

Splunk® Enterprise 6.5.0

监视 Splunk Enterprise

生成时间：2016 年 9 月 26 日，下午 10:22

Table of Contents

关于分布式管理控制台	3
关于监视控制台	3
监视控制台有什么功能？	3
监视控制台如何工作	4
配置监视控制台	5
多实例部署监视控制台设置步骤	5
单实例监视控制台设置步骤	5
哪个实例应布置控制台？	5
监视控制台设置前提条件	7
设置群集标签	8
将实例作为搜索节点添加到监视控制台	9
在独立模式中配置监视控制台	9
在分布式模式中配置监视控制台	9
为监视控制台配置转发器监视	10
平台告警	11
评估和自定义运行状况检查	12
监视控制台仪表板参考	14
搜索活动仪表板	14
搜索使用情况统计信息仪表板	15
计划程序活动	15
索引性能：实例	16
索引性能：部署	17
资源使用情况：实例	17
资源使用情况：计算机	18
资源使用情况：部署	18
KV 存储：实例	19
KV 存储：部署	20
搜索头群集化仪表板	21
分布式搜索仪表板	23
HTTP 事件收集器仪表板	23
索引器群集化：状态	24
索引器群集化：服务活动	24
索引：索引和卷仪表板	25
转发器仪表板	25
许可授权	26

关于分布式管理控制台

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。

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），这会允许您访问默认的平台告警。
- 您可以查看[分布式模式的配置步骤](#)，以便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
	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

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”。	<p>索：实例（如果您了解哪个搜索节点出现问题。）</p> <ul style="list-style-type: none"> 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段，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。

文件	这里有什么关于监视控制台的信息	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创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： <code>[distributedSearch:dmc_group_cluster_master]</code>	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。此处存储在监视控制台 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	<p>包含两个重要文件：</p> <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	<p>包含两种类型的宏：</p> <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。 <p>请参阅 macros.conf.spec。</p>	<p>默认情况下搜索宏在此处存储。</p> <p>每次编辑完一个自定义然后单击保存即表明设</p>

	请参阅 props.conf.spec 。	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 转发器 - 构建资产表”）将运行。	默认情况下
splunk_management_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_management_console_assets.conf 的更多详情，请查看

`$SPLUNK_HOME/etc/apps/splunk_monitoring_console/README`。

配置监视控制台

多实例部署监视控制台设置步骤

本主题概述了要进行的步骤，以便设置您的[监视控制台](#)来监视整个 Splunk Enterprise 部署。要在单个实例上配置监视，请参阅本手册中[单实例监视控制台设置步骤](#)。

1. 为您的部署确定哪个实例应托管监视控制台。请参阅[哪个实例应托管控制台？](#)
2. 请确保部署满足前提条件，包括转发内部日志。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. 如果您想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. 您也可以选择启用预配置的平台告警。请参阅[平台告警](#)。
8. 您也可以选择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. 您也可以选择自定义[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

确定要在部署中托管监视控制台的位置。请参阅[哪个实例应托管控制台？](#)。

单实例监视控制台设置步骤

本主题概述了让[监视控制台](#)监视单个 Splunk Enterprise 实例和其转发器，和使用所包含的[平台告警](#)所需的设置步骤。要在 Splunk Enterprise 部署上配置监视控制台，请参阅[多实例部署设置步骤](#)。

1. 确保您的实例满足前提条件。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. 如果您想使用监视控制台转发器仪表板，请设置转发器监视。请参阅[为监视控制台配置转发器监视](#)。
4. 您也可以选择启用预配置的平台告警。请参阅[平台告警](#)。
5. 您也可以选择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. 您也可以选择自定义[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

确认您实例的前提条件。请参阅[监视控制台设置前提条件](#)。

哪个实例应布置控制台？

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。请参阅[关于监视控制台](#)。

一旦您在分布式模式中配置好监视控制台，您可以仅通过部署中的一个实例导航到该监视控制台并查看您整个部署的控制台信息。但是这应该是哪个实例呢？

对于托管监视控制台的位置，有几个选项。您选择的该实例必须配置为搜索头。请参阅《容量规划手册》中的“参考硬件”。出于安全和某些性能原因，仅 Splunk Enterprise 管理员应具有此实例的访问权限。

