您的权限。
    - 启用或禁用告警操作
    - 更新权限
    - 检查使用统计
    - 查看日志事件
3. （可选）单击**浏览更多**以找到带有内置自定义告警操作的应用。

触发的告警

在**触发的告警**页面查看最近触发的所有告警。

有关配置“添加至触发的告警”操作的详细信息，请参阅“监视触发的告警”。

触发的告警列表

满足以下条件时，告警会显示在**触发的告警**页面。

- 此告警的“添加至触发的告警”操作已启用。
- 告警最新触发。
- 告警的保存时长还未过。
- 未删除触发的告警列表。

在**触发的告警**页面，详细信息按以下类别显示。

类别	描述
时间	触发日期和时间。
触发的告警	触发的告警的名称。
应用	告警应用上下文。
类型	告警类型。
严重程度	所分配的告警严重性级别。严重性级别有助于将此页面中的告警进行排序或筛选。
模式	告警触发配置模式。“按结果”表示此告警是由单个事件触发的。“摘要”表示此告警是由一组事件触发的。

默认情况下可获得 24 小时内触发的告警的记录。您可以根据告警配置失效时间。例如，您可以将告警的触发的告警记录的寿命设为 7 天，而不是 24 小时。请参阅“更新触发的告警寿命”了解有关更改各告警的告警记录的寿命相关信息。

访问和更新触发的告警

这里介绍访问和使用**触发的告警**页面的步骤。

前提条件
（可选）审阅触发的告警列表。

步骤

1. 从顶层导航栏中选择**活动 > 触发的告警**。
2. 根据**应用**、**所有者**、**严重性**和**告警**（告警名称）来过滤所有显示的告警。
3. （可选）使用关键字搜索以按告警名称或应用上下文查找触发的告警。
4. （可选）从“告警管理器”上执行以下操作。

    - 查看告警搜索结果。
    - 编辑告警搜索。
    - 删除触发的告警列表。

删除触发的告警列表

默认情况下，**触发的告警**页面中的触发的告警记录会在 24 小时后过期。有几种方式可以更改设置，确定是否在本页面显示触发的告警列表。

- 更新触发的告警列表过期时间。
- 从**触发的告警**页面中删除触发的告警列表。
- 禁用告警以防止其触发。

其他告警配置选项

建议在**搜索**页面中新建告警，在**告警**页面中编辑告警。在少数情况下，获得授权的用户可以访问以下配置的**搜索**、**报表**和**告警**页面。

启用摘要索引

计划告警具有摘要索引。摘要索引有助于对较长时间范围内的大量数据执行分析或报表。如果多个用户定期运行相似的搜索，通常会相当耗时并会影响性能。

前提条件
确保告警的搜索产生统计和摘要数据。

步骤

1. 从顶层导航栏中选择**设置** > **搜索、报表和告警**。
2. 针对您想要修改的告警，单击**编辑** > **高级编辑**。
3. 要启用摘要索引定期收集数据，在窗口左上角的搜索窗口中搜索 "alert_type"。将 **alert_type** 设为**always**。
4. 对于计划告警，搜索“摘要”查看摘要索引选项。将 **action.summary_index** 设为 **true**。若之前没有指定，此设置会将**告警条件**设为“始终”。此选项对实时告警不可用。
5. 单击**保存**。

搜索和摘要索引

若要让告警使用摘要索引，新建一个搜索来计算一段时间内的统计数据或事件摘要。搜索结果都将保存到您指定的摘要索引中。您可以使用这一较小的摘要索引进行搜索，而不必使用较大的原始数据集。

通常会在用来填充摘要索引的搜索中使用报表命令。请参阅*知识管理器手册*中的“使用摘要索引提高报表效率”。

更新触发的告警记录寿命

默认情况下，**触发的告警**页面中的每个触发的告警记录会在 24 小时后过期。您可以根据告警更新触发的告警记录寿命。

以下是更新特定告警的触发的告警记录寿命的步骤。这些步骤仅适用于启用“添加至触发的告警”操作的告警。

1. 从顶层导航栏中选择**设置** > **搜索、报表和告警**。
2. （可选）选择**类型** > **告警**筛选列表，以便仅显示告警。
3. 在**名称**下面找到要修改的告警。
4. 选择**编辑** > **编辑告警**。
5. 通过设置**过期**字段定义触发的告警记录的寿命。
   输入一个整数并从下拉列表中选择时间单位。例如，要使此告警的所有已触发告警记录寿命为三天，请输入 3 并选择**天数**。
6. 单击**保存**。

