使用 vRealize Log Insight

2018 年 9 月 20 日

vRealize Log Insight 4.7

vmware®

最新的技术文档可以从 VMware 网站下载：

https://docs.vmware.com/cn/

您如果对本文档有任何意见或建议，请把反馈信息提交至：

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

北京办公室
北京市海淀区科学院南路 2 号
融科资讯中心 C 座南 8 层
www.vmware.com/cn

上海办公室
上海市浦东新区浦东南路 999 号
新梅联合广场 23 楼
www.vmware.com/cn

广州办公室
广州市天河北路 233 号
中信广场 7401 室
www.vmware.com/cn

目录

vRealize Log Insight

使用 vRealize Log Insight 主题提供了有关使用 Web 用户界面的信息，包括有关筛选和搜索日志消息，执行分析和可视化搜索结果，处理警示查询，以及从基于自定义查询的日志消息中动态提取字段的步骤。

这些信息专为需要使用 vRealize Log Insight 的用户提供。

使用 vRealize Log Insight 功能

1

vRealize Log Insight 提供可扩展的日志汇总和 vCloud Suite 索引（包括所有的 vSphere 版本），并提供接近实时的搜索和分析功能。

vRealize Log Insight 可收集、导入并分析日志，以便对与系统、服务和应用程序相关的问题给出解答，并从中获取重要信息。

高性能载入

vRealize Log Insight 可以处理任何类型的日志生成数据或计算机生成数据。它支持高吞吐率和低延迟，并通过 syslog 和数据获取 API 接受数据。

可扩展性

通过使用多个虚拟设备实例，vRealize Log Insight 可以扩展。这将实现载入吞吐量的线性增长，提高查询性能，并实现载入高可用性。在群集模式下，vRealize Log Insight 提供主节点和工作线程节点。主节点和工作线程节点均负责数据子集。主节点和查询节点可以查询所有数据子集并汇总结果。

接近实时的搜索

由 vRealize Log Insight 载入的数据在几秒钟之内即可用于搜索。而且，历史数据也可以通过相同的界面进行搜索，延迟也是同样的低。

vRealize Log Insight 支持完整关键字查询。关键字可定义为任意字母数字、连字符或下划线字符。除了完整关键字查询外，vRealize Log Insight 还支持通配符匹配操作符查询（例如，`erro?` 或 `vm*`）和基于字段的筛选（例如，主机名“不”与 test* 相匹配、IP 包含“10.64”）。而且，包含数字值的日志消息字段还可用于定义选择筛选器（例如，CPU>80、10<线程数<100 等等）。

搜索结果展示为各个不同的事件。每个事件来自单个源，但搜索结果可能来自多个源。可以使用 vRealize Log Insight 关联一个或多个维度中的数据（例如时间和请求标识符），从而在堆栈中提供一致的视图。这样，根本原因的分析就变得简单得多。

Windows 和 Linux 代理

vRealize Log Insight 包含用于在 Linux 和 Windows 计算机上收集事件和文件的代理。

智能分组

vRealize Log Insight 使用一种新的计算机学习技术。智能分组扫描入站的非结构化数据，并按问题类型将消息组合在一起，从而使您能够快速了解可能跨物理、虚拟和混合云环境的问题。

汇总

从日志数据中提取的字段可用于汇总。这与 GROUP-BY 查询在关系数据库提供的功能或 Microsoft Excel 中的数据透视表相类似。区别在于无需提取、转换和加载 (ETL) 过程，并且 vRealize Log Insight 可扩展为任意大小的数据。

您可以生成数据的汇总视图，并识别特定事件或错误，而无需访问多个系统和应用程序。例如，查看重要的系统衡量指标（如每分钟错误数）时，可以向下细分到特定时间范围的事件，并检查环境中出现的错误。

运行时字段提取

原始日志数据并不总是容易理解，可能会需要处理一些数据来确定对搜索和汇总至关重要的字段。vRealize Log Insight 提供了运行时字段提取来解决此问题。可以通过提供正则表达式从数据中动态提取任何字段。提取的字段可用于选择、投影和汇总，与在解析时提取的字段的使用方式相类似。

仪表板

可以创建要严密监控的有用衡量指标的仪表板。任何查询都可以转换为仪表板小组件，并按任意时间范围进行汇总。可以选择最近五分钟、一小时或一天的系统性能。可以按小时查看错误的细分，并观察日志事件中的趋势。

安全注意事项

IT 决策者、架构师、管理员以及必须自行熟悉 vRealize Log Insight 安全组件的其他人员都必须阅读*管理 vRealize Log Insight* 中的安全主题。

这些主题提供了对 vRealize Log Insight 安全功能的简明参考。主题包括产品外部接口、端口、身份验证机制和用于配置和管理安全功能的选项。

本章讨论了以下主题：

- vRealize Log Insight Web 用户界面概览
- 搜索和筛选日志事件
- 使用“交互式分析”图表分析日志
- 动态字段提取
- 管理搜索查询
- 使用仪表板
- 使用内容包

- 创建内容包
- vRealize Log Insight 中的警示查询

vRealize Log Insight Web 用户界面概览

您可以访问的功能取决于登录到 vRealize Log Insight Web 用户界面所使用的用户帐户。

“仪表板”选项卡

仪表板选项卡包含自定义仪表板和内容包仪表板。在**仪表板**选项卡上，可以查看环境中日志事件的图表，或创建自定义小组件集以访问对您来说最重要的信息。

“交互式分析”选项卡

在**交互式分析**选项卡上，可以搜索和筛选日志事件，并创建查询以基于日志事件中的时间戳、文本、源和字段提取事件。vRealize Log Insight 提供了查询结果的图表。可以保存这些图表，以便以后在**仪表板**选项卡上查找它们。

内容包

内容包包含与特定产品或日志集相关的仪表板、已提取字段、已保存查询和警示。可以从 vRealize Log Insight Web 用户界面右上角的下拉菜单中访问内容包。

内容包可由 vRealize Log Insight 用户导入或创建。请参见使用内容包。

管理用户界面

vRealize Log Insight 管理员可以管理用户帐户，配置存储位置和存档，为电子邮件通知配置出站 SMTP 服务器，以及更改多个其他参数。管理 UI 的 URL 格式为 https://*log_insight-host*/admin/，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

搜索和筛选日志事件

可以在**交互式分析**选项卡上搜索和筛选日志事件。

您可以在搜索文本框中键入任何完整的关键字、通配符匹配操作符或短语，然后单击**搜索**以仅查找包含指定关键字的事件。

可以在 Web 用户界面的**仪表板**或**交互式分析**页面上指定时间范围。筛选时包含时间范围。

可以搜索与特定字段的特定值匹配的日志事件。在主搜索字段中使用引用文本将匹配确切的短语。在主搜索字段中输入空格表示逻辑 AND 运算符。搜索仅使用完整令牌：搜索“err”将不会查找“error”作为匹配项。

可以通过使用日志事件列表上方的下拉菜单和文本框来指定字段搜索条件或筛选器。

在单行筛选器内，可以使用逗号分隔值列出 OR 筛选器。例如，选择 **hostname contains**，并键入 **`127.0.0.1, 127.0.0.2`**。搜索将返回包含主机名 127.0.0.1 或 127.0.0.2 的事件。

注意　**文本包含**筛选器将每个逗号分隔的值视为一个完整关键字。

无法处理且不应使用包含使用内部查询语言语法名称（如 `from` 或 `in`）的字段的查询。

可以通过为每个字段创建一个新的筛选器行来组合多个字段筛选器。可以切换应用于多行筛选器的运算符。

- 选择**全部**以应用 AND 运算符。
- 选择**任何**以应用 OR 运算符。

注意　无论切换值如何，单个筛选器行内逗号分隔值的运算符始终为 OR。

可以在搜索词中使用通配符匹配操作符。例如，vm* 或 vmw?re。

- 使用 * 表示 0 或更多个字符
- 使用 ? 表示一个字符。

注意　不能将通配符匹配操作符用作搜索词的第一个字符。例如，可以在筛选查询中使用 192.168.0.*，但不能使用 *.168.0.0。

事件类型分组

Log Insight 使用机器学习将相似事件分组在一起。事件类型分组使故障排除和根本原因分析变得更容易。

在 Log Insight 中运行查询时，结果数取决于查询和时间范围。通常，查询会返回大量结果。机器学习可从导入到 Log Insight 的事件中动态学习和调整模式。

事件类型选项卡位于“交互式分析”页面上的搜索栏下方。单击**事件类型**选项卡时，您会看到组合在一起的相似事件的列表。

机器学习可分析这些事件并发现相似日志消息所包含的字段类型。例如，类型可能是时间戳、字符串、整数、十六进制数等。发现的类型在**事件类型**列表中显示为超链接。

机器学习发现的每种类型都表示一种新的字段类型，称为智能字段。智能字段的默认名称采用以下格式：智能字段 - *类型数字* [*事件类型*]。可以更改智能字段的默认名称。命名智能字段后，它将像其他字段那样显示在“字段”部分中。可以重命名或删除智能字段，但无法修改其定义。

机器学习引入了一种新的静态字段，称为事件类型。可以使用“事件类型”作为筛选器，以在查询中包括或排除特定的事件类型。

日志事件中的信息

vRealize Log Insight 收集和分析计算机生成的所有类型的日志数据，其中包括应用程序日志、网络跟踪、配置文件、消息、性能数据和系统状况转储。

可以将 vRealize Log Insight 连接到您环境中的一切元素（包括操作系统、应用程序、存储、防火墙和网络设备）以供企业级使用日志分析进行查看。

配置好 vRealize Log Insight 且准备好收集日志时，您可以通过许多方法来载入日志数据，其中包括：

- vSphere 集成—vRealize Log Insight 可与 vSphere 集成以自动载入 vCenter Server 中的事件和 ESXi 主机中的日志。
- vRealize Operations Manager 集成—vRealize Log Insight 可与 vRealize Operations Manager 集成以启用各类警示从而向管理员发送 vRealize Operations Manager 中的通知事件以及电子邮件。
- 代理—vRealize Log Insight 拥有可用的收集代理以将文件和事件日志从 Linux 或 Windows 发送到 vRealize Log Insight。
- Syslog—vRealize Log Insight 可通过 syslog 载入任何源中的数据。只需将 vRealize Log Insight 服务器设置为您的 syslog 目标。
- Syslogd —
- CFAPI—使用 cfapi 将事件以其原始格式发送到 vRealize Log Insight。通过 cfapi 发送的事件不需要遵守 syslog 事件的准则，也不需要进行修改以符合 syslog RFC。

每个事件均包含以下信息。

类型	描述
时间戳	事件发生的时间
源	事件的起源地。这可能是 syslog 消息的发送方（如 ESXi 主机）或转发方（如 syslog 聚合）。
文本	事件的原始文本。
字段	从事件中提取的名称-值对。仅当代理使用 CFAPI 协议时，将字段作为静态字段传送到服务器。

注意 vRealize Log Insight 不负责来自其他 VMware 产品的日志消息的内容。如果您对日志内容有疑问，请联系生成此日志消息的产品团队。

按时间范围筛选日志事件

可以筛选日志事件以仅查看特定时段内的事件。

可以在 Web 用户界面的**仪表板**或**交互式分析**页面上指定时间范围。筛选时包含时间范围。

前提条件

验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 从**搜索**按钮左侧的下拉菜单中，选择一个预定义时段。

2 （可选）要设置时间范围的始点和终点，请选择**自定义时间范围**。

搜索包含完整关键字的日志事件

可以搜索包含完整关键字的日志事件。关键字包含字母数字、连字符和下划线字符。

前提条件

验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 导航到**交互式分析**选项卡。

2 在搜索文本框中，键入要在日志事件中搜索的完整关键字，然后单击**搜索**按钮。

包含指定完整关键字的日志事件将显示在列表中。

您搜索的字符串会以黄色突出显示。

下一步

可以保存当前查询，以便在以后加载。

按字段运算搜索日志事件

可以使用现有字段的列表搜索其中某个字段具有特定值的日志事件。

重要事项 vRealize Log Insight 会对完整、字母数字、连字符和下划线字符编制索引。

前提条件

验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 导航到**交互式分析**选项卡。

2 单击**添加筛选器**。

3 在搜索文本框下方的筛选器行中，使用第一个下拉菜单选择在 vRealize Log Insight 中定义的任何字段。

例如，**hostname**。

此列表包含在内容包和自定义内容中静态可用的所有定义字段。这些字段按名称排序，但 **text** 字段除外。因为 **text** 是一个表示消息文本的特殊字段，**text** 显示在列表顶部，默认情况下处于选中状态。

注意 数字字段包含字符串字段不包含的其他运算符：**=**、**>**、**<**、**>=**、**<=**。这些运算符执行数字比较，与使用字符串运算符相比，使用它们可生成不同的结果。例如，筛选器 **response_time = 02** 将匹配包含值为 2 的 **response_time** 字段的事件。筛选器 **response_time contains 02** 将不会具有相同匹配。