重要提示：除了单个、独立的 Splunk Enterprise 实例的情况，托管监视控制台的实例不应该用作生产搜索头，不应该运行任何与监视控制台功能无关的任何搜索。

该表描述了监视控制台的建议位置（基于部署类型）。

分布式模式？	索引器群集化？	搜索头群集化？	监视控制台选项
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。实例的使用应该限于监视控制台和这些特定功能。如果没有可用的许可证主服务器或部署服务器，则在不用于其他目的的专用搜索头上运行监视控制台。
是	单个群集	不相关	主节点。首选的话，您反而可以在不用于其他目的的专用搜索头上运行监视控制台。
是	多个群集	不相关	配置为跨所有群集的搜索头节点的搜索头。该搜索头必须仅限于监视控制台使用。
是	否	是	搜索头群集 Deployer。首选的话，您反而可以在不用于其他目的的专用搜索头上运行监视控制台。请勿在搜索头群集成员中运行监视控制台。

在带有单个索引器群集的部署中：在主节点上

在索引器群集中（无论是单个站点还是多个站点），将监视控制台托管在群集主节点上。请参阅《管理索引和群集手册》中的“系统要求”。

作为替代方法，您可以将监视控制台托管在群集中的搜索头节点上。但是，如果您如此做，则不能使用搜索头来运行任何非监视控制台搜索。

在带有多个索引器群集的部署中：在搜索头节点上

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。

实现此功能的主要步骤为：

1. 将单个搜索头配置为每个索引器群集上的节点。请参阅《管理索引和群集手册》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“[将实例作为搜索节点添加](#)”。

警告：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。

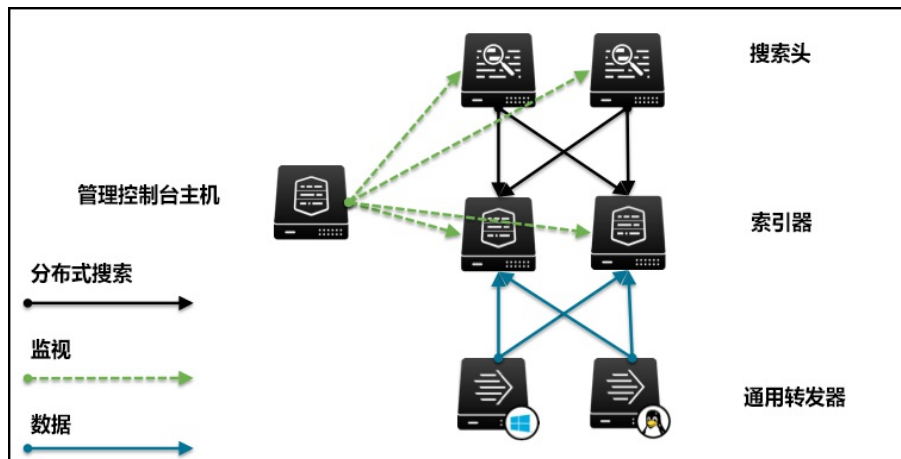
在非索引器群集环境中，选项 1：在许可证主服务器上

如果以下事件是真的，则您可在专用许可证主服务器上配置监视控制台：

- 您的许可证主服务器可处理搜索负载，即符合或超过搜索头参考硬件要求。请参阅《容量规划手册》中的“参考硬件”。
- 仅 Splunk Enterprise 管理员可访问您的许可证主服务器。

在非索引器群集环境中，选项 2：在新实例上

另一个选项为配置新实例，将其配置为搜索头的搜索头和索引器的搜索头，并在此分布式模式中配置监视控制台。



在搜索头群集环境中

使用 Deployer 或专用许可证主服务器托管监视控制台。监视控制台不可以置于搜索头群集成员上。此应用在搜索头群集成员启动时禁用。请参阅《[分布式搜索手册](#)》中的“搜索头群集的系统要求和其他部署注意事项”。

