



Splunk[®] Enterprise 8.2.0

监视 Splunk Enterprise

生成时间：2021 年 5 月 24 日，14:28

Table of Contents

简介	3
《监视 Splunk Enterprise》概述	3
关于监视控制台	4
关于监视控制台	4
监视控制台有什么功能？	4
监视控制台如何工作	5
使用整合的 Splunkd 部署运行状况报告故障排除	6
配置监视控制台	7
多实例监视控制台设置步骤	7
单实例监视控制台设置步骤	7
哪个实例应布置控制台？	7
监视控制台设置前提条件	9
设置群集标签	10
将 Splunk Enterprise 实例添加至监视控制台。	11
在独立模式中配置监视控制台	11
在分布式模式中配置监视控制台	11
为监视控制台配置转发器监视	12
启用和配置平台告警	12
评估和自定义运行状况检查	14
监视控制台仪表板参考	17
摘要	17
索引：性能	18
索引：索引和卷	19
索引：输入：HTTP 事件收集器	19
索引：输入：数据质量	20
索引：许可证使用情况	21
索引：SmartStore	21
索引：索引器群集化：状态	21
索引：索引器群集化：服务活动	22
搜索：搜索活动	22
搜索：搜索使用情况统计信息	23
搜索：KV 存储	24
搜索：计划程序活动	25
搜索：分布式搜索	26
搜索：知识软件包复制	27
搜索：搜索头群集化	27
资源使用情况	29
资源使用情况：CPU 使用率	30
转发器	33
主动 Splunk 组件监视	35
关于主动 Splunk 组件监视	35
要求	37
配置 splunkd 运行状况报表	37
为 Splunkd 运行状况报表设置告警	41
为 Splunkd 运行状况报表设置访问控制	45
调查功能运行状况更改	45

简介

《监视 Splunk Enterprise》概述

Splunk Enterprise 提供两种类型的部署监视：

- 监视控制台（基于搜索的监视）。
- 主动 Splunk 组件监视（基于 REST 的监视）。

监视控制台

监视控制台是基于搜索的监视工具，您可以用此工具查看 Splunk Enterprise 部署的拓扑和性能的相关的详细信息。监视控制台提供预构建仪表板，使部署中许多部分可视化，包括搜索和索引性能、资源使用情况、许可证使用情况和更多内容。您可以使用监视控制台追踪所有类型的部署拓扑的状态，从单个实例（独立）部署到复杂的多站点索引器群集。

有关更多信息，请参阅“关于监视控制台”。

主动 Splunk 组件监视

主动 Splunk 组件监视是基于 REST 的监视工具，使您可以查看 REST API 端点输出的 Splunk Enterprise 功能的运行状况。单独功能通过提供部署运行状况的持续、高级视图的树状结构报告运行状况状态。您可以使用 Splunk Web 中的 splunkd 运行状况报表访问功能运行状况信息，或从 /server/health/splunkd 端点访问功能运行状况信息。

请参阅“关于主动 Splunk 组件监视”了解更多信息。

关于监视控制台

关于监视控制台

什么是监视控制台？

监视控制台是 Splunk Enterprise 的监视工具。您可以查看有关 Splunk Enterprise 部署的详细拓扑和性能信息。在 Splunk Enterprise 6.5.0 之前的版本中，监视控制台称为分布式管理控制台。

仪表板可用来深入了解您的部署或实例的以下内容：

- 搜索性能和分布式搜索框架
- 索引性能
- 操作系统资源使用情况
- Splunk 应用键值存储性能
- 搜索头和索引器群集化
- 索引和卷使用情况
- 转发器连接和 Splunk TCP 性能
- HTTP 事件收集器性能
- 许可证使用情况

监视控制台仪表板使用来自 Splunk Enterprise 的内部日志文件（例如 metrics.log）的数据，以及从 Splunk Enterprise 平台工具中可获得的数据。

找到监视控制台

在 Splunk Web 上的任何地方，单击设置，然后单击左边的监视控制台图标。



监视控制台仅对具备 Splunk Enterprise 管理员角色的用户可见。

有关 Splunk Cloud 中的监视控制台的信息，请参阅 Splunk Cloud 《管理员手册》中的“监视您的 Splunk Cloud 部署”。

监视控制台有什么功能？

监视控制台主要有三种配置状态。

- 当 Splunk Enterprise 实例处于独立模式时，可以不配置监视控制台。这意味着您可以在所部署的单个实例中导航到监视控制台，并查看该实例的性能。
- 您可以查看配置步骤（仍然在独立模式中），这样您就可以访问默认的平台告警。
- 您可以查看分布式模式的配置步骤，以登录到一个实例并查看部署中每个实例的控制台信息。

查找常见问题的答案

监视控制台是关于您 Splunk Enterprise 部署的故障排除信息的富数据来源。下面是您可以使用此工具调查问题的一些示例：

症状	仪表板
我的用户们在运行搜索时会报错，如“对等节点 x 不响应”，“对等节点未参与搜索”或“结果可能不完整”。	起始点可能包括： <ul style="list-style-type: none">分布式搜索：部署运行状况检查或分布式搜索：实例（如果您了解哪个搜索节点出现问题。）关于资源使用情况：部署（选择搜索节点，并查找任何过度订阅的节点。）在分布式搜索和资源使用情况视图中对比出现问题的时间周期，以考虑容量规划。
我的用户们的 UI 运行很慢	资源使用情况：实例针对出现问题的实例。
我的搜索性能很慢	资源使用情况：部署、计划程序活动或搜索活动
我的索引器/搜索头当前正常吗？	概述 > 拓扑
索引器在实例中的工作负荷分布均匀吗？	索引性能：部署
我的索引保存策略是什么？	建立索引 > 索引和卷：实例
KV 存储并未初始化	搜索 > KV 存储：部署
Splunk Web 出错，因为磁盘已满	资源使用情况：计算机或索引和卷仪表板

监视控制台如何工作

本主题列出监视控制台在 Splunk Enterprise 文件系统中修改的文件。

这些文件位于 \$SPLUNK_HOME/etc/apps/splunk_monitoring_console/，除非另行指定。此目录包含默认目录和设置监视控制台之后的本地目录中的配置文件。请参阅《管理员手册》中的“关于配置文件目录”。

文件	文件所含信息	填充时间
app.conf	关于监视控制台的基本信息：确定是否为分布式模式，以及为 Splunk Web 提供简短描述，以便在启动程序中使用。请参阅 app.conf.spec。	默认情况下。当您单击应用更改时更新。
etc/system/local 中的 distsearch.conf	包含引用监视控制台新建的分布式搜索组的段落。这些组的名称通常以 dmc_group_* 开头。例如：[distributedSearch:dmc_group_cluster_master]	当您切换至监视控制台设置中的分布式模式并单击应用更改
dmc_alerts.conf	某些情况下，您可以在平台告警中编辑阈值，而无需直接修改该告警的搜索字符串。对于此类告警，监视控制台具有搜索字符串、描述字符串和可编辑参数的模板。此外存储在监视控制台告警设置页面中使用的模板数据，它所在的段落根据 default/savedsearches.conf 已保存搜索的名称而命名。	默认情况下
查找目录	包含两个重要文件： <ul style="list-style-type: none">assets.csv 列出监视控制台识别的实例及其对等节点 URI（唯一名称）、服务器名称、主机、计算机（主机 fqdn）、搜索组（服务器角色、自定义组或群集）。此 CSV 供每个监视控制台仪表板使用。启用转发器监视时生成 dmc_forwarder_assets.csv。启用转发器监视的同时也将启用填充此 .csv 文件的 savedsearches.conf 中的计划的搜索（DMC 转发器 - 构建资产表）。请参阅本手册中的为监视控制台配置转发器监视。	默认情况下（初始启动时）。单击应用更改或重建转发器资产表后相应更新。
macros.conf	包含两种类型的宏： <ul style="list-style-type: none">针对所有监视控制台仪表板的搜索宏。在监视控制台 > 设置 > 概述偏好中设置的概述页面自定义。 请参阅 macros.conf.spec。	默认情况下搜索宏在此处存储。 每次编辑完一个自定义然后单击保存即表明设置完自定义。
props.conf	搜索时字段提取和查找应用程序及 eval。请参阅 props.conf.spec。	默认情况下
savedsearches.conf	平台告警的计划和搜索字符串。启用转发器监视时，已保存的搜索（命名为“DMC 转	默认情况下

saveusearchnes.conf	发器 - 构建资产表”) 将运行。	默认情况下
splunk_monitoring_console_assets.conf	此文件包含： <ul style="list-style-type: none"> 通过监视控制台配置的搜索节点以及您已禁用监视的任何节点的列表。 在设置过程中通过监视控制台手动覆盖的任何搜索节点标识符，如主机、host_fqdn、索引器群集标签或搜索头群集标签。 描述每个搜索节点是哪个索引器或搜索头群集成员的段落。 	单击设置 > 常规设置中的“应用更改”时
transforms.conf	assets.csv 和转发器 csv 文件的查找定义	默认情况下

有关 dmc_alerts.conf 和 splunk_monitoring_console_assets.conf 的更多详情，请查看 \$SPLUNK_HOME/etc/apps/splunk_monitoring_console/README。

使用整合的 Splunkd 部署运行状况报告故障排除

监视控制台中的摘要仪表板允许您对 splunkd 运行状况报告检测到的 Splunk Enterprise 部署中的运行状况问题进行故障诊断。每个仪表板中的模式标签指示与异常关联的独立或分布式实例。

调查特征运行状况问题

摘要仪表板中的异常面板列出了当前处于红色或黄色状态的 Splunkd 运行状况报告特征。红色或黄色状态的特征表明您的部署可能出现了严重的问题。使用异常面板查看各问题的说明，然后访问健康检查以调查根本原因。

要调查特征运行状况问题：

- 单击设置 > 监视控制台 > 摘要。
 - 在异常面板中，查看列出的红色和黄色状态特征的说明。
 - 要进一步调查特定问题，单击调查。
- 运行状况检查页面将打开。页面显示推荐的已报告问题的运行状况检查。
- 运行推荐的运行状况检查以了解根本原因以及建议的问题解决方案。

示例：调查跳过搜索

此示例说明了如何使用摘要仪表板故障排除 splunkd 运行状况报告检测到的严重运行状况状态问题。

- 单击设置 > 监视控制台 > 摘要。
- 在异常面板中，“跳过搜索”特征显示为严重的“红色”状态。这表明有一个严重的问题对搜索性能产生了负面的影响。
- 查看 splunkd 运行状况报告提供的说明获取问题的基本信息。
- 单击调查。
- 运行状况检查页面打开，显示建议用于调查“搜索计划程序跳过比率”、“独立的计划搜索”和“资源使用情况”。
- 运行推荐的运行状况检查。
- “搜索计划程序跳过比率”健康检查失败。
- 单击失败的运行状况检查查看运行状况检查结果、造成问题的原因和解决问题的建议操作。
- 查看以下监视控制台仪表板进一步分析根本原因：搜索 > 计划程序活动：实例/部署、资源使用情况：实例/部署。

关于可更新的运行状况检查的更多信息，请参阅“下载运行状况检查更新”。

有关 splunkd 运行状况检查报告的更多信息，请参阅“关于主动 Splunk 组件监视”。

配置监视控制台

多实例监视控制台设置步骤

本主题概述了要进行的步骤，以便为分布式 Splunk Enterprise 部署设置监视控制台。要在独立的实例上配置监视控制台，请参阅本手册中“单一实例监视控制台设置步骤”。

要为分布式部署设置监视控制台，请执行以下步骤：

步骤编号	步骤说明	如何执行此步骤
1	为您的部署确定哪个实例将托管监视控制台。	请参阅“哪个实例应托管控制台？”
2	确保部署满足前提条件。	请参阅“监视控制台设置前提条件”。
3	设置搜索头群集和索引器群集标签。	请参阅“设置群集标签”。
4	将所有实例作为搜索节点添加。	请参阅“将实例作为搜索节点添加到监视控制台”。
5	在分布式模式中设置监视控制台。	请参阅“在分布式模式中配置监视控制台”。
6（可选）	使用监视控制台转发器仪表板。	请参阅“为监视控制台配置转发器监视”。
7（可选）	启用平台告警。	请参阅“启用和配置平台告警”。
8（可选）	修改或添加运行状况检查项目。	请参阅“自定义运行状况检查”。
9（可选）	自定义概述页面的颜色映射。	导航至监视控制台 > 设置 > 概述偏好。

开始

要为分布式部署设置监视控制台，首先要确定要在部署中托管监视控制台的位置。从“哪个实例应托管控制台？”开始。

单实例监视控制台设置步骤

本主题概述了要进行的步骤，以便为独立的 Splunk Enterprise 实例设置监视控制台。若要为分布式 Splunk Enterprise 部署配置监视控制台，请参阅“多实例监视控制台设置步骤”。

要为独立的部署设置监视控制台，请执行以下步骤：

步骤编号	步骤说明	如何执行此步骤
1	确保部署满足前提条件。	请参阅“监视控制台设置前提条件”。
2	在独立模式中设置监视控制台。	请参阅“在独立模式中配置监视控制台”。
3（可选）	使用监视控制台转发器仪表板。	请参阅“为监视控制台配置转发器监视”。
4（可选）	启用平台告警。	请参阅“启用和配置平台告警”。
5（可选）	修改或添加运行状况检查项目。	请参阅“自定义运行状况检查”。
6（可选）	自定义概述页面的颜色映射。	导航至监视控制台 > 设置 > 概述偏好。

开始

要为独立部署配置监视控制台，首先要验证实例的前提条件。从“监视控制台设置前提条件”开始。

哪个实例应布置控制台？

本主题介绍设置用于分布式 Splunk Enterprise 部署的监视控制台的过程中的一步。

开始前，请确认哪个实例最适合托管监视控制台。对于在哪里托管监视控制台，有若干选择，具体取决于部署的性质：

- 您选择的实例必须满足或超出搜索头参考硬件要求。请参阅*容量规划手册*中的“参考硬件”。
- 出于安全和性能原因，仅 Splunk Enterprise 管理员可以具有此实例的访问权限。

- 托管监视控制台的实例不得作为监视控制台运行任何与其功能不相关的搜索。这一规则的例外是当您正在使用控制台监视独立的单一实例部署。

该表根据部署类型列出了监视控制台的建议位置。

分布式模式？	索引器群集化？	搜索头群集化？	推荐的位置
否	N/A	N/A	独立的实例。
是	否	否	服务少数（< 50 个）客户端的许可证主服务器或部署服务器。否则，在专用于运行监视控制台搜索的搜索头中运行监视控制台。
是	单点索引器群集	不相关	主节点，如果主节点上的负载低于 <i>管理索引器和索引器群集</i> 手册中的“主节点的其他角色”中指定的限制。否则，在专用于运行监视控制台搜索的搜索头节点中运行监视控制台。如果您使用的是 SmartStore，则必须将监视控制台托管在专用搜索头上。
是	多个索引器群集	不相关	配置为跨所有群集的搜索头节点的搜索头。该搜索头必须专用于监视控制台。
是	否	是	搜索头群集 <code>deployer</code> 、许可证主服务器，或专用于运行监视控制台搜索的独立搜索头。请勿在搜索头群集成员中运行监视控制台。

有关管理组件共存的常规讨论，请参阅《*分布式部署手册*》中的“帮助管理部署的组件”。

请参阅特定部署类型的详细信息之后的章节内容。

非群集化部署中

您可以在这些实例的任何一个中找到监视控制台：

- 许可证主服务器
- 服务少量（<50）客户端的部署服务器
- 专用搜索头

在带有单个索引器群集的部署中

在单个索引器群集中，如果主节点上的负载低于*管理索引器和索引器群集*手册中的“主节点的其他角色”中指定的限制，则可以在运行主节点的实例中托管监视控制台。

您还可以将监视控制台托管在群集中的搜索头节点上，但是您必须将该节点专门用于监视控制台搜索。您无法使用搜索头运行任何其他搜索。

如果您使用的是 SmartStore，则必须将监视控制台托管在专用搜索头上。

在带有多个索引器群集的部署中

如果您的部署有多个索引器群集，将监视控制台托管在（配置为每个索引器群集上的搜索头节点的）搜索头上。切勿使用该搜索头去运行任何非监视控制台搜索。

为此：

1. 配置搜索头以将其作为每个索引器群集上的节点使用。请参阅*管理索引器和索引器群集*手册中的“跨多个索引器群集搜索”。这是您的监视控制台实例。
2. 将每个主节点以及群集中的所有搜索头节点配置为监视控制台实例的搜索节点。请参阅本手册的“添加实例作为搜索节点”。

切勿将群集对等节点（索引器）配置为监视控制台节点的搜索节点。作为索引器群集中的节点，对于它们群集中的所有搜索头节点（包括监视控制台节点）来说，它们都是已知的。

在有搜索头群集但是无索引器群集的部署中

您可以在这些实例的任何一个中找到监视控制台：

- 搜索头群集 deployer
- 许可证主服务器
- 独立、专用搜索头

请勿在搜索头群集成员中运行监视控制台。

监视控制台不支持搜索头合并部署。搜索头池首先在 Splunk Enterprise 6.2.0 中被弃用，并且该功能已从 Splunk Enterprise 8.0.0 及后续版本中删除。

