Splunk® Enterprise 8.2.0

继承 Splunk Enterprise 部署

生成时间：2021 年 5 月 24 日，14:31

Copyright (c) 2021 Splunk Inc. All Rights Reserved

Table of Contents

继承的部署任务

继承的部署

如果您是继承 Splunk 软件部署责任的系统管理员，使用此手册可获得对您的部署网络特点、数据来源、用户填充和知识对象的理解。此信息会帮助您了解在您的环境中运行的 Splunk 平台的重要方面。它包括一些具体建议，关于如何发现正在运行的是什么、运行情况如何、谁在使用它和从哪里可以获得更详细的信息。

要获取 Splunk Enterprise 软件的深入介绍，请参阅《Splunk Enterprise 概览》手册。

要了解使用 Splunk 软件搜索和报表的基础知识，请使用《搜索教程》。

如果 Splunk 软件对您而言是陌生的，有可用的资源来帮助您：

- Splunk Answers
- Splunk Education
- Splunk 用户组
- Splunk 用户组 Slack

Splunk 专业服务团队也可用来实施 Splunk 环境的技术评估以确保您的部署和内部进程遵循最佳做法。

绘制部署图表

绘制部署图表是一个有用的工具，使您在了解您的部署时可以直观了解详细信息，还可以用作未来参考。

阅读本手册中的主题时，请新建 Splunk 部署图表。发现详细信息时请添加。

您可以将图表画在纸上，刚开始最好画在纸上。如果您更想使用如 Visio 或 Omnigraffle 之类的画图工具，这里是您可以使用的一些图标：

http://wiki.splunk.com/Community:Splunk_Visio_Stencil

您的图表应显示以下项目：

- 每个搜索头。
- 每个索引器。
- 任何其他组件，如
  - 索引器群集管理器节点
  - 搜索头群集 Deployer
  - 部署服务器
  - 许可证主服务器
  - 监视控制台
  - KV 存储
- 转发器，或带有大量转发器的服务器类（即转发器集）。
- 每个实例之间的连接。

在图表中的每个节点间留下空间，以便您可以在发现信息时进行添加。每个节点包括以下信息：

- 正在运行的 Splunk Enterprise 版本。
- 是否运行 KV 存储。
- 全部打开的端口。
- 如操作系统、CPU、物理内存、存储类型和虚拟化等计算机信息。

请参阅下一个主题“部署拓扑”以了解大多数组件的定义。继续阅读以下主题以了解使用任一监视控制台发现它们的步骤，如果您有监视控制台就这么做；如果没有，就使用配置文件调查。请参阅“审阅应用和加载项”了解发现您的部署中服务器类和 KV 存储的相关信息和步骤。

部署拓扑

要支持基于部门大小的环境，您可能只需要一个 Splunk Enterprise 实例，在单个计算机上运行。

不过，要支持许多计算机都会生成数据，而且许多用户都需要搜索数据的大型环境，您可以通过跨多个计算机分布多个 Splunk Enterprise 实例，将每个实例配置以实施专门用途来调整部署的规模。

本主题和紧接着的几个主题的目的是帮助您确定当前部署中每个 Splunk Enterprise 实例的角色。如果您已经有该信息，或您的部署由单个实例组成，您可以跳过这些主题。

本主题提供 Splunk Enterprise 部署概览，有部署可能包含的组件和拓扑类型的描述。然后列出步骤，您可以用以了解继承的部署规格。

计划受众

本主题和随后的主题中描述的拓扑发现过程专为 Splunk Enterprise 经验很少或没有 Splunk Enterprise 经验的系统管理员而写。

最基础形式的发现之路只需要一些简单的系统工具，如文件浏览器和文本编辑器。

也有使用 Splunk Enterprise 监视控制台的其他发现过程。监视控制台提供部署的图形概览，以备新的 Splunk Enterprise 管理员使用。但是，作为发现工具使用需要之前的 Splunk Enterprise 管理员已进行过配置。

有经验的 Splunk Enterprise 管理员可能会倾向于使用多种 Splunk 特定工具和方式，如 CLI 命令、搜索、日志文件调查等，更快地实施发现进程。这些方法都需要之前有 Splunk Enterprise 经验，所以新的 Splunk Enterprise 管理员并不能立即使用这些方法。

Splunk Enterprise 如何调整规模

本主题中显示的材料提供通用 Splunk Enterprise 部署拓扑和组成拓扑的实例类型概览。要了解更多详细信息，请参阅*《分布式部署手册》*。

Splunk Enterprise 会在处理数据时执行许多功能。这些功能归为三类：

1. 从文件、网络或其他来源获取数据。

2. 分析、索引并存储数据。

3. 对索引的数据运行搜索。

要调整系统规模，您可以跨多个专门的 Splunk Enterprise 实例分布这些功能。这些实例数量从几个到数千个不等，具体取决于数据数量、访问数据的用户数量和环境中的其他变量。

比如，您的部署可能有上百个只引入数据的实例，多个索引和存储数据的其他实例和管理有关数据的搜索的单个实例组成。

Splunk Enterprise 组件

Splunk Enterprise **组件**是实施特定任务（如索引数据）的 Splunk Enterprise 实例。有多种匹配部署中任务类型的组件类型。

组件分为两大类：

- 处理组件。这些组件处理数据。
- 管理组件。这些组件支持处理组件的活动。

处理组件

处理组件的类型是：

- 转发器
- 索引器
- 搜索头

转发器引入原始数据并将数据转发到另一个组件、另一个转发器或索引器。

转发器通常共存于运行产生数据的应用程序的计算机上，如网络服务器。

通用转发器是转发器最通用的类型。部署还可能包含**重型转发器**和**轻型转发器**。

通常，转发器引入数据并直接转发该数据到索引器。然而，在一些拓扑中，成组的转发器将数据转发至中间转发器，然后将已整合的数据转发到索引器。任何类型的转发器都可以作为中间转发器使用。

索引器索引并存储数据。它们还跨数据进行搜索。

索引器通常驻留在专用计算机上。

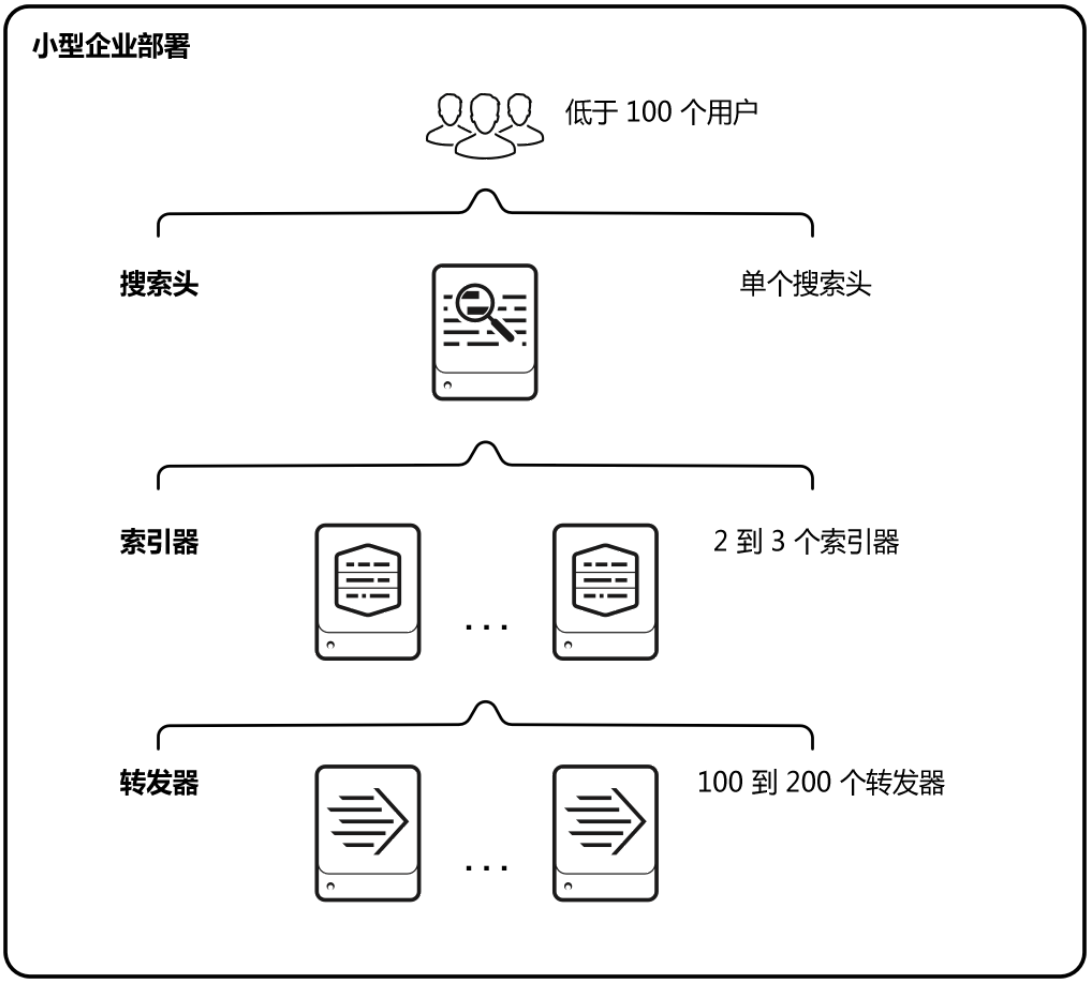
索引器可以是独立的（非群集）索引器，也可以是群集索引器。群集索引器，也称为**对等节点**，是**索引器群集**中的节点。

搜索头管理搜索。它们处理来自用户的搜索请求，并跨搜索本地数据的索引器集分布请求。然后，搜索头合并所有索引器的结果，并将它们提供给用户。搜索头为用户提供各种工具，如**仪表板**，以协助提高搜索体验。

搜索头通常驻留在专用计算机上。

搜索头可以是独立搜索头、**搜索头群集成员**、索引器群集中的搜索头节点或**搜索头池成员**。

以下非群集分布式搜索拓扑的图提供处理组件如何共同协作处理数据的简单示例。说明了可以支持小型企业需求的部署类型。



图表显示支持处理的三个主要层级的组件。从图表的底部开始，这些是处理层级：

- **数据导入。**数据通过转发器进入系统，转发器引入外部数据，对于数据进行少量的预处理，然后将数据转发到索引器。根据您的数据源，您可能有数百个引入数据的转发器。
- **索引。**两个或三个索引器接收、索引和存储来自转发器的传入数据。索引器还会搜索该数据，以响应搜索头的请求。
- **搜索管理。**单个搜索头管理搜索并与用户交互。

要调整系统规模，您可以将更多的组件添加到每一层。为了易于管理，或者为了满足高可用性需求，您可以将组件分为索引器群集或搜索头群集。

管理组件

管理组件是支持处理组件活动的 Splunk Enterprise 实例专有配置版。部署通常包括这些管理组件中的一个或多个：

- 在 Splunk Enterprise 6.2 及更高版本中可用的**监视控制台**执行整个部署的集中监视。请参阅“使用监视控制台确定拓扑”。
- **部署服务器**分布配置更新和应用到一些处理组件，主要是转发器。
- **许可证主服务器**处理 Splunk Enterprise 许可授权。

- **索引器群集主节点**协调**索引器群集**活动。也会处理群集的更新。
- **搜索头群集 Deployer**处理**搜索头群集**的更新。

您的部署可能包括所有这些组件或不包括这些组件中的任何一个，这取决于部署拓扑的规模和规格。

多个管理组件有时共享一个 Splunk Enterprise 实例，有时可能与处理组件一起共享。但是，在大型部署中，每个管理组件可能驻留在专用计算机上。

常用部署拓扑

分布式搜索拓扑提供调整您的部署规模的灵活方式。分布式搜索有很多变体，以便您的部署可以符合组织的需求。

所有的 Splunk Enterprise 部署拓扑都是分布式搜索的变体。变量与拓扑整合索引器群集化或搜索头群集化有关，或与两者都有关。在所有分布式拓扑中，转发器处理数据导入。

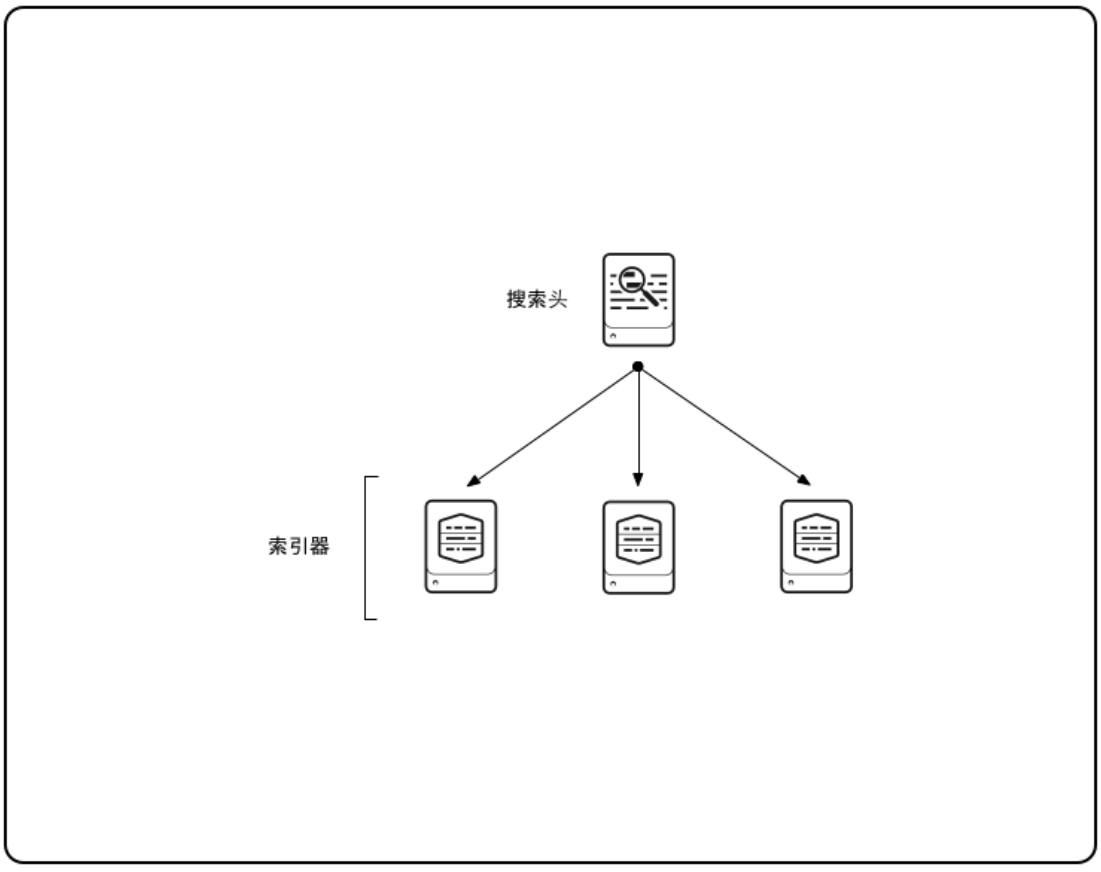
- **基本分布式搜索。**在基本的分布式搜索中，独立的搜索头为许多独立索引器管理搜索。请参阅“基本分布式搜索”。
- **索引器群集。**在**索引器群集**中，许多索引器互相复制数据确保较高的数据可用性。管理器节点提供索引器的集中管理。正如在基础分布式搜索中，转发器和搜索头处理数据导入和搜索管理。请参阅“索引器群集”。
- **搜索头群集。**在**搜索头群集**中，一组搜索头共同承担搜索管理责任。它们将搜索分布到索引器，独立索引器或索引器群集中的节点。请参阅“搜索头群集”。
- **组合的索引器群集和搜索头群集。**此拓扑常见于大型部署中。它遵循索引器群集的模式，除了搜索管理功能由搜索头群集而不是单个搜索头处理。请参阅“组合的索引器群集和搜索头群集”。