搜索头池环境不支持 DMC。

为何不在生产搜索头中托管控制台

基于某些原因，您应在未用作生产搜索头（即运行您自身搜索或应用的搜索头）的实例中配置监视控制台。

监视控制台分布式搜索组会修改默认搜索行为。此项修改确保针对监视控制台仪表板的搜索范围尽可能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创建一个搜索组。那样就能确保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。但由于所有搜索都会遵循此行为，非监视控制台搜索可能会产生不完整的结果。

另外，您不应将监视控制台布置在生产搜索头上，因为所有生产搜索头的性能都会被监视，而监视控制台本身会影响性能。要在同一个实例中将 DMC 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”。

后续步骤

要继续在分布式模式中设置监视控制台，下一步是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

本主题介绍配置用于 Splunk Enterprise 部署或者单个 Splunk Enterprise 实例的监视控制台的过程中的一步。请参阅本手册的[关于监视控制台](#)。

目前为止您已确定在您的部署中[哪个实例应托管监视控制台](#)。在继续进行[设置群集标签](#)（用于部署）或[在独立模式中配置监视控制台](#)（用于单个 Splunk Enterprise 实例）之前，确保您满足这些前提条件：

- 具有功能性 Splunk Enterprise 部署。请参阅《[分布式部署手册](#)》中的“分布式 Splunk Enterprise 概述”。
- 确保部署运行正常，即所有对等节点都在运行。
- 请确保部署中每个实例（每个搜索头、许可证主服务器等）具有唯一的 `server.conf` `serverName` 值和 `inputs.conf` `host` 值。
- 必须为每个您想要监视的 Splunk Enterprise 实例（除了转发器）启用平台工具。每个实例必须满足平台工具系统要求：
 - 每个节点必须正在运行 Splunk Enterprise 6.1 或更高版本。
 - Windows、Linux 和 Solaris 都支持平台工具。
- 从所有其他实例类型中将内部日志（`$SPLUNK_HOME/var/log/splunk` 和 `$SPLUNK_HOME/var/log/introspection`）转发到索引器。请参阅最佳做法：《[分布式搜索手册](#)》中“转发搜索头数据”。如果没有此步骤，很多仪表板将缺少数据。这些其他实例类型包括：
 - 搜索头。
 - 许可证主服务器。

- 群集主服务器。
- 部署服务器。
- 用户设置分布式管理控制台需要具备 `admin_all_objects` 操作。

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。许多数据来自平台工具，已在 Splunk Enterprise version 6.1 中推出。此外，平台工具在后续版本中已有所增强，例如在 Splunk Enterprise 6.4.0 中添加有关 `iostats` 的日志。下表汇总了哪些数量在哪个版本中推出。

在控制台监视的实例必须满足这些版本要求，否则相关的仪表板面板将显示为空白。

仪表板	面板	系统要求
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（已推出此功能）
搜索头群集仪表板	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 事件收集器仪表板	所有面板	Splunk Enterprise 6.3.0（已推出此功能）
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

后续步骤

要继续在分布式部署中设置您的监视控制台，请参阅[设置群集标签](#)。

要继续在单实例中设置您的监视控制台，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 部署的分布式管理控制台的过程中的一步。请参阅上文的[关于监视控制台](#)。

为监视控制台在您的群集（索引器群集和搜索头群集）上设置标签来识别与它们关联的实例。该识别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

建议您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“启用索引器群集主节点”。

要在部署期间设置搜索头群集标签，请参阅“部署搜索头群集”。

在群集部署之后

如果您正在部署新群集，建议您在部署过程中设置群集标签。但是如果您的群集已经部署完，例如倘若您正在升级群集，则根据这些表格在开始设置监视控制台时设置群集标签。

Splunk Enterprise 版本、群集类型	位置	方法
6.3.0+ 索引器群集	在群集主节点上	请参阅下文
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

要在部署后设置 6.3.0 或之后版本的索引器群集标签，请参阅“使用仪表板配置主节点”或使用以下群集主节点的 CLI 命令：

```
splunk edit cluster-config -cluster_label <CLUSTER_LABEL>
```