4 在搜索文本框下方的筛选器行中，使用第二个下拉菜单选择要应用于在第一个下拉菜单中选择的字段的运算。

例如，选择 **contains**。**contains** 筛选器匹配完整令牌：搜索“err”将不会查找“error”作为匹配项。

5 在此筛选器下拉菜单右侧的文本框中，键入要用作筛选器的值。

可以列出以逗号分隔的多个值。这些值之间的运算符是 OR。

注意 如果在第二个下拉菜单中选择 **exists** 运算符，则此文本框不可用。

6 （可选）要添加更多筛选器，请单击**添加筛选器**。

此时将在筛选器行上方显示一个切换按钮。

7 （可选）对于多个筛选器行，请选择筛选器之间的运算符。

选项	描述
全部	选择以在筛选器行之间应用 AND 运算
任何	选择以在筛选器行之间应用 OR 运算

默认情况下，**全部**处于选中状态。

8 单击**搜索**按钮。

示例：搜索其名称中包含常见字符串的主机组

假定您拥有多个主机，其中一个主机称为 w1-stvc-205-prod3，另一个主机称为 w1-stvc-206-prod5。

要查找这两个主机的所有日志，请创建以下查询。

1 1. 保留搜索文本框为空。

2 定义筛选器。

a 从第一个下拉菜单中选择**主机名**。

b 从运算符下拉菜单中选择**开头为**。

c 在值文本框中键入 **`w1-stvc`**。

或者，您可以使用 **contains** 运算符，但之后必须在搜索值中使用通配符匹配操作符。在此示例中，必须在值文本框中键入 **`w1-stvc-*`**。

3 单击**搜索**按钮。

下一步

可以保存当前查询，以便在以后加载。

搜索某个事件之前、之后或附近发生的事件

可以在日志事件列表中搜索列表中的某个事件之前、之后和附近发生的事件。

如果要了解有关某个事件之前和之后的环境状态的更多信息，可以检查附近事件。

前提条件

验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 在**交互式分析**选项卡上，在列表中找到此事件。

2 在事件行左侧，单击 ⚙，然后选择**设置起自此事件的时间范围**。

3 在“通过事件设置时间范围”对话框中，使用下拉菜单选择时间范围的时段和方向。

可以在预定义时段列表中从 1 秒到 10 分钟之间进行选择。

4 单击**设置范围**。

选定事件附近的事件将显示在列表中。

注意 此操作可清除之前已指定的所有搜索参数和筛选器。

在环境中查看事件

您可以查看某个日志事件的环境，并浏览在该日志事件前后到达的日志事件。

如果要了解有关某个事件之前和之后的环境状态的更多信息，可以检查附近事件。

前提条件

验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 在**交互式分析**选项卡上，在列表中找到此事件。

2 在事件行左侧，单击 ⚙，然后选择**在环境中查看事件**。

3 （可选）向上或向下滚动至窗口边沿以加载更多事件。

4 （可选）单击紫色时间戳，以向后滚动到突出显示的消息。

5 （可选）要添加筛选器，请单击顶部的**添加筛选器**，或单击突出显示的事件中的某个字段。

6 （可选）通过指向某个事件并单击 ⚙，可添加或移除特定的事件类型。

分析事件趋势

您可以分析日志事件以了解趋势和异常情况。

前提条件

验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 导航到**交互式分析**选项卡。

2 通过使用搜索文本框和应用筛选器来构建并运行您的查询。

3 在“通过事件设置时间范围”对话框中，使用下拉菜单选择时间范围的时段和方向。

4 单击**事件趋势**选项卡。

vRealize Log Insight 会将您的查询与之前的同一时间段进行比较，并显示相应结果。

清除所有筛选规则

可以清除筛选和搜索结果以查看所有日志事件的列表。

对事件列表执行搜索后，搜索结果将始终保留在屏幕上，直到清除所有查询。

前提条件

验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 在**交互式分析**选项卡上，移除所有筛选器。

2 如果在搜索文本框中显示文本，请将其删除。

3 单击**搜索**按钮。

搜索查询示例

在 vRealize Log Insight 的**交互式分析**选项卡上构建查询时，可以使用这些示例。

示例：查询昨天上午 9-10 点由 ESX/ESXi hostd 进程报告的所有检测信号事件

重要事项 vRealize Log Insight 会对完整、字母数字、连字符和下划线字符编制索引。

要查询由 ESX/ESXi hostd 进程报告的所有检测信号事件，请执行以下操作：

1 在搜索文本框中，键入 **`heartbeat*`**。

2 定义筛选器。

a 从第一个下拉菜单中选择 **appname**。

b 从第二个下拉菜单中选择 **contains**。

c 在值文本框中键入 **`hostd`**。

3 定义时间范围。

a 在**时间范围**下拉菜单中，选择**自定义**。

b 在第一个文本框中，输入昨天的日期和 9am。

c 在第二个文本框中，输入昨天的日期和 10am。

4 单击**搜索**按钮。

示例：搜索其名称中包含常见字符串的主机组

假定您拥有多个主机，其中一个主机称为 w1-stvc-205-prod3，另一个主机称为 w1-stvc-206-prod5。

要查找这两个主机的所有日志，请创建以下查询。

1 1. 保留搜索文本框为空。

2 定义筛选器。

a 从第一个下拉菜单中选择**主机名**。

b 从运算符下拉菜单中选择**开头为**。

c 在值文本框中键入 **`w1-stvc`**。

或者，您可以使用 **contains** 运算符，但之后必须在搜索值中使用通配符匹配操作符。在此示例中，必须在值文本框中键入 **`w1-stvc-*`**。

3 单击**搜索**按钮。

示例：查询由 vCenter Server 任务、事件和警报报告的所有错误

要查询由 vCenter Server 任务、事件和警报报告的所有错误，请执行以下操作：

1 在搜索文本框中，键入 **`error`**。

2 定义筛选器。

a 从第一个下拉菜单中选择 **vc_event_type**。

b 从第二个下拉菜单中选择 **exists** 运算符。

3 单击**搜索**按钮。

示例：查询由 ESX/ESXi 报告的超过一秒的 SCSI 延迟

要查询由 ESX/ESXi 报告的超过一秒的 SCSI 延迟，请执行以下操作：

1 在搜索文本框中，键入 **`scsi latency "performance has"`**。

2 定义筛选器。

a 从第一个下拉菜单中选择 **vmw_vob_component**。

b 从第二个下拉菜单中选择 **contains** 运算符。

c 在文本框中键入 **`scsiCorrelator`**。

3 定义另一个筛选器。

a 从第一个下拉菜单中选择 **vmw_latency_in_micros**。

b 从第二个下拉菜单中选择 **>** 运算符。

c 在文本框中键入 **1000000**。

4 单击**搜索**按钮。

正则表达式示例

可以在字段值的文本框中键入正则表达式，以从日志事件中提取字段。

键入的表达式必须使用 Java 正则表达式语法。

表 1-1 字符运算符

正则表达式	描述
\	对特殊字符进行转义处理
\b	单词边界
\B	不是单词边界
\d	一个数字
\D	一个非数字
\n	换行符
\r	回车符
\s	一个空格
\S	除空格之外的任何字符
\t	选项卡
\w	一个字母数字或下划线字符
\W	一个非字母数字或下划线字符

例如，如果您具有字符串 1234–5678 并应用以下正则表达式

正则表达式	结果
\d	1
\d+	1234
\w+	1234
\S	1234-5678

表 1-2 限定符运算符

正则表达式	描述
.	除换行符之外的任何字符
*	零个或多个尽可能长的字符
?	零个或一个字符或尽可能短的字符
+	一个或多个

表 1-2 限定符运算符（续）

正则表达式	描述
{<n>}	恰好 <n> 次
{<n>,<m>}	<n> 至 <m> 次

例如，如果您具有字符串 `aaaaa` 并应用以下正则表达式

正则表达式	结果
.	a
*	aaaaa
.*?	aaaaa
.{1}	a
.{1,2}	aa

表 1-3 组合运算符

正则表达式	描述
.*	任意内容
.*?	前面为尽可能短的任意内容

例如，如果您具有字符串 `a b 3 hi d hi` 并应用以下正则表达式

正则表达式	结果
a.* hi	b 3 hi d
a .*? hi	b 3

表 1-4 逻辑运算符

正则表达式	描述
^	行首（如果在括号中，则不是）
$	行尾
()	封装
[]	一个在括号中的字符
|	OR
-	范围
\A	字符串开头
\Z	字符串结尾

例如，如果应用以下正则表达式

正则表达式	结果
(hello)?	包含或不包含 hello
(a|b|c)	a 或 b 或 c

正则表达式	结果
[a-cp]	a 或 b 或 c 或 p
world$	以 world 结尾，后面没有其他内容

表 1-5 前向运算符

正则表达式	描述
?=	肯定性前向（包含）
?!=	否定性前向（不包含）

例如，如果应用以下正则表达式

正则表达式	结果
is (?=\w+)\w{2} primary	is FT primary? false
opid=(?!WFU-1fecf8f9)\S+	WFU-3c9bb994

表 1-6 其他正则表达式示例

正则表达式	描述
[xyz]	x、y 或 z
(info|warn|error)	info、warn 或 error
[a-z]	一个小写字母
[^a-z]	不是小写字母
[a-z]+	一个或多个小写字母
[a-z]*	零个或多个小写字母
[a-z]?	零个或一个小写字母
[a-z] {3}	恰好三个小写字母
[\d]	一个数字
\d+$	一个或多个数字，后跟消息结尾
[0-5]	0 到 5 之间的一个数字
\w	一个单词字符（字母、数字或下划线）
\s	空格
\S	除空格之外的任何字符
[a-zA-Z0-9]+	一个或多个字母数字字符
([a-z] {2,} [0-9] {3,5})	两个或更多个字母，后跟三到五个数字

使用“交互式分析”图表分析日志

通过**交互式分析**页面顶部的图表，可以对查询结果执行可视化分析。

图表表示日志搜索查询的图形快照。您可以使用图表下方的下拉菜单更改图表类型。

可以使用左侧的第一个下拉菜单控制图表的聚合级别。默认情况下，**计数**函数处于选中状态。

图表类型

可以选择不同的图表类型，以更改在“交互式分析”页面上可视化数据的方式。

不同的图表类型需要不同的聚合函数、使用时间序列以及分组依据字段。图表显示仅限于 2,000 个最新的结果。

图表类型	聚合函数	时间序列要求	分组依据字段要求
列	任意	时间序列	不可用
行	任意	时间序列	不可用
区域	任意	时间序列	不可用
条形图	任意	非时间序列	至少一个字段
饼图	计数或唯一计数	非时间序列	至少一个字段
气泡图	任意	非时间序列	两个字段
仪表图	计数	非时间序列	不可用
标量图	计数	非时间序列	不可用
表格	任意	任意	不可用

多功能图表

可以使用多功能图表比较刻度不同的变量。

通过多功能图表，可以为每个系列分配一个 Y 轴；如果要比较不同类别的数据集，则可以分配一个 X 轴。可以将每个轴放置在图表的右侧或左侧。可以交换函数，以交换相应 Y 轴（在此轴上，从右向左绘制函数图表）。

例如，除了可以对按通道和级别分组的任务平均计数绘制图表外，还可以对按通道和级别分组的事件计数绘制图表。

聚合函数

vRealize Log Insight 提供了多个聚合函数。

类型	字段	描述
计数	仅事件	创建针对特定查询的事件数目图表。
唯一计数	任何字段	创建字段的唯一值数目图表。
最低	仅数字字段	创建字段的最小值图表。
最大值	仅数字字段	创建字段的最大值图表。
平均值	仅数字字段	创建字段的平均值图表。
标准差	仅数字字段	创建字段值的标准偏差图表。
总和	仅数字字段	创建字段的值总和图表。
方差	仅数字字段	创建字段值的方差图表。

您可以修改查看查询结果的方式。

查看	描述
按特定字段值对查询结果分组	使用图表下方的第二个下拉菜单按特定字段值而不是时间序列（或者按特定字段值以及时间序列）对查询结果进行分组。
查看字段的事件数	例如，每一主机的事件数，取消选中**“时间序列”**复选框，然后选中相应字段的复选框。
查看按时间分组的字段堆栈条形图	选中**“时间序列”**复选框并选中相应字段的复选框。

使用图表

可以在**交互式分析**选项卡上更改图表的外观，向自定义仪表板中添加图表，并管理仪表板图表。

任务	步骤
更改图表的时间范围	在**交互式分析**选项卡上，使用**搜索**按钮左侧的下拉菜单切换图表上显示的时间段。
更改图表的粒度	在**交互式分析**选项卡上，使用右上角的按钮在图表上表示的每个点所对应的不同时间范围之间进行切换。可用范围取决于为查询指定的时间范围。
在**交互式分析**选项卡上加载仪表板图表	在**仪表板**选项卡上，找到图表并单击**在交互式分析中打开**图标 。 时间范围设置为仪表板的当前时间范围。如果需要，可以修改时间范围。
将图表保存到自定义仪表板	1 在**交互式分析**选项卡的左上角，单击**添加到仪表板**。或者，从**搜索**按钮右侧的菜单中，选择**将当前查询添加到仪表板**。 2 键入名称，从下拉菜单中选择目标仪表板，选择小组件类型，添加有关小组件的信息，然后单击**添加**。
将查询以图表形式保存到自定义仪表板	1 单击**搜索**按钮旁边的**将当前查询添加到仪表板**。 2 键入名称，从下拉菜单中选择目标仪表板，确保小组件类型设置为**图表**，添加有关小组件的信息，然后单击**添加**。
将查询以字段表形式保存到自定义仪表板	1 单击**搜索**按钮旁边的**将当前查询添加到仪表板**。 2 键入名称，从下拉菜单中选择目标仪表板，确保小组件类型设置为**字段表**，添加有关小组件的信息，然后单击**添加**。
从自定义仪表板中删除小组件	1 在**仪表板**选项卡上，选择包含要删除的小组件的自定义仪表板。 2 在小组件右上角，单击**其他操作**图标 ，然后选择**删除**。 3 在“删除小组件”对话框中，单击**删除**以进行确认。

更改“交互式分析”图表的类型

可以更改图表中所显示查询结果的聚合和分组，以便以图形方式分析日志事件。

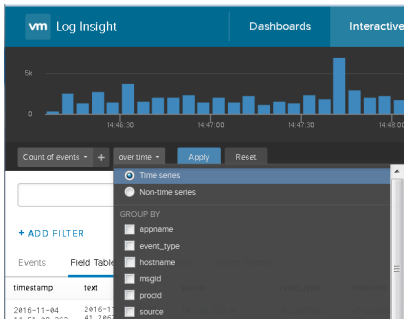
可以在图表下方看到的下拉菜单的数目取决于选定的聚合函数。

前提条件

验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 使用“交互式分析”图表下的下拉菜单以更改聚合函数和分组类型。