为何不在生产搜索头中托管控制台

请勿在正在使用的现有生产搜索头上配置监视控制台，原因如下：

- 在此搜索头上运行的非监视控制台搜索可能会产生不完整的结果。监视控制台分布式搜索组可修改默认的搜索行为，以确保针对监视控制台仪表板的搜索范围缩小至他们的目标搜索节点列表。在分布式模式中设置监视控制台时，它将为每个服务器角色、已标识群集或自定义组新建一个搜索组。默认情况下只有是索引器组成员的搜索节点才能搜索到，除非您使用 "splunk_server_group" 或 "splunk_server" 选项。因为在监视控制台实例上运行的所有搜索都遵循此行为，非监视控制台搜索可能会产生不完整的结果。
- 所有生产搜索头的性能都应被监视，监视控制台会影响托管该控制台的搜索头的性能。要在同一个实例中将监视控制台资源使用情况与生产资源使用情况分开可能比较困难。

监视控制台和部署服务器

在多数情况下，您不能将分布式监视控制台托管在部署服务器上。例外情况是部署服务器仅处理少数的部署客户端（不超过 50 个）。监视控制台和部署服务器功能在客户端数量更大的情况下会互相妨碍。请参阅 *更新 Splunk Enterprise 实例手册* 中的“部署服务器配置”。

下一步

要继续在分布式模式中设置监视控制台，请确保您的部署满足前提条件。请参阅“监视控制台设置前提条件”。

监视控制台设置前提条件

本主题介绍设置用于分布式 Splunk Enterprise 部署或者独立的 Splunk Enterprise 实例的监视控制台的过程中的一步。

要执行监视控制台部署，请验证是否符合以下设置前提条件：

- 具有功能性 Splunk Enterprise 部署。
- 请确保部署中每个实例具有唯一的 server.conf serverName 值和 inputs.conf host 值。
- 为要监视的每个 Splunk Enterprise 实例（转发器除外）启用平台检测。请参阅“关于 Splunk Enterprise 平台检测”。
- 从所有其他组件中将内部日志（\$SPLUNK_HOME/var/log/splunk 和 \$SPLUNK_HOME/var/log/introspection）转发到索引器。如果没有此步骤，很多仪表板将缺少数据。请参阅最佳做法：《*分布式搜索手册*》中“转发搜索头数据”。
- 用户设置监视控制台需要具备 admin_all_objects 功能。

仪表板版本依赖性

监视控制台中的仪表板依赖于从 Splunk Enterprise 内部日志文件和端点收集的数据。许多数据来自平台检测，已在 Splunk Enterprise version 6.1 中推出并在后续版本中有所增强。下表汇总了特定平台检测功能的最低 Splunk Enterprise 版本要求。如果控制台监视的实例不满足这些最低版本要求，那么相关的仪表板面板将为空白。

功能	面板	最低版本要求
所有仪表板	大部分面板	Splunk Enterprise 6.1
KV 存储仪表板	所有面板	Splunk Enterprise 6.2.0（已推出 KV 存储）
搜索头群集化仪表板	所有面板	Splunk Enterprise 6.2.0
分布式搜索仪表板	关于软件包复制的面板	Splunk Enterprise 6.3.0
HTTP 事件收集器（HEC）仪表板	所有面板	Splunk Enterprise 6.3.0（已推出 HEC）
计划程序仪表板	大部分面板	Splunk Enterprise 6.3.0
资源使用情况：计算机，资源使用情况：部署	I/O 面板	Splunk Enterprise 6.4.0

运行状况检查	N/A	在托管监视控制台实例中的 Splunk Enterprise 6.5.0
--------	-----	--------------------------------------

下一步

要继续在分布式部署中设置监视控制台，请参阅“设置群集标签”。

要继续在独立的实例中设置监视控制台，跳至“在独立模式中配置监视控制台”。

设置群集标签

本主题介绍配置用于 Splunk Enterprise 部署的监视控制台的过程中的一步。

在索引器群集和搜索头群集上设置标签，这样监视控制台可识别与之关联的实例。标签允许监视控制台填充索引器群集化和搜索头群集化仪表板。

在群集部署期间

在群集的初始部署期间设置标签。如有需要，以后您可以设置或更改标签。

要在部署期间设置索引器群集标签，请参阅《管理索引器和索引器群集》手册中的“启用索引器群集管理器节点”。

要在部署期间设置搜索头群集标签，请参阅分布式搜索手册中的“部署搜索头群集”。

在群集部署之后

如果您正在部署新群集，在部署过程中设置群集标签。如果您的群集已经部署完，则根据以下表格在开始设置监视控制台时设置群集标签。

Splunk Enterprise 版本和群集类型	位置	方法
6.3.0+ 索引器群集	在群集主节点上	请参阅《管理索引器和索引器群集》手册中的“使用仪表板配置管理器”。或者，运行群集主节点中的以下 CLI 命令： <code>splunk edit cluster-config -cluster_label <CLUSTER LABEL></code>
6.3.0 之前版本的索引器群集	在监视控制台设置页面	为群集中的所有实例设置标签

Splunk Enterprise 版本和群集类型	位置	方法
6.3.0+ 搜索头群集成员	在任何搜索头群集成员上	请参阅分布式搜索手册中的“配置搜索头群集”。或者，运行任何群集成员中的以下 CLI 命令： <code>splunk edit shcluster-config -shcluster_label <CLUSTER LABEL></code>
6.3.0 之前版本的搜索头群集成员	在监视控制台设置页面	为群集中的所有实例设置标签
搜索头群集 Deployer	在监视控制台设置页面	为 Deployer 实例设置标签

无论使用哪种方法来编辑群集标签，转到监视控制台设置页面并单击应用更改以更新监视控制台资产表。

关于监视控制台设置页面

Splunk Web 中的监视控制台设置页面位于监视控制台 > 设置 > 常规设置。

编辑群集标签之后，单击应用更改。

下一步

要继续在分布式部署中设置您的监视控制台，请参阅“将实例作为搜索节点添加到监视控制台”。

将 Splunk Enterprise 实例添加至监视控制台。

本主题介绍设置用于分布式 Splunk Enterprise 部署的监视控制台的过程中的一步。

监视控制台是一个用作搜索头的 Splunk Enterprise 实例。可跨其他实例运行搜索以收集那些实例中的信息。但是，要收集信息，您必须将这些实例添加为搜索头的搜索节点。

您必须将您想要监视的各实例添加到监视控制台作为搜索节点，不考虑服务器角色，作为索引器群集一部分的索引器除外。

要将作为搜索节点的 Splunk Enterprise 实例添加到监视控制台：

1. 登录到您想要配置监视控制台的实例。
2. 在 Splunk Web 中，单击 **设置 > 分布式搜索 > 搜索节点**。
3. 单击 **新建**。
4. 填写所请求的字段并单击 **保存**。
5. 为每个搜索头、部署服务器、许可证主服务器、非群集索引器和群集搜索头重复步骤 3 和 4。请勿添加群集索引器。如果您正在监视一个索引器群集，并且您正将监视控制台布置在除群集主节点之外的一个实例上，则必须将群集主节点作为搜索节点添加，且必须在该群集中将监视控制台实例配置为搜索头。

下一步

要继续在分布式部署中设置监视控制台，请参阅“在分布式模式中配置监视控制台”。

在独立模式中配置监视控制台

本主题介绍设置用于独立的 Splunk Enterprise 实例的监视控制台的过程中的一步。

要为独立的实例配置监视控制台：

1. 在 Splunk Web，导航到 **监视控制台 > 设置 > 常规设置**。
2. 请检查搜索头、许可证主服务器和索引器是否列于 **服务器角色** 下，且无其他内容。如果没有，则单击 **编辑** 以更正。
3. 单击 **应用更改**。

下一步

要继续为独立的部署设置监视控制台，请跳到“为监视控制台配置转发器监视”。

在分布式模式中配置监视控制台

本主题介绍设置用于分布式 Splunk Enterprise 部署的监视控制台的过程中的一步。

要在分布式模式中配置监视控制台：

1. 登录到您想要配置监视控制台的实例。默认情况下，实例在独立模式中，未配置。
2. 在 Splunk Web，选择 **监视控制台 > 设置 > 常规设置**。
3. 单击 **分布式模式**。
4. 确认以下内容：
 - 标有 **实例** 和 **计算机** 的列是否正确填充，且每列中的值都具唯一性。
 - 服务器角色是否正确。例如，搜索头（也是许可证主服务器）必须具有列出的两个服务器角色。如果没有，请单击 **编辑 > 编辑服务器角色**，然后为实例选择正确的服务器角色。
 - 如果使用索引器群集，请确保将群集主实例设置为群集主服务器角色。如果没有，请单击 **编辑 > 编辑服务器角色**，然后选择正确的服务器角色。
 - 如果您正将监视控制台布置在除群集主节点之外的一个实例上，则必须将群集主实例添加为搜索对等节点，且必须在该群集中将监视控制台实例配置为搜索头。请参阅“将 Splunk Enterprise 实例添加至监视控制台”。
 - 请确保任何标记过的索引器其实真的都是索引器。
5. （可选）设置自定义组。自定义组为直接映射到分布式搜索组的标记。例如，如果您有多站点索引器群集化（每个组可包含一个位置的索引器）或索引器群集加上独立对等节点时，您可能会发现组很有用。允许自定义组重叠。例如，一个索引器可属于多个组。请参阅 *分布式搜索手册* 中的“新建分布式搜索组”。
6. 单击 **应用更改**。

如果您稍后会为您的部署添加其他节点，请单击 **设置 > 常规设置**，并检查这些项目是否准确。

重新启动后重新设置服务器角色

在分布式模式中配置监视控制台之后，重新启动托管监视控制台的实例可能会导致您正在监视的实例上的服务器角色设置的任何更改丢失。

重新启动分布式监视控制台之后要适当重新设置服务器角色：

1. 单击**设置** > **一般设置** > **重新设置所有设置** > **刷新**。
这样操作会将监视控制台恢复到初始默认配置。
2. 单击**分布式**。
3. 关于您想要更改服务器角色的远程实例，单击**编辑**。
4. 选择或删除特定的服务角色。单击**保存**。
5. 单击**应用更改**。

下一步

要为转发器配置监视控制台，请参阅“为监视控制台配置转发器监视”。

为监视控制台配置转发器监视

本主题介绍配置用于分布式或独立的 Splunk Enterprise 部署的监视控制台的过程中的一步。

前提条件

对于要运行的若干仪表板监视面板，您的转发器需要具有唯一和持久的 GUID。完成此操作的方式之一是启动之前复制转发器。转发器 GUID 在 `instance.cfg` 中，在启动转发器时填充。

设置

在 Splunk Web 中，单击**监视控制台** > **设置** > **转发器监视设置**，然后按设置步骤完成操作。

关于时间设置

在转发器监视设置页面中，您可以启用或禁用转发器监视并设置数据集间隔。启用转发器监视会运行计划的搜索来填充驻留在监视控制台节点上的查找文件 `dmc_forwarder_assets.csv`，搜索运行于 `$SPLUNK_HOME/etc/apps/splunk_monitoring_console/lookups`。监视控制台使用此转发器资产表了解哪些转发器显示关于转发器监视仪表板中的信息。

在 Splunk Web 中，单击**设置** > **搜索和报表** > **DMC 转发器 - 构建资产表查看计划的搜索**。

单击**监视控制台** > **设置** > **转发器监视设置**，并针对数据集间隔从若干数值中选择。此间隔决定计划的搜索运行的频率。默认值为 15 分钟。

当计划的搜索运行以重新构建转发器资产表时，它都会回溯 15 分钟。此回溯时间不可配置，并且与数据集间隔有所不同。例如，如果您将数据集间隔设为 24 小时，计划的搜索将每 24 小时运行一次，但仅检查开始运行前 15 分钟。

如果您有许多转发器，则计划的搜索会很昂贵。您可能想要运行搜索的频率低于默认值。

重建转发器资产表

转发器资产表中的数据可累加。如果任意转发器连接到一个索引器，其记录将存在于表格中。如果您后续从部署中移除转发器，则转发器记录不会从资产表中移除。相反，它在资产表中标记为“缺失”，并且仍会出现在 DMC 转发器仪表板中。

如要从监视控制台仪表板中完整地移除转发器，请单击**监视控制台** > **设置** > **转发器监视设置**中的**重建转发器资产表**。您执行此操作时可选择一个回溯时间。此操作期间的回溯选择不会更改本主题中其他地方所讨论的计划搜索的 15 分钟回溯时间或者数据集间隔。

下一步

要设置平台告警，请参阅“启用和配置平台告警”。本步骤可选。

启用和配置平台告警

平台告警是包含在监视控制台中的已保存搜索。平台告警通知 Splunk Enterprise 管理员可能危及他们的部署环境的条件。告

警触发后，监视控制台概览页面将显示一个通知。您可以通过前往概览 > 告警 > 管理的触发的告警查看告警及其结果。该包含的平台告警从 REST 端点获取它们的数据。默认情况下禁用平台告警。

启用平台告警

前提条件

配置您的监视控制台。请参阅“单一实例监视控制台设置步骤”或“多实例监视控制台设置步骤”，具体取决于部署类型。

- 1. 从监视控制台概览中，单击触发的告警 > 启用或禁用。
- 2. 单击您要启用的告警旁边的已启用复选框。

您也可以设置一个告警操作，如电子邮件通知。

配置平台告警并设置告警操作

您可以查看和配置平台告警的默认设置和参数，包括以下方面：

- 告警阈值（如适用）
- 告警计划
- 抑制时间
- 告警操作（如发送一封电子邮件或启动一个自定义脚本）

要更改告警阈值，请执行以下步骤：

- 1. 从监视控制台中，单击预览 > 告警 > 启用或禁用。
- 2. 找到要配置的告警，并单击编辑。
- 3. 将阈值字段编辑为所需值。
- 4. 单击保存。

要查看和编辑高级设置，如告警计划、触发条件和告警操作，请执行以下步骤：

- 1. 从监视控制台中，单击预览 > 告警 > 启用或禁用。
- 2. 找到要配置的告警，并单击高级编辑。
- 3. 必要时修改设置。
- 4. 单击保存。

如果启用电子邮件通知，请确保在设置 > 服务器设置 > 电子邮件设置中定义一个有效的邮件主机。

有关告警操作的指南，请参阅告警手册中的“设置告警操作”。

您还可在 \$SPLUNK_HOME/etc/apps/splunk_management_console/default/savedsearches.conf 中查看平台告警的默认参数完整列表。如果您选择直接编辑配置文件，则将新配置放置在本地目录，而非默认目录。

切勿在默认目录中编辑配置文件。

监视控制台中的默认平台告警

监视控制台中的以下平台告警默认可用。要使用平台告警监视您的部署，启用您想要的单个告警。

告警名称	描述	相关信息
索引器处理器的异常状态	它在一个或多个索引器报告异常状态时触发。此异常状态可被限制或停止。	有关哪个索引器处于异常状态和要开始调查原因的详细信息，请参阅监视控制台索引性能：部署仪表板的通过实例索引性能面板。有关仪表板的信息，请参阅本手册中的“索引性能仪表板”。
临界系统物理内存使用情况	当一个或多个实例超过 90% 内存使用率（被任何进程、Splunk 软件或其他占用）时触发。在大多数 Linux 分布中，如果该 OS 忙于缓存和文件系统缓存活动，则此告警可触发。如果其他进程需要此内存，此 OS 会释放它，所以它不会始终指示严重的问题。	有关实例内存使用情况的详细信息，请导航到监视控制台资源使用情况：部署仪表板中提供更详细的信息。有关仪表板的信息，请参阅本手册中的“资源使用情况仪表板”。
到期和不久到期的许可证	当您有到期的或将在两周内到期的许可证时触发。	有关您许可证和许可证使用情况的信息，请单击监视控制台中的许可授权。

缺少转发器	当缺少一个或多个转发器时触发。	请参阅监视控制台中的转发器仪表板。
接近临界磁盘使用情况	它在您使用磁盘容量的 80% 时触发。	有关磁盘使用情况的更多信息，请导航到三个监视控制台 资源使用情况 仪表板，并阅读本手册中的“资源使用情况仪表板”。
饱和的事件处理队列	它在一个或多个索引器队列报告在过去 15 分钟，平均填充百分比达到 90% 或以上时触发。该告警可通知您潜在索引延迟。	有关索引器队列的详细信息，请导航到两个监视控制台 索引性能 仪表板，并阅读本手册中的“索引性能仪表板”。
搜索节点无反应	它在任何一个搜索节点（索引器）无法连接时触发。	有关您所有实例的状态，请查看监视控制台 实例 视图。
许可证使用总量接近每日配额	它在您使用每日许可证总配额的 90% 时触发。	有关您许可证使用情况的更多信息，请单击监视控制台中的 许可授权 。

平台告警搜索项目的寿命

在 `savedsearches.conf` 中，此 `dispatch.ttl` 设置指示来自平台告警的搜索保存搜索项目四个小时。但是，如果触发了告警，它的搜索项目会保存七天。这意味着在电子邮件中发送的链接（用于检查触发的告警的搜索结果）将在七天后到期（默认情况下）。

下一步

要设置运行状况检查，请参阅“访问和自定义运行状况检查”。本步骤可选。

评估和自定义运行状况检查

监视控制台提供了预配置的运行状况检查。您可以修改现有运行状况检查并新建或下载新检查。

使用运行状况检查

在**监视控制台** > **运行状况检查**中找到运行状况检查。单击**开始**启动运行状况检查。

每个运行状况检查项目都会运行一个独立的搜索。这些搜索按顺序运行。当一个搜索结束时，下一个即会开始。当所有搜索都结束时，结果会按严重性程度排列：错误、警告、信息、成功、或不适用。