Splunk Enterprise 版本、群集类型	位置	方法
---------------------------	----	----

6.3.0+ 搜索头群集成员	在任意 SHC 成员上	请参阅下文
6.3.0+ 搜索头群集 Deployer	在监视控制台设置页面	为 Deployer 实例设置标签
6.3.0 之前版本的搜索头群集	在监视控制台设置页面	为群集中的所有实例设置标签

要在部署后设置 6.3.0 或之后版本的搜索头群集标签，请参阅“配置搜索头群集”或使用以下任意群集成员的 CLI 命令：

```
splunk edit shcluster-config -shcluster_label <CLUSTER LABEL>
```

无论使用哪种方法来编辑群集标签，确保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**。

在编辑群集标签之后，务必单击右上方的**应用更改**。

后续步骤

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](#)。

将实例作为搜索节点添加到监视控制台

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。请参阅[关于监视控制台](#)。

1. 登录到您要在上面配置监视控制台的[实例](#)。
2. 在 Splunk Web 中，选择**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、许可证主服务器和非群集索引器重复步骤 3 和 4。切勿添加群集式索引器，但您必须添加群集式搜索头。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。

后续步骤

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

本主题介绍独立 Splunk Enterprise 实例上配置监视控制台的过程中的一步。请参阅“[单实例监视控制台设置步骤](#)”。

要配置：

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**。
3. 单击**应用更改**以完成设置。

监视控制台设置的下一步是“[配置转发器监视](#)”。

在分布式模式中配置监视控制台

本主题介绍在多实例 Splunk Enterprise 部署中配置监视控制台的过程中的一步。请参阅“[多实例部署监视控制台设置步骤](#)”。

1. 登录到您要在上面配置分布式管理控制台的[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. 打开左上方的**分布式模式**。
4. 确认：

- 标有**实例**和**计算机**的列是否填充正确，且填充的值是否为列中的唯一值。**注意：**如果您的部署具有运行 Splunk Enterprise 6.1.x（而非 6.2.0+）的节点，则不会填充它们的**实例（主机）**和**计算机**值。
 - 要查找**计算机**值，通常您可登录到 6.1.x 实例并在 *nix 或 Windows 上运行 `hostname`。这里，**计算机**代表计算机的 FQDN。
 - 要查找**实例（主机）**值，使用 `bttool : splunk cmd bttool inputs list default`。
 - 当您知道这些值时，在**设置**页面，单击**编辑** > **编辑实例**。显示弹出消息，需要填入两个字段：**实例（主机）名称**和**计算机名称**。
- 此服务器角色正确，其具有基本或主要角色。例如，搜索头（也是许可证主服务器）应具有两个标记的角色。如果没有，则单击**编辑**以更正。
- 如果您正在使用索引器群集化，则会识别群集主节点。如果没有，则单击**编辑**以更正。

警告：请确保任何标记为索引器的东西都是真正的索引器。

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。在您第一次（或曾经）查看监视控制台设置时，您不需要添加组。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。也就是说，一个索引器可属于多个组。请参阅《[分布式搜索手册](#)》中的分布式搜索组。

6. 单击页面右上方的**应用更改**。

7.（可选）设置**平台告警**。

如果您稍后将其他节点添加到您的部署，则返回到**设置 > 常规设置**，并检查步骤 4 中的项目是否准确。

后续步骤

要选择性地监视转发器，请参阅[配置转发器监视](#)。

或者若要选择性地启用预配置的平台告警，请参阅[平台告警](#)。

为监视控制台配置转发器监视

本主题介绍在多实例 Splunk Enterprise 部署中配置监视控制台的过程中的一步。请参阅“[多实例部署监视控制台设置步骤](#)”。

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。转发器的 GUID 位于 `instance.cfg`。

设置

遵循 Splunk Web 中的设置步骤，位于**监视控制台 > 设置 > 转发器设置**。

关于时间设置

在转发器设置中，您可以启用/禁用转发器监视并设置数据收集间隔。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 上**设置 > 搜索和报表 > DMC 转发器 - 构建资产表**中，您可以查看已计划搜索（但不要修改）。