- 要查看一段时间内事件的数目，请选择**时间序列**按钮。
- 要仅查看事件值，请选择**非时间序列**按钮，然后至少选择一个字段。

2 单击**更新**。

示例：“交互式分析”图表中的聚合和分组

下表包含的示例说明了 vRealize Log Insight 图表中的聚合和分组。

表 1-7 “交互式分析”图表中的聚合和分组示例

第一个下拉菜单中的选择	第二个下拉菜单中的选择	时间序列选择	屏幕上显示的文本	结果
计数	**时间序列**	**时间序列**	**一段时间内**事件的**计数**	该图表显示了有关一段时间内针对当前查询的事件数量的条形图。
平均值	**vmw_op_latency (VMware - vSphere)**	**时间序列**	**一段时间内 vmw_op_latency (VMware - vSphere)** 的**平均值**	该图表显示了有关一段时间内操作延迟平均值的线图。
计数	**vmw_esx_problem** **注意** 默认情况下，不会显示 vmw_esx_problem 字段。必须提取 vmw_esx_problem 字段并保存查询，以便在下拉菜单中显示 vmw_esx_problem。	**非时间序列**	**按 vmw_esx_problem 分组**的事件的**计数**	该图表显示了有关包含 vmw_esx_problem 字段的事件数目的条形图。
计数	**时间序列**、**vmw_esx_problem**	**时间序列**	**一段时间内按 vmw_esx_problem 分组**的事件的**计数**	该图表显示了一段时间内按 vmw_esx_problem 分组的堆栈条形图。

动态字段提取

在具有许多日志事件的大型环境中，无法始终找到对您来说非常重要的数据字段。

vRealize Log Insight 提供了运行时字段提取来解决此问题。可以通过提供正则表达式从数据中动态提取任何字段。请参见正则表达式示例。

注意 通用查询可能是非常缓慢的。例如，如果尝试通过使用 `\(\d+\)` 表达式来提取字段，则查询将返回包含用括号括起的数字的所有日志事件。验证您的查询是否包含尽可能多的文本上下文。例如，`Event for vm\(\d+\)` 将是一个更好的字段提取查询。

您可以使用已提取字段来搜索和筛选日志事件的列表，或在“交互式分析”图表中聚合事件。

通过使用一键式提取来提取字段

可以使用一键式提取功能，来代替键入上下文值以动态提取字段。

一键式提取可以填充与在日志事件中选择的字段相对应的所有上下文值。

注意 一键式提取选项仅在“事件”选项卡中可用。

前提条件

验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1. 导航到**交互式分析**选项卡。
2. 在日志事件列表中，突出显示表示要提取的字段的文本。

   将在此事件中存在的字段名称集上方显示一个操作菜单。
3. 单击**提取字段**。

   将使用提取突出显示字段所需的上下文自动填充“字段”窗格中的前后上下文值。
4. （可选）在“字段”窗格中修改“提取的值”正则表达式。
5. （可选）在“字段”窗格中修改“上文”和“下文”正则表达式。
6. （可选）单击 ➕**添加其他上下文**以添加其他关键字和筛选器。

   可以添加一个或多个关键字，并将单个静态字段用作筛选器。
7. 如果是管理员用户，请从下拉菜单中选择哪些用户可以访问该字段。

选项	描述
所有用户	所有用户都将在其事件中和筛选器下拉菜单中看到该字段。
只是我	只有字段的创建者会在其事件中和筛选器下拉菜单中看到该字段。

8. （可选）在“字段”窗格的顶部，单击 *i*，然后**编辑**以向该字段添加备注。在**编辑备注**窗口中添加备注，然后单击**确定**。
9. 单击**保存**。

下一步

您可以使用已提取字段来搜索和筛选日志事件的列表，或在“交互式分析”图表中聚合事件。

如果不再需要，可以修改或删除已保存字段的定义。

修改已提取字段

可以修改已提取字段的定义。

vRealize Log Insight 可以创建您在创建图表、查询或警示时使用的字段的副本。如果修改字段定义，使用已修改字段的所有图表、查询和警示都会更新以反映新的定义。

普通用户仅可以修改其自己的内容。管理员用户可以修改其自己的内容及其共享内容。

内容包字段是只读的。

前提条件

验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 导航到**交互式分析**选项卡。

2 在“字段”窗格的顶部，单击**管理提取的字段**  并从列表中选择提取的字段。

3 修改值，然后单击**更新**。

将显示一个对话框，其中会列出将受已更新字段影响的内容。如果此字段在多个用户之间共享，则此对话框还会列出受影响的用户。

4 （可选）在“字段”窗格的顶部，单击  ，然后**编辑**以向该字段添加备注。在**编辑备注**窗口中添加备注，然后单击**确定**。

5 单击**更新**以确认更改。

vRealize Log Insight 即会更新使用已修改字段的所有查询、警示和图表。

筛选提取字段的内容包

您可以指定要从中提取字段的内容包。这样做可以避免提取不必要的字段并提高效率。

您可以从“交互式分析”页面上的“内容包”下拉菜单中选择内容包。

复制已提取字段

可以复制已提取字段。

当您希望从事件中提取多个字段且这些字段都出现在类似上下文中时，可以使用“复制”选项。提取某个字段并将其保存后，打开已提取字段的定义，然后使用“复制”选项。复制的字段具有与原始提取字段完全相同的定义。可以修改复制字段的定义，以匹配您感兴趣的事件中的另一个值。

普通用户仅可以复制其自己的内容。管理员用户可以修改其自己的内容及其共享内容。

前提条件

验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 导航到**交互式分析**选项卡。

2 在“字段”窗格的顶部，单击**管理提取的字段** 并从列表中选择提取的字段。

3 单击**复制**以创建此字段的副本。

4 （可选）在“字段”窗格中修改“提取的值”正则表达式。

5 （可选）在“字段”窗格中修改“上文”和“下文”正则表达式。

6 （可选）单击 **添加其他上下文**以添加其他关键字和筛选器。

可以添加一个或多个关键字，并将单个静态字段用作筛选器。

7 如果是管理员用户，请从下拉菜单中选择哪些用户可以访问该字段。

选项	描述
所有用户	所有用户都将在其事件中和筛选器下拉菜单中看到该字段。
只是我	只有字段的创建者会在其事件中和筛选器下拉菜单中看到该字段。

8 单击**保存**。

下一步

您可以使用已提取字段来搜索和筛选日志事件的列表，或在“交互式分析”图表中聚合事件。

如果不再需要，可以修改或删除已保存字段的定义。

删除已提取字段

可以删除不再需要的已提取字段。

vRealize Log Insight 可以创建您在创建小组件、查询或警示时使用的字段的副本。如果删除在小组件、查询或警示中使用的字段，则 vRealize Log Insight 会为使用已删除字段的每个小组件、查询或警示创建此字段的临时副本。

您只可以删除名称旁带有**编辑此字段**图标 的字段。普通用户仅可以删除其自己的内容。管理员用户可以删除其自己的内容及其共享内容。

内容包字段是只读的。

前提条件

验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 导航到**交互式分析**选项卡。

2 在“字段”窗格顶部，单击**管理已提取字段**  ，并将鼠标悬停在列表中的某个已提取字段上。

3 单击  。

此时将显示一个对话框，其中会列出使用要删除字段的内容。如果您是管理员用户，且此字段由多个用户共享，则此对话框还会列出受影响的用户。

4 单击**删除**以进行确认。

如果在现有查询中使用了已删除字段，则 vRealize Log Insight 会创建此字段的临时副本，并在您加载使用已删除字段的查询时显示它。

如果导出包含临时字段的内容，则 vRealize Log Insight 会在导出的内容包中创建这些字段，以避免使用临时字段。

管理搜索查询

可以导出查询结果，与其他用户共享查询，以及保存、删除、重命名和加载现有查询。可以生成查询快照并将其保存到仪表板。

在 vRealize Log Insight 中保存查询

可以在 vRealize Log Insight 中保存当前查询和时间范围以便以后查看。仅可以从**交互式分析**页面中加载已保存的查询。

前提条件

验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 在**交互式分析**选项卡上，执行要保存的查询。

2 单击**将当前查询添加到收藏夹**图标  。

3 键入名称，然后单击**保存**。

> **注意** 已保存查询包括固定时间范围，且不会更新。通过保存查询，您可以在保存时生成此时间范围内可用的日志消息的快照。

查询即会添加到“常用查询”列表中。

包括管理员在内的所有用户都有一个已保存查询的单独列表。

在 vRealize Log Insight 中重命名查询

可以在 vRealize Log Insight 中更改已保存查询的名称。

前提条件

验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 导航到**交互式分析**选项卡。

2 单击常用查询图标 ⭐

3 指向要重命名的查询，然后单击**编辑此保存查询**图标 ✏️。

4 键入新名称，然后单击**保存**。

在 vRealize Log Insight 中加载查询

可以加载内容包中的查询或已保存的查询，以在**交互式分析**选项卡上查看它们。

已保存的查询独立于仪表板项目。它们不显示在任何自定义仪表板上。如果要查看已保存的查询，必须加载它。

包括管理员在内的所有用户都有一个已保存查询的单独列表。

前提条件

验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 导航到**交互式分析**选项卡。

2 单击常用查询图标 ⭐

3 在“常用查询”列表中，单击要在**交互式分析**选项卡上查看的查询。

将在**交互式分析**选项卡上加载此查询。查询的时间范围将显示在事件列表上方。

下一步

可以将此查询添加到仪表板，更改图表的粒度，或向查询结果应用其他筛选。

从 vRealize Log Insight 中删除查询

可以从 vRealize Log Insight 中删除已保存的查询。

前提条件

验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 导航到**交互式分析**选项卡。

2 从**搜索**按钮右侧的下拉菜单中，选择**加载查询**。

3 单击常用查询图标 

4 在“常用查询”列表中，单击 要删除的查询旁边的  。

5 单击**删除**以进行确认。

共享当前查询

可以向您的同事发送当前查询的链接。

前提条件

验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 在**交互式分析**选项卡上，执行要共享的查询。

2 单击  并选择**共享查询**。

vRealize Log Insight 会为查询创建并显示缩短的 URL。该 URL 会在最后一次使用后保留 93 天，之后将被删除。

3 复制此 URL，并将其发送给要与其共享的人。

导出当前查询

可以导出日志查询的结果以与其他系统共享，或将其转发给您的支持联系人。

前提条件

验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 在**交互式分析**选项卡上，执行要导出的查询。

2 单击  ，然后选择**导出事件结果**。

3 选择保存查询要使用的格式，然后单击**导出**。

菜单项	描述
原始事件	选择以使用 TXT 格式保存结果
JSON	选择以使用 JSON 格式保存结果
CSV	选择以使用 CSV 格式保存结果

生成查询快照

您可以在 vRealize Log Insight 中生成当前查询和时间范围的快照，以方便快速查看或保存到仪表板。可从交互式分析页面生成快照。

快照可以保存生成快照时的时间范围内可用的日志消息。生成快照后，单击快照可返回到生成快照的查询。如果要保存一个或多个快照，请将它们添加到现有仪表板或新建一个仪表板。

前提条件

验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 在**交互式分析**选项卡上，执行要保存为快照的查询。

2 单击快照图标。

该快照将显示在屏幕底部。

3 （可选）更改查询，并生成其他快照。

这些快照将显示在屏幕底部。

4 （可选）在屏幕的底部，单击 并选择**全部保存到仪表板**。

a 选择现有仪表板或新建一个仪表板。

b 单击**添加**。

快照将添加到选定的仪表板或新仪表板。

5 （可选）单击某个快照上的“X”可将其删除。

6 （可选）单击 并选择**全部删除**可删除所有快照。

vRealize Log Insight 查询结果故障排除

仪表板小组件旁边或“交互式分析”页面上的警告图标指示所显示的数据可能存在问题。

当 vRealize Log Insight 必须处理数量庞大的日志事件以提供准确的结果时，可能会出现问题。有时，一小部分收集的日志会由于未进行处理，而未包含在最终结果中。根据当时的 vRealize Log Insight 负载及其必须为查询处理的日志数量，已进行处理的日志数量和查询结果可能会有所不同。

对于包含 group-by 子句、涵盖大量日志或返回数量相对庞大的结果的查询，可能会出现这种情况。

您可以通过替换生成时间序列结果而不是单个值的查询来解决此问题。此类型的查询可生成更准确的结果，因为查询处理不受日志量的影响。

使用仪表板

vRealize Log Insight 中的仪表板是图表、字段表和查询列表小组件的集合。

自定义仪表板

自定义仪表板由当前 vRealize Log Insight 实例的用户创建。自定义仪表板分为两类，即“我的仪表板”和“共享仪表板”。“共享仪表板”对 vRealize Log Insight 实例的所有用户可见。