告警示例

告警示例

通过这些示例了解如何使用告警类型和触发选项。每个示例均包括告警使用案例和组件的摘要。这些示例还包含了新建告警的步骤。

计划的告警示例

计划告警定期搜索事件。如果结果满足指定的条件，则会触发告警操作。

告警示例摘要

使用案例
: 追踪 Splunk 实例上的错误。如果在 24 小时的时间周期内产生了 5 个以上的错误，则会发送电子邮件通知。

告警类型
: 计划

搜索
: 查找过去 24 小时内的错误事件。

计划
: 每天在同一时间运行此搜索。在本案例中，每天上午 10:00 运行此搜索。

触发条件
: 如果搜索产生了五个以上的结果，则会触发告警操作。

告警操作
: 发送电子邮件通知，并在通知中提供搜索结果的详细信息。

设置告警

1. 从“搜索页面”新建如下搜索。 `index=_internal " error " NOT debug source=*splunkd.log* earliest=-24h latest=now`
2. 选择**另存为 > 告警**。
3. 为**另存为告警**对话框中的字段指定如下值。
   - **标题**：过去 24 小时内产生的错误
   - **告警类型**：计划
   - **时间范围**：每天运行
   - **计划**：10:00
   - **触发条件**：结果数量
   - **在结果数满足下列条件时触发**：大于 5。
4. 选择**发送电子邮件**告警操作。
5. 使用**主题**和**消息**字段中的令牌，进行如下电子邮件设置。
   - **收件人**：电子邮件的收件人
   - **优先级**：正常
   - **主题**：错误告警过多：$name$
   - **消息**：$trigger_date$ 报告了 $job.resultCount$ 个错误。
   - **包含**：告警链接和结果链接

   接受所有其他选项的默认值。
6. 单击**保存**。

实时告警示例

实时告警实时地持续搜索结果。您可以配置实时告警，使其在每次产生结果时即触发或只有当特定时间窗内产生的结果符合触发条件时才触发。

告警示例摘要

使用案例

当 Splunk 实例上产生错误时即对其进行监视。如果一分钟内产生的错误超过五个，则发送电子邮件通知。

告警类型
实时

搜索
持续查找实例中的错误。

触发条件
如果一分钟内的搜索结果超过五个，则触发告警。

告警操作
发送电子邮件通知。

设置告警

1. 从“搜索页面”新建如下搜索。 `index=_internal " error " NOT debug source=*splunkd.log*`
2. 选择**另存为 > 告警**。
3. 为告警字段指定以下值。
   - **标题**：报告的错误（实时）
   - **告警类型**：实时
   - **触发条件**：结果数量
   - **当结果数量满足下列条件时触发**：在 1 分钟内大于 5。
4. 选择**发送电子邮件**告警操作。
5. 使用**主题**和**消息**字段中的令牌，指定如下电子邮件设置。
   - **收件人**：电子邮件的收件人
   - **优先级**：正常
   - **主题**：实时告警：$name$
   - **消息**：有 $job.resultCount$ 个错误。
   - **包含**：告警链接、结果链接、触发条件和触发时间。

   接受所有其他选项的默认值。
6. 单击**保存**。

限制实时告警

对告警进行限制以减少其触发频率并限制告警操作行为。例如，如果一个告警所产生的电子邮件通知的数量太多时，即可对其进行限制。

限制实时告警示例。以下设置更改了告警触发行为，使每 10 分钟内只会产生一个电子邮件通知。

1. 从**搜索和报表**应用中的**告警**页面，选择该告警。此告警的详细信息页面会打开。
2. 选择告警**触发条件**旁边的**编辑**。
3. 选择**限制**选项。指定 10 分钟的时间周期。
4. 单击**保存**。