在**监视控制台 > 设置 > 转发器监视设置**页面中，可以针对**数据收集间隔**从若干数值中选择。此间隔决定计划搜索运行的频率。默认值为 15 分钟。

当计划搜索运行以重新构建转发器资产表时，无论选择哪个计划，它都会回溯 15 分钟。此回溯时间不可配置，并且与数据收集间隔有所不同。

例如，您可以将数据收集间隔设置为 24 小时。然后，计划搜索每 24 小时运行一次，但是它仍然要在开始运行前回溯 15 分钟。

如果您有许多（如成百上千的）转发器，则计划搜索会很昂贵。您可能会发现，您想要运行搜索的频率低于每 15 分钟一次（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**。此次您运行该填充的搜索时，可选择回溯时间。该选择不会更改[上述](#)计划搜索的 15 分钟回溯时间或者数据收集间隔。

平台告警

什么是平台告警？

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 Splunk 环境的条件。通知会出现在监视控制台用户界面中，并且可以选择启动告警操作，如电子邮件。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[单实例监视控制台设置步骤](#)或[多实例监视控制台设置步骤](#)。

1.从监视控制台**概览**页面，单击**触发的告警 > 启用或禁用**。

2.单击此告警或您要启用的告警旁边的**已启用**复选框。

告警触发后，监视控制台**概览**页面将显示一个通知。您还可以通过前往**概览 > 告警 > 管理的触发的告警**查看告警及其结果。

您可以选择设置一个告警操作，如电子邮件通知。

配置平台告警并设置告警操作

从监视控制台上，导航到**预览 > 告警 > 启用或禁用**。找到要配置的告警，并单击**编辑**。

您可查看此默认设置并更改参数，例如：

- 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）

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。

包含什么告警？

要使用平台告警开始监视您的部署，您必须启用您想要的单个告警。请参阅上文的[“启用平台告警”](#)。

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。有关仪表板和“索引如何工作”的信息，请参阅 “索引性能：部署” 。
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，并参阅本手册中的 “资源使用情况：部署” 。
到期和不久到期的	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 。

许可证		
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，并阅读本手册中的相应主题。
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。该警告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，并阅读本手册中的相应主题。
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 。

关于搜索项目

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）。

评估和自定义运行状况检查

监视控制台除带有预配置平台告警之外，还有预配置的运行状况检查。您可以修改现有运行状况检查或创建新的检查。

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。单击右上方的**开始**启动运行状况检查。

每个运行状况检查都是一个临时搜索。这些搜索按顺序运行。当一个结束时，下一个即开始。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。

排除检查

您可禁用某项检查以防止在您单击**开始**时会一起运行该项检查。

1. 导航至**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. 重新加载或导航回到**监视控制台 > 运行状况检查**。您无需重启 Splunk Enterprise。

修改现有检查

您可以修改现有检查。例如，假设您想将**物理内存使用率过高**的警告阈值从 90% 改为 80%。

1. 导航至**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您的文件系统中：`$SPLUNK_HOME/etc/apps/splunk_monitoring_console/local/checklist.conf`

创建新检查

要添加一个新的运行状况检查项目：

- 1. 导航至**监视控制台 > 设置 > 运行状况检查项目**。
- 2. 单击右上方的**新运行状况检查项目**。
- 3. 填写表单字段。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。请参阅以下内容了解如何填写**搜索**和**钻取**字段。
- 4. 单击**保存**。

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

关于搜索

在单实例模式中，搜索字符串生成最终结果。在多实例模式中，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

关于钻取

您可以选择性地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。此仪表板应有一个下拉列表可选择实例或计算机。
- 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，找到或创建一个带 `$` 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已经与平台告警有所对应。如果您想将另一个运行状况检查项设置为告警，也是可以的。

下表列出了具有平台告警对应项的运行状况检查项。

运行状况检查	对应的平台告警	条件
	未识别的异常	

索引状态	索引器处理器的当前状态	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	检查已到期或将于两周内到期的许可证。
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创建一个新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**的小望远镜图标。
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搜索，例如，用邮件通知管理员。