*《分布式部署手册》*提供完整部署拓扑的详细描述和示例。

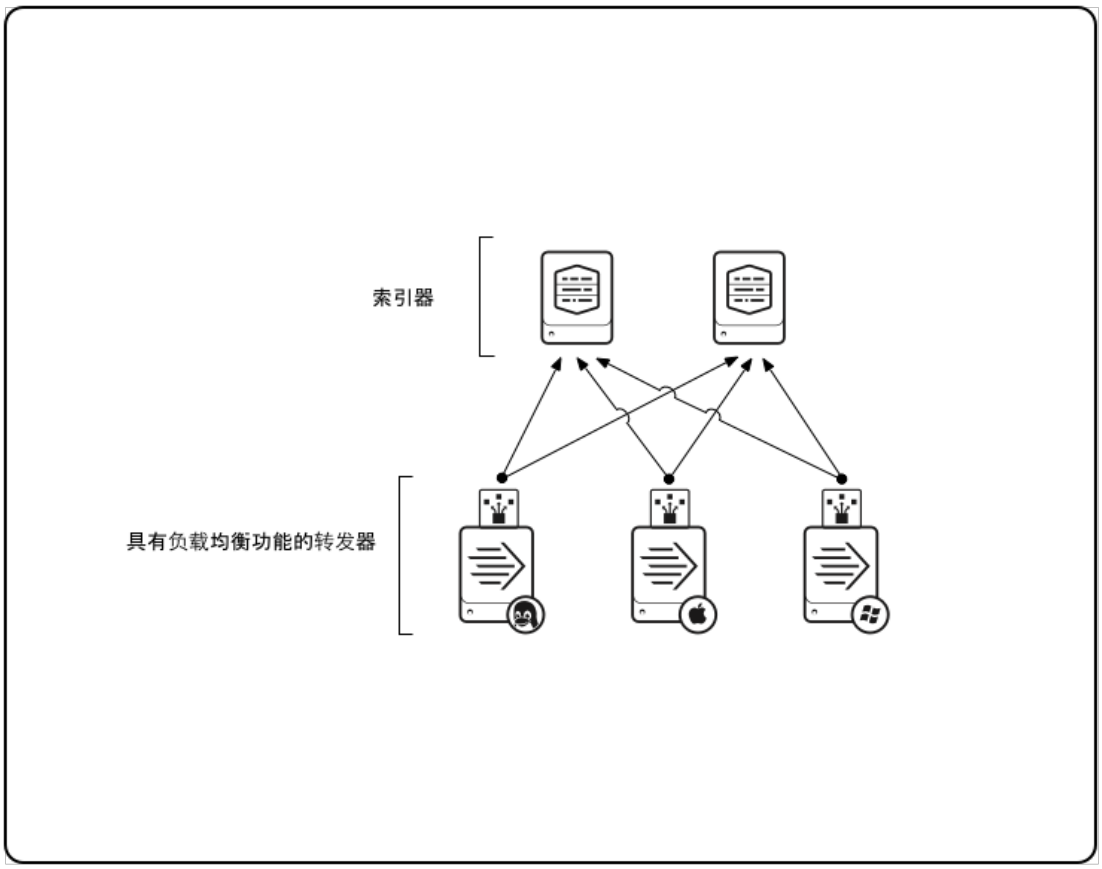
注意：有一个其他的非重复拓扑，**搜索头合并**。在本拓扑中，搜索头使用配置和用户数据的共享存储。本拓扑并不常见，并已为搜索头群集化弃用，但是您可能会发现继承的部署会使用搜索头合并。

基本分布式搜索

此图显示含一个搜索头和三个索引器的分布式搜索拓扑：



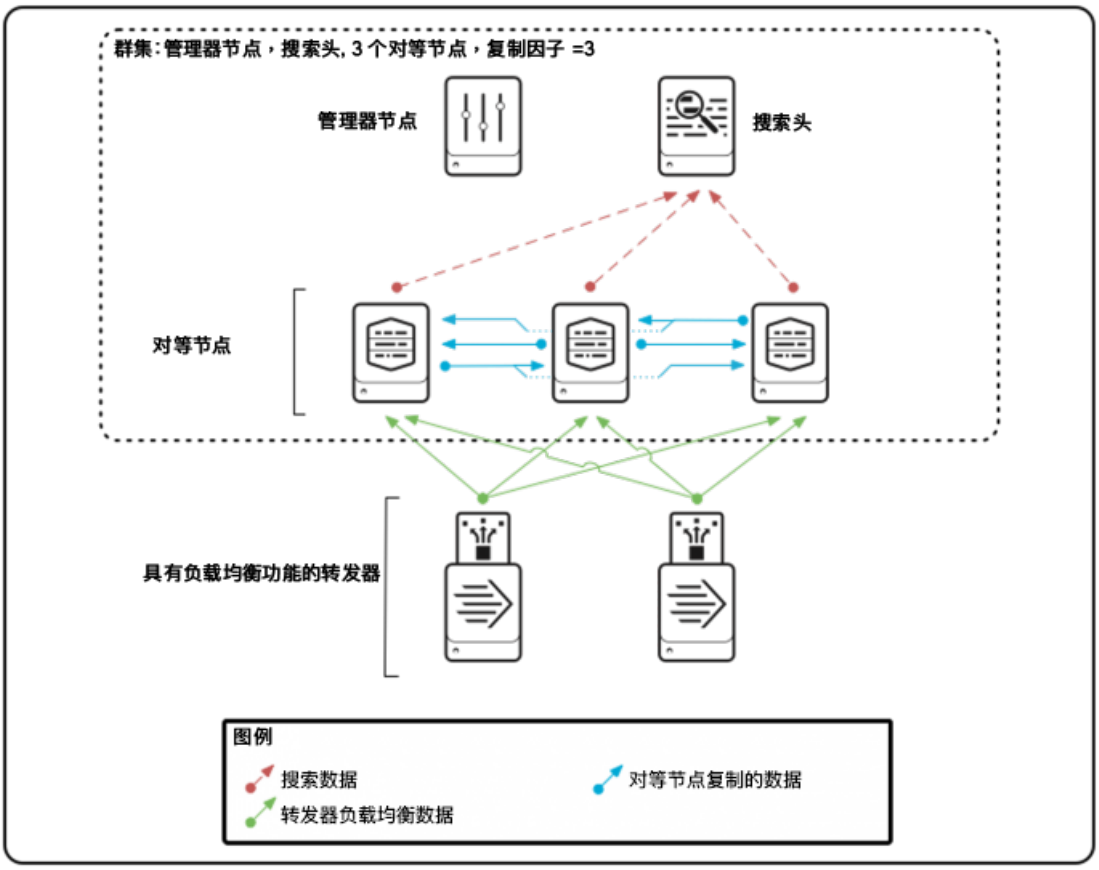
图表不显示引入外部数据并将它发送到索引器的转发器。这是使用负载均衡将数据发送到多个索引器的转发器图：



有关分布式搜索的详情，请参阅*《分布式搜索》*中的“关于分布式搜索”及其之后的几个主题。

索引器群集

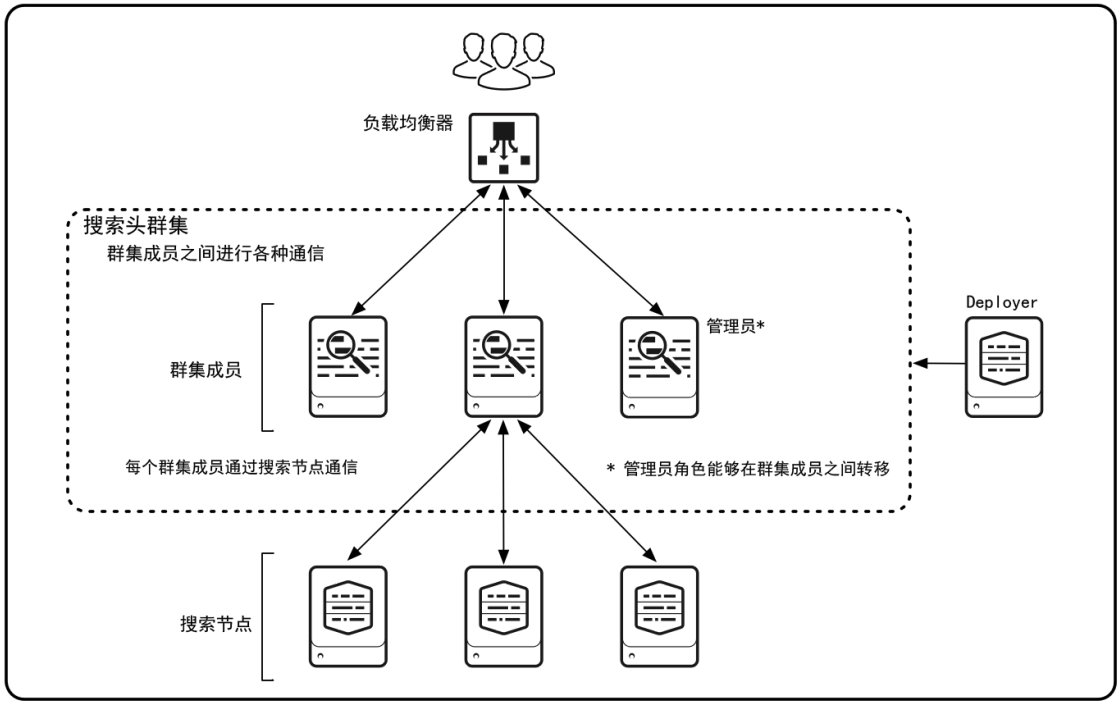
此图表使用一个搜索头和三个索引器（对等节点）显示一个简单的索引器群集。管理器（主）节点控制节点间的互动。和所有分布式拓扑中一样，转发器将数据发送到索引器。



有关索引器群集的详细信息，请参阅*《管理索引器和索引器群集》*中的“关于索引器群集和索引复制”。

搜索头群集

此图表显示一个简单的搜索头群集，有三个搜索头或“成员”。搜索头协调三个独立的索引器或“搜索节点”。



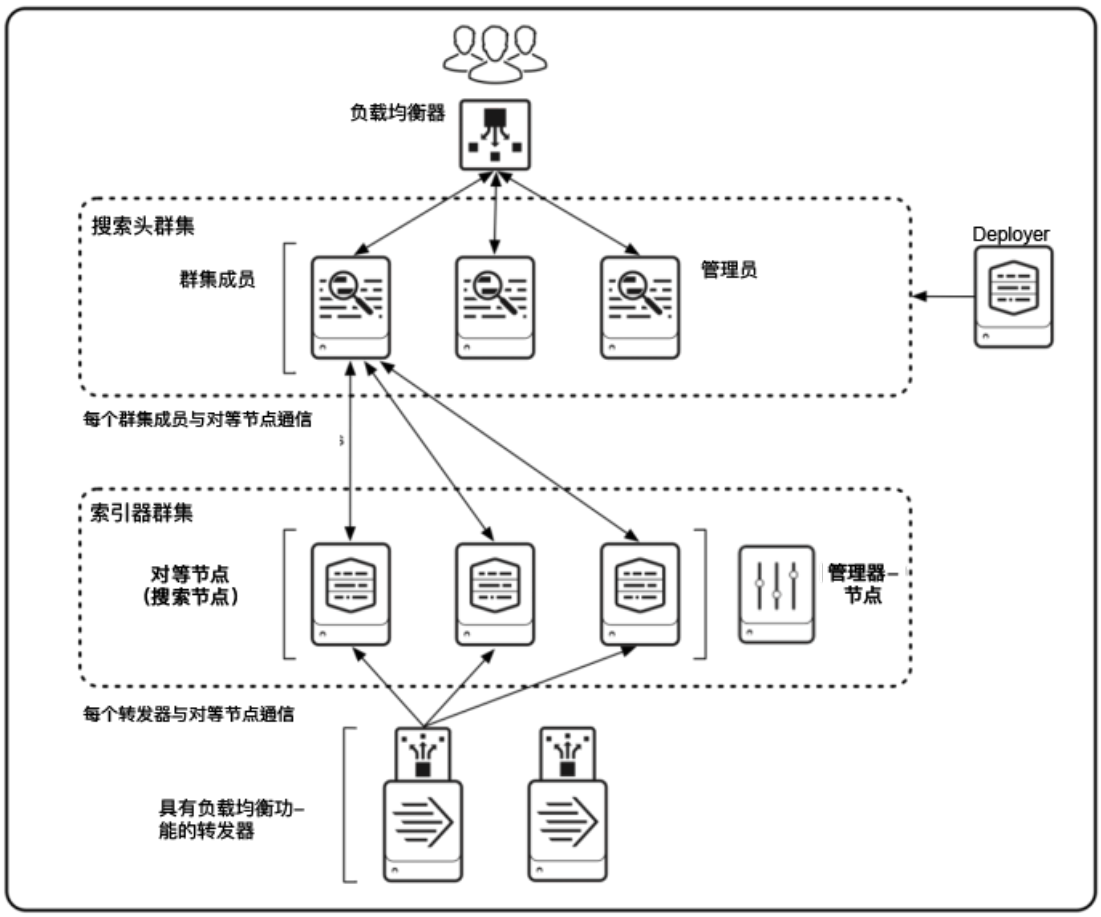
和所有分布式拓扑一样，转发器（未显示）引入外部数据并将它发送到索引器。

Deployer 驻留在搜索头群集外，并处理群集配置的特定更新。

有关搜索头群集的详细信息，请参阅*《分布式搜索》*中的“关于搜索头群集化”及其之后的几个主题。

组合的索引器群集和搜索头群集

在此图表中，搜索头群集管理索引器群集的搜索：



关于将搜索头群集与索引器群集组合的详细信息，请参阅*《分布式搜索》*中“集成搜索头群集和索引器群集”。

发现路径

要确定部署的拓扑，您必须识别组件及其关系。

发现涉及这些步骤：

1. 找到您的 Splunk Enterprise 和通用转发器实例。

   确定哪台计算机包含部署实例。虽然单个计算机可以托管多个实例，这样的配置是不常见的，除非在测试环境中。在生产环境中，每个 Splunk Enterprise 实例通常驻留在自己的计算机中。
2. 识别您的组件。