“我的仪表板”是特定于用户的。

普通用户仅可以修改“我的仪表板”部分中的仪表板。

管理员用户可以修改“我的仪表板”部分中的仪表板以及他们在“共享仪表板”部分中创建的仪表板。

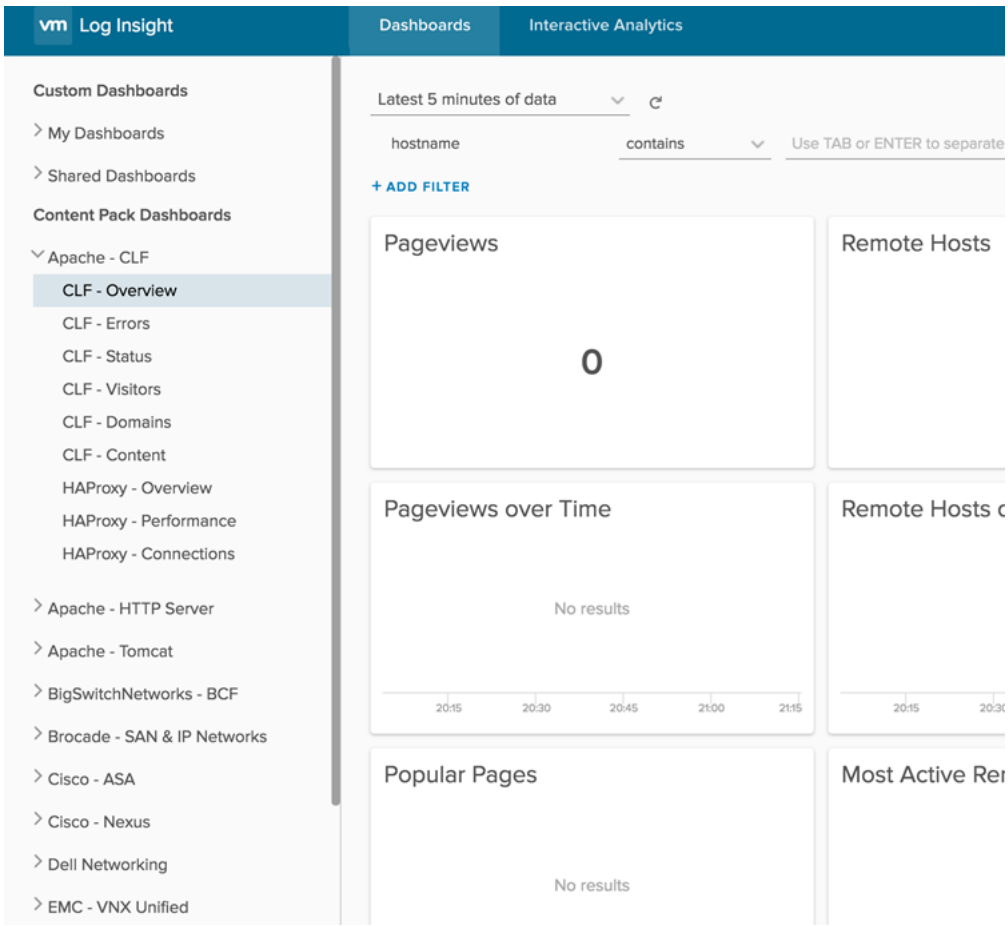
内容包仪表板

内容包仪表板可以随内容包一起导入，且对 vRealize Log Insight 实例的所有用户可见。

注意 内容包仪表板为只读。无法将其删除或重命名。但是，可以将内容包仪表板克隆到自定义仪表板。可以克隆整个仪表板或单个小组件。

要查看在您的 vRealize Log Insight 实例中提供的仪表板，请单击 vRealize Log Insight 用户界面左上角的**仪表板**。显示的左窗格列出了您可以访问的所有仪表板，这些仪表板按“自定义仪表板”和“内容包仪表板”进行分组。可以单击每个子组旁边的 **>** 显示关联的仪表板。可以单击组名称旁边的 **>** 每次打开一个仪表板组。可以单击另一个组名称旁边的 **>** 打开一个新组并关闭以前的组。每次只能打开一个组。

要查看仪表板的内容，请单击左侧列表中的仪表板名称。



管理仪表板

可以在“自定义仪表板”空间中添加、修改和删除仪表板。

内容包仪表板是您下载的预建仪表板，无法进行修改，但可以将这些仪表板克隆到“自定义仪表板”空间中，然后修改这些克隆。

重要事项 vRealize Log Insight 不会对您保存或克隆的仪表板、查询和警示的重复名称执行检查。vRealize Log Insight 保存查询时，显示名称不是唯一标识符。因此，可以使用相同名称保存多个图表、警示和仪表板。为了使数据更易于检索，请勿在保存图表、警示或仪表板时复制名称。

使用自定义仪表板

下表列出了可用于创建或修改自定义仪表板的产品功能。

任务	步骤
创建自定义仪表板。	在**仪表板**选项卡上，选择**我的仪表板**，然后单击左下角的**新建仪表板**。
编辑自定义仪表板的名称。	在**仪表板**选项卡上，指向仪表板名称，单击菜单图标 并选择**重命名**。输入新名称，然后单击**保存**。

任务	步骤
删除自定义仪表板。	在**仪表板**选项卡上，指向仪表板名称，单击菜单图标 并选择**删除**。在确认对话框中，选择**删除**。
将内容包中的仪表板克隆到自定义仪表板。	1 在**仪表板**选项卡上，选择内容包，然后指向要克隆的仪表板。 2 单击菜单图标 并从下拉菜单中选择**克隆**。 3 键入名称，然后单击**保存**。 如果您是管理员用户，则可以选择是否与其他用户共享仪表板。
向仪表板中添加图表小组件。	1 在**交互式分析**选项卡的左上角，单击**添加到仪表板**。或者，从**搜索**按钮右侧的菜单中，选择**将当前查询添加到仪表板**。 2 键入名称，从下拉菜单中选择目标仪表板，选择小组件类型，添加有关小组件的信息，然后单击**添加**。
向仪表板中添加查询列表小组件。	请参见向仪表板中添加查询列表小组件。
向仪表板中的查询列表小组件添加查询。	请参见向仪表板中的查询列表小组件添加查询。
向仪表板中的字段表小组件添加查询。	请参见向仪表板中添加字段表小组件
向仪表板中添加事件类型小组件。	将事件类型小组件添加到仪表板
向仪表板中添加事件趋势小组件。	将事件趋势小组件添加到仪表板
从仪表板中删除小组件。	1 在**仪表板**选项卡上，选择包含要删除的小组件的自定义仪表板。 2 在小组件右上角，单击**其他操作**图标 ，然后选择**删除**。 3 在“删除小组件”对话框中，单击**删除**以进行确认。
为所有小组件显示时间已同步的数据。	默认情况下，可以通过将光标悬停在小组件中的某个给定数据点上，来显示该点的图例标签。您还可以通过启用**显示所有小组件的图例**设置，来同时显示所有小组件的图例标签，该设置适用于所有仪表板。该设置基于 Cookie，可跨浏览器会话持久保留。 1 在**仪表板**选项卡上，选择一个仪表板。 2 在仪表板的左上角，将**在所有小组件上显示图例**的切换开关设置为活动。
对显示警告符号的小组件进行故障排除。	请参见 vRealize Log Insight 查询结果故障排除。

向仪表板中添加查询列表小组件

可以通过创建查询列表小组件将搜索查询的列表保存到自定义仪表板中。

前提条件

验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 在**交互式分析**选项卡上，运行要添加到仪表板的查询。

2 单击**将当前查询添加到仪表板**图标 。

3 从**仪表板**下拉菜单中，选择要向其添加查询的仪表板。

4 从**小组件类型**下拉菜单中选择**查询列表**。

5 从**查询列表**下拉菜单中，选择**新建查询列表**，键入此列表的名称，然后单击**保存**。

6 单击**添加**。

查询列表小组件即会显示在您指定的仪表板上。

下一步

可以向创建的查询列表小组件中添加查询。请参见向仪表板中的查询列表小组件添加查询。

向仪表板中的查询列表小组件添加查询

通过查询列表小组件，可以快速访问仪表板中的一个或多个已保存查询。

可以修改自定义查询列表小组件以添加新查询。

前提条件

验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 在**交互式分析**选项卡上，运行要添加到查询列表小组件的查询。

2 单击**将当前查询添加到仪表板**图标  。

3 从**仪表板**下拉菜单中，选择包含此查询列表小组件的仪表板。

4 从**小组件类型**下拉菜单中选择**查询列表**。

5 从**查询列表**下拉菜单中，选择要向其添加查询的小组件的名称，然后单击**保存**。

6 单击**添加**。

vRealize Log Insight 即会将此查询添加到您选择的小组件中。

注意 查询列表小组件使用消息查询。如果在图表小组件中使用相同的消息查询并选择任何消息中均不存在的分组依据字段，则此图表将不会显示任何结果。

向仪表板中添加字段表小组件

通过字段表小组件，可以快速访问仪表板中的一个或多个已保存字段。

前提条件

验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 在**交互式分析**选项卡上，运行要添加到字段表小组件的查询。

2 单击**将当前查询添加到仪表板**图标  。

3 从**仪表板**下拉菜单中，选择要向其添加字段表的仪表板。

4 从**小组件类型**下拉菜单中选择**字段表**。

5 选择要在字段表中包括的字段。

6 单击**添加**。

字段表小组件即会显示在您指定的仪表板上。

将事件类型小组件添加到仪表板

事件类型小组件允许访问各个事件类型分组，这些分组是通过机器学习将相似事件归为一组来创建的。

前提条件

验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 在**交互式分析**选项卡上，运行要添加到小组件的查询。

2 单击**将当前查询添加到仪表板**图标  。

3 从**仪表板**下拉菜单中，选择要向其添加小组件的仪表板。

4 从**小组件类型**下拉菜单中，选择“事件类型”。

5 单击**添加**。

该小组件即会显示在您指定的仪表板上。

将事件趋势小组件添加到仪表板

事件趋势小组件允许访问有关事件趋势的信息，它们可分析指定时间段内的趋势。

前提条件

验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 在**交互式分析**选项卡上，运行要添加到小组件的查询。

2 单击**将当前查询添加到仪表板**图标  。

3 从**仪表板**下拉菜单中，选择要向其添加小组件的仪表板。

4 从**小组件类型**下拉菜单中，选择“事件趋势”。

5 单击**添加**。

该小组件即会显示在您指定的仪表板上。

使用图表中的字段值筛选

可以使用图表中的字段值作为包含此图表的仪表板、使用此字段的另一个仪表板以及“交互式分析”上的筛选器。

如果您在图表中看到有关字段值的问题，则可以快速使用此字段值作为输入，并跳至使用此字段的另一个仪表板。如果没有其他仪表板使用此字段，则可以在同一仪表板上使用此字段值作为筛选器，或在“交互式分析”中运行它。

前提条件

验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 从**仪表板**下拉菜单中，选择包含图表小组件的仪表板。

2 在图表小组件中，将鼠标悬停在图表数据上，并查看显示为工具提示的字段值。

3 单击要用作筛选器的字段值。

此时将显示**添加值作为筛选器**菜单。

4 选择要使用此字段值作为筛选器的位置。

选项	操作
交互式分析	“交互式分析”页面将打开并显示图表查询的结果。您在步骤 3 中选择的字段值将用作筛选器。
此仪表板	您在步骤 3 中选择的字段值将用作同一仪表板上的筛选器。
其他仪表板	您在步骤 3 中选择的字段值将用作包含此字段的另一个仪表板上的筛选器。

使用内容包

内容包包含与特定产品或日志集相关的仪表板、已提取字段、已保存查询和警示。

要查看系统上加载的内容包，请从 vRealize Log Insight 用户界面右上角的下拉菜单中选择**内容包**。

要查看内容包的内容，请单击左侧列表中的内容包。

内容包

“内容包”类别包含导入的仪表板、已提取字段、查询和警示的集。默认情况下，会导入“常规”内容包和 VMware - vSphere 内容包。

注意 内容包仪表板为只读。无法将其删除或重命名。但是，可以将内容包仪表板克隆到自定义仪表板。可以克隆整个仪表板或单个小组件。

自定义内容

“自定义内容”类别包含在当前 vRealize Log Insight 实例中创建的仪表板、已提取字段和查询。“我的内容”部分包含当前登录用户的自定义内容。“共享内容”部分包含在 vRealize Log Insight 的所有用户之间共享的内容。

只有管理员用户可以与其他用户共享内容。只有管理员用户可以管理共享内容。

注意 无法从“自定义内容”部分中卸载内容。如果要从“自定义内容”部分中移除已保存的信息，必须删除各个元素（如仪表板、查询、警示和字段）。

安装内容包商城中的内容包

您无需离开 vRealize Log InsightUI 即可安装内容包商城中的内容包。

前提条件

验证是否已以具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log-insight-host*，其中 *log-insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1. 从右上角的下拉菜单中，选择**内容包**。
2. 在左侧的**内容包商城**中，单击**商城**。
3. 单击要安装的内容包。
4. 选中相应的复选框以接受任何许可协议的条款。
5. 单击**安装**。

在安装完成后，内容包将显示在左侧的“已安装的内容包”列表中。

更新已从内容包商城安装的内容包

您无需离开 vRealize Log Insight 即可更新已从内容包商城安装的内容包。

注意 启用内容包警示后，警示会被复制到用户的配置文件。用户可以修改副本的描述或条件。从 4.0 中实例化的警示定义开始，更新内容包，仍至更新其警示定义，都会更新或移除这些副本以匹配改进的内容包。如果您希望保留任何用户修改，请先将修改内容导出为内容包，然后在更新之后再导回到用户配置文件。

前提条件

验证是否已以具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log-insight-host*，其中 *log-insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 从右上角的下拉菜单中，选择**内容包**。

2 从左侧的菜单中，选择**更新**，以查看有更新可用的内容包列表。

- 要更新单个内容包，请单击其图标以打开信息窗口。单击**更新**以开始导入。根据内容包的不同，在导入完成后，您可能会看到进一步说明。如果显示这些说明，请按照配置步骤成功完成升级。
- 要以静默方式使用挂起的更新来更新所有内容包，请单击**全部更新**。阅读信息弹出窗口中的说明，然后单击**更新**以继续。升级后，单击每个内容包，以查看在导入后成功完成升级的进一步配置步骤。如果已导出内容包以保留用户修改，请将其导回到用户配置文件。

更新的内容包将显示在左侧的“已安装内容包”列表中。

导入内容包

您可以导入内容包，以将用户定义的信息与其他 vRealize Log Insight 实例进行交换，或利用更高版本来升级旧内容包。

您只能导入 vRealize vRealize Log Insight 内容包 (vRealize Log Insight Content Pack, VLCP) 文件。

注意 如果您导入现有内容包的新版本，且该新版本包含已修改字段定义，则使用已修改字段的所有查询、警示和图表都会更新以反映新的定义。

启用内容包警示后，警示会被复制到用户的配置文件。用户可以修改副本的描述或条件。从 4.0 中实例化的警示定义开始，更新内容包，仍至更新其警示定义，都会更新或移除这些副本以匹配改进的内容包。如果您希望保留任何用户修改，请先将修改内容导出为内容包，然后在更新之后再导回到用户配置文件。

您还可以从 VMware Solutions Exchange（网址为 https://marketplace.vmware.com）中下载内容包。在“内容类型”列表下查找 vRealize Log Insight 内容包，然后将其作为内容包进行安装

前提条件

- 如果要将“作为内容包安装”作为导入方法，请确认您以具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log-insight-host*，其中 *log-insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。
- 如果要使用“导入到‘我的内容’”，您可以使用任何权限级别登录到 vRealize Log InsightWeb 用户界面。