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”图标。
4. 选择结果格式（XML、CSV 或 JSON），以及（可选）文件名称和结果数。
5. 单击**导出**。

监视控制台仪表板参考

搜索活动仪表板

本主题是分布式管理控制台中的**搜索活动：实例**和**搜索活动：监视控制台中的部署**仪表板。请参阅[关于监视控制台](#)。

这些视图显示什么？

有关跨 Splunk Enterprise 部署搜索活动的多个面板及按实例给出的细分资料。

解释这些视图的结果

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”）。

解释这些视图的结果

这里仅显示搜索的内存和 CPU 使用情况。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。

在这些视图中查找的内容

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》中的“容纳许多同时进行的搜索”。

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。

对这些视图进行故障排除

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 [正在将您的自检日志转发到您的索引器](#)，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”。

搜索使用情况统计信息仪表板

本主题是分布式管理控制台中**搜索使用情况统计信息实例**和**搜索使用情况统计信息：监视控制台**中的部署仪表板。请参阅[关于监视控制台](#)。

这些视图显示什么？

关于部署中所有搜索头的搜索使用情况统计信息，以及每个实例的详情。

解释这些视图的结果

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，则可能为实时搜索。
- 如果“最早时间”为“-”，则意味着最早时间未指定，最早时间为计算机 epoch 时间的开始。大多数 *nix 环境中为 1970 年 1 月 1 日。
- 如果“最晚时间”为“-”，则意味着最晚时间未指定，则为“现在”。

在**搜索使用情况统计信息:: 实例 > 常用搜索命令**，运行时以秒为单位。

在这些视图中查找的内容

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”。

对这些视图进行故障排除

此视图中的历史面板从 audit.log 中获取数据。如果面板为空白或来自非索引器的信息缺失，则验证您是否 [正在将您的自检日志转发到您的索引器](#)。

此**长时间运行的搜索**面板还使用来自 REST 端点的信息。

计划程序活动

本主题为针对监视控制台中**计划程序活动**仪表板的参考资料。请参阅[关于监视控制台](#)。

这些视图显示什么？

分布式管理控制台中的**计划程序活动：监视控制台中的部署**视图显示搜索或报表计划程序的概览。

这些视图显示计划程序的活动和成功率。在尝试运行的所有搜索中，什么是成功率？并发，计划工作负荷可能会成为障碍。这些视图中的面板可以解释故障类型。跳过比率 and 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。如果您拥有 SHC，请注意还有另外一个视图非常有用，即位于搜索头群集化部分中的计划程序委派（与管理员安排计划程序任务相关）。

解释这些视图的结果

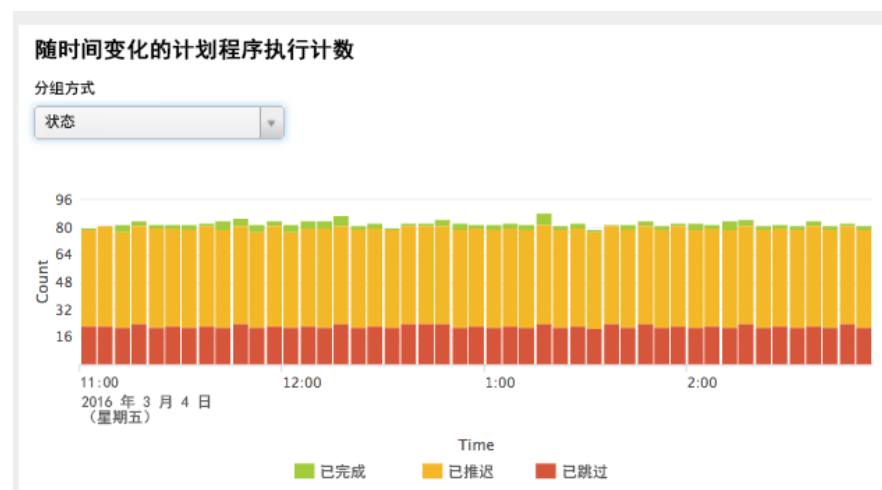
在部署视图中，**统计信息**面板描述的是如何针对实例进行操作，但包括部署中的所有实例。例如，最大值是指部署中任何单个实例中的最大数。