   识别每个实例托管的组件。组件定义实例在部署中扮演的角色。单个实例可以托管多个组件。
3. 识别组件之间的关系。

   确定组件如何参与整体部署拓扑。

在您进行发现进程时，绘制部署的图表会很有帮助。请参阅“绘制部署图表”。

1. 找到您的 Splunk Enterprise 和通用转发器实例

第一步是在计算机上找到 Splunk Enterprise 和通用转发器实例。请注意这些要点：

- 除通用转发器外，所有组件在 Splunk Enterprise 实例上运行。通用转发器是有自己的执行文件的轻型 Splunk Enterprise。
- Splunk Enterprise 实例通常驻留在专有计算机上，这是最佳做法。但是，您可能会发现在计算机上运行的实例还在执行

完全不同的功能。
- 通用转发器实例通常驻留在托管其他应用程序（如网络服务器）的计算机上。转发器引入由那些应用程序产生的数据。
- 单个计算机可以托管多个实例，虽然最佳做法是使每个实例驻留在自己的计算机中。
- Splunk 图形用户界面 **Splunk Web** 的缺失并不一定表示计算机未托管 Splunk Enterprise 实例。在大多数部署中，只有 Splunk Enterprise 实例的子集，如搜索头和一些管理组件，有正在运行的 Web 界面。

您可以通过查看计算机文件系统上是否显示 Splunk 子目录，识别托管 Splunk Enterprise 和通用转发器实例的计算机。

Splunk 文档将 Splunk 文件系统的基本目录称为 $SPLUNK_HOME。

实例通常驻留在文件系统上的这些位置之下：

操作系统	Splunk Enterprise $SPLUNK_HOME 的位置	通用转发器 $SPLUNK_HOME 的位置
Windows	\Program Files\Splunk C:\Splunk C:\SPL	\Program Files\SplunkUniversalForwarder C:\SplunkUniversalForwarder
Linux Solaris AIX HP-UX FreeBSD	/opt/splunk	/opt/splunkforwarder
Mac OS X	/Applications/splunk	/Applications/splunkforwarder

警告：此表格显示 $SPLUNK_HOME 的默认或典型位置。但是，安装进程允许用户安装到任何位置并更改基本目录名称。因此，如果您无法立即识别 $SPLUNK_HOME，查找包含 Splunk 子目录集的目录。这些子目录包含 bin, etc, include, lib, openssl, share 和 var.

您还可以通过查找包含 splunk, splunkd 和 btool 执行文件的 bin 子目录，验证计算机是否托管 $SPLUNK_HOME。bin 子目录的父级是 $SPLUNK_HOME。

识别有已安装实例的计算机后，确认实例当前正在运行。使用如 ps 或“任务管理器”等系统工具查找 splunkd 进程。

2. 识别您的组件

您可以使用这些方式中的任何一个识别您的组件：

- 使用监视控制台。
- 检查每个实例的配置文件。

如果您的 Splunk Enterprise 部署有正在运行的监视控制台，请用该控制台发现组件和组件之间的关系。请参阅“使用监视控制台确定拓扑”。

如果您的 Splunk Enterprise 部署没有监视控制台，您必须检查每个实例的配置。浏览配置文件集，这些文件集是存有所有实例配置的文本文件。请参阅“检查配置文件以确定您的拓扑”。

请参阅“Splunk Enterprise 组件”。

3. 识别组件之间的关系

您了解组件后，组件间的关系通常是明显的。比如，如果在非群集环境中您有搜索头和三个索引器，每个索引器是搜索头的**搜索节点**，意味着索引器为搜索头处理搜索请求。类似地，如果您发现您有索引器群集的组件，那么您的部署包含一个索引器群集。

如果部署有监视控制台，您可以用来识别组件关系和组件。

您的部署拓扑通常是这些大类中的一种：

- 基本分布式搜索
- 索引器群集
- 搜索头群集
- 组合的索引器群集和搜索头群集

请参阅“通用部署拓扑”。

组件类型摘要

本摘要列出了在您执行组件发现过程中需要牢记的要点。

Splunk Enterprise 部署包括作为处理和管理组件的实例。部署通常只包含可能的组件类型的子集。在发现过程中，您会识别驻留在每个实例上的组件。

一个实例通常托管最多一个处理组件，虽然处理组件还可以实施次要处理功能。比如，一些搜索头将其内部数据转发到索引器。然而，搜索头上的转发功能严格次于其主要功能，因为转发仅涉及内部数据。

管理组件通常是共存于一个带有处理组件或其他管理组件的实例上的。

有些处理组件类型有变量。比如，索引器可以是独立的，也可以是索引器群集的对等节点。

这些是处理组件和他们的变体：

- 搜索头可以是以下类型中的任何一个：
  - 独立搜索头
  - 索引器群集的搜索头节点
  - 搜索头群集成员
  - 索引器群集的搜索头节点和搜索头群集成员
  - 搜索头池成员
- 索引器可以是以下类型中的任何一个：
  - 独立索引器
  - 索引器群集的对等节点
- 转发器可以是以下类型中的任何一个：
  - 通用转发器
  - 重型转发器
  - 轻型转发器
  - 中间转发器（任何类型的转发器的次要特征）

这些是管理组件：

- 监视控制台
- 部署服务器
- 许可证主服务器
- 索引器群集管理器节点
- 搜索头群集 Deployer

使用监视控制台确定拓扑

如果随和的管理员留给您关于监视控制台的信息（之前称之为分布式管理控制台 DMC），您可以用此来发现部署拓扑。

前提条件

阅读部署拓扑。本主题说明了 Splunk Enterprise 部署的要素，提供了如何发现部署拓扑的相关指导。

访问监视控制台

参考您之前的管理员或您的组织提供的任何信息。

监视控制台可以托管在自己的实例上，或者与索引器群集管理器节点共存。较不常见的情况是，它可以与另一个管理组件共存。请参阅*《监视 Splunk Enterprise》*中的“哪个实例应托管控制台？”。

在有可能成为监视控制台的节点上登录 Splunk Web。如果您不知道什么节点是您的监视控制台，尝试索引器群集管理器节点。如果该操作不能给您结果，请尝试任意搜索头。

当您找到运行监视控制台的节点时，导航到监视控制台：

1. 在 Splunk Web 中单击**设置**
2. 单击面板左侧的“监视控制台”图标以打开监视控制台。

监视控制台概览

监视控制台的主页是“概览”页面。

监视控制台有两个模式（独立和分布式）。根据以下截图，确定实例中的监视控制台是在独立模式下还是分布式模式下进行配置。

独立模式下的概览：

分布模式下的概览：

如果您未在分布式模式下对部署中的任何实例配置监视控制台，不要在此时设置。相反，请继续到“检查配置文件以确定您的拓扑”。

发现来自监视控制台的组件和拓扑

从“概览”页面，单击**拓扑**切换以了解您的部署拓扑。

1. 请参阅部署中的实例。
2. 单击每个实例以查看详细信息，包括其 Splunk Enterprise 版本。
3. 在您的部署图表中记录此信息。

查看共存于一个实例的所有组件：

1. 单击**实例**。
2. 使用**组**下拉列表以查看您的部署中的每个组件，将 KV 存储作为最后一个候选。
3. 针对每个实例，注意显示在表格中的信息。“角色”下的信息是组件。
4. 在您的部署图表中记录此信息。

自 Splunk Enterprise 6.3.0 起，管理员可以选择性地在监视控制台中设置转发器监视。要查看转发器信息：

1. 单击**转发器 > 转发器部署**。
2. 使用**拆分依据**下拉列表以了解您的转发器集。
3. 向下滚动至“状态和配置”面板。
4. 在图表中记录转发器类型、Splunk 版本、OS 和系统架构信息。

先不启用转发器监视。

您可以选择性地重建转发器资产表格。如果转发器取消配置，它留存在转发器仪表板上，直到您重新建立转发器资产表格。此

步骤可能不需要立即操作，但是如果您发现您的转发器仪表板包含来自多个转发器的空的结果，您可能会想要重新建立资产表格。如果您有很多转发器，该过程可能需要一段时间。

1. 在监视控制台上，单击**设置 > 转发器监视设置**。
2. 单击**重建转发器资产**。
3. 选择一个时间范围或保持默认 24 小时。
4. 单击**开始重建**。

以后，您将在“审阅应用和加载项”中调查被称为服务器类的许多转发器。

验证您的监视控制台设置

如果已使用监视控制台填充您的图表，那步骤基本完成。

要确保准确性，验证监视控制台是否由您之前的管理员正确配置。使用接下来的配置文件方法。验证监视控制台设置：

1. 使用多个服务器角色（也被称为组件）测试一个或两个实例。
2. 验证监视控制台**实例**页面上针对该实例所显示的服务器角色与使用配置文件方法所收集的信息相匹配。
3. 如果不是，调查其他实例的配置文件并使用该信息填充您的部署图表。
4. 在您完成本手册中的方向任务并到达监视系统运行状况后，纠正监视控制台设置。

检查配置文件以确定您的拓扑

采用此发现方法，检查驻留在每个 Splunk Enterprise 实例上的特定配置文件。文件包含一些设置，这些设置是否存在可帮您确定实例所充当的**组件**。设置还有助于确定组件间的关系，从而，您可以了解整个拓扑。

发现进程查找每个组件类型的特征性配置。

在您进行发现进程时，绘制部署的图表会很有帮助。请参阅“绘制部署图表”。

前提条件

阅读以下材料：

- *《管理员手册》*中的“使用配置文件管理 Splunk Enterprise”这一章。本章节中的主题提供了有关配置文件的重要背景信息：它们是什么，驻留在哪里以及它们如何堆叠在彼此层级之上。
- 部署拓扑。本主题说明了 Splunk Enterprise 部署的要素，提供了如何发现部署拓扑的相关指导。

配置文件位置

配置文件的副本可能驻留在多个位置，包括系统目录和应用目录。如果配置文件在多个位置中有副本，文件中每个设置的操作值根据优先顺序，由文件分层过程确定。

要了解配置文件位置的详细信息，请参阅*《管理员手册》*中的“配置文件目录”。要了解配置文件副本如何分层，请参阅*《管理员手册》中的“配置文件优先顺序”*。

像 `server.conf` 这种包含组件配置的文件，通常只驻留在 `$SPLUNK_HOME/etc/system/local` 下，因为组件设置是系统级别的配置且不依赖于应用。但是，要确定配置必须检查每个相关文件副本所有可能的位置。

如何检查配置文件

要检查配置文件，您可以使用文本编辑器或 `btool` 实用工具。

警告：如果使用文本编辑器，请不要对文件做任何更改。

`$SPLUNK_HOME/bin` 中的 `btool` 实用工具提供筛选配置文件所有副本的快捷方式。`btool` 的优势在于它报告对所有文件副本进行分层后产生的配置集。有关语法和其他详细信息，请参阅*《故障排除手册》*中的“使用 btool 排除配置问题”。

发现处理组件

首先，检查每个实例以查看它是否托管处理组件。然后，检查实例以查看它们是否托管管理组件。

要发现处理组件，请遵循这两个步骤：

1. 识别**搜索头**和**索引器**。
2. 识别**转发器**。

实例通常最多包含一个处理组件。因此，对于每个实例，按顺序遵循每个步骤，直到您识别实例包含哪些处理组件。

步骤中正在处理的组件已通过加粗文本进行标识。

识别搜索头和索引器

确定实例是否是搜索头或索引器，如果是，是什么类型的搜索头或索引器。

1. 检查 `$SPLUNK_HOME/etc/system/local` 中的 `server.conf`。
    1. 查找 `[clustering]` 段落。如找到，则此实例是**索引器群集**的节点。

       要确定索引器群集节点类型，检查 `mode` 设置：
        1. 如果 `mode = master` 或 `mode = manager`，则此实例是**索引器群集管理器节点**。停在此处。

           注意：管理器节点是管理组件，不是处理组件。因为它在 `server.conf` 中进行配置，但是，检查 `server.conf` 中的处理组件时查看主节点也说得通。
        2. 如果 `mode = slave` 或 `mode = peer`，则此实例是**索引器群集对等节点**，也被称为是**群集索引器**。停在此处。
        3. 如果是 `mode = searchhead` ，此实例是**索引器群集搜索头节点**。继续下一步，确定此索引器群集搜索头是否也是**搜索头群集**成员。
    2. 查找 `[shclustering]` 段落。如找到，此实例是**搜索头群集成员**。停在此处。

       注意：搜索头群集成员还可能是索引器群集中的搜索头节点，这取决于部署拓扑。
    3. 查找 `[pooling]` 段落。如找到，此实例是**搜索头池成员**。停在此处。
2. 检查 `$SPLUNK_HOME/etc/system/local` 中的 `distsearch.conf`。
    1. 查找 `[distributedSearch]` 段落中已填充的 `servers` 设置。如找到，此实例是**独立搜索头**。停在此处。