步骤

1 从右上角的下拉菜单中，选择**内容包**。

2 在左下角单击**导入内容包**。

3 选择导入方法。

选项	描述
作为内容包安装	内容会导入为只读内容包，该内容包对 vRealize Log Insight 实例的所有用户可见。 **注意** 内容包仪表板为只读。无法将其删除或重命名。但是，可以将内容包仪表板克隆到自定义仪表板。可以克隆整个仪表板或单个小组件。
导入到“我的内容”	内容作为自定义内容导入到您的用户空间，该内容仅对您可见。您可以编辑导入的内容，而无需克隆它。 **注意** 内容包元数据（比如名称、作者、图标等）不会在此模式中显示。 一旦将内容包导入到“我的内容”中，则无法将内容包作为包进行卸载。如果要从“我的内容”中移除内容包，则必须分别移除其各个元素（如仪表板、查询、警示和字段）。

普通用户仅可在其自己的用户空间中导入内容包。

4 浏览您要导入的内容包，然后单击**打开**。

5 单击**导入**。

如果您选定了作为自定义内容导入的选项，则会向您显示一个对话框，便于您选择要导入的内容。

6 （可选）如果您选择了导入为自定义内容，则使用复选框可选择要导入的项，然后再次单击**导入**。

注意 也会导入用于导入的查询、图表和警示中的字段。

7 （可选）对于某些内容包，如果首次导入内容包，将会在导入完成后看到安装说明弹出窗口。请按照这些说明完成内容包安装。

8 （可选）对于某些内容包，如果以升级方式导入内容包，将会在导入完成后看到升级说明弹出窗口。请按照这些说明完成内容包安装。

导入的内容包可以直接使用，并显示在左侧的“内容包”或“自定义内容”列表中。

注意 默认情况下，导入的警示处于禁用状态。请参见启用警示查询。

导出内容包

可以将您的自定义仪表板、已保存查询、警示和已提取字段导出为内容包，以在 vRealize Log Insight 实例间或与社区中的 vRealize Log Insight 用户共享内容。

内容包另存为 vCenter vRealize Log Insight 内容包 (VLCP) 文件。

用于您导出的查询、图表和警示中的所有字段均包括在导出的内容包中。

如果导出内容包含临时字段，则 vRealize Log Insight 会在导出期间在内容包中创建这些字段。

步骤

1 从右上角的下拉菜单中，选择**内容包**。

2 单击要导出的内容包，然后从内容包名称旁的下拉菜单  中选择**导出**。

3 （可选）选择要包括在内容包中的内容。

注意 您无法取消选择用于为导出所选择的仪表板、查询或警示的字段。

4 在右侧文本字段中，为您的内容包填充元数据。

选项	描述
名称	当您将包导入到 vRealize Log Insight 实例中时，会显示名称。内容包文件名派生自**名称**文本框。建议的格式为*供应商* - *产品* 例如，VMware - vSphere。
版本	如果计划升级此内容包，请键入版本。如果尝试安装已存在于“内容包”列表中的内容包，则 vRealize Log Insight 会显示版本。
命名空间	命名空间是内容包的唯一标识符。使用反向 DNS 命名，例如 **com.companyname.contentpackname**。
Author	也可以选择键入您的名称或贵公司名称。
网站	也可以选择提供指向与内容包相关联网站的链接。可查看内容包的所有用户也均可看到网站链接。
描述	或者，您可以提供有关包的内容和目标相关信息。
图标	您也可以选择浏览要显示在内容包名称旁边的图标。 **注意** 图标文件格式必须为 PNG 或 JPG，且在大小上将扩展为 144 x 144 像素。

注意 仅当通过使用**作为内容包安装**选项来导入内容包时，此数据才可见。如果选择将内容包导入为自定义内容，则您无法查看此信息。

5 单击**导出**，浏览到要保存文件的位置，然后单击**保存**。

导出的 VLCP 文件下载到选定位置。

查看有关内容包元素的详细信息

可直接从“内容包”视图中打开用于构建仪表板的查询，或打开字段、查询和警示的定义。

您可能希望使用内容包元素的定义作为自定义定义的模板。

步骤

1 从右上角的下拉菜单中，选择**内容包**。

2 选择包含要查看的元素的内容包。

3 单击要查看的元素类型对应的按钮。

例如，单击**警示**可查看内容包包含的所有警示。

4 在元素列表中，单击要查看的元素的名称。

交互式分析页面将打开并显示与选定元素对应的查询。

下一步

可以修改内容包元素的查询或定义，并将其保存到自定义内容中。

卸载内容包

您可以卸载内容包。卸载内容包将移除自定义仪表板、已保存查询、警示和已提取字段。

内容包另存为 vCenter vRealize Log Insight 内容包 (VLCP) 文件。

内容包经卸载后，所有用户将永久无法使用。先将内容包导出为 VLCP 文件进行备份。请参见导出内容包。

前提条件

验证是否已以具有**编辑管理员**权限的用户身份登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log-insight-host*，其中 *log-insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 从右上角的下拉菜单中，选择**内容包**。

2 单击要卸载的内容包，然后从内容包名称旁的下拉菜单 中选择**卸载**。

3 单击**卸载**。

该内容包已从“已安装的内容包”列表中移除。

创建内容包

任何 Log Insight 用户都可以创建内容包以供私人或公共使用。

内容包是 vRealize Log Insight 中的不可变或只读插件，提供有关特定类型事件（如日志消息）的预定义知识。内容包的目的是以管理员、工程师、监控团队和执行者易于理解的格式提供有关特定事件集的知识。

内容包提供了有关产品或应用程序健康状况的信息。此外，内容包还有助于您了解产品或应用程序的工作方式。

可以通过使用 vRealize Log Insight 中的“仪表板”或“交互式分析”页面来保存内容包中的信息。内容包中的信息包括：

- 查询 - 通常，内容包针对每个仪表板包含至少三个查询和三个图表小组件，这意味着查询总数超过九个
- 字段 - 内容包应至少具有二十个已提取字段
- 聚合
- 警示 - 每个内容包至少包含五个警示
- 仪表板 - 每个内容包中至少具有三个仪表板
- 仪表板筛选器 - 请参见搜索和筛选日志事件
- 可视化 - 请参见使用“交互式分析”图表分析日志

默认情况下，vRealize Log Insight 随附 VMware - vSphere 内容包。如果需要，可以导入其他内容包。

内容包术语

内容包创建工作流基于多个概念和术语。您应熟悉它们，以便有效地创建和维护内容包。

实例

只有 vRealize Log Insight 管理员可以将内容包文件作为内容包导入。如果将内容包文件作为内容包导入，则无法编辑此文件。

所有用户都可以将内容包文件导入到用户空间中。如果将内容包文件导入到用户空间中，此操作可选择性导入“我的内容”下的对象。将内容包导入到用户空间中时，可以在 vRealize Log Insight 实例中编辑内容包。如果要发布或修改内容包，则需要使用导出的内容包。

用户

可以通过“自定义仪表板”（也称为用户空间，更具体地说是“仪表板”页面上的“我的仪表板”或“共享仪表板”）下保存的内容在某种程度上创建内容包。虽然可以选择性导出自定义仪表板中的对象，但是建议每个单独内容包应由 vRealize Log Insight 中的单独用户实体来编写，以确保每个内容包具有一个干净的用户空间。

有关在 vRealize Log Insight 中创建用户的信息，请参见《VMware vRealize Log Insight 管理指南》。

为您创建的每个内容包使用 vRealize Log Insight 中的单独内容包作者用户。

事件

必须在尝试创建内容包之前收集相关事件，以确保内容包中包含产品或应用程序的所有相关事件。收集相关事件的一个常见方法是咨询质量保证和支持团队，因为这些团队通常可以访问并了解常见事件。

在创建内容包时尝试生成事件是非常耗时的，且会导致重要事件丢失。如果 QA 和支持团队无法提供事件，则可以在产品或应用程序事件已知且已记录的情况下模拟事件并使用它们来代替。

收集相应日志后，必须将它们载入 vRealize Log Insight 中。

作者

内容包的作者需要具备下列资格：

- VMware vRealize Log Insight 的使用经验。
- 产品或应用程序的实际操作知识。
- 了解并能够生成优化的正则表达式。
- 使用日志调试产品或应用程序的多个问题的经验。
- 支持背景，接触过无数问题。
- 系统管理员背景，拥有 syslog 经验。

工作流

建议的内容包创建方法是，首先在“交互式分析”页面上开始查询特定类型的事件（如错误或警告）。查看查询结果，然后根据需要分析并提取潜在的字段候选者。对事件类型和事件中提供的有用信息有一定了解后，根据需要构建并保存相关查询。对于强调需要快速操作的问题的查询，创建并保存警示。保存查询时，使用筛选将其从结果列表中移除，以显示可能是新保存查询的潜在候选事件的其他事件。保存所有相关查询后，在“仪表板”页面上以逻辑方式组织和显示它们。

查询

vRealize Log Insight 中的查询可以检索和概述事件。

可以从“交互式分析”页面中创建并保存查询。查询包含下列一项或多项：

关键字	完整字符或全文、字母数字、连字符和/或下划线匹配。
通配符匹配操作符	完整字符或全文、字母数字、连字符和/或下划线匹配。
正则表达式	基于 Java 正则表达式的复杂字符串模式匹配。
字段运算	应用于已提取字段的关键字、正则表达式和模式匹配。
聚合	应用于一个或多个结果子组的函数。

vRealize Log Insight 支持以下类型的查询：

- 消息。由关键字、正则表达式和/或字段运算组成的查询。
- 正则表达式或字段。由关键字和/或正则表达式组成的查询。
- 聚合。由函数、一个或多个分组和任何数目的字段组成的查询。

可以在 vRealize Log Insight 中定义自定义警示，并从任何类型的调度查询中触发它们。

创建消息查询的最佳做法

创建消息查询的基本概念。

可以通过使用搜索栏或通过输入筛选来输入消息查询。

使用搜索栏可在 vRealize Log Insight 实例中细化事件的结果。虽然可以使用筛选来代替搜索栏，但是利用搜索栏的查询通常比利用等效筛选的查询更易于理解。最佳做法是，尽可能使用搜索栏来代替等效筛选。

筛选允许您通过使用正则表达式、字段、逻辑 OR 运算或搜索栏和筛选查询的组合来创建查询。

通过使用搜索栏和筛选创建查询时，适用以下最佳做法：

- 确保查询不是特定于环境的。公用内容包需要通用于任何环境，因此不需要依赖于环境特定的信息。环境特定的信息示例包括源、主机名和潜在设施（如果设施使用 *local**）。
- 构建查询时，如果可能请使用关键字，如果关键字不足请使用通配符匹配操作符，如果通配符匹配操作符不足请使用正则表达式。关键字查询是耗资源最少的查询类型。通配符匹配操作符是简化版的正则表达式，是耗资源较少的查询类型。正则表达式是耗资源最多的查询类型。
- 使用正则表达式或字段时，请提供尽可能多的关键字。如果正则表达式包括逻辑 OR（例如 *this*|*that*），则不要包括关键字。vRealize Log Insight 已经过优化，可在正则表达式之前执行关键字查询，以便最大程度减少正则表达式开销。

字段查询

字段是向非结构化事件添加结构的强有力方式，允许操控数据的文本和可视化表示形式。

字段是内容包中的最重要项目之一，因为可以通过不同的方式（包括聚合和筛选）使用它们。通过聚合可以向字段应用函数和分组。通过筛选可以对字段执行运算。

必须提取日志消息中可能适用于查询或聚合的任何部分。字段是一种正则表达式查询且对复杂模式匹配是非常有用的，因此您无需了解、记住或学习复杂的正则表达式。

字段上下文值	定义
值前面的正则表达式	包括尽可能多的关键字。如果此字段为空或仅包含特殊字符，则值后面的正则表达式必须包括关键字。
值后面的正则表达式	包括尽可能多的关键字。如果此字段为空或仅包含特殊字符，则值前面的正则表达式必须包括关键字。
名称	仅使用字母数字字符。确保所有字符都是小写的且使用下划线而不是空格，因为这使字段更易于查看。请记住，内容包字段和用户字段的名称可以相同，但是内容包字段将在字段名称右侧具有一个用括号括起的命名空间。在内容包字段前面添加缩写（例如 vmw_）作为前缀，以避免出现混淆。
关键字搜索项	以空格分隔的一个或多个关键字，显示在包含此字段的事件中。
筛选	显示在包含此字段的事件中的静态字段、运算符和可能值。 通常将其与不包含关键字的事件的 vRealize Log Insight 代理和标记一起使用。
信息（“i”按钮）	用于提供有关字段的信息，包括其含义、可能返回的值，以及值与人工可理解信息之间的用户友好的映射。

最佳做法

除了组成字段的各种要素之外，还有多个最佳做法适用。

- 仅为正则表达式模式创建字段。如果可以使用关键字查询来查询字段，或者字段将仅返回单个值，则使用关键字查询而不是预定义的字段。如果字段将仅返回两个值，则考虑构建单独查询，而不是提取字段。字段可用于向未结构化数据添加结构，并提供了一种查询事件特定部分的方式。
- 仅为返回全部事件的一部分的正则表达式模式创建字段。将匹配大多数事件和/或返回大量结果的字段不适合进行字段提取。正则表达式将需要应用于在耗费大量资源的操作中产生的大量事件。如果可能，添加其他关键字以减少返回的结果数并优化查询。
- 如果字段在正则表达式语法中包含关键字，则在没有正则表达式语法的情况下将这些关键字作为筛选进行添加。例如，如果字段的值或上下文在正则表达式语法中包含关键字（如 *this|that*），则将这些关键字作为文本筛选进行添加，以优化查询（如 **`text contains this, that`**）。
- 建议使用具有一个或多个关键字的附加上下文，而不是在之前或之后的上下文中使用复杂正则表达式。
- 向提取的所有字段添加附加上下文，以便优化查询性能。

临时字段

临时字段是作为查询的一部分存在的字段，但不会在 vRealize Log Insight 实例中全局保存或作为已安装内容包的一部分保存。

vRealize Log Insight 可以通过自动更新依赖于正修改字段的查询，来减少创建临时字段的机会。

注意 如果删除已保存查询所依赖的字段，则此已保存查询将包含临时字段。

当在“交互式分析”页面中运行已保存查询，且此已保存查询中使用的字段在字段名称右侧包含命名空间 Temporary 时，您会看到临时字段。

执行查询以包含一个或多个字段。对于 vRealize Log Insight 中的已保存查询，保存查询时使用的字段定义将会在修改此字段时得到相应修改。字段修改包括

