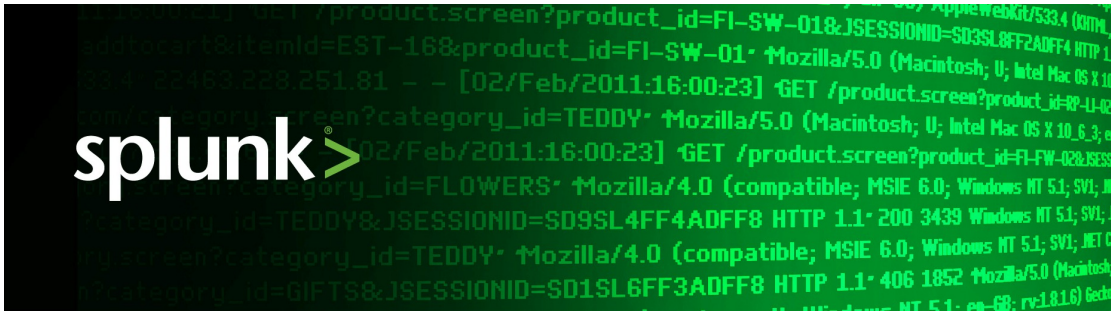


Splunk® Enterprise 6.5.0

分布式部署手册

生成时间：2016 年 9 月 26 日，下午 10:21

Table of Contents

Splunk Enterprise 分布式部署概述

使用 Splunk Enterprise 组件调整您的部署规模

在单实例部署中，由一个 Splunk Enterprise 实例处理数据处理的所有方面，从导入、创建索引到搜索。单实例部署非常适用于测试和评估目的，可以满足部门规模环境的需求。

不过，要支持大型环境，许多计算机都会生成数据，而且许多用户都需要搜索数据，此时您可以通过跨多个计算机分布 Splunk Enterprise 实例来调整您的部署规模。执行此操作时，您可以配置实例以便每个实例执行一个专门的任务。例如，一个或多个实例可以索引数据，而另一个实例则管理跨数据的搜索。

本手册介绍如何跨多个计算机分布 Splunk Enterprise。分布式部署可用来：

- 调整 Splunk Enterprise 功能以解决任何规模和复杂程度不等的企业的数据需求。
- 访问不同的或分散的数据源。
- 实现高可用性并确保数据复制和多站点部署的灾难恢复。

Splunk Enterprise 如何扩展

Splunk Enterprise 会在处理数据时执行三项关键功能：

1. 从文件、网络或其他来源获取数据。

2. 分析并索引数据。

3. 对索引的数据运行搜索。

要调整您的系统规模，您可以跨多个专门的 Splunk Enterprise 实例拆分此功能。这些实例数量从几个到数千个不等，具体取决于您所处理的数据数量以及您环境中的其他变量。

在一个典型的分布式部署中，每一个实例都占用对应于关键处理功能的三层中的一层：

- 数据导入
- 索引
- 搜索管理

例如，您可以创建一个包含以下实例的部署：若干个只获取数据的实例、其他若干个建立数据索引的实例以及一个管理搜索的实例。

可以结合这些层中的一些或者以其他方式配置处理，但这三层是大多数分布式部署的典型层。

Splunk Enterprise 组件

专门的 Splunk Enterprise 实例统称为**组件**。其中一个例外是，组件是完整 Splunk Enterprise 实例，已配置为专注于一个或多个特定的功能，如索引或搜索。该例外是**通用转发器**，它是使用单独的可执行文件的轻型 Splunk Enterprise 版本。