自定义触发条件示例

在新建告警时可以从已有的结果或字段计数触发条件选项中选择一个。也可以指定自定义的触发条件。自定义条件作为初始结果集的辅助搜索使用。

告警示例摘要

使用案例
使用**触发的告警**列表来记录警告类错误实例。

告警类型
实时

搜索
实时查找所有错误。

触发条件
在告警搜索结果中查找警告类的错误。如果结果中包含任何警告类错误，则触发告警操作。

告警操作

在**触发的告警**页面列出告警。

设置告警

1. 在**搜索和报表**主页中，新建如下搜索。 `index=_internal source="*splunkd.log" ( log_level=ERROR OR log_level=WARN* OR log_level=FATAL OR log_level=CRITICAL)`
2. 选择**另存为 > 告警**。
3. 指定以下告警字段值。
   - **标题**：警告类型的错误
   - **告警类型**：实时
   - **触发条件**：自定义
   - **自定义条件**：`search log_level=WARN* in 1 minute`
4. 选择**列入触发的告警**告警操作。
5. 单击**保存**。

使用 .conf 文件手动配置告警

在 savedsearches.conf 中配置告警

可以使用 Splunk Web 来配置大部分告警。如果有 Splunk Enterprise，您可以通过编辑 savedsearches.conf 配置告警。若需参考，请参阅 Splunk Enterprise*《管理员手册》*中的 savedsearches.conf。

前提条件

- 只有拥有文件系统访问权限的用户，如系统管理员，才可以使用配置文件配置告警。
- 请参阅 Splunk Enterprise*《管理员手册》*中的“如何编辑配置文件”了解具体步骤。
- 您可以有几个具有相同名称的配置文件，分散在默认目录、本地目录和应用目录中。请参阅 Splunk Enterprise*《管理员手册》*中“在何处放置（或查找）已修改的配置文件”。

不要更改或复制默认目录中的配置文件。默认目录中的文件必须保持原样并位于其原始位置。更改本地目录中的文件。

配置文件路径

在本地目录中创建或编辑 savedsearches.conf： `$SPLUNK_HOME/etc/system/local/`

如果是应用，则在应用程序目录中创建或编辑 savedsearches.conf： `$SPLUNK_HOME/etc/apps/<app name>/local`

savedsearches.conf 段落示例

告警使用已保存的搜索来查找事件。savedsearches.conf 针对每个已保存的搜索都包含一个段落。以下示例为一保存的搜索对应的段落，包括其告警操作设置。在此案例中，告警在触发时即会发送电子邮件通知。

```
[Too Many Errors Today]
# send an email notification
action.email = 1
action.email.message.alert = The alert condition for '$name$' in the $app$ fired with $job.resultCount$ error events.
action.email.to = address@example.com
action.email.useNSSubject = 1

alert.suppress = 0
alert.track = 0

counttype = number of events
quantity = 5
relation = greater than

# run every day at 14:00
cron_schedule = 0 14 * * *

#search for results in the last day
dispatch.earliest_time = -1d
dispatch.latest_time = now

display.events.fields = ["host","source","sourcetype","latitude"]
display.page.search.mode = verbose
display.visualizations.charting.chart = area
display.visualizations.type = mapping

enableSched = 1

request.ui_dispatch_app = search
request.ui_dispatch_view = search
search = index=_internal " error " NOT debug source=*splunkd.log* earliest=-7d latest=now
disabled = 1
```

若需配置告警的示例，请参阅 Splunk Enterprise*《管理员手册》*中的 savedsearches.conf.example 文件。

配置告警操作的脚本

正式弃用运行脚本告警操作。它已被自定义告警操作替换为整合自定义操作的更具可扩展性和更强大的框架。有关构建可包括脚本的自定义告警操作的信息，请参阅“使用自定义告警操作”。

如果有 Splunk Enterprise，您可以配置一个告警，以在该告警触发时运行 shell 脚本或批处理文件。本主题显示了如何访问有关作为告警操作运行的脚本中的告警的信息。