单击结果顶部的严重性级别可只查看该级别的搜索结果。单击一行可查看更多信息，包括建议的操作。

要想只运行部分检查，单击**开始**之前按标记或类别过滤。在监视控制台中，您可以运行为安装于监视控制台节点上任意应用所新建的运行状况检查。使用应用下拉列表来按应用上下文筛选运行状况检查。

排除检查

您可禁用某项特定检查以防止在您单击**开始**时会一起运行该项检查：

1. 单击**监视控制台** > **设置** > **运行状况检查项目**。
2. 请在列表中查找您要禁用的检查项。
3. 单击**禁用**。
4. 重新加载**监视控制台** > **运行状况检查**。

单击**开始前**，您还可以在页面顶部按组、应用、标记和类别过滤检查。

修改现有检查

您可以修改现有检查。例如，要将物理内存使用率过高的警告阈值从 90% 改为 80%。

1. 单击**监视控制台** > **设置** > **运行状况检查项目**。
2. 在物理内存使用率过高行中，单击**编辑**。
3. 编辑**搜索**和**描述**字段。

4. （可选）重命名此运行状况检查项目以反应您的修改。
5. 单击**保存**。

您所做的修改会保存到文件系统中：`$SPLUNK_HOME/etc/apps/splunk_monitoring_console/local/checklist.conf`

下载运行状况检查更新

运行状况检查页面允许您通过 Splunkbase 下载 Splunk Health Assistant 加载项提供的新的运行状况检查项目。

当新的运行状况检查项目可直接通过监视控制台 UI 获取时，您可以下载这些项目，如下所示：

1. 单击**设置 > 监视控制板 > 运行状况检查**。
2. 单击**更新运行状况检查**。如果这个按钮是灰色的，那么就没有运行状况检查更新可用。
3. 登录 Splunkbase。
4. 单击**接受并继续**以安装新的运行状况检查。
这样将在 `$SPLUNK_HOME/etc/apps` 中安装最新版本的 `splunk_health_assistant_addon`，然后自动将新的运行状况检查添加到运行状况检查页面。不需要重新启动。

您现在可以在监视控制台的“运行状况检查”页面访问新的运行状况检查。

当运行状况检查更新可用时，通知消息也会显示在 Splunk Web 中。

如果您因为防火墙限制无法通过监视控制台直接下载运行状况检查更新，您也可以通过 Splunkbase 直接下载 Splunk Health Assistant 加载项，然后使用命令行安装。关于安装说明，请参阅“管理应用和加载项对象”。

创建新的运行状况检查

您可添加一个新的运行状况检查项目，如下所示：

1. 单击**监视控制台 > 设置 > 运行状况检查项目**。
2. 单击**新的运行状况检查项目**。
3. 填写标题和 ID 字段。
4. （可选）为此次检查选择应用上下文。默认为监视控制台。
5. 继续填写字段。确保在搜索中包含严重性级别 (`| eval severity_level`)。若未包含此内容，搜索则会返回结果 N/A。请参阅“关于搜索”，了解如何填写搜索字段。
6. （可选）关于**要排除的环境**，请选择独立环境或分布式环境。忽略本字段中的任何其他值。请参阅“监视控制台有什么功能？”了解有关独立和分布式模式的信息。
7. 单击**保存**。

修改会保存到您的文件系统中：`*nix` 上的 `$SPLUNK_HOME/etc/apps/<app_name>/local/checklist.conf` 或 Windows 上的 `%SPLUNK_HOME%\etc\apps\<app_name>\local\checklist.conf`。如果您没有指定应用上下文，修改会保存到应用目录 `splunk_monitoring_console`。

搜索结果格式

在独立模式中，搜索字符串会生成最终结果。在分布式模式中，此搜索在结果表中为每个实例生成一行结果。

搜索结果必须采用以下格式。

实例	指标	严重性级别
<实例名>	<指标编号或字符串>	<级别编号>

严重性级别名与值的对应关系如下。

严重性级别名	严重性级别值
错误	3
警告	2
信息	1
成功	0
N/A	-1

向搜索或仪表板添加一个钻取

您还可以在运行状况检查结果中为另一个搜索或仪表板包含一个钻取，例如监视控制台仪表板。

要包含一个监视控制台仪表板钻取：

1. 在监视控制台中选择一个现有仪表板，确保它与您要执行运行状况检查的数据相关。选择有下拉菜单的仪表板以选择实例或计算机。
2. 用下拉列表检查 URL，查看需要使用 URL 的哪些部分来指定所需的实例。在 URL 末端查找
&form.splunk_server=\$instance\$。
3. 将此 URL 修剪为以 /app/ 开头的 URI，且 \$ 分隔变量名作为一列出现在运行状况检查的搜索结果中。例如，
/app/splunk_monitoring_console/distributed_search_instance?form.splunk_server=\$search_head\$

要包含一个搜索钻取，找到或新建一个带 \$ 分隔变量的搜索。此变量必须作为一列的名称出现在运行状况检查搜索结果中。例如，index=_internal \$instance\$ 的钻取会正常工作，只要 "instance" 是运行状况检查搜索中的一个列名。

很可能您想对刚运行的搜索添加一个钻取搜索。在这种情况下，将 \$rest_scope\$ 或 \$hist_scope\$ 替换为 \$instance\$，其中 "instance" 是运行状况检查搜索中的一个列名。例如：

```
`dmc_set_index_internal` host=$instance$ earliest=-60m source=*splunkd.log* (component=AggregatorMiningProcessor OR component=LineBreakingProcessor OR component=DateParserVerbose) (log_level=WARN OR log_level=ERROR)
```

运行状况检查条件中的主动告警

许多运行状况检查项目已有对应的平台告警。您还可以将其他运行状况检查转换成告警。

此表列出了有对应的平台告警的运行状况检查项目：

运行状况检查	对应的平台告警	条件
索引状态	索引器处理器的异常状态	测试索引器实例中索引器处理器的当前状态。
物理内存使用率过高	临界系统物理内存使用情况	评估全系统范围内的物理内存使用率，并在服务器的内存使用率超过 90% 时发出警告。
即将过期或已过期的许可证	到期和不久到期的许可证	检查已到期或将于 2 周内到期的许可证。
缺少转发器	缺少转发器	检查最近与索引器断开连接超过 15 分钟的转发器。
接近临界磁盘使用情况	接近临界磁盘使用情况	检查 Splunk Enterprise 读取或写入数据的分区中磁盘使用率达 80% 的分区。
事件处理队列饱和	饱和的事件处理队列	一个或多个索引器队列正报告过去 15 分钟内，填充百分比为 90% 或以上。
分布式搜索运行状况评估	搜索节点无反应	检查每个搜索头中搜索节点（索引器）的状态。

要从运行状况检查中新建一个告警且此检查没有对应项时：

1. 运行该运行状况检查。
2. 单击在搜索中打开。
3. 用 where 子句修改此搜索。
4. 将其保存为带告警操作的新计划的搜索。例如，通过电子邮件通知管理员。

导出运行状况检查结果

您可以将某个运行状况检查项的结果导出到本地计算机以分享给其他人。

要导出某个运行状况检查项的结果：

1. 运行该运行状况检查。
2. 单击要导出结果的行。
3. 在右边的结果表中，单击导出。
4. 选择结果格式（XML、CSV 或 JSON）。您还可以选择文件名和结果数。
5. 单击导出。

监视控制台仪表板参考

摘要

本主题为监视控制台中的摘要仪表板的参考内容。请参阅本手册的“关于监视控制台”。

此仪表板显示什么？

摘要仪表板将 splunkd 运行状况报告和监视控制台特征（如健康状况检查）整合在一起，以提供动态环境故障排除 Splunk Enterprise 部署的问题。

您可以使用摘要仪表板监视部署组件的运行状态、追踪重要部署指标和调查 splunkd 运行状况报告检测到的严重的运行状况问题。

有关 splunkd 运行状况检查报告的更多信息，请参阅“关于主动 Splunk 组件监视”。

摘要仪表板包括以下面板：

异常

异常面板显示当前处于红色或黄色状态（表示出现问题）的 splunkd 运行状况报告特征。您可以使用此面板查看各问题的说明，然后访问健康检查以调查根本原因和推荐的解决方案。关于故障排除示例的详细信息，请参见“使用整合的 Splunkd 运行状况报告故障排除”。

异常			
状态	描述	功能	操作
	<ul style="list-style-type: none">Replication Factor is not metSearch Factor is not met	Indexer Clustering Data Durability	调查
	<ul style="list-style-type: none">All data is not searchable. Please ensure all the buckets have primary copies	Indexer Clustering Data Searchable	调查
	<ul style="list-style-type: none">Cluster is not indexing ready, please bring up at least RF number of peers	Indexer Clustering Indexing Ready	调查

关于运行状况检查的更多信息，请参阅“访问和自定义运行状况检查”。

部署拓扑

部署拓扑面板显示您的部署包含的组件的数量和类型，包括索引器、搜索头、许可证主服务器等。它还会显示每个组件的当前 Splunk Enterprise 版本，以及其他详细配置信息，例如索引数以及索引器群集复制因子和搜索因子设置。

部署指标

部署指标面板显示您选定的时间范围内关键指标的值。您可以编辑面板以添加或移除监视视图中的特定指标。您可以使用部署指标监视资源使用情况、索引率、搜索延迟和可深入了解性能问题的根本原因的其他指标。

您还可以将自己的自定义指标添加到 splunk_monitoring_console_assets.conf 中的部署指标面板。

部署组件

部署组件面板显示 splunkd 运行状况树中高级别特征类别的当前运行状况。使用此面板快速了解组件的运行状况。

有关 splunkd 运行状况树的更多信息，请参见 Splunkd 运行状况报告。

添加部署

添加部署侧面板允许您将单独的监视控制台实例的位置（URL）添加到书签。添加部署书签有助于在可能属于管理员权限范围内的多个 Splunk Enterprise 部署的监视控制台之间快速切换。

要将部署书签添加到摘要仪表板：

- 在摘要仪表板侧栏中，单击**添加部署**。
- 在单独的 Splunk Enterprise 部署中输入监视控制台仪表板的 URL。URL 必须以 http:// 或 https:// 开头并包含 'splunk_monitoring_console'。
- 单击**提交**。

要添加部署，角色必须有 edit bookmark mc 功能。

索引：性能

本主题为监视控制台中索引菜单中的性能仪表板的参考内容。

关于故障排除索引性能问题的更多信息，请参阅故障排除手册中的“识别和分类索引性能问题”。

索引性能：部署

索引性能：部署仪表板提供 Splunk Enterprise 部署的索引性能简介。

在索引性能概览面板中，将汇总所有索引器的总索引速率。

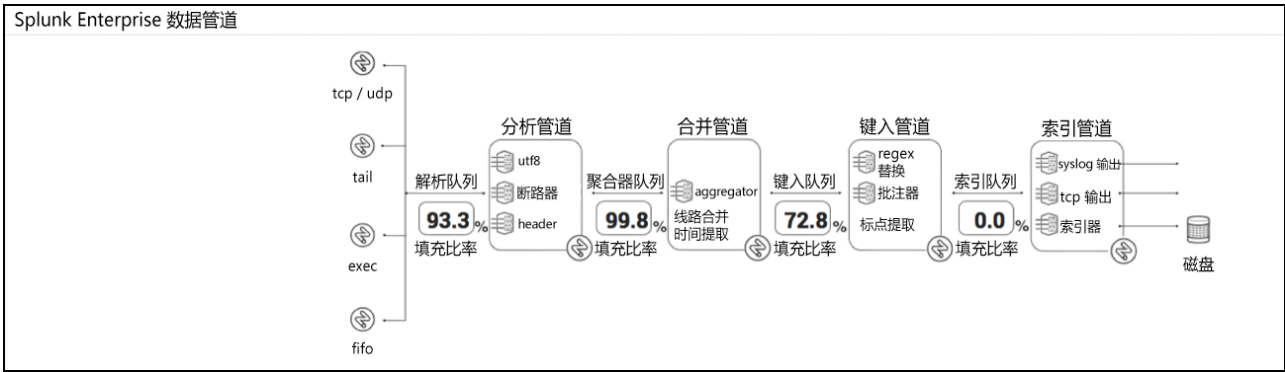
在按评估的索引速率的实例面板中，将评估索引速率，因为它使用 metrics.log（在默认情况下，它仅获取每种类型的前十个结果）。请参阅《故障排除手册》中的“关于 metrics.log”。

索引性能：实例

索引性能：实例仪表板包含有关各索引器索引性能的面板。这些面板可以针对出现在部署范围内仪表板的问题提供相关的更多详细信息。

Splunk Enterprise 数据管道的屏幕截图面板显示队列大小的衰减平均线。此平均线使用先前 15 分钟的数据。此面板和历史面板数据处理队列的填充率中值可帮助您将索引延迟的来源缩小到指定队列。数据从分析开始，并在数据管道上传输以在最后进行索引。

对于具有异常队列的实例，有如下 Splunk Enterprise 数据管道面板示例：



在本例中，尽管分析和聚合器队列具有很高的填充率，但在键入队列中的进程很有可能会发生问题。此键入队列为第一个速度变慢的队列，且数据在等待进入键入队列时正在其他两个队列中备份。

索引性能：高级

索引性能的主要目的：“高级”仪表板提供关于管道集性能的信息。您可以使用仪表板了解管道集及其组件管道的活动。请参阅《管理索引器和索引器群集》中的“管理用于索引并行化的管道集”。

此仪表板主要在咨询 Splunk 支持故障排除性能问题时使用。如果没有专家级的基本流程知识，很难充分解释信息决定性能问题修复。

此仪表板还包括一些提供少数其他高级性能指标（如 CPU 使用情况）的信息的面板。其中，每个索引器处理器活动花费的聚合 CPU 秒数面板允许您“通过子任务拆分索引服务”。该多个索引服务是与准备索引和索引后清理相关的子任务。有关子任务类别的更多信息，请参阅故障排除手册中的 metrics.log 主题。

启用 Splunk 处理器 CPU 分析面板

索引性能：高级仪表板还包括显示数据管道中 Splunk 事件处理器的 CPU 时间指标的面板，包括数据管道、聚合器、正则表达式、指标和指标方案。您可以使用这些面板识别哪些处理器和事件在管道中造成了阻塞。要使用数据填充这些面板，您必须在 limits.conf 中为每个处理器启用相应的 CPU 分析设置，如下所示：

1. 编辑 \$SPLUNK_HOME/etc/system/local/limits.conf。
2. 为每个处理器启用 CPU 分析设置，如下所示：

```
[default]
regex_cpu_profiling = true
```

```
agg_cpu_profiling = true
msp_cpu_profiling = true
mp_cpu_profiling = true
lb_cpu_profiling = true
```

有关处理器 CPU 分析设置的详细信息，请参阅 `limits.conf`。

要在指标处理器面板中查看数据，您必须提取 `statsd` 或 `collectd` 数据。

对这些仪表板进行故障排除

屏幕截图面板从 Splunk REST 端点获取数据以自检。如果屏幕截图面板缺少数据，则检查

- 平台工具的系统要求。
- `server.conf` 中的 `pipelinesets` 设置。当使用管道设置（即，如果 `pipelinesets` 被设为大于 1 的值）时，监视控制台索引性能仪表板中的一些面板将为空。

这些仪表板的历史面板从 `metrics.log` 获得数据。

索引：索引和卷

本主题是监视控制台中的所有索引：索引和卷仪表板的参考资料。请参阅“关于监视控制台”。

这些视图显示什么？

索引和卷仪表板由六个关于索引的单独仪表板组成，每个仪表板包含若干个面板。

总之索引和卷仪表板描述如何在您的索引器上使用磁盘。这些视图分解资源使用情况视图中显示的数据。

解释这些视图的结果

如果您的系统存储空间紧张，请访问索引和卷仪表板。使用该数据来帮助您评估和修改您的保存策略。请参阅 *管理索引器和索引器群集* 中的“索引器如何存储索引”。

在这些视图中查找的内容

在索引和卷：实例仪表板中，以蓝色突出显示的实例将数据桶滚动到冻结。请参阅 *管理索引器和索引器群集* 中的“索引器如何存储索引”。

在索引和卷：部署仪表板中，正在冻结的数据信息可能是一个红色标志。索引和卷面板显示此信息。

在索引详情：部署仪表板中，当数据在达到时间限制之前就开始冻结时，请通过 Data Age vs. Frozen Age 检查索引器的实例面板。仪表板中的钻取将帮助您调查研究。

索引：输入：HTTP 事件收集器

本主题为针对监视控制台中 HTTP 事件收集器仪表板的参考资料。请参阅“关于监视控制台”。

这些视图显示什么？

监视控制台为 HTTP 事件收集器提供两个仪表板。一个提供您的部署的整体性能概述，另一个提供您的部署中每个实例的性能详情。

我应该查找什么内容？

您可以在部署范围仪表板中启动，以调查无关的性能。钻取以查找相关实例范围仪表板中问题的更多详情。

解释这些视图的结果

在 HTTP 事件收集器：部署仪表板，所显示的标记列表为当前配置的标记列表。因此如果您的标记已禁用，则不会出现在标记下拉菜单中。相反，实例范围视图中将显示所有启用和禁用的标记。

请参阅 *数据导入手册* 中的“设置和使用 HTTP 事件收集器”。

对这些视图进行故障排除

要使用 HTTP 事件收集器，正在收集的实例所运行的 Splunk Enterprise 必须为 6.3.0 或以上版本。如果您的实例为通用转发器，则监视控制台无法监视，因为它不能是搜索节点。