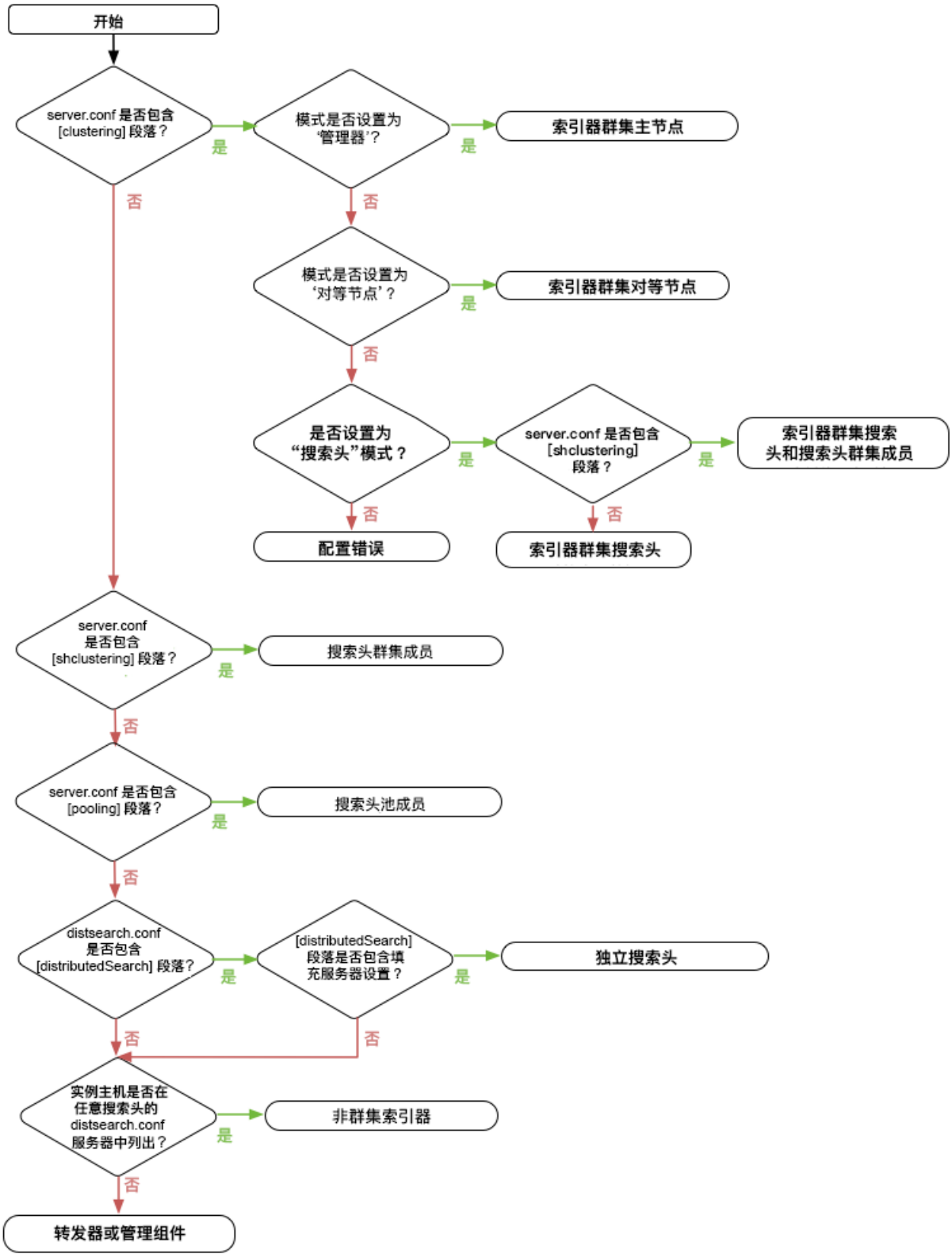
       注意：是搜索头群集或搜索头池的成员的搜索头还有已填充的 `servers` 设置。但是，您已在此程序的早些阶段识别此类搜索头，所以在程序的此处仍相同的有已填充的 `servers` 设置的搜索头必须是独立搜索头。
3. 在之前被识别为搜索头群集成员、搜索头池成员或独立搜索头的所有实例上，检查 `distsearch.conf` 中的 `servers` 设置。

   `servers` 中的地址列表指定此搜索头连接到的索引器的主机。使用此列表确定您的部署中哪个实例是**独立（非群集）索引器**。停在此处。

   注意：在索引器群集中，搜索头不使用 `servers` 列表指定它们的索引器。因此，如果索引器出现在此列表中，它是个非群集索引器。

您识别搜索头和索引器后，所有剩余的实例是转发器或管理组件。

以下流程图包括以上步骤：



警告：在复杂的部署中，搜索头可能为多个索引器群集或为索引器群集和独立索引器集管理搜索。如果您怀疑您有这样的部署拓扑，您可以更深入地调查搜索头的配置。请参阅*《管理索引器和索引器群集》*中的“跨多个索引器群集搜索”和“跨群集和非群集搜索节点搜索”。

识别转发器

如果实例不是索引器或搜索头，它可能是转发器。

Splunk 部署中的索引器提供已安装在该部署中的转发器的相关信息。部署中的索引器记录每个转发器连接和类型。

使用 Splunk 搜索识别转发器

您可以通过登录到 Splunk Enterprise 的索引器或搜索头，并在 Splunk Web 中运行以下搜索，获取已连接到 Splunk 索引器或索引器群集的转发器列表。

```
index=_internal source=*metrics.log group=tcpin_connections | where isnotnull(fwdType) | eval sourceHost=if(isnull(hostname), sourceHost,hostname) | dedup sourceHost | eval connectionType =case(fwdType=="uf","Universal", fwdType=="lwf", "Lightweight", fwdType=="full","Heavy") | rename sourceIp as "Source IP", sourceHost as "Source Host", connectionType as "Forwarder Type" | table "Source IP" "Source Host" "Forwarder Type"
```

如果您有计算机的 IP 地址或主机名称，想要检查计算机的转发器状态和类型，您可以修改搜索以指定主机名称或 IP 地址：

```
index=_internal source=*metrics.log group=tcpin_connections [sourceIp=<ip address>|hostname=<host name>] | where isnotnull(fwdType) | eval sourceHost=if(isnull(hostname), sourceHost,hostname) | dedup sourceHost | eval connectionType =case(fwdType=="uf","Universal", fwdType=="lwf", "Lightweight", fwdType=="full", "Heavy") | rename sourceIp as "Source IP", sourceHost as "Source Host", connectionType as "Forwarder Type" | table "Source IP" "Source Host" "Forwarder Type"
```

如果这些搜索生成的表格没有列出您希望了解其信息的那台计算机的相关信息，或您对 Splunk Web 没有访问权限，可以检查计算机本身以确定转发器类型。

手动识别转发器

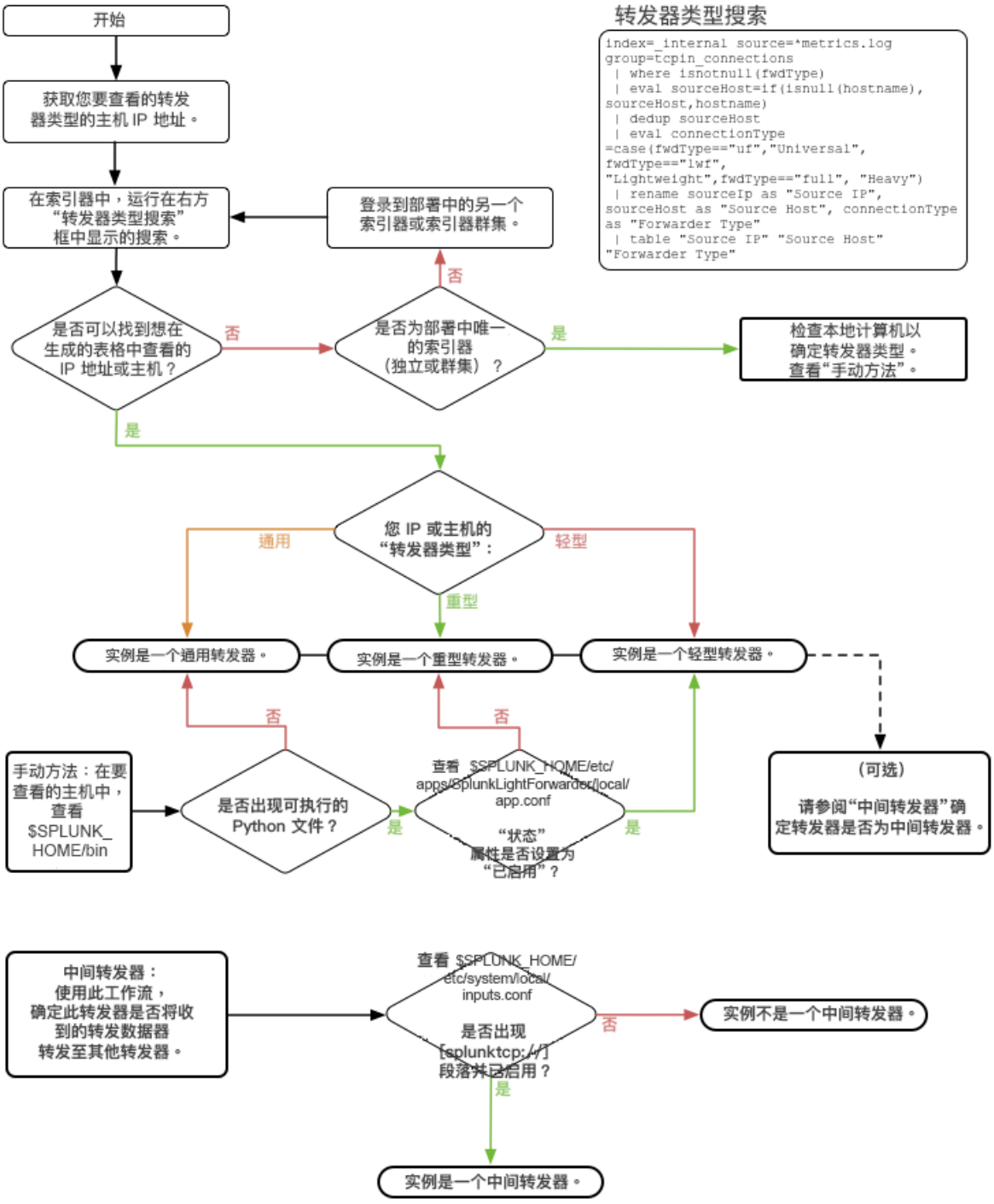
1. 在您想要检查状态的计算机上，查看 `$SPLUNK_HOME/bin` 目录。检查 `python` 可执行文件（Windows 上的 `python.exe`）是否在此目录中。
    1. 如果没有，那么此实例是**通用转发器**。您可以停留在此处或进入下部分的“识别中间转发器”。
2. 如果有，那么检查 `$SPLUNK_HOME/etc/apps/SplunkLightForwarder/local/app.conf` 以查看该文件中的 `state` 是否设置为 `enabled`。
    1. 如果是，那么此实例是**轻型转发器**。这两种情况都请进入下部分的“识别中间转发器”。
    2. 如果不是，那么此实例是**重型转发器**。这两种情况都请进入下部分的“识别中间转发器”。

识别中间转发器

中间转发器接收来自其他转发器的数据以发送到索引器。任何转发器都可以是中间转发器。

1. 查看转发器上的 `$SPLUNK_HOME/etc/system/local/inputs.conf`。是否有 `splunktcp://` 段落并已启用？
    - 如果是，那么此实例是中间转发器。
    - 如果不是，那么此实例不是中间转发器。

请参阅以下工作流理解转发器发现如何运作：



从处理组件到管理组件

所有 Splunk Enterprise 实例到达这个点后，您将了解所有处理组件和索引器群集管理器节点管理组件（如果有）。

如果您无法在特定的实例上找到任何处理组件，实例将只托管管理组件。

在下一部分，确定哪个实例托管管理组件。

发现管理组件

管理组件可以位于它们自己专有的 Splunk Enterprise 实例、与处理组件共存或与其他管理组件共存。因此，任何 Splunk Enterprise 实例都可以包含管理组件。

但是，通用转发器实例无法也包含管理组件。

而且，通常整个部署每个组件最多一个。所以，比如，您识别托管部署服务器的实例（如有）后，您可以停止寻找其他部署服务器实例。

此表格显示每个管理组件它的关键指示器，以及与关键指示器相关的配置文件（如有）。

组件类型	配置文件	关键指示器
监视控制台	$SPLUNK_HOME/etc/apps/splunk_monitoring_console/splunk_management_console_assets.conf	存在 splunk_management_console_assets.conf
部署服务器	$SPLUNK_HOME/etc/system/local/serverclass.conf	[serverClass:<name>] 段落
许可证主服务器	$SPLUNK_HOME/etc/system/local/server.conf	[license] 带有 master_uri = self
索引器群集管理器节点	$SPLUNK_HOME/etc/system/local/server.conf	[cluster] 段落，带有 mode = manager 或 mode = master
搜索头群集 Deployer	N/A	已填充的 $SPLUNK_HOME/etc/shcluster/ 目录

如果您已完成本主题中的所有步骤，您现在应该理解 Splunk Enterprise 拓扑的规格了。您应该了解每个实例的位置和功能，以及实例之间的关系。

组件及其与网络的关系

如果 Splunk Enterprise 组件分布于多个计算机，它们需要网络连接以正常运作，即使是组件都在一个计算机上的情况下，也是如此。

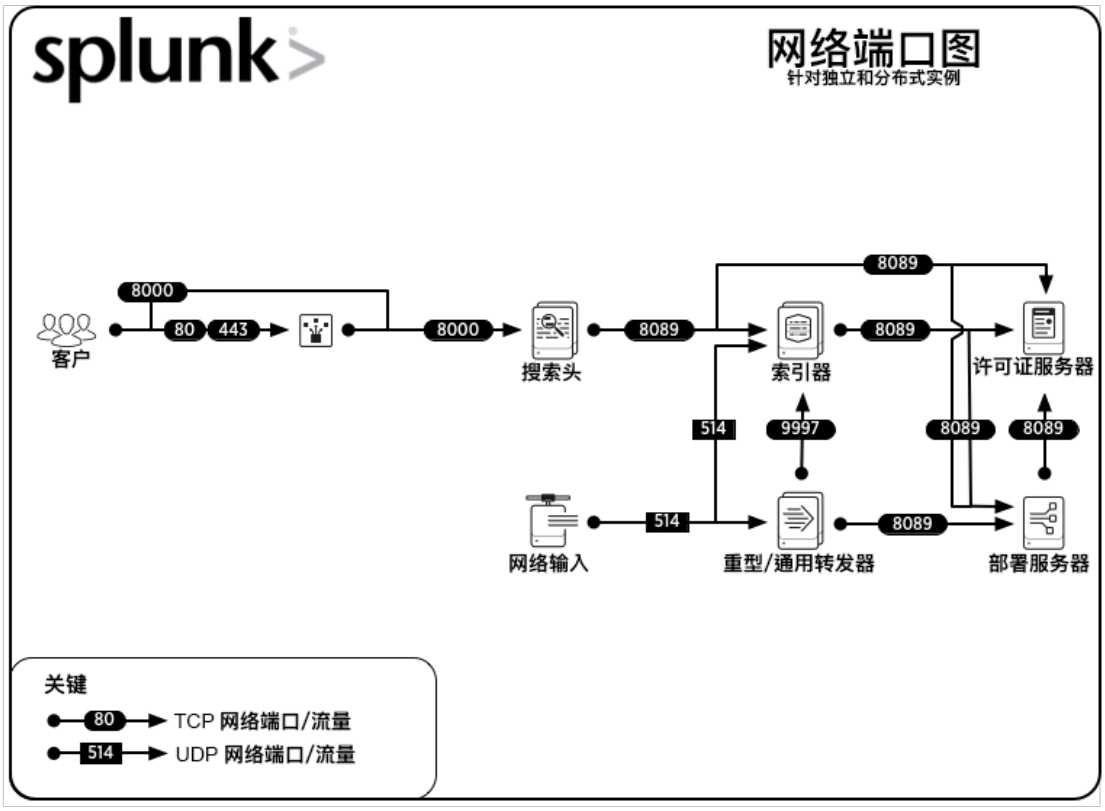
Splunk 组件使用 TCP 和 UDP 网络协议互相通信。配置为允许这些端口打开的防火墙可能会阻断 Splunk 实例之间的通信。