- 更改字段值
- 更改值前面的正则表达式和字段值后面的正则表达式
- 更改字段名称
- 删除字段

导出内容包时，vRealize Log Insight 会将所有临时字段转换为内容包字段。如果在内容包中看到临时字段，则您可能正在从使用临时字段导出的先前产品版本中查看内容包，或者已手动编辑此内容包。

如果临时字段的名称与现有已提取字段的名称相同，则临时字段的末尾将显示 {n}。例如，如果有一个字段名称为 `product_test_field`，导出过程中可能还会看到 product_test_field {2}。如果看到此情况，则表明存在临时字段。要解决此问题，请选择导出对话框底部的**全部不选**选项，并选择每个仪表板和/或警示，直到选中以 {n} 结尾的提取字段。转到这些仪表板和/或警示，并编辑每个查询。发现使用已提取字段的查询时，请将筛选或聚合更改为不使用以 {n} 结尾的字段，运行查询，并保存查询。对所有使用以 {n} 结尾的字段的查询执行这些步骤后，导出过程中将不再显示此字段。

聚合查询

vRealize Log Insight 允许您使用聚合查询来操控事件的可视化表示形式。

聚合查询包含以下两个属性：

- 函数
- 分组

聚合查询需要一个函数和至少一个分组。分组是内容包的一个重要部分。函数和分组可影响图表的显示方式。

图表显示仅限于 2,000 个最新的结果。

条形图

默认情况下，vRealize Log Insight 的“交互式分析”页面中的概览图表显示一段时间内的事件计数。如果将计数函数与时间序列分组结合使用，则 vRealize Log Insight 会创建一个条形图。

如果将计数函数与单个字段分组而不是时间序列结合使用，则 vRealize Log Insight 会创建条形图，从图中可看出数量的变化分布情况。

线图

除计数函数之外的所有函数都是数学函数。它们需要一个字段，您将针对该字段应用等式。对字段执行数学函数并按时间序列分组时，vRealize Log Insight 会创建一个线图。

堆栈图

默认情况下，vRealize Log Insight 的“交互式分析”页面中的概览图表显示一段时间内的事件计数。如果将一个字段添加到时间序列分组中，则 vRealize Log Insight 会创建一个堆栈图。

如果使用按时间序列进行的分组以及字段，并使用除计数之外的任何函数，则 vRealize Log Insight 会创建堆栈线图。在尝试查找对象的异常情况时，堆栈图是非常强大的。

您必须根据聚合查询可能返回的对象数目来决定要使用哪种类型的堆栈图。显示更多对象需要更多资源，而这对解析并显示信息也是必要的。此外，颜色数目是固定的，区分各个对象可能变得具有挑战性，具体取决于返回对象的数目。通常，以下最佳做法适用

- 如果每个条形中返回对象的数目少于十个，则您可能希望使用堆栈图。
- 如果每个条形中返回对象的数目为十个或可能介于十到二十个之间，则堆栈图可能是非常合适的选择。您必须考虑在内容包中以直观的方式来表示图表。
- 如果每个条形中返回对象的数目为二十个或可能多于二十个，则不建议使用堆栈图。

多色图

如果您通过使用多个字段和时间序列来创建分组，则 vRealize Log Insight 会创建一个多色图。此图包含两种可以互换的颜色。每次互换表示一个新的时间范围。多色图可能难以理解，因此，在将其纳入内容包之前，请仔细考虑此类图表的值。

在按多个字段进行分组时，请考虑使用非时间序列。移除时间序列使条形图更易于理解。

如果有多个字段对于给定时间范围都至关重要，则可以在此时间范围内单独为每个字段创建多个图表。然后，可以在内容包内仪表板组的同一列中显示这些图表。

其他图表

可以使用一些其他图表类型，包括饼图、气泡图和表格图。要使用这些图表，需要特定的查询类型。如果这些图表的选项可用，则表明已经具有正确的查询。如果这些图表的选项不可用，请将鼠标悬停在要使用的图表的名称上。此时将弹出一条消息，描述图表类型所需的查询类型。

消息查询

构建聚合查询时，消息查询应仅返回与此聚合查询相关的结果。这使分析变得更容易，且可确保结果仅显示相关字段。要确保消息查询返回与聚合查询相同的结果，必须使用 ***exists*** 运算符为聚合查询中使用的每一个字段添加筛选器。

更改图表类型

如果要更改仪表板上小组件的图表类型，请单击小组件上的齿轮图标，并选择**编辑图表类型**。如果要更改小组件类型，请保存新的小组件并删除旧的小组件。

警示

警示提供了一种在发生特定类型的事件时触发反应的方法。

vRealize Log Insight 支持两种类型的警示

- 电子邮件
- vRealize Operations Manager

可以将这些警示仅保存在一个用户空间中。默认情况下，所有内容包警示都处于禁用状态。如果创建已启用的警示并将其作为内容包的一部分导出，则将在内容包中禁用此警示。

内容包不包含电子邮件和 vRealize Operations Manager 设置。此外，您无法向内容包中添加这些设置。

阈值

阈值可对已触发警示的数目设置限制。

必须了解阈值的工作方式，以确保内容包警示（如果已启用）不会意外地向用户发送垃圾消息。考虑使用阈值时，必须思考两个问题

- 触发警示的频率是多少？Log Insight 附带预定义频率。在给定阈值时间段内，警示将仅触发一次。
- 检查是否已发生警示状况的频率是多少？警示由查询触发。与查询一样，警示在当前版本中不是实时的。对于每个阈值时间段，分配了预定的查询频率。如果更改阈值，则查询时间也将更改。

分组

当创建电子邮件警示时，必须按一个用于确定警示源的字段进行分组。

警示所发送的电子邮件中包含特定聚合查询的结果表。您可以在“交互式分析”页面上查看查询的可视化表示形式。

如果不按唯一标识符分组，您将无法了解结果是否与您环境中的一个或多个系统相关。应按主机名字段而非源字段分组。还可以添加任何能够唯一地确定事件来源的字段。

仪表板最佳做法

仪表板属于内容包。创建仪表板时有一些适用的最佳做法。

创建仪表板时，适用以下最佳做法

- 内容包通常至少包含三个仪表板。最佳做法是从概览仪表板开始，以便为特定产品或应用程序提供有关事件的高级别信息。除了概览仪表板之外，还应基于事件的逻辑分组创建仪表板。逻辑分组是特定于产品或应用程序的，但一些常见方法是性能、故障和审核。为组件（如磁盘和控制器）创建仪表板也很常见。对于组件方法，必须注意它仅在可以构建查询以从特定组件返回结果时有效。如果这不可能实现，则建议使用逻辑方法。
- 命名仪表板时，使用通用标题并避免添加产品或应用程序特定的名称，除非以组件特定方式使用。例如，在 VMware - vSphere 内容包中，具有一个名为 ESX/ESXi 而不是 VMware ESX/ESXi 的仪表板组。
- 仪表板必须包含三个（最少）到六个（最多）仪表板小组件。如果包含的仪表板小组件少于三个，则仪表板可获得的信息量最少。此外，如果具有大量仅包含有限数量仪表板小组件的仪表板，则需要用户在不同页面之间进行切换，且无法以连贯的方式提供信息。

  相反，如果仪表板包含的仪表板小组件超过六个，则可能会产生负面影响。您可能会获得太多可导致混淆的信息。太多小组件需要密集使用系统资源，因为每个小组件都是一个必须针对系统运行的查询。

  当仪表板包含六个以上仪表板小组件时，必须对信息进行分类并创建多个仪表板。如果某个仪表板小组件适用于一个或多个仪表板，请在每个适用的仪表板中创建此小组件。

仪表板筛选器

仪表板筛选器可用于深入查看特定事件。这些筛选器的工作方式类似于“交互式分析”页面上的筛选器，利用字段来深入查看。每个仪表板都应该至少有一个仪表板筛选器，通常包含主机名字段，但最多只能向每个仪表板添加五个字段。

添加的字段应由给定仪表板上的大部分小组件使用，以便在使用仪表板筛选器时，大部分小组件能够返回结果。仪表板筛选器示例可包含一个严重性字段、一个用户字段，或者甚至一个组件字段。

注意 仪表板筛选器使用的字段和运算符将保存在导出的内容包中。导出过程中，不会保存仪表板筛选器使用的任何值，因为该值可能特定于某个环境，并不适用于所有环境。

仪表板小组件

仪表板小组件可帮助您可视化信息。

在 vRealize Log Insight 中，您可以将多种类型的小组件添加到仪表板。这些小组件包括：

- 图表小组件，包含带已保存查询链接的事件的可视化表示形式。
- 查询列表小组件，包含已保存查询的标题链接。
- 字段表小组件，包含事件，其中每个字段代表一列。
- 简化的事件类型表小组件，包含归为一组的相似事件。
- 简化的事件趋势表小组件，显示在查询中找到的事件类型列表，这些事件类型按发生次数进行排序。这便于快速了解哪些类型的事件在查询中非常频繁地发生。

图表

仪表板图表小组件包含事件的可视化表示形式。您可以采用条形图或线图形式来表示图表，且可以将其中任意一种显示为堆栈图。

可采用多种方式来表示图表：

- 图表可以包含大量信息。避免在单行中包含超过两个图表小组件。极少数情况下，可以有效地使用三个图表小组件，但强烈建议最多使用三个。在确定图表小组件是否可读时，请确保使用 vRealize Log Insight 支持的最低分辨率，即 1024 x 768 像素。
- 如果除最后一行之外的所有行都包含单个图表小组件，则使此小组件占满整个宽度
- 命名图表小组件时，请使用描述性标题并避免使用令人费解的字段名称。例如，某个已提取字段称为 `vmw_error_message`。将图表命名为“错误消息计数”，而不是“`vmw_error_message` 计数”
- 可以保存类似图表，并将其堆放在仪表板组的同一列中，以进行可视化比较。例如：
  - 一段时间内的平均事件数 X + 一段时间内的最大事件数 X。考虑到使用了不同函数，图表的 Y 轴可能具有不同的比例。
  - 一段时间内按 X 分组的事件计数 + 一段时间内按 Y 分组的事件计数。

查询列表

仪表板查询列表小组件包含一个或多个预定义查询链接。

可以出于以下原因使用查询列表小组件

- 图表小组件未提供重要值，而基础查询提供了重要值。
- 要保存复杂查询，如使用正则表达式的查询。
- 要在仪表板组内的同一基础查询上使用不同聚合。

字段表

包含事件的字段表，每个字段代表一列。

仪表板字段表小组件以表格式包含给定查询的最新事件，每个字段代表一列。

字段表小组件的用途如下。

- 查看给定查询的最新事件。对于更改管理或出于安全考虑，该小组件非常有用。
- 只查看某个给定查询中您关注的字段。对限制事件输出非常有用。

内容包导入错误

导入内容包时，可能会收到一些警告或错误消息。

升级

您可能会收到升级消息。这意味着，将在系统中安装另一个具有相同命名空间的内容包。在这种情况下，您可以进行升级并替换现有内容包，或取消升级过程并保留现有内容包。

无效格式

您可能会收到一条指明格式无效的消息。这意味着，已手动编辑 VLCP 文件，且其包含语法错误。必须在导入内容包之前修复语法错误。

更新版本

此类消息意味着，仅可在更新版本的 Log Insight 上创建并支持内容包。在版本高于 Log Insight 1.5 的产品上，看到此类消息意味着已手动编辑 VLCP 文件。

无法识别的版本

当已手动编辑 VLCP 文件且其包含语法错误时，您可能会看到此类消息。必须在尝试导入内容包之前修复语法错误。

注意 不应手动编辑 VLCP 文件。因此，很难找到并修复语法错误。

发布内容包的要求

创建并希望发布内容包时，请确保内容包满足基本的发布要求。

必须检查内容包要求和发布要求。

内容包要求

内容包必须满足一些内容、质量和标准要求。

内容要求包括

- 最少三个仪表板
- 每个仪表板最少一个仪表板筛选器，理想情况下为三个，最多为五个
- 每个仪表板最少三个仪表板小组件
- 每个仪表板最多六个仪表板小组件
- 每行最多三个仪表板小组件
- 最少五个警示
- 最少二十个已提取字段

内容包的质量要求如下

- 每个查询至少具有一个全文关键字，最好具有三个或更多个关键字
- 查询不基于环境特定的属性，如源、主机名或 *设施**
- 每个字段至少具有一个全文关键字，最好具有三个或更多个关键字
- 字段特定于产品/应用程序，且将不会为其他产品/应用程序日志返回结果
- 每个仪表板小组件必须包含有关图表显示内容及其重要原因的信息/链接

创建内容包的标准遵循以下规则

内容包部分	格式
内容包名称格式	*Company - Product*
内容包命名空间格式（必须使用命名空间导出内容包）	*Ext.Domain.Product*
已提取字段的格式	*Prefix_Field_Name* 其中 Prefix 是公司名称或公司缩写。

发布要求

发布内容包之前，检查它是否满足发布要求。使用开发人员中心的内容包发布程序获取内容包建议并将要审核的版本上载到 VMware。https://developercenter.vmware.com/web/loginsight

发布要求	描述
内容包文件格式	VLCP 文件。
事件	验证内容包所需的相应事件。
概览	概述内容包的一到两段内容。
突出显示	三处突出显示，展示内容包的价值。
描述	描述内容包及其价值的两到三段内容。
技术规格	介绍最低系统要求，包括产品版本和配置以及 Log Insight 版本和配置。此外，还提供配置产品以登录 Log Insight 和填充内容包所需的所有指示。

发布要求	描述
屏幕截图	展示包含真实数据的内容包的三个或更多屏幕截图。
视频（可选）	内容包如何引入值的示例。
白皮书（可选）	如何配置产品或应用程序以将日志转发到 vRealize Log Insight。