有若干种类型的 Splunk Enterprise 组件。它们分为两大类：

- 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。

本主题介绍 Splunk Enterprise 部署中的处理组件和它们的角色。有关管理组件的信息，请参阅"帮助管理部署的组件"。

处理组件的类型

有三种主要类型的处理组件：

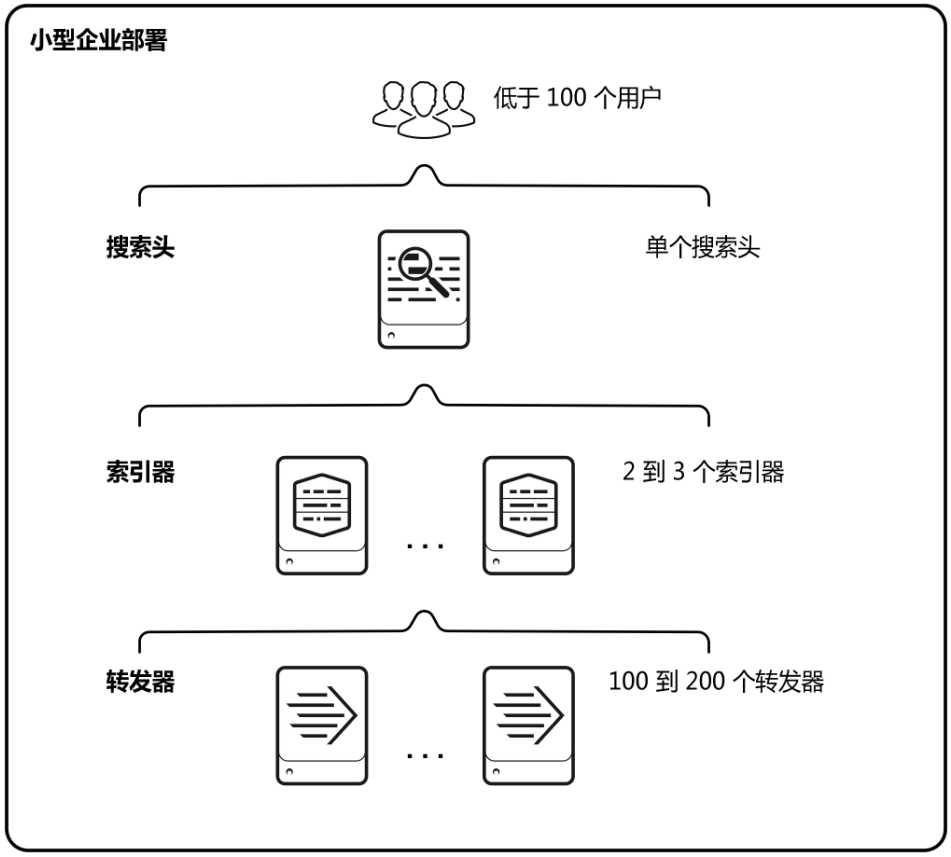
- 转发器
- 索引器
- 搜索头

转发器获取数据。虽然有几种类型的转发器，但在大多数情况下通用转发器是正确的选择。它使用轻型 Splunk Enterprise 版本，只是导入数据，对数据执行最低层次的处理，然后将数据转发到索引器。因为它的资源需求最小，所以可以共存于产生数据的计算机（例如 Web 服务器）上。

索引器和**搜索头**从 Splunk Enterprise 实例构建，您可以分别配置来执行索引或搜索管理的专门功能。每个索引器和搜索头都是一个通常驻留在自己计算机上的单独实例。

处理组件实例

该图提供一个关于处理组件如何驻留在各种处理层的简单示例。它说明了可以支持小型企业需求的部署类型。



从底部开始，该图说明了一个小型企业部署环境中处理的三层：

- **数据导入。**数据通过转发器进入系统，转发器获取外部数据，对于数据进行少量的预处理，然后将数据转发到索引器。转发器通常共存于产生数据的计算机上。根据您的数据源，您可以有数百个获取数据的转发器。
- **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。索引器驻留在专用计算机上。
- **搜索管理。**单个搜索头执行搜索管理功能。它会处理来自用户的搜索请求，并将请求分布到一组索引器上，这些索引器对于它们的本地数据执行实际搜索。搜索头然后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。搜索头驻留在专用计算机上。

要调整您的系统规模，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**。请参阅"为了高可用性和易于管理，使用群集"。

本手册介绍了如何根据您的确切需求调整部署规模，无论您是要管理单一部门的数据、全球企业的数据还是介于二者之间的任何方面的数据都可以进行调整。

后续内容

本章的余下部分主要介绍**数据管道**，即从数据进入系统的点到用户可对数据执行搜索的点。然后通过将 Splunk Enterprise 处理组件与其角色关联来简化数据管道。