在这些视图中查找的内容

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。

快照量化跳过比率 and 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。

对这些视图进行故障排除

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](#)。

索引性能：实例

本主题是分布式管理控制台中的**索引性能：监视控制台中的实例**仪表板。请参阅“[关于监视控制台](#)”。

此视图显示什么？

有关您部署中潜在多个实例中一个实例的索引性能的多个面板。

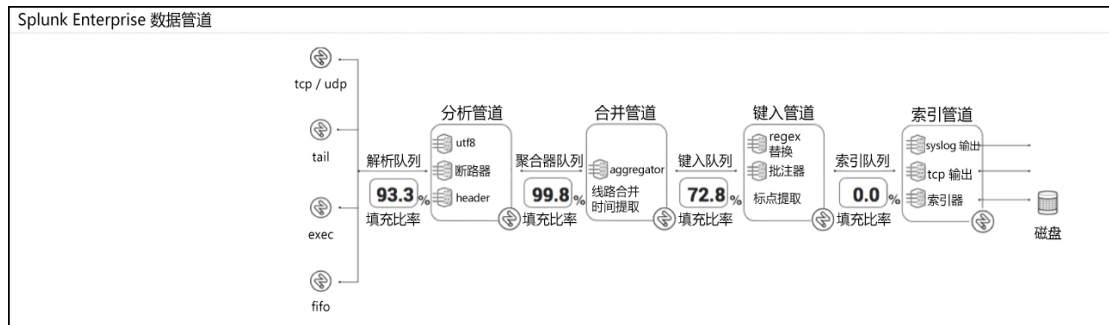
在此视图中解释结果

此名为 **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。

此**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。有关子任务类别含义的更多信息，请参阅《[故障排除手册](#)》中的 metrics.log 主题。

在此视图中查找的内容

此 **Splunk Enterprise 数据管道** 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。

排除此视图的故障

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。

此视图的历史面板从 metrics.log 中获取数据。

索引性能：部署

本主题是分布式管理控制台中的**索引性能：监视控制台中的部署**仪表板。请参阅[“关于监视控制台”](#)。

此视图显示什么？

有关跨 Splunk Enterprise 部署索引性能的多个面板。

在此视图中解释结果

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”。

排除此视图的故障

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。

此视图的历史面板从 metrics.log 中获取数据。

资源使用情况：实例

本主题是分布式管理控制台中的**资源使用情况：监视控制台中的实例**仪表板。请参阅[“关于监视控制台”](#)。

此视图显示什么？

有关资源使用情况的多个面板，作用域由 Splunk Enterprise 实例划分。

在此视图中解释结果

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

进程类意味着一个类上的进程聚合。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 的更多信息，请参阅 DMC 中的“[KV 存储：监视控制台中的实例](#)”视图。

索引服务包含与索引相关的维护任务。它们在索引管道的末尾运行，但异步。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。

在此视图中查找的内容

如果某个正使用很多资源的进程类最后成为搜索，则转到**搜索活动：实例**仪表板。

对于长时间运行的进程，要查找的令人担心的内容为随时间不断增加的内存使用情况。

排除此视图的故障

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[正在将您的自检日志转发到您的索引器](#)，以及
- 平台工具的系统要求。

资源使用情况：计算机

本主题是分布式管理控制台中的**资源使用情况：监视控制台中的计算机**仪表板。请参阅“[关于监视控制台](#)”。

此视图显示什么？

有关在 Splunk Enterprise 部署中单个计算机如何使用资源的多个面板。

在此视图中解释结果

此视图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](#)》。

有关此视图中物理内存使用情况：在 Linux 上，OS 开始使用空闲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。

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。

此视图中的磁盘空间仅指其上具有 Splunk Enterprise 实例的分区。

在此视图中查找的内容

对于长时间运行的进程，要查找的令人担心的内容为随时间不断增加的内存使用情况。

排除此视图的故障

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[正在将您的自检日志转发到您的索引器](#)，和
- 平台工具的系统要求。