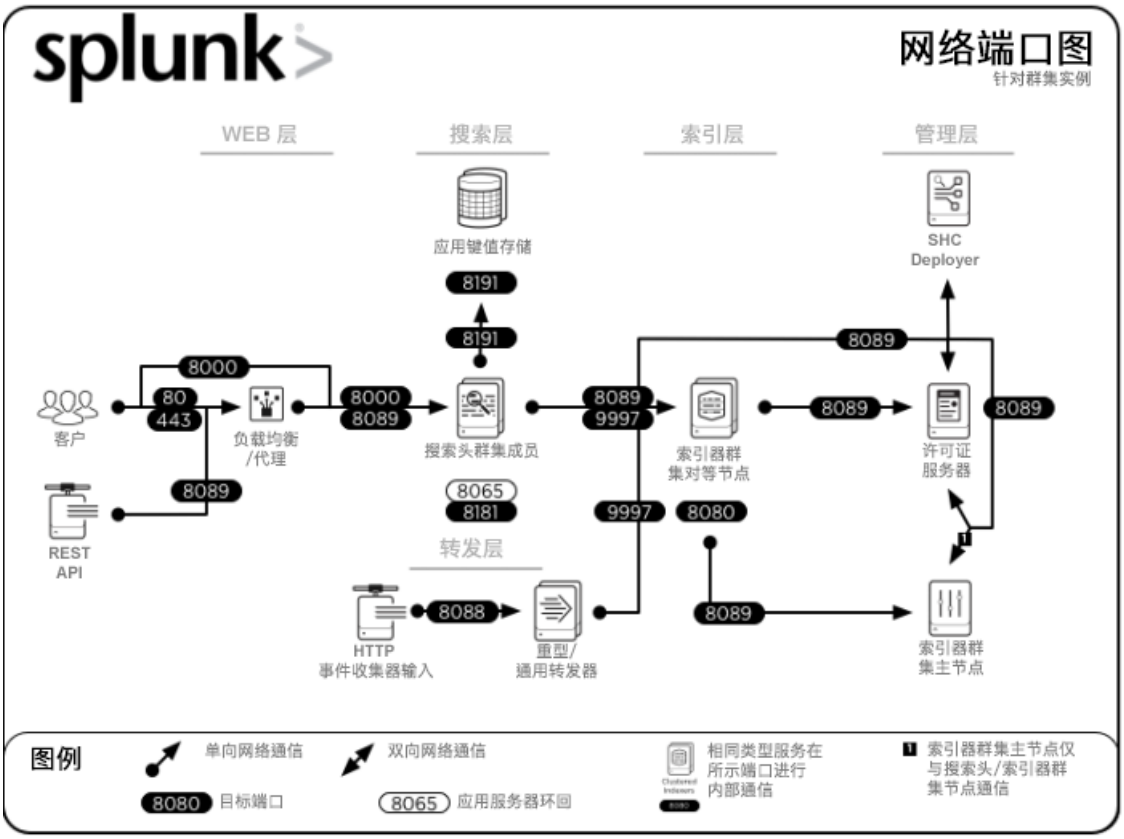
默认情况下或按照惯例，Splunk 软件使用以下网络端口以与它的组件通信。您可以在主机上进行网络端口扫描以确定它是否侦听端口。在部署图表上记录打开的端口号。

组件	用途	通信	侦听
所有组件*	管理 / REST API	N/A	TCP/8089
搜索头 / 索引器	Splunk Web 访问	任意选项	TCP/8000
搜索头	应用键值存储	任意选项	TCP/8065, TCP/8191
索引器	接收来自转发器的数据	N/A	TCP/9997
搜索头群集成员	群集复制	N/A	TCP/8081、TCP/9887、TCP/8181
索引器群集对等节点	群集复制	N/A	TCP/8080, TCP/9887
重型转发器或索引器	通过 HTTP 事件收集器 (HEC) 接收数据	N/A	TCP/8088

图表

以下图表显示 Splunk 软件侦听的网络端口。





了解 Splunk 部署中的数据

发现和绘制 Splunk 部署拓扑图表后，下一个任务是了解部署中的数据。

要理解的 Splunk 部署中的数据有两部分。第一部分是部署中如何管理存储的数据。第二部分是 Splunk 部署如何引入数据。

了解存储的数据

在您控制部署前，已配置从特定数据**来源**引入数据。拥有数据的人或组决定以下内容：

- 可用数据的量
- 数据与组织的相关性
- 组织想要保留 Splunk 软件引入的数据的时间长度
- 组织的数据保存策略
- 需要数据访问权限的人员
- 对敏感数据进行匿名的需求

然后，它们与其他组合作设置 Splunk 软件以索引和存储数据。

您可以使用以下方法了解由 Splunk 软件索引的数据。

- 查看数据摘要
- 对数据运行搜索

查看数据摘要

使用 Splunk Web 中的“数据摘要”，您可以确定数据来源、**来源类型**和产生数据的主机。这是了解 Splunk 部署中有哪些数据的最全面方式。

1. 登录到 Splunk 实例。如果部署是分布式的，请登录搜索头。
2. 单击**搜索和报表**。
3. 单击**数据摘要**。
4. 单击标签以获取实例索引的**主机**、**数据来源**或**来源类型**的信息。
5. （可选）单击**数据摘要**列表中的一个条目以运行结果中包含该条目的搜索。

有关搜索应用的更多信息，请参阅*《搜索手册》*中“关于搜索应用”。

对数据运行搜索

使用 Splunk **搜索**，您可以通过运行搜索命令和调整时间线参数新建显示何时引入数据的时间线。您想要运行的搜索类型取决于您要搜索的数据类型。您可以使用“数据摘要”了解实例中索引的内容和您可以搜索的内容。

1. 登录到 Splunk 实例。
2. 单击**搜索和报表**。
3. 输入代表您想要看到的数据的搜索。如果不知道您有什么数据，可以使用“数据摘要”。
4. （可选）使用事件时间线以确定事件返回多久。
5. （可选）将时间挑选器设置为不同的时间范围以查看只在该范围发生的事件。
6. 单击结果中的单独项以更改搜索参数或根据该项目运行新的搜索。

关于搜索的信息，请参阅*《搜索手册》*中的“搜索剖析”。

了解部署中的数据生成器

要使 Splunk 软件接收数据，它必须配置有**数据导入**。可以在 Splunk 索引器上配置输入，但是在大多数部署中，**转发器**配置有输入，并进行数据收集。数据从转发器流入索引器，Splunk 软件将数据划分为可以形成搜索基础的**事件**、**报表**和**仪表板**，或进行修改以符合您组织中的数据使用者的需求。

Splunk 软件可以引入许多不同类型的计算机数据。*《导入数据》*手册提供有关 Splunk 软件可以引入的计算机数据的相关信息，包括但不限于：

- 日志文件
- 脚本和进程中的数据
- 网络流，包括使用 HTTP 事件收集器监视 TCP、UDP、HTTP 流量
- Windows 数据，包括 Windows 事件日志、注册表更改和性能监视指标

了解 Splunk 软件如何使用输入配置获取数据

您可以在发现 Splunk 部署拓扑后确定数据生成的位置。您还可以在发现部署拓扑的进程中进行此操作，但是在发现部署拓扑后要获取配置信息更简单。

转发器和索引器可以用多种方式获取数据导入和其他配置：

- 在本地，通过 `inputs.conf` **配置文件**。这是 Splunk 实例获取配置信息的最常见的方法
- 通过已安装在实例上的**应用**或**加载项**
- 从连接到转发器或索引器的**部署服务器**

部署服务器是不属于本主题范围的高级配置主题。要了解更多关于部署服务器和它如何运作的信息，请参阅*《更新 Splunk Enterprise 实例》*中的“关于部署服务器和转发器管理”。

inputs.conf 文件定义数据导入并为转发器或索引器控制数据集合各个方面。

- 何时收集数据
- 要收集的数据类型
- 收集数据的频率
- 将已收集的数据索引到何处
- 如何索引已收集的数据

关于转发器，有一个被称为 outputs.conf 的文件控制转发器将数据发送到何处。像 inputs.conf 一样，它可以是独立配置，属于应用或加载项的一部分或是从部署服务器上检索到的配置。

Splunk 软件使用被称为配置文件优先顺序的方案建立主配置文件以处理多个数据集合和转发方案。请参阅*《管理员手册》*中的“配置文件优先顺序”。

发现 Splunk 数据集合配置

以下程序代表确定您的 Splunk 部署中的输入的高级指导。

1. 在您找到部署中的索引器和转发器后，确认它们是否有数据导入的本地配置，获取来自应用或加载项的配置，或检索部署服务器的配置。
2. 如果转发器配置为连接到部署服务器的，请检查部署服务器以查看其配置。连接到此服务器的任何转发器都获取这些配置。配置可以是独立的，或包含在应用或加载项中。
3. 查看 inputs.conf 配置文件以了解收集的数据。您可以在以下位置找到这些文件：
    1. 在自己本身的 $SPLUNK_HOME/etc/system/local
    2. 在应用或加载项中 $SPLUNK_HOME/etc/apps/<name of app>/local
    3. 在部署服务器中 $SPLUNK_HOME/etc/deployment-apps/<name of app>/local
4. 请参阅*《数据导入》*手册以获得每个实例收集的数据类型的信息。
5. 如果您有 Splunk 部署的图表，请指出图表中数据收集实例的位置和它们正在收集的数据。

后续步骤

在您发现数据导入在何处后，您可以进行以下操作：

- 确定导入配置是否需要添加、更改或移除，这取决于业务目标或数据收集性能的改善。
- 确定您是否想要设置监视控制台（如果还未设置）
- 确定是否需要根据 Splunk 导入数据的最佳做法进行修改以索引数据。

查看应用和加载项

如果您继承了大型组织的 Splunk Enterprise 部署，在您的系统中可能有很多应用和加载项正在运行。本主题提供 Splunk 应用和加载项概览，并帮助您识别安装在 Splunk Enterprise 实例中的应用和加载项。

识别在系统上运行的 Splunk Premium Solution 应用很重要。这些应用提供具体使用案例（如 IT 运维和安全）的综合数据分析，可能需要其他资源和管理。

Splunk 应用和加载项概览

Splunk 应用和加载项是您安装在 Splunk Enterprise 实例上的配置文件的打包集。应用和添加项定义如下：

应用：Splunk 应用提供方便您使用数据的用户界面。应用通常使用一个或更多个加载项以引入不同类型的数据。请参阅 Splunk Enterprise*《管理员手册》*中的“应用和加载项”。

加载项：加载项使 Splunk Enterprise 或 Splunk 应用能够引入或映射特定类型的数据。请参阅*《Splunk 加载项》*手册中的“关于 Splunk 加载项”。

Splunk Enterprise 上运行的所有 Splunk 应用和加载项。Splunk Enterprise 包括“Splunk 搜索”和“报表应用”。此应用提供 Splunk Enterprise 的核心搜索环境，允许您新建和管理 Splunk **知识对象**，如**保存的搜索**、**报表**、**告警**、**仪表板**、**数据集**等。

部署要求和注意事项

Splunk 应用和加载项在任意支持的 Splunk Enterprise 部署拓扑上运行，包括单个实例、分布式环境、群集化环境和云环境。要了解现有 Splunk Enterprise 部署拓扑的更多信息，请参阅此手册中的“部署拓扑”。

要熟悉您应用和加载项的任意特殊要求和注意事项，请查看具体应用或加载项的文档。要获取所有支持的 Splunk 应用和加载

项文档，请参阅“Splunk 文档”。

许多 Splunk 应用都通过检查，可以在 Splunk Cloud 中部署。如果您遇到 Splunk Cloud 中的应用部署问题，或如果您想要部署其他应用到 Splunk Cloud，请联系 Splunk 支持。

有关更多信息，请参阅：

- *《管理员手册》*中的“应用部署概览”。
- *《Splunk 加载项》*手册中的“将 Splunk 加载项安装于何处”。

调查应用和加载项

您可以使用 Splunk Web （也就是 Splunk Enterprise UI），或使用命令行导航搜索头上的文件系统，查看所有已安装在您的系统上的应用和加载项。

查看 Splunk Web 中的应用和加载项

Splunk Web 中的“管理应用”页面使您可以访问安装在部署中的所有应用和加载项。您可以查看有关应用的信息，包括应用名、文件名和版本。您还可以启用或禁用应用，使用基于角色的访问控制设置应用权限，并进行如编辑属性和查看对象这类的操作。

1. 打开 Splunk Web。
   所有启用的应用出现在左边的“应用”列。
2. 单击**应用 > 管理应用**。
   “管理应用”页面打开。
3. 查看安装在 Splunk Enterprise 实例上的应用和加载项清单。

有关更多信息，请参阅：

- 本主题中的“查看应用和加载项”。
- *《管理员手册》*中的“编辑应用和加载项属性”。

使用“搜索头”上的文件系统查看应用和加载项

1. 登录到搜索头。
2. 导航到目录 `$SPLUNK_HOME/etc/apps`。
   安装在系统中的所有应用和加载项位于 `apps` 目录。
3. 查看应用和加载项。

应用和加载项命名约定

Splunk 应用文件夹名称使用应用产品名称的变体或缩写。以下表格提供一些示例。

应用名称	应用文件夹名称
Splunk Enterprise Security	SplunkEnterpriseSecuritySuite
Splunk IT Service Intelligence	itsi