其他主题介绍了索引器和搜索头群集、管理组件和对每种类型的组件提供详细配置的手册。

本手册中的其余章节为实施分布式部署提供实用指导。首先，它们介绍了有代表性的部署类型。接下来，它们为实现这些部署的每一个提供端到端的框架。最后，它们介绍了管理员需要执行的部署之后的操作。

为了高可用性和易于管理，使用群集

您可以将一定的 Splunk Enterprise **组件**划分为群集，以便它们能紧密地协调它们的活动。这有两个关键目的：

- 高可用性
- 易于管理

索引器群集

索引器群集是配置为复制彼此数据的一组 Splunk Enterprise 索引器，这样系统便会保留所有数据的多个副本。此过程称为**索引复制**。通过保留 Splunk Enterprise 数据的多个相同副本，群集能够阻止数据丢失，同时还便于数据搜索。

Splunk Enterprise 群集功能会自动从一个索引器故障转移到下一个索引器。这意味着，如果一个或多个索引器出现故障，可继续为传入数据创建索引且可继续对索引数据执行搜索。

除了增强高可用性，群集有其他功能，能帮助简化分布式部署的管理。例如：

- 群集可以轻松地在所有索引器之间协调配置更新。
- 群集内置了分布式搜索操作。
- 群集的特点是索引器发现，这会启用一组转发器以对于群集中的所有索引器进行自动负载均衡。

即使在您的环境中不需要考虑高可用性问题，您仍然可以通过部署一个没有索引复制的索引器群集来利用简化管理的功能。

有关实现索引器群集的指导，请参阅"高可用性部署：索引器群集"。

搜索头群集

搜索头群集是一组作为搜索中心资源的搜索头。搜索头共享知识对象、应用和所有其他配置。您可以从群集中的任一个搜索头上运行相同的搜索、查看相同的仪表板和访问相同的搜索结果。

搜索头群集提供若干个重要好处：

- **横向扩展。**当用户数量和搜索负载增加的时候，您可以向群集中添加新的搜索头。通过结合使用搜索头群集和放置于用户和群集间的第三方负载均衡器，该拓扑结构可以对用户透明。
- **高可用性。**如果一个搜索头发生故障，您可以从群集中其他的任一个搜索头运行相同的搜索集和访问相同的搜索结果集。
- **没有单点故障。**搜索头群集使用动态**管理员**来管理群集。如果管理员发生故障，其他搜索头自动接管群集的管理。