在分布式或独立模式下，如果这些仪表板缺少数据，则确认您是否已完成监视控制台的所有设置步骤。

索引：输入：数据质量

本主题为监视控制台中数据质量仪表板的参考资料。请参阅“关于监视控制台”。

此仪表板显示什么？

数据质量仪表板报告与事件处理相关的问题，例如：

- 自动键入数据来源
- 换行
- 时间戳提取
- 时区检测
- 线路合并
- 超大事件（高线计数和/或大事件，len(_raw)）
- 索引延迟（_indextime - _time）
- 指标数据集
- 将日志事件转换为指标数据

数据质量仪表板包括以下面板：

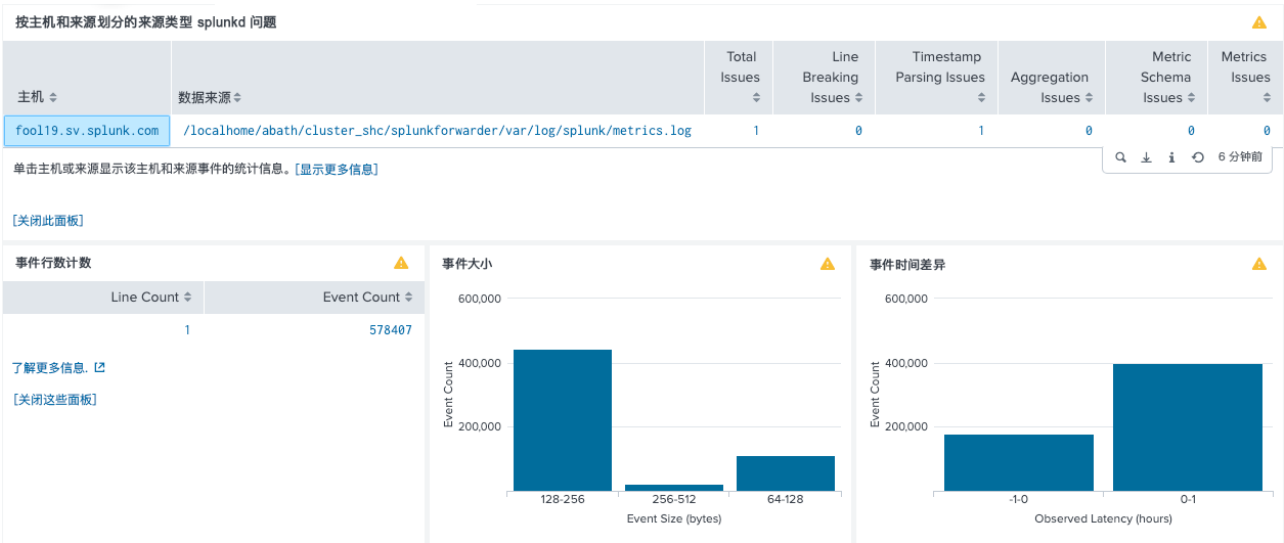
按源类型分类的事件处理问题

按源类型分类的事件处理问题面板按源类型显示在选定时间范围内指定索引器上发生的事件处理问题的数量。单击表中的任何数字即可查看相关搜索结果，了解特定问题的更多信息。单击源类型的名称即可按主机和源查看适用于该源类型的问题。

按来源类型划分的事件处理问题								
Sourcetype	Total Issues	Host Count	Source Count	Line Breaking Issues	Timestamp Parsing Issues	Aggregation Issues	Metric Schema Issues	Metrics Issues
syslog	71	5	6	68	3	0	0	0
splunkd	1	1	1	0	1	0	0	0

按主机和源分类的源类型问题

按主机和源分类的源类型问题面板按主机和源显示事件处理问题的数量。该面板可用于识别特定问题的来源。单击主机或源的名称即可查看来自该主机和源的事件的其他统计信息，包括事件行计数、事件大小和事件时间差异。



在此仪表板中解释结果

有关如何解读和解决此仪表板指示的事件处理问题的相关信息，请参阅以下主题：

- 《数据导入》手册中的“解决数据质量问题”。

- 《指标》中的“指标入门”和“将事件日志转换为指标数据点”。

仪表板故障排除

此仪表板使用 `splunkd.log` 中的数据。

如果钻取搜索结果加载缓慢，则您遇到的问题数量可能多于系统可以适当处理的数量。在页面顶部尝试缩小时间范围。

索引：许可证使用情况

监视控制台中的“许可证使用情况”报表显示的信息与“许可证主服务器”实例上的“许可证使用情况”报表的相同。请参阅《管理员手册》中的“关于 Splunk Enterprise 许可证使用情况报表视图”。

如果您的 Splunk Enterprise 部署中有多个许可证主服务器，则可以使用监视控制台中的“许可证使用情况”报表来选择和查看每个许可证主服务器的许可证报表。

索引：SmartStore

多个仪表板监控 SmartStore 状态。仪表板的使用范围或者是单个实例，或者是整个部署。在索引菜单和 SmartStore 子菜单下找到仪表板：

- SmartStore Activity：实例
- SmartStore Activity：部署
- SmartStore Cache Performance：实例
- SmartStore Cache Performance：部署

SmartStore Activity 仪表板

SmartStore Activity 仪表板提供远程存储相关的活动信息，如：

- 远程存储连接
- 数据桶上传/下载活动
- 数据桶上传/下载故障计数

SmartStore Activity 仪表板还包括一些复选框，如果您当前正在执行数据迁移或启动，可以从中选择显示进程。

SmartStore Cache Performance 仪表板

SmartStore Cache Performance 仪表板提供本地缓存相关信息，如：

- 影响缓存逐出的 `server.conf` 设置的值
- 数据桶逐出率
- 用于从远程存储下载数据桶的搜索时间部分
- 缓存成功率
- 重复数据桶下载

有关故障排除 SmartStore 的更多信息，请参阅《管理索引器和索引器群集》中的“故障排除 SmartStore”。

索引：索引器群集化：状态

本主题是分布式管理控制台中的索引器群集化：监视控制台中的状态仪表板。请参阅“关于监视控制台”。

此视图显示什么？

此视图类似于索引器群集主节点上的主节点仪表板。请参阅管理索引器和索引器群集手册中的“查看主节点仪表板”。

排除此视图的故障

您应该能在该仪表板上查看您的所有索引器群集的数据。如果您有多个索引器群集并且无法查看所有索引器群集的数据，请检查您是否遵循在 Splunk Enterprise 部署中监视控制台的设置步骤。具体来说，

- 您将监视控制台托管在作为您所有群集中成员的搜索头上。
- 您已标记索引器群集。
- 每个群集主节点已作为搜索节点添加到监视控制台中。

索引：索引器群集化：服务活动

本主题是分布式管理控制台中的索引器群集化：监视控制台中的服务活动仪表板。请参阅“关于监视控制台”。

此视图显示什么？

有关索引器群集化的多个面板。

在此视图中解释结果

该仪表板中的面板可能不会显示数据。仅当进行数据桶修复活动的时候才会显示数据。

这些面板帮助确定有多少 Splunk Enterprise 必须执行的修复任务（也就是它的 backlog）。修复任务会导致多个任务。

最后两个面板测量用于单击群集化端点所用的时间。

Splunk 支持和/或工程师可能会查看该数据以配置群集主节点正进行的活动类型。

在此视图中查找的内容

当在群集中发生意外事件时使用该视图，例如对等节点出现故障。

理想情况下，您永远都不会有任务待定。

如果搜索因子不满足，您的搜索结果将是不完整的。

如果生成条件不满足，整个群集都不可搜索。在 6.1 版本之后，群集不可能发生该情况。

在事件发生后，您可以查看该仪表板以确保任务（和工作）数呈下降趋势。对于运行状况良好的群集，您会希望这些面板上没有数据。

排除此视图的故障

确保您已完成所有监视控制台设置步骤。

特别是：

- 从搜索头和 Deployer 向索引器转发日志。请参阅“监视控制台前提条件”。
- 所有的索引器群集化仪表板都需要索引器群集的成员。请参阅“设置群集标签”。

搜索：搜索活动

本主题是监视控制台中的搜索活动：实例和搜索活动：部署仪表板的参考资料。请参阅“关于监视控制台”。

这些仪表板显示什么？

搜索活动仪表板在 Splunk Enterprise 部署中提供搜索活动概览和按实例划分的更详细的信息。

在这些仪表板中解释结果

在搜索的资源使用情况中值面板中，请注意：

- 将聚合所有搜索的资源使用情况。
- 内存使用情况代表物理内存。
- 在此图表中，CPU 使用情况以一个核心的百分比形式表示，而不是以系统范围 CPU 使用情况表示。结果是，您可能在此看到值大于 100%。对于分布式管理控制台中的 CPU 使用情况的其他示例，并非如此。

在聚合搜索运行时面板中，请注意：

- 对于图表中的每个时间 bin，此监视控制台将在此时间范围运行的所有搜索的运行时都加起来。因此，例如，您可能在 5 分钟内看到 1,000 秒的搜索。这意味着多个搜索在此 5 分钟期间运行。
- 对于历史批处理和 RT 索引的模式，历史批处理仅可在 Splunk Enterprise 内由某些功能派遣（例如，计划程序）。RT 索引意味着索引的实时。

在内存消耗排名前 10 的搜索面板中，SID 意味着搜索 ID。如果您要了解有关保存的搜索的信息，audit.log 会将您保存的搜索的名称（savedsearch_name）与其搜索 ID（search_id）、用户和时间进行匹配。使用 search_id，您可在其他位置查找搜索，如在 Splunk 平台搜索日志中（请参阅“Splunk 记录有关它自身的哪些内容”）。

这些仪表板中显示的内存和 CPU 使用情况仅用于搜索。有关所有 Splunk Enterprise 资源使用情况，请查看资源使用情况仪表板。

在按 CPU 使用情况中值的实例面板上，因为有多核心，CPU 可能大于 100%。

在按内存使用情况中值的实例面板上，内存为物理内存。

对于历史批处理和 RT 索引的模式：历史批处理仅可在 Splunk Enterprise 内由某些功能派遣（例如，计划程序）。RT 索引意味着索引的实时。

在这些仪表板中查找的内容

与您的系统限制相比，考虑您的搜索并发和资源使用情况。

有关信息，请参阅：

- *搜索手册*中的“编写更好的搜索”。
- *搜索手册*中的“搜索入门”。
- *搜索手册*中的“配置计划的报表优先级”。
- *知识管理器手册*中的“基于摘要的搜索和数据透视表加速概述”。
- *容量规划手册*中“并发用户和搜索如何影响性能”。

常规模式就是在此仪表板中查看所有面板，便于寻找即将超过机器中限制的内容。

对这些仪表板进行故障排除

历史面板从自检日志中获取数据。如果面板为空白或来自非索引器的信息缺失，则检查：

- 您是否正在将自检日志转发到索引器，以及
- 平台工具的系统要求。

在搜索活动中：默认情况下，在实例 > 搜索活动面板中，每十秒会进行一次屏幕截屏。因此，如果当前没有搜索运行，或如果您运行的搜索存在时间很短，则屏幕截屏面板为空白并显示“无查找结果”。

搜索：搜索使用情况统计信息

本主题是搜索使用情况统计信息的参考资料：实例和搜索使用情况统计信息：部署仪表板的参考资料。请参阅“关于监视控制台”。

这些仪表板显示什么？

这些仪表板提供部署中所有搜索头的搜索使用方法的相关统计信息和每个实例的详细信息。

在这些仪表板中解释结果

以下描述应用于每个仪表板中长时间运行的搜索表格：

- 如果“最早时间”或“最晚时间”为空，则很可能是一个实时搜索。
- 如果“最早时间”为“-”，表示未指定最早时间，则最早时间将是计算机 epoch 时间的开端。大多数 *nix 环境中为 1970 年 1 月 1 日。
- 如果“最晚时间”为“-”，表示未指定最晚时间，则最晚时间将是“现在”。

在搜索使用情况统计信息：中实例 > 常用搜索命令，运行时以秒为单位。

在这些仪表板中查找的内容

最好查看长时间运行的搜索。您可能找到您可优化的搜索。

有关更多信息，请参阅 *搜索手册* 中的“编写更好的搜索”。

对这些仪表板进行故障排除

此视图中的历史面板从 audit.log 中获取数据。如果面板为空白或缺失来自非索引器的信息，则验证您是否正在将自检日志转发到索引器。

此长时间运行的搜索面板还使用来自 REST 端点的信息。

搜索：KV 存储

本主题是 KV 存储的参考资料：**部署和 KV 存储：监视控制台中的实例仪表板**。请参阅“关于监视控制台”。

这些仪表板显示什么？

部署范围内和实例范围内的 KV 存储仪表板追踪许多从 KV 存储中收集的相同统计信息。

KV 存储：部署仪表板在监视控制台中提供跨 Splunk Enterprise 部署中所有 KV 存储所聚合的信息。按不同的指标值分组实例。对于此仪表板中要包含的实例，它必须使用 **KV 存储**的服务器角色设置。在监视控制台设置页面执行此操作。

监视控制台中的实例级别 KV 存储视图显示有关运行应用键值存储的单个 Splunk Enterprise 实例的性能信息。如果您已将监视控制台配置为分布式模式，则您可在部署中选择要查看的实例。

性能指标

来自 `_introspection` 索引中的 `KVStoreCollectionStats` 组件的集合指标，它为 `/services/server/introspection/kvstore/collectionstats` REST 端点上数据的历史记录。这些指标为：

- 应用程序。集合所属的应用程序。
- 集合。KV 存储中集合的名称。
- 对象数量。在集合中存储的数据对象的计数。
- 加速。在集合中设置的加速的计数。注意：这些是用于性能和搜索加速的传统数据库样式索引。
- 加速大小。在集合中设置的索引的大小，以 MB 为单位。
- 集合大小。在集合中存储的所有数据的大小，以 MB 为单位。

屏幕截图通过 REST 端点收集，它从相关自检组件传输最新的信息。此 KV 存储实例屏幕快照使用端点 `/services/server/introspection/kvstore/serverstatus`。

- 锁定百分比。系统保持全局读取或编写锁定的 KV 存储运行时间的百分比。高的锁定百分比具有普遍影响。它可使复制停止，甚至使应用程序调用变慢、超时或失败。
- 页面故障百分比。导致页面故障的 KV 存储操作的百分比。百分比接近于 1 表示系统性能较差，也是迟缓持续的先行指标，因为 KV 存储被强制回退到磁盘 I/O（而非在内存中有效访问数据存储）。
- 内存使用情况。KV 存储所使用的常驻、映射和虚拟内存数量。对于 KV 存储，虚拟内存的使用情况通常为映射内存的两倍。虚拟内存使用情况超过映射内存的 3 倍可能指示内存泄漏。
- 网络流量。KV 存储网络流量的总流入和流出，以 MB 为单位。
- 刷新百分比。KV 存储刷新磁盘所有写入内容所需分钟的百分比。接近于 1 指示写入磁盘困难或一致的大量写入操作。某些 OS 刷新数据的时间快于 60 秒。在这种情况下，即使有写入瓶颈，此数字可能还是很小。
- 操作。发布到 KV 存储的操作的计数。包括命令、更新、查询、删除、getmores 和插入。此自检进程发布命令以传送 KV 存储 stats，以使命令计数器的优先级通常比大多数其他操作高。
- 当前连接。KV 存储上打开的连接计数。
- 总队列。排队等待锁定的总操作。
- 总断言。由 KV 存储引发的断言的总数。一个非负数值可指示需要检查 KV 存储日志。

历史

本节中的许多统计信息存在于**快照**部分。此**历史**视图显示一组时间跨度上的指标的趋势信息。这些 stats 收集在 `KVStoreServerStats` 中。默认情况下，此**历史**面板显示过去 4 小时的信息。历史图形中的间隙通常表示 KV 存储或 Splunk Enterprise 无法连接的点。

- 内存使用情况 - 请参见上面的章节。
- 复制滞后。在 Primary OpLog 中记录的最后操作和应用于第二个节点的最后操作之间的时间量。超过主要 opLog 窗口的复制滞后可导致数据在复制集的所有节点中无法正确复制。在不具有复制的独立实例中，此面板不返回任何结果。注意：复制滞后收集在 `_introspection` 索引的 `KVStoreReplicaSetStats` 组件中。
- 操作计数（按分钟平均计算） - 请参见上面的章节。此面板显示所有操作的各个操作类型（例如，命令、更新和删除）。
- 断言 - 请参见上面的章节。此面板允许基于断言的类型筛选 - 消息、正则表达式、滚动更新、用户、警告。
- 锁定百分比。系统保持全局、读取或编写锁定的 KV 存储运行时间的百分比。通过保持锁定的类型筛选此面板：
 - 读取。用于读取操作的保持锁定。
 - 编写。用于编写操作的保持锁定。KV 存储锁定为“写入者贪婪”，因此写入锁定可组成集合上总锁定的大部分。
 - 全局。由全局系统保持的锁定。KV 存储实施“集合”级别锁定，以减少全局锁定的攻击式使用需求。
- 作为总操作百分比的页面故障 - 请参见上面的章节。
- 网络流量 - 请参见上面的章节。添加到此面板的内容为对 KV 存储作出的请求。
- 队列超时。队列的数量，通过以下方式拆分：
 - 读取。等待读取锁定打开的读取操作的计数。
 - 编写。等待写入锁定打开的写入操作的计数。
 - 总计。