提交内容包

提交在 VMware Solutions Exchange 上创建的内容包。

前提条件

- 验证您的内容包是否满足发布内容包的要求。
- 如果您在 http://solutionexchange.vmware.com 上没有帐户，请单击**注册**并选择**合作伙伴**。填写《合作伙伴注册申请》表单，然后提交。如果您的登录请求获得批准，则将收到通知电子邮件。

步骤

1. 转到 http://solutionexchange.vmware.com，然后单击页面右上角的**立即登录**。
2. 输入用户名和密码，然后单击**立即登录**。
3. 单击**管理**，然后选择**管理解决方案**以添加或编辑解决方案。
4. 单击**添加解决方案**，然后填写所需信息。

   经常使用**保存草稿**按钮，以确保不会丢失任何工作。
5. 单击**提交供审批**。

   您的解决方案将会发送到 VMware Solution Exchange 联盟团队，以进行审核和批准。

您将收到一封有关解决方案审批状态的电子邮件。

下一步

有关完成解决方案列表的详细信息，请单击页面顶部的**合作伙伴之角链接**。如果找不到所需的信息，请联系 VSXAlliance@vmware.com 解决任何问题。

vRealize Log Insight 中的警示查询

可以将 vRealize Log Insight 配置为以调度的时间间隔运行特定查询。

如果与查询匹配的事件数目超过已设置的阈值，则 vRealize Log Insight 会发送电子邮件或 Webhook 通知并在 vRealize Operations Manager 中触发通知事件。

要查看可用警示的列表，请导航到“交互式分析”页面，然后从**搜索**字段旁边的**创建和管理警示...**下拉菜单中选择**管理警示...**。每个警示的状态显示在警示名称下方。

注意 警示查询是用户特定的。仅可管理您自己的警示。您必须分配有“超级管理员”角色才能管理其他用户警示。

可以在 vRealize Log Insight 中创建的警示类型

可以通过选择一种警示类型来控制警示查询运行的时间间隔，以及 vRealize Log Insight 发送警示通知的条件。

针对任何匹配的警示	此警示查询每五分钟自动运行一次。当最后 5 分钟内至少一个事件与查询匹配时，将会触发通知。
基于事件类型的警示	此警示查询每五分钟自动运行一次。当发现指定的事件类型时，将会触发通知。
自定义时间段内基于事件数目的警示	警示查询间隔取决于设置。当最后 *Y* 分钟内发生的匹配事件数目大于或小于 *X* 时，将根据设置触发通知。 如果触发此类型的警示，则会推迟其整个时间段，以防止为同一组事件发出重复警示。如果要在推迟时启用警示，则可以禁用然后重新启用它。
基于聚合查询的警示	如果分组中的函数值超过定义的值，聚合查询警示将触发通知。如果图表中的至少一个条形在指定的时间段内高于或低于设置的阈值，您可以在图表上看到该通知。 不会可视化**一段时间内**的事件**计数**的图表设置此警示类型。

内容包警示

内容包可以包含警示查询。默认情况下，vRealize Log Insight 中包括的 vSphere 内容包包含多个预定义的警示查询。如果 ESXi 主机停止发送 syslog 数据，vRealize Log Insight 无法再从 vCenter Server 中收集事件、任务和警报数据，或者警报状态更改为红色，则它们可能会触发警示。可以使用这些警示查询作为模板来创建特定于环境的警示。

默认情况下，所有内容包警示都处于禁用状态。

启用 **vCenter Server: ESX/ESXi 停止日志记录**警示是一种很好的做法，因为特定版本的 ESXi 主机可能会在您重新启动 vRealize Log Insight 时停止发送 syslog 数据。此警示监控 vCenter Server 事件 `esx.problem.vmsyslogd.remote.failure` 来检测是否存在已停止发送 syslog 源的 ESXi 主机。有关 syslog 问题和解决方案的详细信息，请参见 VMware ESXi 5.x 主机停止向远程服务器发送 syslog (2003127)。

可以向警示查询添加以下筛选器，并将其另存为新的警示以仅检测停止向 vRealize Log Insight 实例发送源的 ESXi 主机：**vc_remote_host (VMware - vSphere) contains** *log-insight-hostname*。

内容包警示查询是只读的。要将更改保存到内容包警示，必须将此警示保存到自定义内容。

- 添加警示查询以发送电子邮件通知

  可以在 vRealize Log Insight 中配置警示查询，以便在日志中显示特定数据时发送电子邮件通知。
- 关于使用 Webhook 向第三方产品发送警示

  您可以使用 Webhook 向第三方产品发送 vRealize Log Insight 用户警示。
- 查看警示查询

  可以查看已创建的警示查询，并检查是否已为这些查询启用通知。

- 修改警示查询

  可以更改警示查询的触发器，启用或禁用查询发送的通知，或者更改通知方法（电子邮件、Webhook 或发送到 vRealize Operations Manager）。

- 启用警示查询

  禁用警示查询时，vRealize Log Insight 不会发送电子邮件或 Webhook 通知，且不会触发 vRealize Operations Manager 通知事件。

- 删除警示查询

  可以删除不再需要的警示查询。

添加警示查询以发送电子邮件通知

可以在 vRealize Log Insight 中配置警示查询，以便在日志中显示特定数据时发送电子邮件通知。

前提条件

- 验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。
- 验证管理员是否已配置 SMTP 来启用电子邮件通知。请参见为 Log Insight 配置 SMTP 服务器。

步骤

1 在**交互式分析**选项卡上，运行要为其发送通知的查询。

2 在**搜索**按钮右侧的**创建或管理警示**菜单中，单击  ，然后选择**根据查询创建警示**。

3 在“添加警示”对话框中，键入警示的名称，并为触发此警示的事件提供简短而有意义的描述。

警示名称和描述将包括在 vRealize Log Insight 发送的电子邮件中。

4 选中**电子邮件**复选框，然后键入您希望 vRealize Log Insight 向其发送通知的电子邮件地址。

使用逗号分隔多个地址。

5 设置警示阈值。

警示类型	选择
任意匹配	选择**基于任意匹配**选项。 每 5 分钟运行查询。
基于事件类型	选择**在过去 *<time period>* 中首次显示新事件类型时**选项并从下拉菜单中选择时间段。 每 5 分钟运行查询。

警示类型	选择
基于一段时间内的事件数	选择第三个选项，然后使用下拉菜单设置参数。 基于您在下拉菜单中的选择运行查询。
基于图表值	选择第四个选项，然后使用下拉菜单配置参数。 **注意** 仅当选择根据至少一个字段对事件进行分组，此警示类型才可用。无法为仅显示时间序列的图表创建此警示类型。 基于您在第二个下拉菜单中的选择运行查询。

预览图表中的橙色行显示当前阈值。

6 单击**保存**。

下一步

可以启用、禁用或删除保存的警示。

注意 警示查询是用户特定的。仅可管理您自己的警示。您必须分配有“超级管理员”角色才能管理其他用户警示。

关于使用 Webhook 向第三方产品发送警示

您可以使用 Webhook 向第三方产品发送 vRealize Log Insight 用户警示。

vRealize Log Insight 使用 Webhook 通过 HTTP POST 向其他应用程序发送警示。vRealize Log Insight 使用自己的专用格式发送 Webhook，但第三方解决方案希望入站 Webhook 使用这些解决方案自己的专用格式。要使用通过 vRealize Log InsightWebhook 发送的信息，第三方应用程序必须本机支持 vRealize Log Insight 格式，否则，您必须使用填充码在 vRealize Log Insight 格式和第三方使用的格式之间创建映射。填充码会将 vRealize Log Insight 格式转换或映射到另一种格式。

使用消息查询创建的警示、使用汇总查询创建的警示，以及系统通知每个都有自己的 Webhook 格式。

支持 HTTP 基本身份验证。请使用 {{https://*username*:*password*@*hostname*/*path*}} 格式在 url 中嵌入凭据。

vRealize Log Insight 实施 Webhook 时会向远程服务器发送出站 HTTP 请求。服务器可能会报告成功或失败。对于失败的请求，vRealize Log Insight 会重试。所有 HTTP/2*xx* 状态代码响应都将被视为成功，所有其他响应，包括超时或拒绝连接，将被视为失败，并且会在稍后重试。

您必须是 vRealize Log Insight 管理员才能创建系统通知。

添加警示查询以发送 Webhook 通知

可以在 vRealize Log Insight 中配置警示查询，以便在日志中显示特定数据时将 Webhook 通知发送到远程 Web 服务器。Webhook 通过 HTTP POST 提供事件通知。

注意 服务器可能会报告成功或失败。如果失败，vRealize Log Insight 会重试。vRealize Log Insight 将所有 HTTP/2*xx* 状态代码响应视为成功。所有其他响应，包括超时或拒绝连接，均被视为失败，并会在稍后重试。

前提条件

- 验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。
- 确认 Web 服务器已配置为接收 Webhook 通知。

步骤

1. 导航到**交互式分析**选项卡。
2. 在**搜索**按钮右侧的**创建或管理警示**菜单中，单击  ，然后选择**根据查询创建警示**。
3. 在“添加警示”对话框中，输入警示的名称，并为触发此警示的事件提供简短而有意义的描述。

   警示名称和描述将包括在 vRealize Log Insight 发送的通知中。
4. 选中 **Webhook** 复选框，然后输入您希望 vRealize Log Insight 向其发送通知的 URL。
5. 设置警示阈值。

警示类型	选择
任意匹配	选择**基于任意匹配**选项。 每 5 分钟运行查询。
基于事件类型	选择**在过去 *<time period>* 中首次显示新事件类型时**选项并从下拉菜单中选择时间段。 每 5 分钟运行查询。
基于一段时间内的事件数	选择第三个选项，然后使用下拉菜单设置参数。 基于您在下拉菜单中的选择运行查询。
基于图表值	选择第四个选项，然后使用下拉菜单配置参数。 **注意** 仅当选择根据至少一个字段对事件进行分组，此警示类型才可用。无法为仅显示时间序列的图表创建此警示类型。 基于您在第二个下拉菜单中的选择运行查询。

   预览图表中的橙色行显示当前阈值。
6. 单击**保存**。

下一步

可以启用、禁用或删除保存的警示。

注意 警示查询是用户特定的。仅可管理您自己的警示。您必须分配有“超级管理员”角色才能管理其他用户警示。

关于 vRealize Log Insight 警示的书写转换填充码

填充码用于映射各种 Webhook 格式。

vRealize Log Insight 使用其自己的专用格式发送 Webhook，但第三方解决方案希望入站 Webhook 使用这些解决方案的专用格式。这意味着第三方解决方案需要本机支持 vRealize Log Insight 格式，或者需要在 vRealize Log Insight 和第三方解决方案之间放置一个填充码，这个填充码可以将 vRealize Log Insight 格式转换为第三方格式。

下图显示了一个用户警示查询，以及为此生成的 Webhook。您可以使用此信息来更好地了解支持填充码所需的映射。

图 1-1 用户定义的警示查询

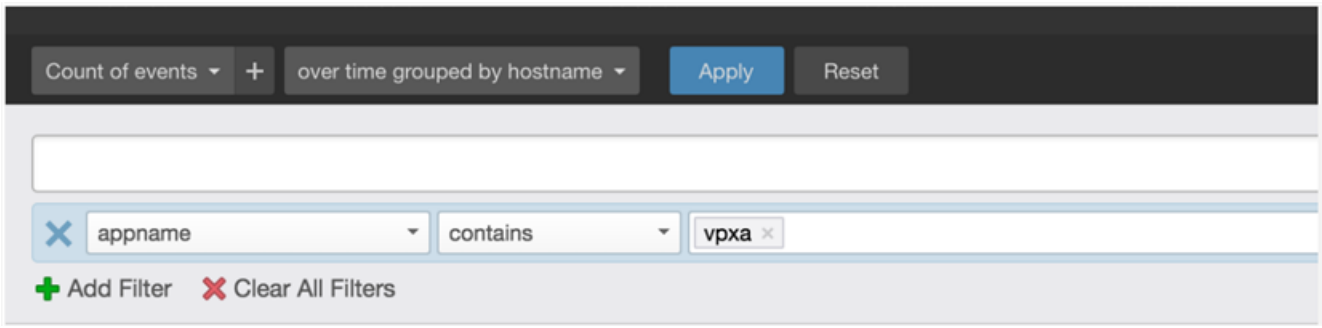


图 1-2 用户警示聚合查询的 Webhook 输出

```
{
   "AlertType":1,
   "AlertName":"ESXi Vpxa Alert",
   "SearchPeriod":300000,
   "HitCount":0.0,
   "HitOperator":2,
   "messages":[
      {
         "text":"2016-06-24T15:42:42.055Z esx01 Vpxa: [4845FB90 verbose 'VpxaHalCnxHostagent' opID=WFU-
dcfc2d3a] [WaitForUpdatesDone] Starting next WaitForUpdates() call to hostd",
         "timestamp":1451940578545,
         "fields":[
            {
               "name":"hostname",
               "content":"esx01"
            },
            {
               "name":"appname",
               "content":"vpxa"
            }
         ]
      },
      {
         "text":"2016-06-24T15:42:42.055Z esx02 Vpxa: [4845FB90 verbose 'vpxavpxaInvtVm' opID=WFU-
dcfc2d3a] [VpxaInvtVmChangeListener] Guest DiskInfo Changed",
         "timestamp":1451940561008,
         "fields":[
            {
               "name":"hostname",
               "content":"esx02"
            },
```

```
            {
               "name":"appname",
               "content":"vpxa"
            }
         ]
      }
   ],
   "HasMoreResults":false,
   "Url":"https://10.11.12.13/s/8pgzq6",
   "EditUrl":"https://10.11.12.13/s/56monr",
   "Info":"This is an alert for all the 'ESXi Vpxa' messages",
   "NumHits":2
}
```

用户警示消息查询的 Webhook 格式

vRealize Log Insight Webhook 使用的格式取决于创建它的查询类型。系统通知、用户警示消息查询，以及从聚合用户查询生成的警示每个都有不同的 Webhook 格式。