有关实现搜索头群集的指导，请参阅"中型到大型企业部署：使用多个索引器的搜索头群集"。

数据如何通过 Splunk 部署移动：数据管道

Splunk 部署中的处理层对应于**数据管道**，它是数据通过 Splunk 软件的通道。

处理层和数据管道

Splunk 部署通常有三个处理层：

- 数据导入
- 索引
- 搜索管理

请参阅"使用 Splunk Enterprise 组件调整您的部署规模"。

每个 Splunk 处理**组件**都驻留在其中一层上。这些层共同支持发生在数据管道中的进程。

当数据沿着数据管道移动时，Splunk 组件将数据从其外部原始来源（例如日志文件和网络源）转换为封装有价值知识的可搜索事件。

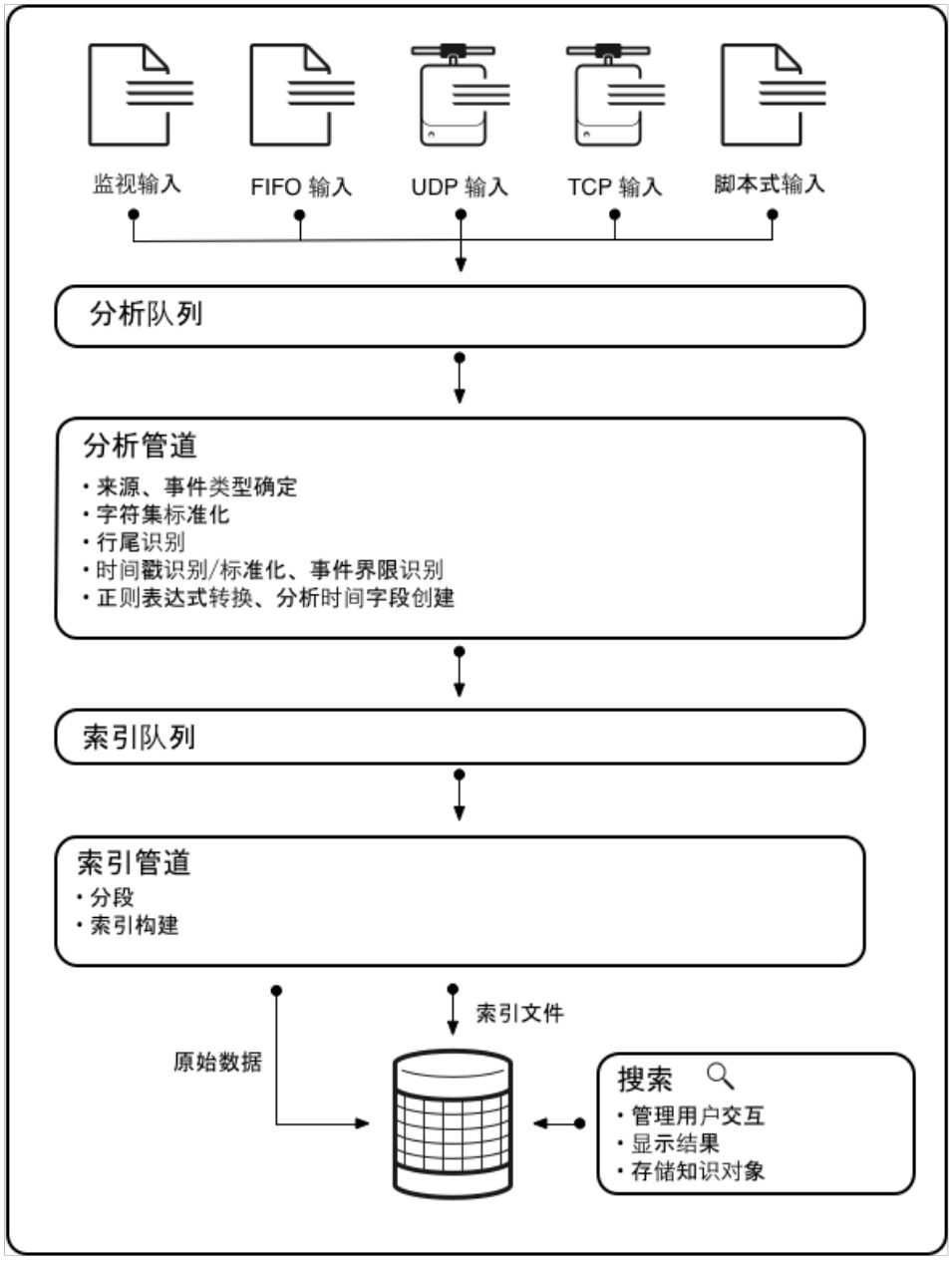
数据管道包括以下几段：

- **输入**
- **分析**
- **索引**
- **搜索**

三个典型处理层和四个数据管道段之间的对应关系如下：

- 数据导入层处理输入段。
- 索引层处理分析和索引段。
- 搜索管理层处理搜索段。

下图概述了数据管道：



Splunk 组件参与数据管道的一个或多个段。请参阅"组件和数据管道"。

注意：此图是索引架构的简化视图。它提供了架构的功能视图，而且没有详细介绍 Splunk 软件内部过程。特别的是，分析管道实际上是由三个管道组成：**分析**、**合并**和**键入**，这三个管道共同处理分析功能。故障排除期间，该区别是有意义的，但通常不会影响您配置或部署 Splunk Enterprise 组件的方式。有关数据管道的更详细的图，请参阅社区 Wiki 中的"索引如何工作"。

深入了解数据管道段

本部分介绍关于数据管道段的更多详细信息。有关分析和索引段的更多信息，也请参阅*《管理索引器和索引器群集》*手册中的"索引如何工作"。

输入

在输入段中，Splunk 软件获取数据。它会从其来源获取原始数据，将数据拆分为若干个 64K 大小的块，然后用一些元数据键批注每个块。这些键将应用到整个输入来源。它们包括数据的**主机**、**来源**和**来源类型**。还可以包括内部使用的一些值（例如，数据流的字符编码），以及用于控制后续数据处理的值（例如，应存储事件的索引）。