- 连接超时。
- 刷新磁盘所用的每分钟百分比 - 请参见上面的章节。
- 最慢的操作。在选定时间期间由 KV 存储记录的十个最慢的操作。如果关闭所有集合的配置文件，则即使操作运行很慢，也可能不会有结果。在 collections.conf 中，针对每一个集合启用配置文件。

部署快照

部署快照统计信息访问 /services/server/introspection/kvstore/serverstatus REST 端点。

这些仪表板从哪里获得数据？

KV 存储在 _introspection 索引中收集数据。

这些统计信息拆分为以下组件：

- KVStoreServerStats。有关 KV 存储进程如何作为一个整体执行的信息。每 27 秒轮询一次。
- KVStoreCollectionStats。有关 KV 存储内集合的信息。每 10 分钟轮询一次。
- KVStoreReplicaSetStats。有关跨 KV 存储实例复制数据的信息。每 60 秒轮询一次。
- KVProfilingStats。有关慢速操作的信息。每 5 秒轮询一次。仅当配置文件启用时可用。注意：仅在开发系统或对 KV 存储性能超过其在默认面板中可用的性能问题排除故障时，启用配置文件。配置文件可负面影响系统性能，所以不应该在生产环境中启用它。

另外，KV 存储在由 Splunk Enterprise 收集的许多内部日志中生成条目。

解释这些仪表板

面板	严重	警告	正常	解释
每个操作的页面故障	1.3+ 读取需要大量磁盘 I/O，这可指示需要更多 RAM。	0.7 - 1.3 读取定期需要磁盘 I/O。	0 - 0.7 读取很少需要磁盘 I/O。	衡量 Splunk Enterprise 内存中的内容不满足读取请求的频率并要求 Splunk Enterprise 连接磁盘。Windows 计算软页面错误，因此 Windows 计算机显示更多页面错误。改用锁定百分比和队列。
锁定百分比	50%+	30% - 50%	0 - 30%	高的锁定百分比可使复制停止和/或导致应用程序调用变慢、超时或失败。高的锁定百分比通常意味着在节点上发生的大量写入活动。
网络流量	N/A	N/A	N/A	网络流量应与系统使用 and 应用程序预期相称。无默认阈值应用。
复制延迟	大于 30 秒	10 - 30 秒	0 - 10 秒	复制需求取决于系统。通常，复制设置成员不应显著落后于 KV 管理员。超过 30 秒的复制延迟可指示增加的复制问题。
主要操作日志窗口	N/A	N/A	N/A	用于参考。这是系统保存在操作日志中用于恢复的数据量（以时间表示）。
刷新率	50% - 100%	10% - 50%	0 - 10%	高的刷新率指示大量写入操作或迟缓的系统性能。

对这些仪表板进行故障排除

历史面板从 _introspection 和 _internal 索引中获取数据。这些面板中的时间间隔表示 KV 存储或 Splunk Enterprise 无法连接的时间。如果某个面板完全空白或缺失来自特定 Splunk Enterprise 实例的数据，则检查：

- 您是否正在将日志转发到索引器，和
- 平台工具的系统要求。

搜索：计划程序活动

本主题为“监视控制台”中计划程序活动仪表板的参考资料。请参阅“关于监视控制台”。

这些仪表板显示什么？

分布式管理控制台中的计划程序活动：部署仪表板显示搜索或报表计划程序简介。实例仪表板显示特定实例中计划程序相关的更详细的信息。

这些仪表板显示计划程序的活动和成功率。即所有尝试运行的搜索，有多少成功了？计划的搜索可能因为并发问题或因为搜索

负载失败。

这些仪表板中的面板符合故障类型。跳过比例和执行延迟量化计划程序的性能。

无论您是否正在使用搜索头群集化，计划程序活动视图都非常有用。如果您有搜索头群集，还可以使用[搜索头群集化：处理管理员如何安排计划程序任务的相关问题的计划程序委派仪表板](#)。

在这些仪表板中解释结果

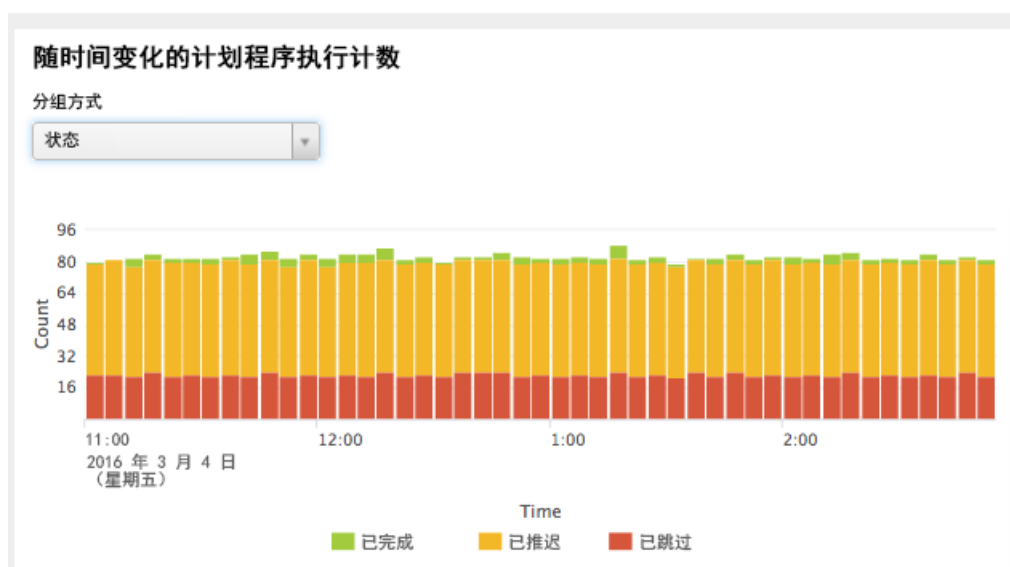
在部署仪表板中，统计信息面板描述的是计划程序实施每个实例的情况，但包括部署中的所有实例。例如，最大值是指部署中任何单个实例中的最大数。

在这些仪表板中查找的内容

如果您的计划程序达到所允许的并发搜索的最大数，则可能会在计划其他或长时间运行搜索时遇到一些问题。请参阅[“配置计划的报表优先级”](#)，以了解更多相关信息。

快照量化跳过比例和平均执行延迟都会较低。

以下是计划程序活动的示例：正在跳过报表的计划程序的实例面板。



如要了解计划程序为何跳过报表，请向下滚动至标签为[根据名称和原因跳过报表的计数的面板](#)。

对这些仪表板进行故障排除

计划程序活动仪表板需要运行 Splunk Enterprise 6.3.0 或以上版本的受监视实例。

确保您已完成所有监视控制台设置步骤。

搜索：分布式搜索

本主题是与分布式搜索相关的监视控制台的参考资料。请参阅本手册的[“关于监视控制台”](#)。

这些视图显示什么？

分布式搜索视图会显示分布式搜索框架的运行状况、活动和性能。

搜索过程中，这些视图专注于搜索头与其对等节点的通信。与此相反，搜索头群集化仪表板描述的是搜索头之间的通信。

使用这些视图有如下两种基本的方式：

1. 导航至特定于此产品区域的视图顶部的运行状况检查。验证这些基本的检查已通过。
2. 如果您的用户报告分布式搜索问题，则使用这些视图来了解组件执行的方式。例如，用户可能会看到类似“搜索节点无法参与搜索”或关于搜索节点无法使用或耗时太长的消息。对于此类消息类型，请使用这些仪表板。如果您知道实例正在报告问题，则直接跳到[分布式搜索：实例视图](#)；否则从[分布式搜索：部署视图](#)开始。查看这些实例行为方式的历史记录。这些视图可以帮助您了解分布式搜索框架。有助于您更好地了解问题的性质。

解释这些视图的结果

对于任一视图（实例或部署），您都可以通过选择页面顶部**搜索头**或**索引器**检查搜索头或搜索节点。仪表板显示的指标更改取决于您选择的角色。

在“实例”视图中，选择搜索头，以从此搜索头操作上下文查看搜索头与其对等节点的通信方式。

在这些视图中查找的内容

针对每个视图顶部**运行状况检查**中红色标记进行扫描。整个分布式搜索基础架构间的运行状况检查并不复杂，相反，它们为基础内容的高级检查。

快照面板显示请求响应时间和软件包复制时间。这些时间至关重要，因为一般来说非常短暂（一秒内）。通常，如果这些时间是几秒或更长，则可能出错。

在**部署**视图中，选择搜索头径向并使用列排序检查时间指标：

- Dispatch 目录根据操作获取，因此时间超过 15 秒表明出现问题。
- 软件包目录的获取同样应当少于 15 秒。

这三种**检测信号**指标在搜索头中至关重要。当该数值比较高时，搜索节点可能过度订阅，并且无法及时响应通信请求。如果响应时间超过 1 秒，则说明结果并不理想，可能表示有潜在问题。响应时间如果超过 5 秒或 10 秒，则会针对超时开始请求。出现这种情况时，搜索可能会真正出现故障。如要继续排除故障，则通过对应于此对等节点的**资源使用情况：计算机**视图进行匹配。请参阅**故障排除手册**中“搜索节点中的间歇性验证超时”，以了解更多信息。

有关分布式搜索问题的其他帮助，请参阅**分布式搜索手册**中的“一般故障排除问题”。

对这些视图进行故障排除

Splunk Enterprise 6.3.0 中详细介绍了这些视图所使用的指标。如果您部署组件所在的 Splunk Enterprise 版本低于 6.3.0，则这些视图不会包含来自该组件的数据。

快照面板使用来自各种端点的数据。

这些视图中的所有历史面板从 `metrics.log` 中获取数据。

搜索：知识软件包复制

有两个仪表板监视知识软件包活动。在**搜索**菜单和**知识软件包复制**子菜单下找到仪表板：

- 知识软件包复制
- 级联复制

要想查看仪表板，必须在“分布式模式”下配置监视控制台。

知识软件包复制仪表板

知识复制仪表板提供当前和历史软件包复制活动的信息。还提供配置信息。此仪表板适用于所有复制策略。

级联复制仪表板

级联复制仪表板是特定于使用级联复制策略的部署。此仪表板提供的信息包括当前和历史信息。

有关故障排除知识软件包复制的信息，请参阅《**分布式搜索**》中的“故障排除知识软件包复制”。

搜索：搜索头群集化

本主题是与搜索头群集化相关的所有监视控制台仪表板的参考资料。请参阅“关于监视控制台”。

状态和配置

状态和配置仪表板是搜索头群集的概述。它是高级信息。

配置复制

配置复制仪表板可用来深入了解用户对任何搜索头群集成员（如一个新事件类型）进行更改的配置以及这些更改如何通过群集传输。如果您在此传输期间发现明显的滞后，则可以使用此仪表板。

操作参考：以下是**超时操作计数**和**超时操作所用时间**面板中显示的低级别操作。这些面板对于故障排除很有用。

操作	描述
accept_push	在管理员上，接受来自成员的复制更改。
acquire_mutex	获取“保护”配置系统的互斥锁（互相排斥）。
add_commit	在成员上，记录更改。
base_initialize	初始化配置的“根路径”（例如 \$SPLUNK_HOME/etc）。
check_range	比较配置更改的两种范围。
compute_common	找到成员和管理员之间最新的共同更改。
pull_from	在成员上，提取来自管理员的更改。
purge_eligible	在成员上，清除来自 repo 较早的更改。
push_to	在成员上，将更改推送给管理员。
release_and_reacquire_mutex	释放然后重新获取“保护”配置系统的互斥锁。这类似于 acquire_mutex。
reply_pull	在管理员上，回复成员的 pull_from 请求。
repo_initialize	（从磁盘中）初始化配置的 repo。

我们期望该信息被 Splunk 支持使用。如果您的配置复制有问题，您可以查看该仪表板获得线索。但是，我们期望您在报告支持案例后更频繁地使用该仪表板收集信息，而不是凭借自己的洞察力。

项目复制

项目复制仪表板包含描述要复制的搜索项目的群集 backlog 的多个面板。请参阅《分布式搜索手册》中的“搜索头群集化架构”。

警告和错误模式面板基于消息中的文本对于警告和错误事件进行分组。分组功能使用群集命令。

如果您的搜索头群集准时复制项目，则其**等待复制的项目数**为零或接近于零。少量等待复制的项目可能不是告警标志。项目数始终很高，特别是项目数的增长，可能表示复制出现问题。如果您有许多项目正在等待复制，一些使用另一个搜索头的项目可能不会获得本地缓存，并且在搜索可用性上将遇到响应缓慢的情况。

要复制的项目的中值计数（如其所示）是一个中值。这意味着如果在短时间内出现高峰，在更大的时间范围内则不会看到它们。

项目复制任务活动面板显示复制任务的更改率（特别是 backlog 的更改率）。backlog 的更改率可以是负数，如果您的群集追上其 backlog 的话。在该面板中，要查找的红色标志是不断增长的 backlog（即，如果 backlog 的更改率始终是正数的话）。如果此情况发生，上文**要复制的项目的中值计数**面板会显示持续增长的 backlog。

计划程序委派

请参阅《分布式搜索手册》中的“搜索头群集化架构”。

在**计划程序状态**面板中，请注意 max_pending 和 max_running 是 30 秒周期内的“最高纪录”。即，它们是 30 秒跨度内待定或运行的任务数的最大值。您可以在该面板中选择若干个功能中的一个。“最大值”功能用最直接的方式处理这些统计值。但是要花一些时间来思考一下“平均值”、“中值”或“90%”是什么意思。例如：假定 max_pending 在 30 秒内是 4，那么对于 max_pending 的值进行平均。最终您将获得高值的平均值，而不是所有值的平均值。所以如果待定任务数波动很大，平均的 max_pending 值可能并不接近于待定任务数的直接平均值。

应用部署

当应用从 Deployer 分发到搜索头群集成员时，应用部署仪表板会监视这些应用。

请参阅《更新 Splunk Enterprise 实例手册》中的“关于部署服务器和转发器管理”。

在**应用状态**面板中，始终不一致表明 Deployer 尚未完成将应用部署给其成员。

对这些仪表板进行故障排除

搜索头群集化仪表板需要运行 Splunk Enterprise 6.2.0 或以上版本的受监视实例。

确保您已完成所有监视控制台设置步骤。

特别是：

- 从搜索头和 Deployer 向索引器转发日志。请参阅“监视控制台前提条件”。
- 对于所有的搜索头群集化仪表板，需将搜索头设为监视控制台的搜索节点。
- 所有的搜索头群集化仪表板都需要搜索头群集的成员。请参阅“设置群集标签”。请注意，应用 Deployer 也需要标签。

对于“应用部署”仪表板：

- Deployer 需要是监视控制台的搜索节点，或者监视控制台可以托管在 Deployer 上。请参阅“将实例作为搜索节点添加”。
- Deployer 需要具备 Deployer 角色（它可以自动检测）。在监视控制台 > 设置 > 常规设置中检查。
- Deployer 需要手动标记为 SHC 的成员。（它不会自动检测。）在监视控制台 > 设置 > 常规设置中设置。
- Deployer 必须如上文所述转发日志。请参阅“监视控制台前提条件”。

资源使用情况

本主题为监视控制台中的“资源使用情况”仪表板的参考内容。请参阅“关于监视控制台”。

这些仪表板显示什么？

有几个“资源使用情况”仪表板，可通过**资源使用情况**菜单访问。资源使用情况：部署仪表板提供部署级的资源信息，例如 CPU 使用情况、物理内存使用情况和磁盘使用情况。这些面板对于容量规划很有用。

其他仪表板提供实例或计算机的使用信息。

在这些仪表板中解释结果

有关这些仪表板中物理内存使用情况：在 Linux 上，OS 使用可用物理内存以缓存文件系统资源。但此内存为自由绑定，如果更高优先级的进程需要它，OS 就会将其释放。监视控制台报表无法识别此方法自由锁定的内存的数量。

这些仪表板中的历史数据来自 resource_usage.log（位于 _introspection 索引）。请参阅《故障排除手册》中的章节“平台检测记录了哪些数据”。

资源使用情况：部署

此部署范围磁盘使用情况中值面板将每个 Splunk Enterprise 实例所使用的所有分区考虑在内。

资源使用情况：计算机

此仪表板对于操作事后总结以及容量规划很有用。有关更多信息，请参阅**容量规划手册**。

在 **CPU 使用情况** 中值面板上，100% 意味着整个系统，无论此系统具有多少个核心。这与**搜索活动**仪表板相反，其中 100% 意味着一个核心。

此仪表板中的磁盘空间仅指其上具有 Splunk Enterprise 实例的分区。

资源使用情况：实例

在两个“进程类”面板上，进程类的值可以是 splunkd 服务器、搜索、Splunk Web、索引服务、脚本式输入、KVStore 或其他内容。

进程类是某个类中的进程聚合。有关

- splunkd 的更多信息，请参阅**安装手册**中的“Splunk Enterprise 架构和流程”。
- 有关搜索的更多信息，请参阅**搜索手册**中的“搜索入门”和“编写更好的搜索”。
- splunkweb 的更多信息，请参阅**安装手册**中的“Splunk Enterprise 架构和流程”。
- 脚本式输入的更多信息，请参阅**数据导入手册**中的“通过脚本式输入从 API 及其他远程数据接口获取数据”。
- KVStore，请参阅监视控制台中的 KV 存储仪表板仪表板。