Splunk 加载项文件夹名称一般使用下列前缀：

加载项前缀	加载项描述	示例名称
TA	Splunk 技术加载项	Splunk_TA_stream
SA	Splunk 支持加载项	SA-ITOA
DA	Splunk 域加载项（ITSI 模块）	DA-ITSI-OS

查看应用和加载项对象

当您新建应用或加载项时，Splunk Enterprise 新建组成应用或加载项的对象集合。这些对象可以包括视图、命令、导航项目、事件类型、保存的搜索、报表等等。

另外，每个应用对象有关联的基于角色的权限，可以确定谁可以查看或编辑对象。默认情况下，Splunk Enterprise 管理员用户有写入权限并可以编辑系统中所有对象。

使用 Splunk Web 查看有关具体应用或加载项的所有对象，步骤如下：

1. 在 Splunk Web 中单击**设置 > 所有配置**。
2. 在**应用上下文**菜单中，选择您要查看其对象的应用的名称。
3. 选择**只显示在本应用上下文中新建的对象**复选框。

有关更多信息，请参阅：

- *《管理员手册》*中的“管理应用和加载项对象”。
- *《管理员手册》*中的“应用架构和对象所有者”。

识别使用 KV 存储的应用

默认情况下，**KV 存储**驻留在每个 Splunk Enterprise 版本 6.2 或更高版本实例中，通常在搜索头上活跃。KV 存储可以维护关于应用的状态信息。另外，一些应用，如 Enterprise Security，针对查找使用 KV 存储。默认情况下，KV 存储使用端口 8191 复制搜索头中数据。KV 存储进程独立于搜索头群集进程。

使用 Splunk 命令行界面发现 KV 存储成员。请参阅*《管理员手册》*中的“关于 CLI”。

1. 登录到搜索头。
2. 类型 `./splunk show kvstore-status`

记录以下内容：

- 是否禁用为 1 或 0。
- 哪个节点是 KV 存储群集的成员。
- KV 存储正在使用的端口号。

将 KV 存储成员和端口号添加到您的部署图表。此命令还返回有关哪个节点是管理员的信息，但是在此阶段此信息没用。管理员职责可能会更改，所以表格上不要绘制此细节。

下一步，确定哪个应用（如有）使用 KV 存储。

使用 KV 存储的应用在 `$SPLUNK_HOME/etc/apps/<app name>/default` 中定义 `collections.conf`。另外，`transforms.conf` 引用带 `external_type = kvstore` 的集合。

想要获取定义了集合的应用列表：

1. 登录到搜索头。
2. 在命令行，从 Splunk 安装目录，键入 `./splunk btool collections list --debug`
3. 在结果中，在 `$SPLUNK_HOME/etc/apps`

有关更多信息，请参阅：

- 使用开发人员门户上的键值存储管理状态。
- *《知识管理器手册》*中的“配置 KV 存储查找”。
- *《管理员手册》*中的“关于应用键值存储”。
- *《管理员手册》*中的“KV 存储故障排除工具”。

识别部署应用

分布式 Splunk Enterprise 部署使用**部署服务器**将应用和配置文件更新分布到 Splunk Enterprise 组件组，如转发器、非群集索引器和搜索头。这些应用和配置文件被称为**部署应用**。部署应用驻留在已分配到部署服务器角色的 Splunk Enterprise 实例中，并位于目录 `$SPLUNK_HOME/etc/deployment-apps` 下。

在 Splunk Web 中查看部署应用：

1. 识别哪个 Splunk Enterprise 实例被分配了部署服务器角色。要帮助发现正确的 Splunk Enterprise 实例，请参阅此手册中的“发现管理组件”。
2. 登录到部署服务器。
3. 单击**设置 > 转发器管理**。
4. 在“转发器管理”页面，注意以下内容：
   - **应用**。应用是当前由部署服务器分布的部署应用。
   - **客户端**。客户端是远程 Splunk Enterprise 实例，部署服务器将部署应用分布到此实例。
   - **服务器类**。服务器类是部署客户端组。服务器类确定接收应用更新的具体客户端集。
5. 在部署图表上记录服务器类。

使用部署服务器上的文件系统查看您的部署应用：

1. 登录到托管部署服务器的计算机。

2. 转到 `$SPLUNK_HOME/etc/deployment-apps`
3. 记录由部署服务器当前分布的应用。

有关更多信息，请参阅：

- *《更新 Splunk Enterprise 实例》*中的“关于部署服务器和转发器管理”。
- *《更新 Splunk Enterprise 实例》*中的“将应用部署到客户端”。

有关将应用部署到**搜索头群集**、**索引器**和**索引器群集**的信息，请参阅：

- *《分布式搜索》*中的“使用 deployer 分布应用和配置更新”。
- *《管理索引器和索引器群集》*中的“更新通用节点配置和应用”。

从 Splunkbase 下载应用

Splunk 提供许多免费或收费的应用和加载项，可以帮助您拓展数据引入、搜索和分析功能。Splunk 应用和加载项可以在 Splunkbase 下载。

Splunk Premium Solutions 概览

Splunk Premium Solutions 是由 Splunk 开发的应用，为特定使用案例（如 IT 运维分析、安全威胁检测和分析）提供综合数据搜索和分析功能。

Splunk 提供以下 Premium Solutions：

- Splunk Enterprise Security (ES)
- Splunk IT Service Intelligence (ITSI)
- Splunk User Behavior Analytics (UBA)

ES 和 ITSI 要求和注意事项

Splunk ES 和 ITSI 生产部署可能会耗费很多资源。根据多个因素，如并发搜索数、日常索引量和环境未使用的功能，除了基准 Splunk Enterprise 硬件外，可能还需要其他硬件。对于最新的 Splunk Enterprise 硬件要求，请参阅 Splunk Enterprise *《容量规划手册》*中的“参考硬件”。

熟悉影响 ES 和 ITSI 性能的因素，包括各自的关联数或运行的 KPI 搜索以及系统上的并发用户数。这将会帮助您评估系统的性能并确定如何和何时调整您的部署。

熟悉可能会影响部署配置的搜索头和索引器注意事项很重要。比如，Splunk ES 需要专用的搜索头，而 ITSI 不需要。

关于 ES 性能和容量规划的相关信息以及搜索头和索引器注意事项，请参阅 Splunk Enterprise Security *《安装和升级手册》*中的“部署计划”。

关于 ITSI 性能和容量规划、搜索头和索引器注意事项，请参阅 Splunk ITSI *《安装和配置手册》*中的“部署计划”。

Splunk Enterprise Security 概览

Splunk Enterprise Security (ES) 会检测您数据中的模式，并使用相关性搜索评估安全相关事件。**相关性搜索**检测到可疑模式时，相关性搜索可以新建**重要事件**。应用提供专用仪表板和可视化，您可以用来识别、分类并分析安全事件。

请参阅 Splunk Enterprise Security 文档。

查看 ES 相关性搜索

查看 Splunk Enterprise Security 中可用的相关性搜索和另外一些搜索，即那些已经启用以更好地了解正在使用 Splunk Enterprise Security 检测的使用案例的那些搜索。要获取在 Splunk Enterprise Security 中已启用的相关性搜索列表，您可以使用 REST 搜索查看表格中的信息。请参阅*《管理 Splunk Enterprise Security》*中的“列出 Splunk Enterprise Security 中的相关性搜索”。

“内容管理”数据模型行扩展

删除“内容简况”仪表板以支持“内容管理”数据模型行扩展。Enterprise Security 使用已映射到 CIM 特定或 ES 特定数据模型的数据并在广泛的技术中产生更快的搜索结果。查看环境中使用的数据模型，并获得对应数据模型的知识对象概览。请参阅“展开内容管理搜索以查看 Splunk Enterprise Security 中的依赖关系和使用信息”。

数据模型审计仪表板

另外，您可以查看“数据模型审计”仪表板上的数据模型状态和数据模型的保存和加速设置。没有完全加速的数据模型可能导

致 Splunk Enterprise Security 中仪表板或重要事件上信息缺失或过时。请参阅*《使用 Splunk Enterprise Security》*中的“数据模型审计”和 Splunk Enterprise Security *《安装和升级手册》*中的“为 Splunk Enterprise Security 配置数据模型”。

了解更多关于 Splunk Enterprise Security 的内容

要了解更多重要的 Splunk Enterprise Security 概念和功能，请参阅：

- *《管理 Splunk Enterprise Security》*中的“事件审阅”。
- *《管理 Splunk Enterprise Security》*中的“相关性搜索概览”。
- *《管理 Splunk Enterprise Security》*中的“添加资产和身份信息到 Splunk Enterprise Security”。
- *《管理 Splunk Enterprise Security》*中的“添加威胁情报到 Splunk Enterprise Security”。
- *《使用 Splunk Enterprise Security》*中的“风险分析”。
- *《使用 Splunk Enterprise Security》*中的“使用安全情报加速调查”。
- *《使用 Splunk Enterprise Security》*中的“监视安全域活动”。

Splunk IT Service Intelligence 概览

Splunk IT Service Intelligence（ITSI）使用关键绩效指标（KPI）监视 IT 服务的运行状况，KPI 可以追踪 IT 性能指标的严重性等级。KPI 值满足阈值条件时，ITSI 生成重要事件。此应用提供聚合和分析重要事件、仪表板和可视化的功能，使您可以不断监视 IT 服务并进行根本原因调查。

请参阅“Splunk IT 服务情报文档”。

查看 ITSI 服务和 KPI

检查服务和服务内包含的 KPI 以了解您的服务正在监视的 IT 操作和业务流程。KPI 有助于您识别用于评估服务运行状况的性能指标。KPI 搜索属性包括数据来源搜索类型（数据模型、临时或基本搜索）、计算（搜索频率和已计算的统计信息）和确定 KPI 运行状态的严重性级别阈值。

1. 从 ITSI 主菜单中，单击**配置 > 服务**。
2. 查看服务列表。
3. 单击任何服务，然后查看该服务中的 KPI 列表。一个 KPI 代表一个 IT 性能指标，如 `CPU Utilization %`、`Memory Free %`、`Response Time` 等。
4. 在列表中选择任何 KPI，然后展开**搜索和计算**面板。
5. 对于数据来源，请注意**阈值字段**。这是您数据中的字段，KPI 将搜索针对该字段返回一个值。如，cpu_load_percent。单击**编辑**检查数据来源搜索详细信息。注意该基本搜索，如 ITSI 模块提供的搜索，往往会提供最佳搜索性能。
6. 对于实体，注意实体筛选字段。这些字段确定了 KPI 搜索针对哪些实体运行。
7. 对于计算，注意 KPI 计算的统计数据。例如，`Average`。也要注意 KPI 频率和时间范围。KPI 可以每 1、5 或 15 分钟运行。
8. 展开**阈值**面板。
9. 在阈值预览图片中，记下为 KPI 设置的严重性级别阈值。当 KPI 值满足阈值条件时，KPI 状态会改变，如，从高变为重要。

有关更多信息，请参阅 ITSI *《服务洞察》*手册中的“在 ITSI 中创建服务概览”。

查看相关实体

识别与您的服务相关的实体。实体是用作 ITSI 服务的主要数据来源的 IT 组件。KPI 搜索根据您定义的筛选条件针对实体运行。在更加复杂的 ITSI 部署中，单个实体可以与多个服务相关，并且有多个不同的针对单个实体运行的 KPI。

要查看与服务相关的实体：

1. 从 ITSI 主菜单中，单击**配置 > 实体**。
2. 查看实体列表。在服务列中，注意与每个实体相关的服务。
3. 单击列表中任意实体的**查看运行状况**。
4. 查看实体分析仪表板以及与实体关联的服务、针对此实体运行的 KPI，以及关联的显著事件。

有关更多信息，请参阅 ITSI *《实体集成》*手册中的“ITSI 中实体集成概览”。

查看所有 ITSI KPI

使用 Splunk Web 查看在搜索头上运行的所有 KPI 搜索。这有助于您了解构成搜索负载的并发搜索数。您可以查看其他信息，包括 KPI 搜索字符串、搜索频率、时间范围和最近 KPI 搜索任务运行时间。

1. 在 Splunk Web 中单击**设置 > 搜索、报表和告警**。
2. 选择**只显示在此应用上下文中新建的对象**。
   列表中显示在 ITSI 应用上下文中新建的所有应用。KPI 搜索名称使用以下语法：

```
Indicator - <KPI_id> - ITSI Search
```

例如

```
Indicator - 3bee62acf7f4de2a095e475f - ITSI Search
```

3. 对于任何 KPI 搜索，单击**查看最近**。记录 KPI 运行时间。
4. 单击 KPI 搜索的名称。记录 KPI 搜索字符串、时间范围和计划。

注意，平均 KPI 运行时间、KPI 频率、每个 KPI 引用的实体数和在系统中运行的并发搜索总数会显著地影响性能。更多信息，请参阅 ITSI *《安装和升级》*手册中的“性能注意事项”。

关于 Splunk 用户行为分析

Splunk 用户行为分析（UBA）可帮助您找到环境中的已知、未知和隐藏的威胁。您可以使用 Splunk UBA 直观了解内部和外部威胁及异常并进行调查。Splunk UBA 与 Splunk Enterprise Security 整合以利用 Splunk 事件，并调查您组织中的 UBA 威胁和其他重要事件。

请参阅“Splunk 用户行为分析”文档。

用户、角色和验证

在您熟悉 Splunk 配置和数据后，查看您的用户、权限和它们的验证方式。

Splunk Enterprise 支持几种用户验证系统：

- 使用基于角色的用户访问权限的 Splunk 内部验证
- LDAP
- 用于与外部验证系统结合使用的脚本式验证 API，例如 PAM 或 RADIUS
- 多因子验证
- 单点登录

内部验证和基于角色的用户访问权限

通过基于角色的访问控制，您可以管理用户并限制或共享 Splunk Enterprise 数据。Splunk Enterprise 以类似于关系数据库管理基于角色的访问控制的方式通过掩码向用户显示数据。

发现或修改现有的配置

熟悉现有用户及其分配的角色。角色决定了用户数据访问权限级别和他们能够进行的操作。

在 Splunk Web 中单击**设置** > **访问权限控制**查看所有 Splunk 用户。在“访问控制”页面，您可以单击角色和用户以检查或编辑权限。您可以使用此页面新建对每个用户或用户组可用的数据。请参阅*《确保 Splunk Enterprise 安全》*中的“使用访问权限控制以确保 Splunk 数据安全”。