告警触发的脚本或批处理文件必须位于以下位置之一：

```
$SPLUNK_HOME/bin/scripts
$SPLUNK_HOME/etc/apps/<AppName>/bin/scripts
```

脚本的工作目录

当需要一条路径时，指定一条绝对路径。如果使用相对路径，则务必记住相对路径的根位于**搜索和报表**应用的 bin 文件夹中。

作为告警操作运行的脚本的访问参数

当将脚本作为告警操作运行时，捕获告警信息的位置参数将传递给脚本。位置参数还可用作环境变量。

您可访问来自每个使用以下表格中符号的参数的信息。

Arg	环境变量	值
0	SPLUNK_ARG_0	脚本名称
1	SPLUNK_ARG_1	返回的事件数
2	SPLUNK_ARG_2	搜索术语
3	SPLUNK_ARG_3	完全限定的查询字符串
4	SPLUNK_ARG_4	报表名称
5	SPLUNK_ARG_5	触发原因 例如，“事件数大于 1”。
6	SPLUNK_ARG_6	用于查看报表的浏览器 URL。
7	SPLUNK_ARG_7	由于历史原因不使用。
8	SPLUNK_ARG_8	存储此搜索结果的文件。 包含 gzip 文件格式的原始结果。

您可引用由 UNIX shell 脚本或 Microsoft 批处理文件中的这些参数捕获的信息，如下所示。在其他语言中（如 perl 和 python），使用该语言自带的方法访问脚本参数。

```
# UNIX scripts can access environment variables and positional args
$SPLUNK_ARG_0
$0

# Microsoft batch files capture environment variables reliably
%SPLUNK_ARG_0%
```

访问位置参数的测试脚本

使用以下测试脚本查看访问位置参数的结果。

要使用此测试脚本，新建将脚本作为告警操作运行的告警。然后，检查生成的 echo_output.txt 文件的内容：

```
# $SPLUNK_HOME/bin/scripts/echo.sh
# simple script that writes parameters 0-7 to
# $SPLUNK_HOME/bin/scripts/echo_output.txt
# $SPLUNK_ARG_0 and $0 show how to use the long and short form.
```

```
read sessionKey
echo "'$SPLUNK_ARG_0' '$0' '$1' '$2' '$3' '$4' '$5' '$6' '$7' '$8' '$sessionKey'" >> \
"$SPLUNK_HOME/bin/scripts/echo_output.txt"
```

- 注意：sessionKey 为 URL 编码。

脚本示例：写入 syslog

您可配置告警的脚本以写入系统日志守护程序。如果您将 syslog 设置为向其他应用程序发送告警并且您希望包括来自 Splunk 部署的告警，那么这个配置是非常有用的。

1. 新建一个脚本，logIt 调用 logger，或向 syslog 进行写入的任何其他程序。
   将脚本放入 $SPLUNK_HOME/bin/scripts。
2. 将以下内容添加至 logIt：
   logger $5

   当作为告警操作调用时，该脚本可访问任何可用的参数。

3. 针对将 logIt 作为告警操作运行的报表新建一个告警。
   当告警触发时，日志条目如下所示：
   Aug 15 15:01:40 localhost logger: Report [j_myadmin]: “事件数 (65) 大于 10”。

在配置 syslog 输入时，请参阅 Splunk 社区 Wiki 中的主题来了解有关使用 UDP 的最佳做法的信息。

脚本示例：写入 Windows 事件日志

对于 Windows 平台，您可配置告警操作以运行写入 Windows 事件日志的脚本。

以下示例显示调用写入事件日志的 EVENTCREATE 工具的脚本。脚本可访问任何适用于告警的环境变量。您可使用任何写入事件日志的可执行命令行替换 EVENTCREATE 工具。

1. 新建以下批处理文件 logIt.bat。
   将脚本放入 $SPLUNK_HOME/bin/scripts。
2. 在批处理文件中包含以下命令：
   @echo off
   EVENTCREATE /T ERROR /SO Splunk /D %SPLUNK_ARG_5%
   使用最适合包含在参数中的消息的类型。本示例使用 ERROR。

3. 针对将 logIt.bat 作为告警操作运行的报表新建一个告警。