索引服务包含与索引相关的维护任务。这些任务在索引管道的末尾处运行，但属于异步运行。这些进程独立运行，不通过 splunkd。

此磁盘使用情况和磁盘使用情况中值面板仅列出 Splunk Enterprise 使用的分区。

在这些仪表板中查找的内容

部署范围内的仪表板组实例面板按照值范围分组。在这个仪表板中，查找离群值：区别于其他的实例。

在所有资源使用情况仪表板中，查找时间周期内出现的模式。例如，在实例和计算机仪表板中查找内存使用情况随时间推移只增加不恢复的情况。

在实例仪表板中，如果使用许多资源的进程类是搜索，则通过进入搜索活动：进一步调查。实例仪表板。

对这些仪表板进行故障排除

历史面板从自检日志中获取数据。如果面板为空白或来自非索引器的信息缺失，则检查：

- 您是否正在将自检日志转发到索引器，以及
- 平台工具的系统要求。

资源使用情况：CPU 使用率

本主题是有关监视控制台中的“资源使用情况：CPU 使用率”仪表板的参考内容。请参阅本手册的“关于监视控制台”。

这些仪表板整合了其他“监视控制台”页面中现有的 CPU 使用率视图，提供一个中央位置来监视 Splunk Enterprise 部署的 CPU 资源消耗情况。

CPU 使用率：部署

CPU 使用率：部署仪表板显示整个分布式部署中的物理 CPU 和虚拟 CPU（vCPU）的使用情况。要了解 vCPU 资格的相关内容，请参阅《管理员手册》中“vCPU 针对基础设施许可是如何计算的”。

要查看特定服务器角色的 CPU 使用率，请从角色菜单中选择服务器角色。

快照概述

快照视图包括以下面板，提供 CPU 资源的概要介绍：

- **有效 CPU**：此面板显示部署中所有实例的平均 CPU 使用率（%），以及分配的 vCPU 总数。
- **搜索头**：此面板显示作为搜索头运行的所有实例的 CPU 使用率和 vCPU 计数。
- **索引器**：此面板显示作为索引器运行的所有实例的 CPU 使用率和 vCPU 计数。
- **按主服务器角色分类的 CPU**：此面板显示按服务器角色计算的平均 CPU 使用率（%）和 vCPU 计数。使用此面板可以评估不同服务器角色的当前 CPU 资源消耗情况。



按实例分类的 CPU 使用率

按实例分类的 CPU 使用率面板显示分布式部署中每个实例的 CPU 内核数（CPU/vCPU）、CPU 使用率（%）和平均负载。根据每个实例的 CPU 状态，“CPU 使用率（%）”和“平均负载”列会按如下方式进行颜色编码：0-60 是绿色，60-80 是黄色，80-100 是橙色，100+ 是红色。

您可以使用此面板来跟踪多个实例中 CPU 使用率的状态，并随时了解可能影响性能的 CPU 超载情况。单击列表中的任何实例

即可打开“CPU 使用率：实例”仪表板，然后即可查看该特定实例的详细 CPU 使用率信息。

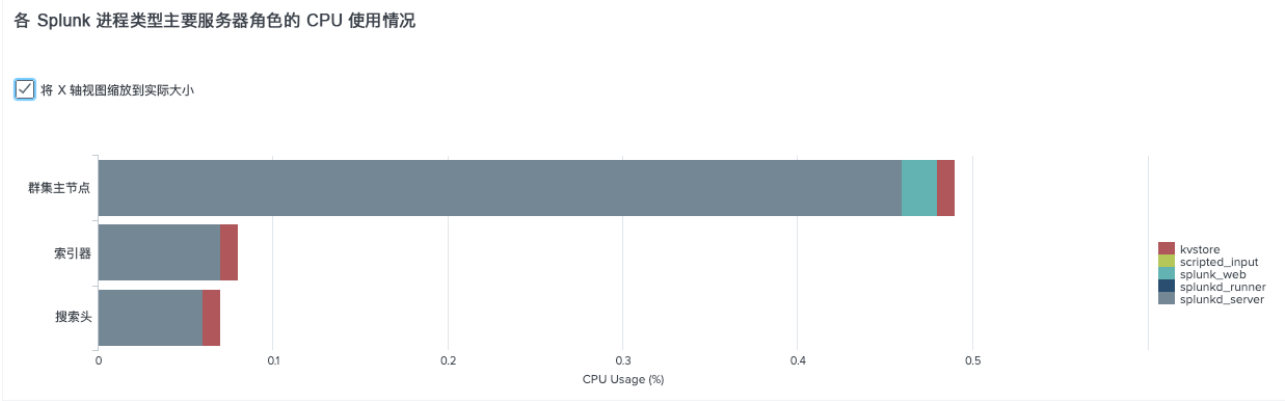
各实例的 CPU 使用情况				
实例	角色	CPU Core (物理/虚拟)	CPU 使用情况 (%)	加载平均
idx2	Indexer	48 / 96	4.88	0.04
sh2	KV Store Search Head	48 / 96	1.52	0.03
master1	Cluster Master Indexer License Master	48 / 96	0.98	0.01
idx1	Indexer	48 / 96	0.64	0.06
sh1	KV Store Search Head	48 / 96	0.50	0.00
sh3	KV Store Search Head	48 / 96	0.45	0.00
idx3	Indexer	48 / 96	0.42	0.01

按主服务器角色、Splunk 进程类型分类的 CPU 使用率

按主服务器角色、Splunk 进程类型分类的 CPU 使用率面板显示部署中每个 Splunk 服务器角色（搜索头、索引器、群集主服务器等）的各种 Splunk 进程类型的 CPU 使用率。进程类型包括 splunkd、搜索、索引服务、Splunk Web、KVStore、脚本输入等。

使用此面板可以跟踪不同 Splunk 进程类型在特定 Splunk 服务器角色上耗用 CPU 资源量。

单击“将 x 轴缩放到实际大小”复选框以最大化水平视图。



部署范围内的平均 CPU 使用率

部署范围内的平均 CPU 使用率面板显示整个部署中随时间推移的总 CPU 使用率 %。

您可以使用此面板来确定 CPU 资源耗用的总体趋势，如 CPU 使用率不断上升，这可能表明您的系统存在问题，需要进行调查。

平均 CPU 使用率

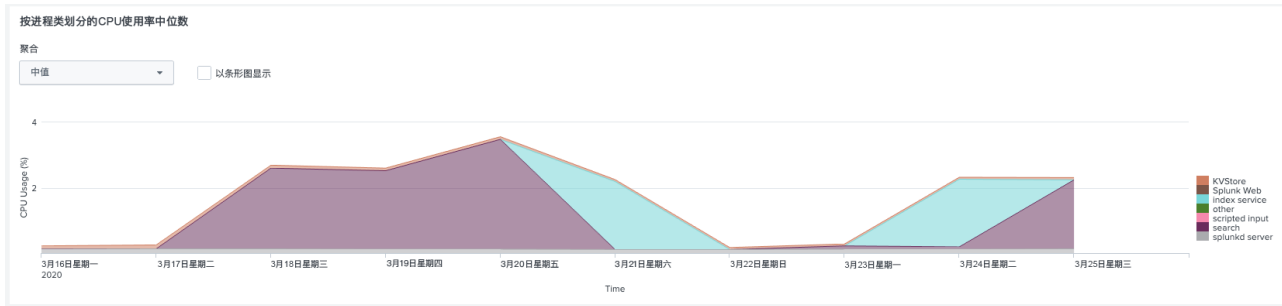
平均 CPU 使用率面板显示部署中各个实例随时间推移的 CPU 使用率 %。

您可以使用此面板来识别可能表明特定实例存在问题的 CPU 资源耗用趋势。

按进程类分类的平均 CPU 使用率

按进程类分类的平均 CPU 使用率面板显示每个 Splunk 进程类的 CPU 资源使用率。“进程类”是某单个类中的进程聚合。

您可以使用此面板来识别特定进程的 CPU 使用率峰值，这种情况可能表示存在潜在问题。例如，脚本输入的高 CPU 使用率 % 可能表示数据引入存在问题。



搜索的平均 CPU 使用率

搜索的平均 CPU 使用率面板可让您根据各种搜索特征（包括搜索类型（临时、计划）、搜索模式（实时、历史）、应用上下文、用户、角色、搜索名称等）监视 CPU 使用率。

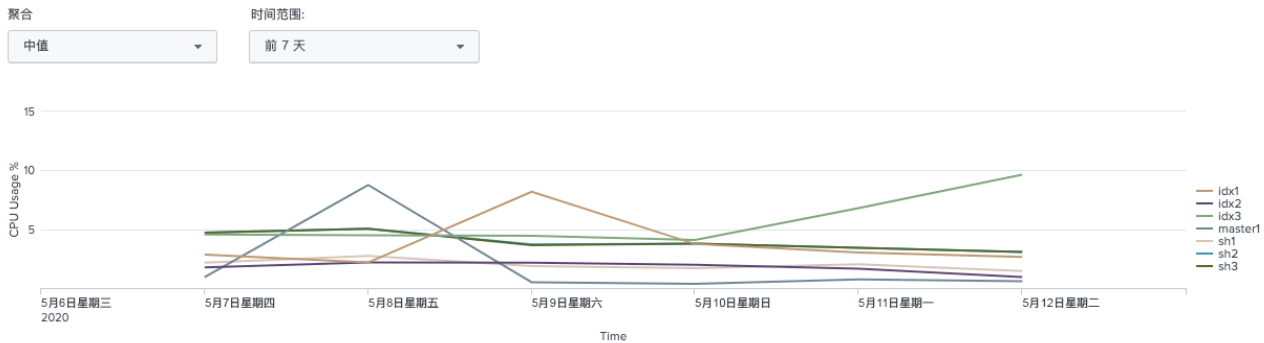
使用此面板可以识别 CPU 使用率峰值，这些峰值可以指示搜索性能的各种问题。例如，计划搜索的 CPU 使用率过高可能表示搜索并发存在问题。

历史平均 CPU 使用率

历史平均 CPU 使用率面板可让您在扩展的历史时间范围内按实例监视 CPU/vCPU 使用率。

您可以使用此面板针对容量规划或许可证规划等情况评估长期 CPU/vCPU 使用趋势和要求。

历史CPU使用中位数



填充此面板的 CPU 使用率指标数据存储在 `_metrics_rollup` 索引中。默认情况下，`_metrics_rollup` 索引会将这些数据保留两年，如在 `indexes.conf` 中指定的那样。有关数据保留设置的信息，请参阅 `index.conf.spec`。

要查看此面板中的数据，必须启用 `metric_rollups.conf` 的 `[index:_metrics]` 段落中指定的指标汇总策略，如下所示：

1. 编辑 `$SPLUNK_HOME/etc/apps/splunk_monitoring_console/local/metric_rollups.conf`。
2. 设置 `disabled = false` 以在 `[index:_metrics]` 段落中启用指标汇总策略，如下所示：

```
[index:_metrics]
defaultAggregation = avg
dimensionListType = excluded
metricList = spl.intr.resource_usage.Hostwide.data.cpu_system_pct,\
spl.intr.resource_usage.Hostwide.data.cpu_user_pct
metricListType = included
rollup.0.rollupIndex = _metrics_rollup
rollup.0.span = 1d
disabled = false
```

上面的指标汇总策略要求 `_metrics_rollup` 索引必须存在。该索引默认存在，并且由 CPU 使用率仪表板专用。

有关在 `metric_rollups.conf` 中配置指标汇总策略的更多信息，请参阅《指标》中的“使用配置文件管理指标汇总策略”。

CPU 使用率：实例

CPU 使用率：通过实例仪表板，您可以监视各个实例的物理 CPU 和 vCPU 使用率。

要查看特定实例的 CPU 使用率，请从实例菜单中选择该实例。

CPU 使用率面板显示物理和虚拟 CPU 的数量，以及所选实例的 CPU 使用率和平均负载。

Splunk 进程类型的 CPU 使用率面板显示所选实例的不同 Splunk 进程类型的 CPU 使用率。

按进程类分类的平均 CPU 使用率面板显示对于所选实例，每个 Splunk 进程类的 CPU 使用率。

搜索的平均 CPU 使用率面板可让您根据各种搜索特征（包括搜索类型（临时、计划）、搜索模式（实时、历史）、应用上下文、用户、角色、搜索名称等）监视 CPU 使用率。

历史平均 CPU 使用率面板可让您查看扩展历史时间范围内特定实例的 CPU 使用率。使用此面板可以评估 CPU 使用率的长期趋势，并用于容量规划或许可规划。

对这些仪表板进行故障排除

CPU/vCPU 仪表板从 `_introspection` 索引和 `/server/status/resource-usage/hostwide` 端点获取 CPU 使用率信息。如果面板缺少数据，请检查以下内容：

- 确保您正在将自检日志转发到索引器。
- 确认您的系统满足平台检测的系统要求。

关于端点信息，请参阅《*REST API 参考手册*》中的 `/server/status/resource-usage/hostwide`。

转发器

本主题是监视控制台中转发器：**部署**，转发器：**实例**，以及**Splunk TCP 输入性能部署**和**实例仪表板**的参考资料。请参阅本手册的“关于监视控制台”。

这些视图显示什么？

监视控制台监视转发器连接（位于**转发器仪表板**）和通信（位于**Splunk TCP 输入仪表板**）。

Splunk TCP 输入视图监视 Splunk TCP 输入，即从某个 Splunk 实例到另一个的数据。通常这是发送数据到索引器的转发器。这些视图不会如 Apache 服务器发送其日志到转发器那样，监视从非 Splunk 设备到收集器的 TCP 输入。

解释这些视图的结果

转发器：部署视图

状态面板可能会显示值为“活动”或“缺失”。当运行计划的搜索以更新此面板时，会回溯 15 分钟。如果转发器在过去的 15 分钟内连接到索引器，那么状态为“活动”。否则，其状态为“缺失”。要永久性从您的仪表板中移除缺失转发器，请重建转发器资产表。请参阅本手册的“配置转发器监视”。

此回溯时间不同于数据集合间隔（在**设置 > 转发器监视设置**），即计划的搜索运行的频率。阅读本手册中“配置转发器监视”，了解时间设置相关信息。

在**状态和配置**面板中，所显示的时间为上次计划的搜索完成的时间。

转发器：实例视图

称为“传出数据速率”的数据量测量索引器从转发器接收的数据。这一测量来自索引器中的 `metrics.log`。请参阅《*故障排除手册*》中的“关于 `metrics.log`”。

如果您无法在 Splunk Enterprise 中找到索引的数据，则可以按如下顺序查看监视控制台仪表板：

1. 转发器视图。
2. Splunk TCP 输入视图。
3. 索引视图。

请参阅**转发数据手册**中的“故障排除转发器/接收器连接”。

在这些视图中查找的内容

从**转发器：部署**视图开始，查看您的转发器是否如期报告，或者是否有其中之一缺失。

该仪表板配备预配置的平台告警（当一个或多个转发器缺失时它会通知您）。

对这些视图进行故障排除

转发器和 Splunk TCP 输入仪表板

在分布式或独立模式下，如果这些仪表板缺少数据，则确认您是否已完成监视控制台的所有设置步骤。

像所有监视控制台仪表板一样，这些仪表板需要来自索引器的 `metrics.log`。监视控制台不会直接通过转发器查询数据，但会从转发器连接的索引器获取其中的数据。

特定于转发器仪表板的步骤

要使任何转发器：部署或转发器：实例仪表板面板开始工作，您必须遵循本手册配置转发器监视中的设置步骤。历史面板需要带有单独 GUID 的转发器，请注意这个前提条件。

直到至少一个“数据集合间隔”（如 [监视控制台 > 设置 > 转发器监视设置](#) 中所定义）过去后，转发器仪表板上的平均值才会开始计算。

主动 Splunk 组件监视

关于主动 Splunk 组件监视

主动 Splunk 组件监视使您从 REST API 端点的输出查看 Splunk Enterprise 功能的运行状况。单独功能通过提供部署运行状况的持续、实时视图的树状结构报告运行状况，不会影响您的搜索负载。

您可以使用 Splunk Web 中的 splunkd 运行状况报表访问功能运行状况信息。请参阅“查看 splunkd 运行状况报表”。

您还可以从 server/health/splunkd 端点以编程方式访问功能运行状况信息。请参阅“查询 server/health/splunkd 端点”。

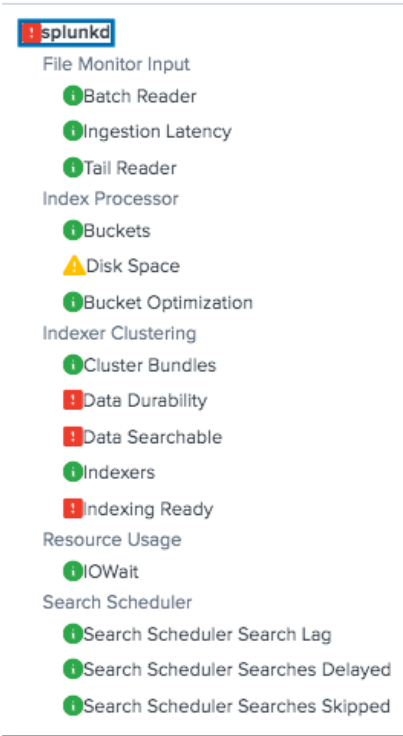
有关 splunkd 进程的详细信息，请参阅《安装手册》中的“Splunk Enterprise 进程”。