要找到具体用户，您可以使用 CLI 以搜索用户和角色。请参阅*《确保 Splunk Enterprise 安全》*中的“查找现有用户和角色”。

LDAP 验证

当管理员配置 Splunk 以与 LDAP 一起使用时，它们新建名为“LDAP 策略”的东西。LDAP 策略是 Splunk 用来与 LDAP 配置结合使用的配置数据集合。搜索 LDAP 用户时，可以引导 Splunk 以特定顺序查询这些“策略”。请参阅*《确保 Splunk Enterprise 安全》*中的“设置使用 LDAP 进行的用户验证。

发现或修改现有的 LDAP 配置

通过研究您所有的策略，熟悉现有的 LDAP 组和权限映射。要查看或编辑现有的 LDAP 策略，请遵循这些步骤：

1. 单击**用户和验证**下的**访问控制**。

2. 单击 **LDAP**。

3. 您可以从此页选择策略并查看它们的信息，追踪那些映射到 Splunk 角色的 LDAP。

请参阅*《确保 Splunk Enterprise 安全》*中的“使用 Splunk Web 配置 LDAP”。

多因子验证

Splunk Enterprise 当前支持使用双重安全的多因子验证。请参阅*《确保 Splunk Enterprise 安全》*中的“有关使用双重安全的双因子验证”。

发现或修改现有的配置

找出您的系统是否通过 Splunk Web 使用双重因子验证。

1. 单击**设置**下的**用户和验证**

2. 对于**验证方式**，选择**双重安全**。

3. 在此页面上，您可以看到系统是否配置了多因子验证。请参阅*《确保 Splunk Enterprise 安全》*中的“配置 Splunk Enterprise 以使用双重安全双因子验证”。

有 SAML 的 SSO

Splunk 软件可以用外部身份提供程序 (IdP) 提供的信息，利用 SAML 验证进行单点登录 (SSO)。请参阅*《确保 Splunk Enterprise 安全》*中的“使用具有 SAML 的单点登录进行验证”。

发现或修改现有的配置

找出您的用户是否配置 SAML SSO。

1. 选择**设置**中的**访问控制**。

2. 选择**验证方式**下的 SAML。

3. 出现一个新的 SAML 配置，您可以关闭此页面以查看现有的配置。

在此页面上，您可以看到系统是否为用户组配置了 SSO 验证。您可以从那里钻取 IdP 信息、映射组和分配到该组的用户。

ProxySSO 验证

通过 ProxySSO，您可以通过反向代理服务器为 Splunk 实例配置单点登录 (SSO)。使用 ProxySSO 登录的用户可以无缝访问 Splunk Web。

发现现有的配置

您可以查看代理服务器发送到 Splunk Web 的所有现有 HTTP 请求的标头。

在 `settings` 段落下的 `web.conf` 中设置 `enableWebDebug=true`:

```
http://<ProxyServerIP>:<ProxyServerPort>/debug/sso
```

ProxySSO 登录事件记录在 `var/log/splunkd.log` 中。

检查系统安全

Splunk 软件随附一组默认证书。启动时生成和配置默认证书并位于 `$SPLUNK_HOME/etc/auth/`。Splunk 建议管理员用自己或第三方签名的证书替代这些默认证书。

下表介绍了最常见情况和默认 SSL 设置。

交换类型	客户端功能	服务器功能	加密	证书验证	公用名检查	交换的数据类型
浏览器到 Splunk Web	浏览器	Splunk Web	默认情况下不启用	由客户端（浏览器）指定	由客户端（浏览器）指定	搜索术语结果
Splunk 间通信	Splunk Web	splunkd	默认情况下启用	默认情况下不启用	默认情况下不启用	搜索术语结果
转发	splunkd 用作转发器	splunkd 用作索引器	默认情况下不启用	默认情况下不启用	默认情况下不启用	要索引的数据
索引器的部署服	splunkd 用作转发	splunkd 用作索引	默认情况下不			不推荐，改用

索引器的部署服务器	splunkd 用作转发器	splunkd 用作索引器	默认情况下不启用	默认情况下不启用	默认情况下不启用	不推荐。改用 Pass4SymmKey。
Splunk 间通信	splunkd 用作部署客户端	splunkd 用作部署服务器	默认情况下启用	默认情况下不启用	默认情况下不启用	配置数据
Splunk 间通信	splunkd 用作搜索头	splunkd 用作搜索节点	默认情况下启用	默认情况下不启用	默认情况下不启用	搜索数据

验证 SSL 配置

Splunk Web

使用以下命令验证 Splunk Web 中的 SSL 连接：

```
index=_internal source=*metrics.log* group=tcpin_connections | dedup hostname | table _time hostname version sourceIp destPort
ssl
```

索引器和转发器

在索引器上，按启动顺序查找以下或类似消息，以验证连接是否成功：

```
02-06-2011 19:19:01.552 INFO TcpInputProc - using queueSize 1000
02-06-2011 19:19:01.552 INFO TcpInputProc - SSL cipherSuite=ALL:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
02-06-2011 19:19:01.552 INFO TcpInputProc - supporting SSL v2/v3
02-06-2011 19:19:01.555 INFO TcpInputProc - port 9997 is reserved for splunk 2 splunk (SSL)
02-06-2011 19:19:01.555 INFO TcpInputProc - Port 9997 is compressed
02-06-2011 19:19:01.556 INFO TcpInputProc - Registering metrics callback for: tcpin_connections
```

在转发器上，按启动顺序查找以下或类似消息，以验证连接是否成功：

```
02-06-2011 19:06:10.844 INFO TcpOutputProc - Retrieving configuration from properties
02-06-2011 19:06:10.850 INFO TcpOutputProc - Using SSL for server 10.1.12.112:9997, clientCert=/opt/splunk/etc/aut/server.pem
02-06-2011 19:06:10.854 INFO TcpOutputProc - ALL Connections will use SSL with sslCipher=
02-06-2011 19:06:10.859 INFO TcpOutputProc - initializing single connection with retry strategy for 10.1.12.112:9997
```

以下显示的是连接成功在索引器 `splunkd.log` 中呈现的样式：

```
02-06-2011 19:19:09.848 INFO TcpInputProc - Connection in cooked mode from 10.1.12.111
02-06-2011 19:19:09.854 INFO TcpInputProc - Valid signature found
02-06-2011 19:19:09.854 INFO TcpInputProc - Connection accepted from 10.1.12.111
```

以下显示的是连接成功在转发器 `splunkd.log` 中呈现的样式：

```
02-06-2011 19:19:09.927 INFO TcpOutputProc - attempting to connect to 10.1.12.112:9997...
02-06-2011 19:19:09.936 INFO TcpOutputProc - Connected to 10.1.12.112:9997
```

关于确保分布式环境安全

搜索头与对等节点之间的通信使用公共密钥加密。

启动时，Splunk 软件会在 Splunk 安装中生成专用密钥和公共密钥。在搜索头上配置分布式搜索时，搜索头会将公共密钥分布到对等节点，以用于确保通信安全。此默认配置提供了内置加密以及数据压缩，因此可提高性能。请参阅*《分布式搜索手册》*中的“分布关键文件”。

确保分布式配置安全的公共密钥加密。但是，可以通过配置搜索头群集的每个成员，为搜索头群集配置 SSL。您可以通过检查 `server.conf` 中的属性 `requireClientCert`，确定您的部署是否已针对 SSL 配置了每个搜索头群集成员。请参阅*《确保 Splunk Enterprise 安全》*中的“使用证书验证确保部署服务器和客户端安全”。

使用 `splunk.secret` 密钥加密

`splunk.secret` 文件包含在配置文件中收集和加密一些验证信息的密钥：

- `web.conf`：每个实例上的 SSL 密码
- `authentication.conf`：LDAP 密码（如果有）
- `inputs.conf`：SSL 密码（如果有） `splunktcp-ssl`
- `outputs.conf`：SSL 密码（如果有） `splunktcp-ssl`
- `server.conf`：pass4symmkey（如果有）

Splunk Enterprise 在初始启动阶段在 $SPLUNK_HOME/etc/auth/ 中新建此文件。在以上列表中新建的任何密码存储于此文件中。如果您手动添加任何非加密密码，Splunk 软件将在启动后覆盖那些密码。

更多信息

- 关于确保 Splunk Web 安全
- 关于确保来自转发器的数据安全
- 关于确保 Splunk 间通信安全
- 使用您自己的证书确保 Splunk Web 安全
- 将 Splunk 转发配置为使用您自己的证书
- 关于确保 splunk 间通信安全

了解许可授权

Splunk Enterprise 许可授权如何运作

Splunk Enterprise 从您指定的数据来源获取数据并加以处理，以便您进行分析。此处理称之为建立索引。有关建立索引过程的信息，请参阅*《数据导入手册》*中的“Splunk 软件如何处理数据”。

Splunk Enterprise 许可证规定了您在每个日历日（从前一天午夜到当天午夜，以**许可证主服务器**上的时钟为准）可以建立索引的数据量。

进行建立索引的任何 Splunk Enterprise 实例必须得到许可才能进行此操作。您可以使用本地安装的许可证来运行独立的索引器，也可以将某个 Splunk Enterprise 实例配置为**许可证主服务器**，并从其他被配置为**许可证从服务器**的索引器中建立**许可证池**，并从中选取。

如果您在任意一个日历日超过您的日许可量，您将收到违规*警告*。如果在连续的 30 天中 Enterprise 许可证出现 5 个或更多个告警，您*违反*了授权许可。除非您正在使用 Splunk Enterprise 6.5.0 或更高的非强制许可证，否则搜索会被禁用以避免攻击**池**。只要所有池的许可证使用总量不超过许可证主服务器的许可证配额总数，其他池便仍可搜索。

除了索引量之外，访问某些 Splunk Enterprise 功能也需要 Enterprise 许可证。

有一些许可证类型，如：

- Enterprise 许可证启用所有 Enterprise 功能，例如验证和分布式搜索。自 Splunk Enterprise 6.5.0 起，新的 Enterprise 许可证为非强制许可证。
- 免费的许可证允许有限的索引量并禁用一些功能，包括验证。
- 转发器许可证允许您转发数据和启用本地验证，但不允许对数据建立索引。
- Beta 许可证通常启用 Enterprise 功能，但仅限于 Splunk Beta 版本。
- 高级应用许可证与 Enterprise 或 Cloud 许可证结合使用以访问应用功能。

有关不同许可证类型的更多信息，请阅读《管理员手册》中的“*Splunk 许可证类型*”。

了解您的许可证

查看您有什么许可证：

1. 在您的许可证主服务器上登录到 Splunk Web。
2. 单击**设置 > 许可授权**。
3. 记录 Enterprise 和应用许可证及它们的有效期。

检查您的许可证使用情况：

1. 在您的许可证主服务器上登录到 Splunk Web。
2. 单击**设置 > 许可授权**。
3. 单击**许可证使用情况报表**。

请参阅*《管理员手册》*中的“关于许可证使用情况报表视图”。也可从监视控制台的**建立索引**页签访问此视图。

监视您的许可证使用情况

要防止违反许可证，设置临近过期许可证和临近配额许可证告警。您可以使用监视控制台所含的两个平台告警。

有关更多信息，请参阅：

- *《监视 Splunk Enterprise》*中的“平台告警”。
- *《管理员手册》*中的“关于许可证违规”。

更新支持团队联系人

Splunk 许可证与在 Splunk 登记的组织客户帐户关联。通常培训后，客户帐户的一个或多个员工可收到 Splunk 支持，此外，客户帐户还会有一位 Splunk 门户管理员，管理授权联系人列表。确保事先了解组织与支持团队的联络方式。

监视系统运行状况

如果您已配置监视控制台，您可以使用平台告警和运行状况检查监视您的系统运行状况。

如果没有配置监视控制台，本主题将介绍一些工具以开始。但是如果您已阅读并理解之前几个主题的内容，是时候考虑设置监视控制台了。

使用监视控制台

运行一次运行状况检查

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新建检查。

请参阅*《监视 Splunk Enterprise》*中的“访问和自定义运行状况检查”。

理解平台告警

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。

查看哪个平台告警已启用：

1. 在监视控制台中，请单击**概览**。
2. 向下滚动仪表板至您看到“触发的告警”面板。
3. 单击**启用**或**禁用**以转到“平台告警设置”页面。
4. 查找已启用的告警。
5. 单击**高级编辑**以查看针对该告警存在的告警操作。如果您想要接收电子邮件告警，添加您的电子邮件地址。如果您不设置如**发送电子邮件**这样的告警操作，请参阅监视控制台“概览”仪表板中的任意触发告警。

请参阅*《监视 Splunk Enterprise》*中的“平台告警”以了解添加告警操作和可用平台告警列表。

重建转发器资产表

如果转发器取消配置，它留存在转发器仪表板上，直到您重新建立转发器资产表格。此步骤可能不需要立即执行，但是如果您发现您的转发器仪表板包含来自多个转发器的空的结果，您可以重新建立资产表格。

1. 在监视控制台上，单击**设置 > 转发器监视设置**。
2. 单击**重建转发器资产**。
3. 选择一个时间范围或保持默认 24 小时。
4. 单击**开始重建**。

不使用监视控制台

确保内部日志可搜索

确保您的部署正在按最佳做法建议，将 `$SPLUNK_HOME/var/log/splunk` 和 `$SPLUNK_HOME/var/log/introspection` 中的内部日志转发到所有其他实例类型的索引器。请参阅最佳做法：*《分布式搜索手册》*中“转发搜索头数据”。这些其他实例类型包括：

- 搜索头
- 许可证主服务器
- 索引器群集管理器节点
- 部署服务器

请参阅*《排除 Splunk Enterprise 故障》*中的“Splunk 软件记录有关它自身的哪些内容”，了解 Splunk Enterprise 内部日志文件概述。

调查现有的监视应用

从 Splunkbase 或之前的管理员开发的自定义应用调查用于监视系统运行状况的应用部署。

- Fire Brigade 应用可以帮助您了解索引器的运行状况。
- 广受欢迎的 Splunk on Splunk 应用 (SoS) 在 Splunk Enterprise 6.3.0 中不再提供，它的大多数功能已并入监视控制台。如果您的监视策略依赖于 SoS，考虑升级到监视控制台。

使用默认监视工具

即使没有监视控制台，也有一些包含在 Splunk Enterprise 的资源供您用来检查系统运行状况。您可以查看一些关于索引器群集化、搜索头群集化、KV 存储的状态信息以及 Splunk 软件内部记录的错误。

有关索引器群集化仪表板的信息，请参阅*《管理索引器和索引器群集》*中的“查看管理器节点仪表板”和接下来的两个主题。

您可以使用 Splunk 命令行运行部分部署的状态检查，如搜索头群集化和 KV 存储。

您可以从命令行检查搜索头群集组件。请参阅*《分布式搜索》*手册中的“使用 CLI 查看有关搜索头群集的信息”。

检查 KV 存储状态：

1. 登录到搜索头。
2. 在终端窗口，导航到 Splunk 安装目录的 bin 目录。
3. 类型 `./splunk show kvstore-status`