向第三方程序发送用户警示消息查询生成的警示时，必须编写一个填充码，以便让第三方程序的格式能够理解 vRealize Log Insight 信息。

用户警示消息查询 Webhook 格式

以下示例显示了用户警示消息查询的 vRealize Log Insight Webhook 的格式。

```
{
   "AlertType":1,
   "AlertName":"Hello World Alert",
   "SearchPeriod":300000,
   "HitCount":0.0,
   "HitOperator":2,
   "messages":[
      {
         "text":"hello world 1",
         "timestamp":1451940578545,
         "fields":[
            {
               "name":"Field_1",
               "content":"Content 1"
            },
            {
               "name":"Field_2",
               "content":"Content 2"
            }
         ]
      },
      {
         "text":"hello world 2",
         "timestamp":1451940561008,
         "fields":[
            {
               "name":"Field_1",
               "content":"Content 1_2"
```

```
            },
            {
               "name":"Field_2",
               "content":"Content 2_2"
            }
         ]
      }
   ],
   "HasMoreResults":false,
   "Url":"https://10.11.12.13/s/8pgzq6",
   "EditUrl":"https://10.11.12.13/s/56monr",
   "Info":"This is an alert for all the 'Hello World' messages",
   "NumHits":2
}
```

用户警示聚合查询的 Webhook 格式

vRealize Log Insight Webhook 使用的格式取决于创建它的查询类型。系统通知、用户警示消息查询，以及从聚合用户查询生成的警示每个都有不同的 Webhook 格式。

向第三方程序发送系统通知时，必须编写一个填充码，以便让第三方程序的格式能够理解 vRealize Log Insight 信息。

用户警示聚合查询的 Webhook 格式

```
{
   "AlertType":2,
   "AlertName":"field_1 aggregated alert",
   "SearchPeriod":300000,
   "HitCount":2.0,
   "HitOperator":2,
   "messages":[
      {
         "fields":[
            {
               "name":"Field_1",
               "content":"Content 1"
            }
         ]
      }
   ],
   "HasMoreResults":false,
   "Url":"https://10.11.12.13/s/r25g3s",
   "EditUrl":"https://10.11.12.13/s/n3gsed",
   "Info":null,
   "NumHits":1
}
```

查看警示查询

可以查看已创建的警示查询，并检查是否已为这些查询启用通知。

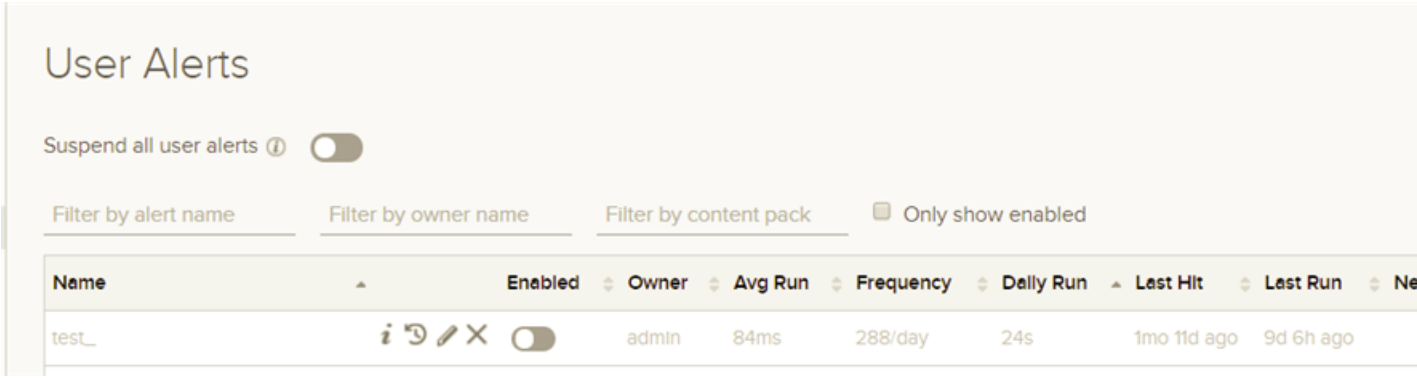
可以将**用户警示**窗口作为起点来查看和管理您作为用户所创建的警示。在此窗口中，您可以监控警示的活动、查看警示历史记录，并管理您的警示。您可以执行以下任务：

- 启用或禁用所有警示或单个警示
- 按警示名称、所有者名称或内容包对警示进行排序
- 更改某个警示的参数
- 删除警示

使用工具提示帮助可了解有关屏幕上每个图标的更多信息。

注意 警示查询是用户特定的。仅可管理您自己的警示。您必须分配有“超级管理员”角色才能管理其他用户警示。

图 1-3 用户警示



“上次命中时间”列中的值在第一次命中发生之前将一直保持为 never。

前提条件

验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 单击配置下拉菜单图标，然后选择**管理**。

2 在左侧菜单的“管理”部分中，单击**用户警示**。

可以查看所有警示查询的列表。警示通知的状态显示在警示名称下方。

下一步

可以单击列表中的警示查询，以修改其参数或删除不再需要的查询。

内容包警示查询是只读的。要将更改保存到内容包警示，必须将此警示保存到自定义内容。

修改警示查询

可以更改警示查询的触发器，启用或禁用查询发送的通知，或者更改通知方法（电子邮件、Webhook 或发送到 vRealize Operations Manager）。

注意 警示查询是用户特定的。仅可管理您自己的警示。您必须分配有“超级管理员”角色才能管理其他用户警示。

内容包警示查询是只读的。要将更改保存到内容包警示，必须将此警示保存到自定义内容。

可以同时对一个或多个警示应用您的更改。

前提条件

- 验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。
- 验证管理员是否已配置 SMTP 来启用电子邮件通知。请参见为 Log Insight 配置 SMTP 服务器。
- 验证管理员是否已将 vRealize Log Insight 与 vRealize Operations Manager 之间的连接配置为启用警示集成。请参见将 Log Insight 配置为向 vRealize Operations Manager 发送通知事件。
- 如果您使用的是 Webhook，则验证 Web 服务器是否已配置为可接收 Webhook 通知。

步骤

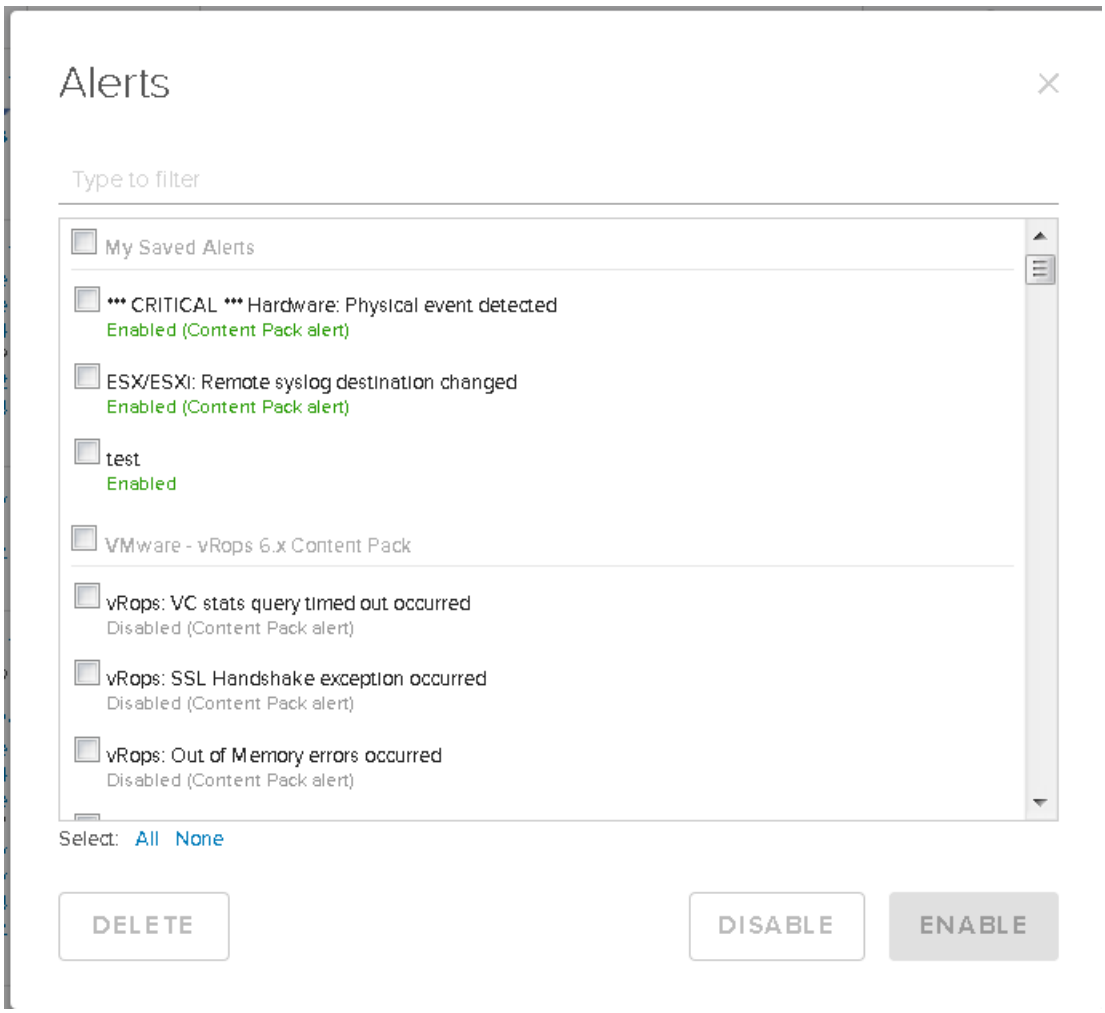
1 导航到**交互式分析**选项卡。

2 在**搜索**按钮右侧的**创建或管理警示**菜单中，单击  ，然后选择**管理警示**。

3 在“警示”列表中，选择要修改的一个或多个警示查询，然后根据需要更改查询参数。

您可以通过输入一个字符串作为筛选条件来查找相应的查询。查询会被标记为已启用或已禁用，以及是否为内容包查询。

注意 如果取消选中所有通知选项，则将禁用警示查询。



4 保存更改。

选项	描述
保存	当您修改自己的警示时，将会显示此按钮。
保存到我的警示	当您修改共享警示或内容包警示时，将会显示此按钮。原始警示仍保持不变，但您可以将此警示的副本保存到自定义内容中。

启用警示查询

禁用警示查询时，vRealize Log Insight 不会发送电子邮件或 Webhook 通知，且不会触发 vRealize Operations Manager 通知事件。

注意 警示查询是用户特定的。仅可管理您自己的警示。您必须分配有“超级管理员”角色才能管理其他用户警示。

在以下情况下，将禁用警示查询。

- 如果在“编辑警示”对话框中禁用所有通知选项。
- 如果警示属于内容包。

内容包警示查询是只读的。要将更改保存到内容包警示，必须将此警示保存到自定义内容。

前提条件

- 验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。
- 验证管理员是否已配置 SMTP 来启用电子邮件通知。请参见为 Log Insight 配置 SMTP 服务器。
- 验证管理员是否已将 vRealize Log Insight 与 vRealize Operations Manager 之间的连接配置为启用警示集成。请参见将 Log Insight 配置为向 vRealize Operations Manager 发送通知事件。

步骤

1. 导航到**交互式分析**选项卡。
2. 在**搜索**按钮右侧的**创建或管理警示**菜单中，单击  ，然后选择**管理警示**。
3. 在“警示”列表中，单击您要启用的一个或多个警示查询。
4. 选择要启用的通知选项，并提供所需参数。

选项	描述
电子邮件	在文本框中输入至少一个电子邮件地址。使用逗号分隔多个地址。
Webhook	输入您希望 vRealize Log Insight 向其发送通知的 URL。
发送到 vRealize Operations Manager	选择 vRealize Operations Manager 资源以与通知事件相关联，然后选择事件的严重级别。

5. 保存更改。

选项	描述
保存	当您修改自己的警示时，将会显示此按钮。
保存到我的警示	当您修改共享警示或内容包警示时，将会显示此按钮。原始警示仍保持不变，但您可以将此警示的副本保存到自定义内容中。

当警示查询返回与警示条件匹配的结果时，vRealize Log Insight 将根据您的配置发送通知。

示例：从 VMware - vSphere 内容包启用警示

VMware - vSphere 内容包包含多个预定义的警示查询，包括 **vCenter Server: ESX/ESXi 停止日志记录**警示。

启用 **vCenter Server: ESX/ESXi 停止日志记录**警示是一种很好的做法，因为特定版本的 ESXi 主机可能会在您重新启动 vRealize Log Insight 时停止发送 syslog 数据。此警示监控 vCenter Server 事件 `esx.problem.vmsyslogd.remote.failure` 来检测是否存在已停止发送 syslog 源的 ESXi 主机。

1 在**交互式分析**选项卡上，展开**搜索**按钮右侧的下拉菜单，然后选择**管理警示**。

2 在 VMware - vSphere 内容包下，单击 **vCenter Server: ESX/ESXi 停止日志记录**。

3 启用电子邮件通知、Webhook 通知或 vRealize Operations Manager 通知事件。

4 单击**保存到我的警示**。

要仅检测停止向 vRealize Log Insight 实例发送源的 ESXi 主机，可以将以下筛选器添加到警示查询：**vc_remote_host (VMware - vSphere) contains** *<log-insight-hostname>*，并将新查询保存到警示中。

有关 syslog 问题和解决方案的详细信息，请参见位于 https://kb.vmware.com/kb/2003127 的知识库文章“VMware ESXi 5.x 主机停止向远程服务器发送 syslog (2003127)”。

删除警示查询

可以删除不再需要的警示查询。

注意 警示查询是用户特定的。仅可管理您自己的警示。您必须分配有“超级管理员”角色才能管理其他用户警示。

前提条件

验证是否已登录到 vRealize Log Insight Web 用户界面。URL 格式为 https://*log_insight-host*，其中 *log_insight-host* 是 vRealize Log Insight 虚拟设备的 IP 地址或主机名。

步骤

1 导航到**交互式分析**选项卡。

2 从**搜索**按钮右侧的菜单中，单击 并选择**管理警示**。

3 选择您要删除的一个或多个警示，然后单击**删除**或者删除图标 。

4 在**删除警示**对话框中，选择**删除**以确认此操作。