Splunk Enterprise 运行状况报表

Splunk Enterprise 运行状况报表以树状结构记录 splunkd 的运行状况，叶节点代表特定 Splunk Enterprise 功能，中间节点对各种功能进行分类。功能运行状况在四种状况下为彩色编码：

- 绿色：功能运行正常。
- 黄色：功能遇到问题。
- 红色：功能有个严重的问题，对部署的功能性产生负面影响。
- 灰色：功能已禁用运行状况报表。

Splunk 部署运行状况



运行状况树状结构

splunkd 运行状况树状结构有以下节点：

运行状况树状结构节点	描述
splunkd	状况树状结构的顶层显示 splunkd 进程的整体运行状况（颜色）。splunkd 的当前状况指示树状结构中最不健康的功能的状况。REST 端点从 splunkd 节点检索实例运行状况。
功能类别	功能类别代表运行状况树状结构中的第二层级。功能类别是功能的逻辑分组。例如：“BatchReader”和“TailReader”是形成名为“File Monitor Input”的逻辑分组的功能。功能类别作为功能组数据桶，没有自己的运行状况。

功能	状况树状结构中的下一个层级是功能节点。每个节点包含特定功能的运行状况相关的信息。每个功能包含确定功能状况的一个或多个指示器。功能的整体运行状况取决于任意指示器最基本的运行状况颜色。
指示器	指示器是 splunkd 运行状况报表的基本元素。这些是每个功能追踪的功能性的最低等级，在功能性变化时颜色相应改变。指示值对照红色或黄色阈值测量以确定功能状况。请参阅“什么确定功能状况？”。

关于支持的 Splunk Enterprise 功能列表，请参阅“支持的功能”。

什么确定功能状况？

状况树状结构中功能的当前状况取决于相关指示器的值。指示器有黄色和红色的可配置阈。指示器的值满足阈值条件时，功能的状况改变。

请参阅“设置功能指示器阈值”了解有关如何配置指示器阈值的信息。

关于如何故障排除功能状态更改的根本原因的信息，请参阅“调查功能运行状况更改”。

默认运行状况告警

默认情况下，splunkd 运行状况报表中的各功能在状态出现变动时会生成告警，例如，从绿色变为黄色，或从黄色变为红色。您可以启用/禁用任何功能的告警，并通过电子邮件、手机、VictorOps、health.conf 中的 PagerDuty 或通过 REST 端点设置告警通知。更多信息，请参阅“配置运行状况报表告警”。

splunkd 运行状况视角

splunkd 运行状况报告从您正在监视的本地实例视角显示 Splunk Enterprise 部署的运行状况。**模式：独立**标签表示单实例运行状况报表。例如，在索引器群集环境中，群集管理器和对等节点分别显示不同的功能级，组成 splunkd 整体的运行状况。

分布式运行状况报告

分布式运行状况报表允许您通过单个中央实例（如搜索头、搜索头管理员或群集管理器）监视分布式部署的整体运行状况。**模式：分布式**标签表示分布式运行状况报表。分布式标签与单实例运行状况报表不同，后者仅从本地实例视角显示特征运行状况。

已启用的分布式运行状况报告上的实例可收集跨部署的已连接实例中的数据。当特征指示器达到特定的阈值，特征运行状况会发生变化，例如从绿色变为黄色或从黄色变为红色，方式与 splunkd 运行状况报告一样。

启用分布式运行状况报告

在能够收集部署中的数据之前，您必须启用 health.conf 中的分布式运行状况报告。默认情况下，禁用分布式运行状况报告。

要启用分布式运行状况报告：

1. 登录您监视部署想要借助的实例。大多数情况下是搜索头、搜索头群集管理员或群集管理器。
2. 编辑 \$SPLUNK_HOME/etc/system/local/health.conf。
3. 在 [distributed_health_reporter] 段落中，设置 disabled = 0。例如：

```
[distributed_health_reporter]
disabled = 0
```

设置分布式运行状况报表告警操作

您可以直接在分布式运行状况报表的中央实例上设置告警操作，例如发送电子邮件或手机告警通知。

与单实例视图运行状况报表（需要在单个实例上设置告警操作）相比，它使您可以在同一个位置配置告警操作，从而简化了告警配置过程。

必须启用分布式运行状况报表，才能接收部署中的告警。

要设置分布式运行状况报表告警操作：

1. 登录分布式运行状况报表的中央实例。在大多数情况下，就是群集管理器或搜索头管理员。
2. 编辑 \$SPLUNK_HOME/etc/system/local/health.conf
3. 确保已启用分布式运行状况报表，如下所示：

```
[distributed_health_reporter]
disabled = 0
```

4. 添加要在分布式运行状况报表收到告警时运行的特定告警操作。例如，要发送电子邮件告警通知，请添加 [alert_action:email] 段落：

```
[alert_action:email]
disabled = 0
action.to = <recipient@example.com>
action.cc = <recipient_2@example.com>
action.bcc = <other_recipients@example.com>
```

有关如何配置可用告警操作的详细信息，请参阅“设置运行状况报表告警操作”。

如果您在中央实例和单个实例上均启用了告警，则分布式运行状况报表会发送重复的告警。为避免重复告警，请禁用单个实例的告警。

查看分布式运行状况报告

分布式运行状况报告目前只能通过 REST 端点查看。从版本 8.0.4 开始，受支持的功能仅限于索引器和群集管理器。

要查看分布式部署的整体运行状态，发送 GET 请求至：

server/health/deployment

请参阅《REST API 参考》中的 server/health/deployment，了解端点详细信息。

要查看分布式运行状况报告（例如索引器）的各功能的运行状况，发送 GET 请求至：

server/health/deployment/details

请参阅《REST API 参考》中的 server/health/deployment/details，了解端点详细信息。

要求

主动 Splunk 组件监视有以下要求和限制。

Splunk Enterprise 版本要求

主动 Splunk 组件监视需要 Splunk Enterprise 7.1 或以上版本。

操作系统和浏览器要求

主动 Splunk 组件监视在 Splunk Enterprise 支持的所有操作系统上可用。有关支持的操作系统和浏览器列表，请参阅《安装手册》中的“系统要求”。

REST 端点访问权限要求

主动 Splunk 组件监视显示来自 server/health/splunkd 端点的信息。您可以在 Splunk Web 中的 splunkd 运行状态报表中查看此消息。

要直接查询 server/health/splunkd 端点需要通过 http 访问 splunkd 管理端口（默认端口 8089）。请参阅《REST API 用户手册》中的“连接到 splunkd”了解更多信息。

请参阅《REST API 参考手册》中的 server/health/splunkd，了解端点详细信息。

配置 splunkd 运行状况报表

splunkd 运行状况报表显示 Splunk Enterprise 功能的预定义集的状态。您可使用 Splunk Web 中的运行状况报表管理器页面或通过编辑 health.conf 修改某些运行状况报表设置，包括功能阈值。

请参阅《管理员手册》中的 health.conf.spec，了解关于 health.conf 中运行状况报表配置设置的更多信息。

支持的功能

splunkd 运行状况报表允许您监视这些 Splunk Enterprise 功能：

功能类别	功能
数据转发/Splunk-2-Splunk Forwarding	TCPOutAutoLB
文件监视输入	BatchReader、TailReader、引入延迟、转发器引入延迟
索引处理器	数据桶、磁盘空间、索引优化
索引器群集化	群集软件包、数据持久性、可搜索数据、索引器、索引准备就绪、主服务器连接、复制失败、从属状态、从属版本、搜索头连接
资源使用情况	IOWait
搜索头群集化	管理员连接成员、管理员通用基线、管理员选举概述、成员概述、快照新建
搜索计划程序	已跳过搜索、延迟搜索、滞后搜索
工作负荷管理	配置检查、系统检查

IOWait 功能仅在以下情况下启用：

- 平台为 Linux
- IOWait 自检在默认 server.conf 中启用

有关 splunkd 运行状况报告功能的详细信息，请参阅 \$SPLUNK_HOME/etc/system/default/health.conf。

设置功能指示器阈值

运行状态树状结构中的每个功能有一个或多个指示器。每个指示器针对预设置的阈报告值，确定功能状态。指示器值满足阈条件时，功能变化的运行状态改变，比方说会从绿色变为黄色，或从黄色变为红色。

每个指示器有两个有效阈值：黄色和红色。您可使用 Splunk Web 或 health.conf 文件修改任何功能指示器的阈值。更改任何功能的阈值适用于所有相关联的搜索头或搜索头管理员。

使用 Splunk Web 设置阈值

在 Splunk Web 中设置功能阈值：

1. 在您正在监视的实例中，登录到 Splunk Web。
2. 单击**设置 > 运行状况报表管理器**。
3. 查找您想要修改的功能，单击**编辑阈值**。
编辑阈值模式打开，显示每个功能指示器的详细说明。
4. 设置新的指标阈值。例如，要修改搜索计划程序的阈值：已跳过的搜索功能，您可以为 percent_searches_skipped_high_priority_last_24h 和 percent_searches_skipped_non_high_priority_last_24h 指示器设置新的红色或黄色阈值：

编辑 Search Scheduler Searches Skipped 的阈值

指标 percent_searches_skipped_high_priority_last_24h

描述 This indicator tracks the skip rate for high priority scheduled searches. These are scheduled searches where the priority field is set to "higher" or "highest". By default, this indicator is yellow if the skipped search ratio over the last 24 hours is 5%, and red if it is 10%.

红色 10

黄色 5

5. 单击保存。

要查看和编辑运行状况报表管理器页面的阈值设置，您的角色必须具有 `list_health` 和 `edit_health` 功能。更多信息，请参阅“为 Splunkd 运行状况报表设置访问控制”。

使用 `health.conf` 设置阈值

要在 `health.conf` 中设置功能阈值：

1. 请登录您正在监视的实例。
2. 编辑 `$SPLUNK_HOME/etc/system/local/health.conf`
3. 在功能段落中，设置新的指示器阈值。例如，要修改 `batchreader` 功能的指示器阈值，在以下段落中设置 `data_out_rate:yellow` 和 `data_out_rate:red` 阈值的新值：

```
[feature:batchreader]
indicator:data_out_rate:red = 10
indicator:data_out_rate:yellow = 5
```

指示器阈值是适用于大多数使用情况的预设值。当您修改阈值时，以小增量作出更改。将阈值设置过高会导致严重的问题或故障。

关于每个功能指示器的详细说明，请参阅 `$SPLUNK_HOME/etc/system/default/health.conf`。

禁用功能

您可以禁用 `health.conf` 中的任何功能。禁用某个功能将使该功能从 `splunkd` 运行状况树状结构中移除。这很有用，例如：如果您想要在用该功能对问题进行故障排除时，将功能的状态从运行状态报表中排除。所有支持的功能在 `health.conf` 中默认启用。

有三种禁用功能的方式：

- 在 Splunk Web 中禁用功能。
- 在 `health.conf` 中编辑功能段落。
- 使用 `/server/health-config` 端点。

在 Splunk Web 中禁用功能

1. 在您正在监视的实例中，登录到 Splunk Web。
2. 单击设置 > 运行状况报表管理器。
3. 将交换机设为禁用特定功能。
功能已禁用且不再影响 `splunkd` 的整体状态。

禁用 `health.conf` 中的功能

1. 请登录您正在监视的实例。

2. 编辑 `$SPLUNK_HOME/etc/system/local/health.conf`。
3. 在功能段落中，添加 `disabled = 1`。例如，要禁用数据持久性功能：

```
[feature:data_durability]
indicator:cluster_replication_factor:red = 1
indicator:cluster_search_factor:red = 1
disabled = 1
```

要启用功能，请设置 `disabled = 0`

4. 重新加载 `health.conf`：

```
curl -k -u admin:pass https://<host>:<mPort>/services/configs/conf-health.conf/_reload
```

禁用使用 REST 端点的功能

1. 请登录您正在监视的实例。
2. 运行 `server/health-config/{feature_name}` 端点背景下的以下命令。例如，要禁用 `batchreader` 功能：

```
curl -k -u admin:pass \
https://<host>:<mPort>/services/server/health-config/feature:batchreader -d disabled=1
```

3. 验证功能不再出现在 Splunk Web 中的 `splunkd` 状态报表中。
请参阅 *REST API 参考手册* 中的 `server/health-config/{feature_name}` 了解端点详细信息。

要访问 `server/health-config/` 端点，您的角色必须有 `edit_health` 功能。

抑制运行状态更新

运行状态树中的功能在预先定义的间隔内更新状态。运行状态更改频繁的功能会导致 `splunkd` 运行状态报表整体状态出现超出预期的改变。要防止这样的情况发生，请使用 `health.conf` 中的 `suppress_status_update_ms` 属性减少特定功能可以更新运行状态的频率。

使用 `suppress_health_status_update_ms` 属性以：

- 按单独功能将超出的更改限制为内部状态。
- 减少因快速功能状态更改的记录项目数。
- 帮助平息“噪音”功能。

例如：索引器群集化功能，如 `data_durability` 会在影响其指示器的运行期间经历频繁的状态更改：`cluster_replication_factor` 和 `cluster_search_factor`。要避免整体 `splunkd` 运行状态报表的频繁更改，您可以设置 `suppress_status_update_ms = 60000` 以将运行状态更新减少成每分钟一次。

要抑制运行状态更新：

1. 请登录您正在监视的实例。
2. 编辑 `$SPLUNK_HOME/etc/system/local/health.conf`
3. 在合适的功能段落中，添加 `suppress_status_update_ms` 属性。例如：

```
[feature:data_durability]
indicator:cluster_replication_factor:red = 1
indicator:cluster_search_factor:red = 1
suppress_status_update_ms = 60000
```

默认情况下，两次状态更新之间经过的最小时间为 300ms。

请参阅 *管理员手册* 中的 `health.conf.spec` 了解更多信息。

配置运行状态日志

`splunkd` 运行状态树中的每个功能生成 `health.log` 中的日志条目。这些日志条目记录关于随时间变化的功能指示器状态的信息。`health.log` 位于 `SPLUNK_HOME/var/log/splunk/`。

有两种类型的 `health.log` 日志条目：

HealthChangeReporter：这一日志条目记录某个功能指示器的特定运行状态的变化。每个条目包括状态更改的时间戳、功能名称、指示器名称、之前的颜色、新的颜色和可能的原因。只有在功能状态改变时（例如，从绿色变为红色），这一日志条目才出现：


```
02-28-2018 20:26:52.775 +0000 INFO HealthChangeReporter - feature="Data Durability" indicator="cluster_replication_factor"
previous_color=green color=red reason="Replication Factor is not met"
```

PeriodicHealthReporter: 这一日志条目对运行状态树中的每个功能的状态进行持续性记录。每个项目包括时间戳、功能名称和当前颜色。日志条目在用户可配置间隔内记录。例如:

```
02-28-2018 20:27:06.826 +0000 INFO PeriodicHealthReporter - feature="Data Durability" color=red
```

设置 *health.log* 项目间隔

您可以设置将 PeriodicHealthReporter 日志条目添加到 *health.log* 的间隔。如果您想要增加或减少日志条目（显示在以下位置）的整体日志条目数，这很有帮助 *health.log*。

要调整 *health.log* 中的 PeriodicHealthReporter 日志条目的频率:

1. 请登录您正在监视的实例。
2. 编辑 `$SPLUNK_HOME/etc/system/local/health.conf`
3. 在 `[health_reporter]` 段落中, 将 `full_health_log_interval` 属性设置为正确的值, 并以秒为单位。例如:

```
[health_reporter]
full_health_log_interval = 60
```

默认情况下, 每个功能每 30 秒生成一条 PeriodicHealthReporter 日志条目。

为 Splunkd 运行状况报表设置告警

splunkd 运行状况报表会为运行状况树中的所有功能生成告警。当功能指示器满足阈值条件时, 功能的运行状况会改变, 比如从绿色变为红色, 告警触发。无论您是否登录 Splunk Web, 都可以使用运行状况告警保持对部署运行状况的可见性。

您可以按如下方式配置运行状况报表告警:

- 启用/禁用全局、功能或指示器级别的告警。
- 通过电子邮件、手机、VictorOps 或 PagerDuty 发送告警通知。
- 设置触发告警的运行状况颜色（黄色或红色）。
- 设置告警之间必须经过的最小持续时间。

您可以通过直接编辑 *health.conf* 或查询 `server/health-config` 端点配置运行状况报表告警。

禁用运行状况报表告警

默认为 Splunkd 运行状况报表中的所有功能启用告警。您可以禁用全局、功能或指示器级别的告警。禁用全局级别的告警会覆盖功能级别已启用的告警。同样地, 禁用功能级别的告警会覆盖指示器级别已启用的告警。

禁用告警有助于减少非关键功能的噪音, 并在执行维护任务时最大程度减少误报。

使用 *health.conf* 禁用告警

要为 Splunkd 运行状况报表中的所有功能禁用告警:

1. 编辑 `$SPLUNK_HOME/etc/system/local/health.conf`。
2. 在 `health_reporter` 段落中, 设置 `alert.disabled = 1`。例如:

```
[health_reporter]
full_health_log_interval = 30
suppress_status_update = 600
alert.disabled = 1
```

要为 Splunkd 运行状况报表中的所有功能启用告警, 设置 `alert.disabled = 0`。

要为单个功能禁用告警:

1. 编辑 `$SPLUNK_HOME/etc/system/local/health.conf`。
2. 在特定功能的段落中, 设置 `alert.disabled = 1`。例如:

```
[feature:indexers]
...
indicator:missing_peers:yellow = 1
```

```
indicator:missing_peers:red = 1
alert.disabled = 1
```