请参阅*《管理员手册》*中的“关于 CLI”以了解关于使用 Splunk CLI 的信息。

生成一般错误的报表：

1. 在索引器群集管理器节点或搜索头上登录 Splunk Web。
2. 单击**应用 > 搜索和报表**。
3. 单击**报表 > 最近 24 小时的 Splunk 错误**。

查找自定义监视工具

除了自定义监视应用，您之前的管理员可能已新建一些系统运行状况自定义报表或告警。查找自定义报表或告警：

1. 在索引器群集管理器节点或搜索头上的 Splunk Web 中，前往**设置 > 搜索、报表和告警**。
2. 审阅告警操作并确保它们满足您的要求。
3. （可选）请添加您的电子邮件地址或自定义脚本。

计划监视策略

任何生产 Splunk Enterprise 部署都需要功能强大的、预防性的监视以最小化停机时间和其他问题。

您的 Splunk Enterprise 监视策略需要注重以下要点，其监视包含在监视控制台中：

- CPU 负载、内存使用情况和磁盘使用情况
- *nix 系统上的 OS 等级设置，如 THP 和 ulimit
- 索引速度
- 跳过搜索
- 糟糕的数据导入做法

考虑设置监视控制台。很有可能，这将包括为此操作配置一个新的计算机。请参阅*《监视 Splunk Enterprise》*中的“多实例部署监视控制台设置步骤”。

调查知识对象问题

知识对象是丰富现有数据的用户定义的实体。它们包含以下对象：

- **报表**
- **告警**
- **仪表板**
- **数据集**
- **字段提取**
- **已计算字段**
- **事件类型**
- **查找**

- **标记**
- **别名**

通过“搜索”和“报表”视图中的列表页面的知识对象或通过**设置**菜单中的**知识**中所列的页面管理大多数知识对象。

有大型 Splunk Enterprise 部署的组织通常有**知识管理员**，其角色包括为其他 Splunk Enterprise 用户新建、组织和维护知识对象。请参阅*《知识管理器手册》*。

调查知识对象图景

查看 Splunk Enterprise 部署的知识对象集合。您可以使用**设置**中的知识对象页以查看已安装应用中的每个知识对象种类。比如，如果您想要查看已保存的搜索，选择**设置** > **搜索、报表和告警**。

查看知识对象时，注意其名称、应用隶属关系、所有者和权限状态。识别有命名或权限冲突、重复或孤立的知识对象。

有命名冲突的知识对象

查看知识对象的类别时，查找命名规则冲突的两种类型：

- 名称相同但定义不同的对象。
- 定义相同但名称不同的对象。

名称相同，定义不同

一种知识对象类别中的所有对象必须有独一无二的名称。比如，在**设置**的搜索、报表和告警列表页面中的已保存的搜索不能有重复的名称。这些知识对象中的大部分在搜索时间应用于您的搜索结果。如果在一个类别下有多于两个对象有相同的名称，将只应用那些对象中的一个。

对象权限更改时会发生重复命名。比如，您可能在两个不同的应用中有相同名称的查找。在应用层级共享时彼此不冲突。但是，如果那些查找中的一个查找的权限发生更改以至于全局共享，那些查找中的一个可能会被应用，而不是其他。

请参阅*《知识管理器手册》*中的“赋予知识对象相同的名称”。

通过建立命名约定避免此问题。请参阅*《知识管理器手册》*中的“制定知识对象的命名约定”。

定义相同，名称不同

如果一个类别下有多个知识对象有相同的或相似的定义，但名称不同，此为规范化问题。提取字段尤其会成为问题。从多个来源类型索引数据时，您会有不同名称的多个字段，但是这些字段代表同一类型的数据。这会导致对索引数据的误解。您可能会无意间建立搜索，而搜索只考虑了您想要捕获的信息中的一部分。

如果 Splunk Enterprise 部署有数据规范化问题，请安装 Splunk 通用信息模型加载项。CIM 加载项可以帮您规范来自多个来源类型的数据以便您制定报表、相关性搜索和显示数据域统一视图的仪表板。

请参阅*《Splunk 通用信息加载项手册》*。

理解对象权限

管理已继承知识对象时，确保您理解**角色**、**功能**和**权限**是如何为 Splunk 部署设置的。

用户新建知识对象时，默认情况下，权限为该用户专用。根据 Splunk Enterprise 部署的设置方式，该用户可能需要依赖有管理员或超级用户角色的人将该对象与其他用户和角色共享。

权限和知识对象互相依赖

如果所有对象权限相同，解决知识对象之间的依赖问题很容易。比如，有一个使用 `outputlookup` 命令以使用全局权限更新广泛使用的查找的专用计划报表。随着时间的推移，您的用户可能会发现查找不按预期行为，但因为大多数用户无法见到专用知识对象，问题原因很难排查并解决。

更多示例，请参阅“对象相互依赖注意事项”。

其他权限使用

权限有很多方面，不仅仅是扩展或限制知识对象的可见性。您可以对以下任务使用权限功能：

- 使用基于角色的功能限制或扩展新建和编辑知识对象的能力。
- 使管理员和超级用户以外的角色能够设置权限和共享对象。
- 设置知识对象类别的权限。比如，您可以限制特定角色的功能以使用所有事件类型或所有查找。

有关角色和功能的更多信息，请参阅*《确保 Splunk Enterprise 安全》*手册中的“关于配置基于角色的用户权限”。

要了解有关知识对象权限的更多信息，请参阅*《知识管理器手册》*中的“管理知识对象权限”。

对象互相依赖注意事项

对象组之间会有重要的相互依赖。对象更改或删除会影响依赖于该对象的其他对象。比如，您可以有引用自定义字段提取的定义的查找。如果您更改字段提取的方式，它会影响查找的准确性。如果该查找用于添加字段到数据模型数据集，更改将向下传递到所有子数据模型数据集。

许多情况下，显示知识对象互相依赖的唯一方法是研究您的对象定义，或分析当上游对象更改、禁用或删除时发生的下游对象损坏。请参阅*《知识管理器手册》*中的“禁用或删除知识对象”。

搜索时间操作的顺序

如果您有互相依赖的知识对象，理解搜索时间操作顺序很重要。在搜索时间，Splunk 软件以特定顺序将知识对象应用到搜索结果。这意味着您无法根据还未定义的对象设置知识对象相互关系。如果您发现互相依赖的知识对象不工作，这是个可能的原因。

比如，Splunk 软件在处理查找前将自定义字段提取应用于搜索结果。这意味着查找可能引用了搜索时间提取的字段的定义。但是，自定义字段提取无法使用定义下的查找派生字段，因为该查找字段还未存在。只有在自定义字段提取处理后派生。

请参阅*《知识管理器手册》中的*“搜索时间操作顺序”。

查找对象互相依赖

按照设计，**查找**可能与知识对象相互依赖有关。

以下是与查找相关的三个知识对象类别：

- 查找定义
- 查找表文件
- 自动查找

这些类别下的任何对象可以分配自己的权限并分享状态。

您可以使用那些知识对象类别以新建以下查找类型：

- CSV 查找
- 外部查找
- KV 存储查找
- 地理空间查找

所有查找类型需要查找定义。两种查找类型（CSV 和地理空间查找）需要查找表文件。您可以选择为所有查找类型新建自动查找。

删除或修改查找对象时需谨慎。查找表文件可以与多个查找定义关联。查找定义还可以与多个自动查找关联。

使用查找您会遇到权限问题。如果查找表文件的权限比与之关联的定义的权限更具限制性，则查找无法运作。对于查找定义和自动查找，也是如此。

- 查找表文件权限应大于或等同于与之相关的查找定义权限。
- 查找定义权限应大于或等同于与之相关的自动查找权限。

请参阅*《知识管理器手册》*中的“查找配置简介”。

数据模型数据集层级

数据模型可能是有父/子关系的数据模型数据集的按层级组织的集合。对于父数据集的修改会向下传递给由此父数据集派生的所有子数据集。您可以使用**数据模型编辑器**查看这些关系。

请参阅*《知识管理器手册》*中的“设计数据模型”。

数据集扩展

所有数据集类型、查找、数据模型和表格可以**拓展**为**表数据集**。提取时，原先的数据集与从中拓展的表数据集有父级关系。对于原先数据集的更改将影响从中扩展的数据集。通过在“数据集列表”页面展开数据集的行，您可以看到数据集是从什么数据集衍生来的。

请参阅*《知识管理器手册》*中的“数据集扩展”。

查找孤立的对象

知识对象所有者的 Splunk 帐户停用时，它们拥有的知识对象留存在系统中。这些对象是孤立的，它们可能导致问题。孤立的对象可能反过来影响互相依赖的对象。

孤立的计划报表尤其有问题。搜索计划程序无法以不存在的用户身份运行计划报表。这会影响仪表板面板和使用计划报表的嵌入报表。如果报表的结果通过电子邮件发送到相关方，这些电子邮件将停止。

Splunk Enterprise 提供检测孤立的知识对象的多种方式，尤其是孤立的计划搜索。找到孤立的知识对象时，您可以使用“重新分配知识对象”页面以重新分配那些知识对象中的一个或多个到新的所有者。

请参阅*《知识管理器手册》*中的“管理孤立的知识对象”。

计划搜索和搜索并发

如果 Splunk Enterprise 根据大量计划报表和告警部署，检查它是否遇到搜索并发问题。

所有 Splunk Enterprise 部署都对可以并发运行的计划搜索数有限制。到达此限制后，名为**搜索计划程序**的后台进程优先安排超出报表并在其他计划报表和告警完成运行后运行。

搜索计划程序的目标是使得每个计划报表和告警在原计划运行的期间内的同一时间运行。但是您可能遇到特定报表有规律地跳过它们的计划运行的情况。

使用监视控制台识别计划程序问题

您可以使用监视控制台识别频繁跳过的搜索，或使得其他搜索频繁跳过的搜索。您还可以使用监视控制台查看系统范围并发搜索限制。请参阅*《监视 Splunk Enterprise》*中的“计划程序活动”。

减少跳过报表数

您可以将**计划窗口**或**计划优先级**设置应用于计划报表以减少跳过的计划报表的数。这些设置是相互排斥的。将**计划窗口**应用于低重要度报表以启用其他报表在它们之前运行。使用**计划优先级**提高高值报表的运行优先级。请参阅*《知识管理器手册》*中的 Splunk Web 的“优先安排当前计划报表”。

报表、数据模型和数据集加速

您可能继承使用加速以提高报表、数据模型和表数据集的 Splunk Enterprise 部署。您的部署可能包括默认含加速数据模型和报表的应用，如 Splunk Enterprise Security、Splunk IT Service Intelligence 和通用信息模型加载项。

如果您的部署有其他对象加速超过您的应用和加载项提供的对象，请验证它们运作是否正确，确定其摘要是否正在没有必要地使用有限的磁盘空间。

在报表、数据模型和表数据集的列表页面上，加速由黄色的闪电符号表示。

要了解由 Splunk 提供的基于摘要的加速选项概览，请参阅*《知识管理器手册》*中的“基于摘要的搜索加速概览”。

查看报表加速摘要

您可以选择**设置** > **报表加速摘要**访问报表加速摘要数据。

操作	详细信息
识别不必要的摘要。	在“设置”中的“报表加速摘要”页面，查找高**摘要负载**和低**访问统计**摘要。 考虑移除这些摘要。统计信息表明它们正在使用许多系统资源但是并不经常用到。 您可以单击特定摘要的“摘要详情”以查看**磁盘上的大小**。占据许多空间但不频繁使用的摘要也是合适的移除候选。
识别功能失调的摘要。	在“设置”中的“报表加速摘要”页面，如果**摘要状态**是**暂停**或**没有足够的数据进行摘要**，摘要可能有需要解决的问题。如果预测摘要可能过大，Splunk 软件可能不会新建摘要。
解决摘要问题。	1. 选择**设置** > **报表加速摘要**。 2. 找到应移除的摘要，并单击**摘要 ID** 打开详情页面。 3. （可选）如果怀疑摘要包含不一致数据，单击**验证**。 4. （可选）如果摘要在某一时间没有更新，而您想要使它成为当前摘要，单击**更新**。

	5. （可选）单击**重建**以重建验证失败的摘要或可能有数据缺失问题的摘要。大型摘要的重建可能会很耗时。
删除不必要的摘要。	1. 选择**设置** > **报表加速摘要**。 2. 找到应移除的摘要，并单击**摘要 ID** 打开详情页面。 3. 单击**删除**以移除摘要。

请参阅*《知识管理器手册》*中的“管理报表加速”。

调查数据模型和数据集摘要

您可以通过“设置”中的“数据模型”页面管理数据模型和表数据集的加速。扩展数据模型的行和表数据集以查看它们的统计信息。

查找**访问统计**数较低、**磁盘上的大小**数较高的摘要。考虑移除这些摘要，或减少摘要窗口以便他们不占据过多磁盘空间。

如果您有新建进程不完整的摘要，请参考*《知识管理器手册》*中的“加速数据模型”。这一部分介绍了可帮您解决这些问题的高级配置。

查看基于大小的摘要保存规则

包括基于大小的报表、数据模型和表数据集摘要的保存规则的部署可能会使用无限磁盘空间。部署可能已配置基于大小的保存规则以防止发生该情况。

查看这些配置，识别受影响的摘要，评估配置是否需要更新或者移除。

关于报表加速摘要保存配置的信息，请参阅*《知识管理器手册》*中的“管理报表加速”。

有关数据模型和表数据集摘要保存配置的信息，请参阅*《知识管理器手册》*中的“加速数据模型”。

检查数据模型和表数据集的并行摘要

并行摘要是一个后台进程，使用该后台进程可提高 Splunk 软件为数据模型和表数据集新建加速摘要的速度。通过运行并发搜索建立摘要操作。默认对所有 Splunk Enterprise 部署启用。

如果您遇到持续搜索并发或搜索性能问题，检查是否是您的前置程序将并行摘要设置提高到默认以上。可能会运行超出您系统支持的并发搜索。

请参阅*《知识管理器手册》*中的“加速数据模型”。

评估您的摘要索引

摘要索引是您可以用于不符合加速条件的报表的报表加速方法。如果您的部署使用摘要索引，它有可以特定用于摘要索引的索引。查看这些摘要索引和用数据填充的搜索，并评估是否可以用报表加速摘要替代。

请参阅*《知识管理器手册》*中的“基于摘要的搜索加速概览”。