资源使用情况：部署

本主题是分布式管理控制台中的**资源使用情况：监视控制台中的部署**仪表板。请参阅“[关于监视控制台](#)”。

此视图显示什么？

有关跨 Splunk Enterprise 部署资源使用情况的多个面板。这些面板对于容量规划很有用。

在此视图中解释结果

有关此视图中物理内存使用情况：在 Linux 上，OS 开始使用空闲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。

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。

在此视图中查找的内容

此视图的通用主题为按值范围分组的实例。其中一个值得关注的就是离群值：与其他实例有所不同。另一个要注意的内容为随时间出现的模式。

排除此视图的故障

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[正在将您的自检日志转发到您的索引器](#)，和
- 平台工具的系统要求。

KV 存储：实例

本主题是分布式管理控制台中的 **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”](#)。

此视图显示什么？

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。如果您已使用分布式部署[配置此监视控制台](#)，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。本节图形中的任意间隙通常指示无法连接 KV 存储或 Splunk Enterprise 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。

此视图从哪里获取数据？

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。

在此视图中解释结果

有关性能指示器和红色标记的信息，请参阅本手册中的“[KV 存储：部署](#)”。

排除此视图的故障

历史面板从自检日志中获取数据。本节图形中的任意时间间隙通常指示无法连接 KV 存储或 Splunk Enterprise 的点。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：

- 您是否正在将您的[自检日志转发到您的索引器](#)，以及
- 平台工具的系统要求。

KV 存储：部署

本主题是分布式管理控制台中的 **KV 存储：监视控制台中的部署** 仪表板。请参阅“[关于监视控制台](#)”。

此视图显示什么？

KV 存储：部署 视图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。有关此视图中要包含的实例，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。

此视图和 **KV 存储：实例** 视图跟踪很多相同信息。差别在于此部署视图从 KV 存储收集统计信息并显示按这些不同指标值分组的实例。

有关各个仪表板和指标的定义和上下文，请参阅本章中的“[KV 存储：实例](#)”。

性能指标

部署快照

部署快照统计信息 访问 `/services/server/introspection/kvstore/serverstatus` REST 端点。对于部署中的每个 KV 存储实例，**部署快照** 提供以下信息：

- 实例。Splunk Enterprise 实例名称。
- 内存使用情况
- 总队列
- 当前连接
- 每个操作的页面故障
- 锁定 (%)
- 最后刷新 (ms)
- 网络流量 (MB)
- 可使用时间 (以小时为单位)。当前实例无需重启运行的时间
- 复制角色。实例在复制设置中扮演的角色。如果实例不是复制设置的一部分，则它将返回 "N/A"。

此视图从哪里获取数据？

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。

解释此视图

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。
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和应用程序预期相称。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。

排除此视图的故障

历史面板从 _introspection 和 _internal 索引中获取数据。这些面板中的任意时间间隙指示无法连接 KV 存储或 Splunk Enterprise 的点。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[正在将您的日志转发到您的索引器](#)，和
- 平台工具的系统要求。

搜索头群集化仪表板

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，上文的**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。

对这些视图进行故障排除

搜索头群集仪表板需要运行 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，[搜索头需要被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”](#)。

分布式搜索仪表板

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。

HTTP 事件收集器仪表板

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，则确认您已完成监视控制台的所有设置步骤。

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您的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连接群集端点所用的时间。

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”](#)。

索引：索引和卷仪表板

本主题是分布式管理控制台中的所有索引：[监视控制台中的索引和卷仪表板](#)。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。

转发器仪表板

本主题是监视控制台**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。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**数据收集间隔**（在**设置 > 转发器监视设置**），即计划搜索运行的频率。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“数据收集间隔”（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。

许可授权

监视控制台中的**许可授权**视图与许可证使用情况报表视图显示相同的信息。通过监视控制台而非许可证主服务器访问此视图的优势是：如果您的部署具有多个许可证主服务器，则在监视控制台视图中，您可选择要查看的某个许可证主服务器的信息。

有关本视图中信息的详细信息，请参阅《**管理员手册**》中的“有关 Splunk Enterprise 许可证使用情况报表视图”。