要启用某个功能的告警，请设置 `alert.disabled = 0`。

要为单个功能指示器禁用告警：

1. 编辑 `$SPLUNK_HOME/etc/system/local/health.conf`。
2. 在特定功能的段落中，设置 `alert:<indicator_name>.disabled = 1`。例如，在以下段落中，指示器 `s2s_connections` 的告警已禁用：

```
[feature:s2s_autolb]
...
indicator:s2s_connections:yellow = 20
indicator:s2s_connections:red = 70
alert:s2s_connections.disabled = 1
```

要启用某个指示器的告警，请设置 `alert:<indicator_name>.disabled = 0</indicator_name>`。

禁用使用 REST 端点的告警

要禁用功能和指示器的告警，发送 POST 请求至 `server/health-config/{feature_name}`。例如，要禁用您正在监控的实例上的 `batchreader` 功能的告警，运行以下命令：

```
curl -k -u admin:pass https://<host>:<port>/services/server/health-config/feature:batchreader -d alert.disabled=1
```

请参阅 *REST API 参考手册* 中的 `server/health-config/{feature_name}` 了解端点详细信息。

要访问 `server/health-config` 端点，角色必须有 `edit_health` 功能。

设置运行状况报表告警操作

您可以设置因功能运行状态发生变化而触发告警时要执行的告警操作。告警操作包括通过电子邮件、手机、VictorOps 或 PagerDuty 发送通知。告警操作仅适用于全局级别。不支持同一操作类型的多个告警操作。例如，您无法执行多个电子邮件操作和多个 PagerDuty 操作。

设置运行状况报表告警操作时，必须在 `SPLUNK_HOME/etc/system/local/health.conf` 的 `[health_reporter]` 段落中指定告警操作。您可以逗号分隔的形式指定多个告警操作。例如：

```
[health_reporter]
alert_actions=email, mobile, VictorOps, PagerDuty
```

您还必须使用适当的告警操作段落来设置特定的告警操作，如以下各章节内容所示。

在 *health.conf* 中设置电子邮件告警通知

在发送运行状况电子邮件告警通知之前，您必须配置 Splunk Web 中的电子邮件通知设置。请参阅《告警手册》中的“电子邮件通知操作”获取如何配置电子邮件通知的说明。

要设置电子邮件告警通知：

1. 编辑 `SPLUNK_HOME/etc/system/local/health.conf`
2. 添加 `[alert_action:email]` 段落并指定收件人。例如：

```
[alert_action:email]
disabled = 0
action.to = <recipient@example.com>
action.cc = <recipient_2@example.com>
action.bcc = <other_recipients@example.com>
```

在 *health.conf* 中设置手机告警通知

在您为运行状况报告配置手机告警通知之前，您必须从应用商店将 Splunk Mobile iOS 应用下载到手机，并从 Splunkbase 将 Splunk Cloud Gateway 应用下载到 Splunk 实例。关于如何安装和设置 Splunk Cloud Gateway 应用的详细信息，请参阅“安装 Splunk Cloud Gateway”。

要设置手机告警通知：

1. 在 Splunk Web 中单击设置 > 告警操作。在发送到手机行，确认 `splunk_app_cloudgateway` 已启用。
2. 在 Splunk Web 中，单击应用 > **Splunk Cloud Gateway** > 注册。输入移动设备上 Splunk Mobile 应用中显示的激活码。
3. 编辑 `$SPLUNK_HOME/etc/system/local/health.conf`。
4. 添加 `[alert_action:mobile]` 段落并指定收件人。例如：

```
[alert_action:mobile]
disabled = 0
action.alert_recipients = admin
```

在 *health.conf* 中设置 *VictorOps* 告警通知

在您发送告警通知至 VictorOps 之前，必须从 Splunkbase 安装 VictorOps 应用。您还必须在 VictorOps 中创建一个 API 密钥和一个可选的路由密钥。有关如何为 VictorOps 创建 API 密钥的说明，请参阅《适用于 VictorOps 的 Splunk 集成指南》。

要设置 VictorOps 告警通知：

1. 在 Splunk Web 中单击设置 > 告警操作。在 VictorOps 行中，确认 `victorops_app` 已启用，然后单击设置 **VictorOps** 通知。
2. 输入 API 密钥和可选的路由密钥。
3. 单击保存。
4. 编辑 `$SPLUNK_HOME/etc/system/local/health.conf`。
5. 添加 `[alert_action:victorops]` 段落并指定告警消息类型。例如：

```
[alert_action:victorops]
disabled = 0
action.message_type = CRITICAL
```

有关 VictorOps 告警设置的更多信息，包括有效的告警消息类型和可选设置，请参阅《管理员手册》中的 `health.conf.example`。

在 *health.conf* 中设置 *PagerDuty* 告警通知

在您发送告警通知至 PagerDuty 之前，必须从 Splunkbase 安装 PagerDuty 应用。您还必须为 PagerDuty 集成添加新服务，并复制集成密钥。有关更多信息，请参阅 PagerDuty 文档。

要设置 PagerDuty 告警通知：

1. 编辑 `$SPLUNK_HOME/etc/system/local/health.conf`。
2. 添加 `[alert_action:pagerduty]` 段落并指定集成密钥。例如：

```
[alert_action:pagerduty]
disabled = 0
action.integration_url_override = <integration key>
```

有关更多信息，请参阅 `health.conf.example`。

使用 *REST* 设置告警操作

要设置告警操作，发送 POST 请求至 `server/health-config/{alert_action}`。例如，要设置电子邮件告警通知：

```
curl -k -u admin:pass https://localhost:8089/services/server/health-config/alert_action:email -d action.to=admin@example.com -d action.cc=admin2@example.com
```

请参阅 *REST API 参考手册* 中的 `server/health-config/{alert_action}` 了解端点详细信息。

设置分布式运行状况报表告警

如果要借助分布式运行状况报表来监视分布式部署，则可以直接在分布式运行状况报表的中央实例上设置告警操作。有关更多信息，请参阅“设置分布式运行状况报表告警操作”。

设置告警阈值颜色

您可以设置触发告警的阈值颜色。告警阈值可能是黄色或红色。如果阈值是黄色，则告警触发黄色和红色。如果值是红色，则告警仅触发红色。默认告警阈值是红色。

在 *health.conf* 中设置告警阈值颜色

要在全局或功能级别设置告警阈值颜色：

1. 编辑 `$SPLUNK_HOME/etc/system/local/health.conf`。
2. 将 `alert.threshold_color` 设置添加到 `[health_reporter]` 或 `[feature:<feature_name>]` 段落。例如：

```
[feature:replication_failures]
...
alert.threshold_color = yellow
indicator:replication_failures:red = 10
indicator:replication_failures:yellow = 5
```

要在指示器级别设置告警阈值颜色：

1. 编辑 `$SPLUNK_HOME/etc/system/local/health.conf`。
2. 将 `alert:<indicator name>.threshold_color` 设置添加到功能段落。例如：

```
[feature:replication_failures]
...
indicator:replication_failures:red = 10
indicator:replication_failures:yellow = 5
alert:replication_failures.threshold_color = yellow
```

指示器级别的告警阈值颜色设置会覆盖功能级别的告警阈值颜色设置。

使用 *REST* 设置告警阈值颜色

要设置功能或指示器告警阈值颜色，发送 POST 请求至 `server/health-config{feature_name}`。例如，要设置复制失败功能的告警阈值颜色：

```
curl -k -u admin:pass https://localhost:8089/services/server/health-config/feature:replication_failures -d
alert.threshold_color=yellow
```

请参阅 *REST API 参考手册* 中的 `server/health-config/{feature_name}` 了解端点详细信息。

设置告警之间的最小持续时间

您可以设置异常运行状况所持续的时间，然后使用 `alert.min_duration_sec` 设置触发告警。您可以使用此设置通过可以在状态之间（比如绿色和黄色之间或者黄色和红色之间）快速翻转的功能帮助减少噪声。

在 *health.conf* 中设置告警之间的最小持续时间

要在全局或功能级别设置告警之间的最小持续时间：

1. 编辑 `$SPLUNK_HOME/etc/system/local/health.conf`。
2. 将 `alert.min_duration_sec` 设置添加到 `[health_reporter]` 或 `[feature:<feature_name>]` 段落。例如：

```
[feature:replication_failures]
...
alert.min_duration_sec = 600
indicator:replication_failures:red = 10
indicator:replication_failures:yellow = 5
```

要在指示器级别设置告警之间的最小持续时间：

1. 编辑 `$SPLUNK_HOME/etc/system/local/health.conf`。
2. 将 `alert:<indicator name>.min_duration_sec` 设置添加到 `[feature:<feature_name>]` 段落。例如：

```
[feature:replication_failures]
...
indicator:replication_failures:red = 10
indicator:replication_failures:yellow = 5
alert:replication_factor.min_duration_sec = 600
```

功能级别上的告警间的最小持续时间设置会覆盖指示器级别的设置。

使用 REST 设置告警之间的最小持续时间

要设置功能或指示器的告警间的最小持续时间，发送 POST 请求至 `server/health-config/{feature_name}`。例如，要设置复制失败功能的告警间的最小持续时间：

```
curl -k -u admin:pass https://localhost:8089/services/server/health-config/feature:replication_failures -d
alert.min_duration_sec=600
```

请参阅 *REST API 参考手册* 中的 `server/health-config/{feature_name}` 了解端点详细信息。

为 Splunkd 运行状况报表设置访问控制

要监视、编辑和启用 Splunkd 运行状况报表功能，必须为用户角色指定适当的功能。默认为 `role_admin` 启用以下运行状况报表权限：

权限	授予角色的权限
<code>list_health</code>	查看 Splunk Web 中的 Splunkd 运行状况报表和运行状况管理器页面。
<code>edit_health</code>	在 Splunk Web 中或通过 REST 端点编辑和启用运行状况报表功能。

您可以在 Splunk Web 或 `authorize.conf` 中为任何角色添加上述功能。

要在 Splunk Web 中为角色添加功能，请使用 Splunk Web 添加和编辑角色。

要在 `authorize.conf` 中添加功能，请参阅“使用 `authorize.conf` 添加和编辑角色”。

调查功能运行状况更改

有两种从 `/server/health/splunkd` 端点访问功能运行状况信息的方式：

- 查看 Splunk Web 中的 `splunkd` 运行状况报表。
- 查询 `server/health/splunkd` 端点。

您还可以监视 `$SPLUNK_HOME/var/log/health.log` 中的功能运行状况更改。有关 `health.log` 文件项目的更多信息，请参阅“配置运行状况日志”。




查看 splunkd 运行状况报表

`splunkd` 运行状况报表使您可以查看 `splunkd` 运行状况树中的功能当前状态。您可以使用报表识别状态代表问题的功能，调查那些问题的原因。

1. 在您想要监视的实例中，登录到 Splunk Web。
2. 在主菜单中，查看运行状况报表图标的颜色。这一图标的颜色显示 `splunkd` 的整体状态。
3. 单击运行状况报表图标打开运行状况报表。

splunkd






File Monitor Input

-  Batch Reader
-  Ingestion Latency
-  Tail Reader

Index Processor

-  Buckets
-  Disk Space
-  Bucket Optimization




Indexer Clustering

-  Cluster Bundles
-  Data Durability
-  Data Searchable
-  Indexers
-  Indexing Ready

Resource Usage





-  IOWait

Search Scheduler

-  Search Scheduler Search Lag
-  Search Scheduler Searches Delayed
-  Search Scheduler Searches Skipped

如何解释这份运行状况报告:

此运行状况报告显示了来自 `/health/splunkd/details` 端点的信息。一个功能有三种可能的状态:

-  绿色: 功能运行正常。
-  黄色: 功能出现问题。功能的状态可能会自动改善, 也可能随着时间的推移进一步恶化。如需相关详细信息, 请参阅“根本原因”。
-  红色: 功能存在严重问题, 并对您的部署的功能性产生了负面影响。如需相关详细信息, 请参阅“根本原因”。
-  灰色: 已禁用此功能的运行状况报表。

要管理各个功能的红色和黄色阈值, 请前往 [运行状况报表管理器](#)。

有关此运行状况报表的更多信息, 请参阅 [了解更多信息](#)。

4. 在运行状况树中, 单击任意功能以查看有关功能状态的信息。
5. 要了解在红色或黄色状态下的功能, 请查看**根本原因**了解可以帮助您识别功能状态改变原因的信息。此外, 单击“生成诊断”可生成诊断文件以附加到支持案例。默认情况下, 管理员具有 `get_diag` 并且可以授予其他用户打开 RapidDiag 应用的能力。有关更多详情, 请参阅 Splunk Enterprise 《故障排除手册》中的“RapidDiag”。

示例

这一示例显示您可以如何使用 `splunkd` 运行状况报表调查群集主服务器实例中的功能运行状况改变情况。

1. 查看 `splunkd` 运行状况报表。
2. 调查根本原因和相关消息。
3. 确认功能状态改变的原因。

1. 查看 `splunkd` 运行状况报表

1. 在群集主服务器实例中, 登录到 Splunk Web。
2. 在主菜单中查看运行状况报表图标的颜色。红色图标表示 `splunkd` 运行状况树中的一个或多个功能有严重问题。



3. 单击运行状况报表图标打开运行状况报表。以下运行状况报表指示 Indexer Clustering 类别中的 `data_durability` 功能有严重的问题:

splunkd

File Monitor Input

Batch Reader

Ingestion Latency

Tail Reader

Index Processor

Buckets

Disk Space

Bucket Optimization

Indexer Clustering

Cluster Bundles

Data Durability

Data Searchable

Indexers

Indexing Ready

Resource Usage

IOWait

Search Scheduler

Search Scheduler Search Lag

Search Scheduler Searches Delayed

Search Scheduler Searches Skipped

Data Durability

根本原因:

Search Factor is not met

Unhealthy Instances:

debianSplunk

生成诊断

前 50 条相关信息:

03-15-2021 12:09:12.094 -0700 WARN CMMaster [125034 TcpChannelThread] - event=addBucket status=failure bid=_internal~5~0C8302B6-8510-46EC-9A8F-17DF945E2C1A peer=0C8302B6-8510-46EC-9A8F-17DF945E2C1A msg='failed to select streaming targets'

2. 调查根本原因和相关消息

在运行状况树中，单击 data_durability 功能。以下诊断信息出现：

根本原因：“未能满足复制因子。”

如果群集中的对等节点数少于复制因子，复制因子无法满足。因此功能的红色状态的可能原因是离线对等节点。

前 50 个相关消息：搜索相关消息，您会看到包含流媒体错误的日志项目。例如：

```
03-15-2021 12:09:12.094 -0700 WARN CMMaster [125034 TcpChannelThread] - event=addBucket status=failure
bid=_internal~5~0C8302B6-8510-46EC-9A8F-17DF945E2C1A peer=0C8302B6-8510-46EC-9A8F-17DF945E2C1A msg='failed to select streaming
targets'
```

流媒体错误表示数据桶复制失败，因为数据来源对等节点无法与目标对等节点通信。这种错误类型可能因网络干扰或离线对等节点导致。

3. 确认功能状态改变的原因

在您使用 splunkd 运行状况报表调查功能状态更改（表示对等节点为离线）的原因之后，您可以使用监视控制台检查群集对等节点的状态，确认怀疑的原因是否正确。

- 在 Splunk Web 中，单击设置 > 监视控制台。
- 单击索引 > 索引器群集 > 索引器群集：状态。
仪表板显示对等节点 idx5 已停止。

i	对等方名称	完全可搜索	状态	数据桶
>	idx5	否	正在关闭	28
>	idx2	否	待决	6
>	idx3	是	向上	32
>	idx4	是	向上	32

- 单击 idx5 对等节点以查看更多信息。idx5 对等节点 GUID 匹配流媒体错误消息中的目标对等节点的 GUID。这样就能确认导致 data durability 功能为红色状态的原因是离线对等节点。

i	对等方名称	完全可搜索	状态	数据桶
▼	idx5	否	结束	0
	位置	10.16.88.2:9041		
	上一检测信号	3/16/2021, 4:05:35		
	复制端口	9044		
	基本生成 ID	18446744073709552000		
	GUID	0C8302B6-8510-46EC-9A8F-17DF945E2C1A		

4. 您现在可以采取重启对等节点，让它重新加入到群集中，这会将 `data_durability` 功能恢复到绿色状态。

查询 `server/health/splunkd` 端点

您可以使用现有的第三方监视工具和其他应用程序集成主动 Splunk 组件监视。

要查看 `splunkd` 的整体运行状况，请查询 `server/health/splunkd` 端点。例如：

```
curl -k -u admin:pass https://<host>:8089/services/server/health/splunkd
```

请参阅 *REST API 参考手册* 中的 `server/health/splunkd`，了解端点详细信息。

要查看 `splunkd` 的整体运行状况和向状态树报告的每个功能的运行状况以及有关功能运行状况更改的信息，请查询 `server/health/splunkd/details`。例如：

```
curl -k -u admin:pass https://<host>:8089/services/server/health/splunkd/details
```

请参阅 *REST API 参考手册* 中的 `server/health/splunkd/details` 了解端点详细信息。

请参阅 *REST API 用户手册* 中的连接到 `splunkd`，了解有关如何使用 Splunk REST API 端点的更多信息。

请参阅“Splunk Enterprise SDKs”了解支持 Splunk REST API 的 Splunk SDK 的相关信息。