在此阶段中，Splunk 软件不会查看数据流的内容，因此这些键应用于整个来源，而不是单独事件。实际上，此时 Splunk 软件对单独事件根本没有任何概念，只能通过某些全局属性了解数据流。

分析

在分析段期间，Splunk 软件会对数据进行检查、分析及转换。这也称为**事件处理**。在此阶段中，Splunk 软件会将数据流拆分为单独的事件。分析阶段包含许多子阶段：

- 将数据流拆分为单独的行。
- 确定、分析和设置时间戳。
- 用从来源范围内的键复制而来的元数据批注单独事件。
- 按照正则表达式转换规则转换事件数据。

索引

在索引期间，Splunk 软件会获取分析后的事件并将其写入磁盘上的索引中。它会同时写入压缩的原始数据和相应的索引文件。

为简便起见，分析和索引常常统称为索引过程。如果只想大概了解，这样没有问题。但是，如果您需要更加密切地检查数据的实际处理或者决定如何分配您的组件，就可能有必要将这两个段分开考虑。

搜索

搜索段可管理用户如何访问、查看及使用索引数据的所有方面。作为搜索功能的一部分，Splunk 软件可存储用户创建的**知识对象**，例如，报表、事件类型、仪表板、告警和字段提取。搜索功能还管理搜索进程本身。

下一步做什么

虽然数据管道进程始终以大致相同的方式运作，但是无论您部署的规模或性质如何，在设计部署时要考虑到管道，这一点非常重要。要做到这一点，您必须了解 Splunk 组件如何映射到数据管道段。请参阅"组件和数据管道"。

组件和数据管道

数据管道的每个段对应于一个或多个 Splunk Enterprise 处理**组件**。例如，数据导入是一个管道段。您可以使用索引器或转发器输入数据。

大多数数据管道段可由多个组件类型处理。您为段所采用的组件取决于您如何构造您的部署。

例如，虽然您可以直接将数据导入到索引器，但是通常只在由单个实例组成的小型部署中执行此操作。在大型部署中，并且在单个实例部署中也经常如此，您会改用转发器来输入数据。将导入任务委派给转发器可以为您的部署提供更大的灵活性。

有关数据管道的信息，请参阅数据如何通过 Splunk Enterprise：数据管道。

有关处理组件的更多信息，请参阅"使用 Splunk Enterprise 组件调整您的部署规模"。

组件如何支持数据管道

此表将数据管道段与可处理该段的组件相关联：

数据管道段	组件
数据导入	**索引器** **通用转发器** **重型转发器**
分析	索引器 重型转发器
索引	索引器
搜索	索引器 **搜索头**

组件间一些典型的相互作用

以下是分布和管理 Splunk Enterprise 功能的一些方式的示例。

将数据转发到索引器

在大多数部署中，**转发器**仅处理数据导入，收集数据，并将其发送到 Splunk Enterprise 索引器。索引器可以执行解析和索引。但在一些部署中，转发器也会在将数据发送至索引器前对数据进行解析，索引器将仅进行索引。

请参阅数据如何通过 Splunk Enterprise：数据管道，以了解分析与索引之间的区别。

转发器有以下两种：

- **通用转发器。**它们会占用主机的一小块空间。该转发器用于在将传入数据流转发到索引器之前，对传入数据流执行最低程度的处理。索引器然后分析并索引数据。
- **重型转发器。**它们保留完整 Splunk Enterprise 实例的很多功能。在将数据转发到接收索引器之前，它们能够分析数据。当重型转发器解析数据时，索引器仅处理索引段。

在将数据转发到索引器之前，这两种类型的转发器均使用元数据（如主机、来源和来源类型）标记数据。

在处理大量数据或不同类型的数据时，使用转发器可有效利用资源。通过提供**负载均衡**、数据**筛选**和**路由**功能，它们还将启用许多感兴趣的部署拓扑结构。

有关转发器的深入介绍（包括配置和详细用例），请参阅*《转发数据》*中的“关于转发和接收”。

跨多个索引器搜索

在**分布式搜索**中，您可以将索引/解析与搜索段相分离。搜索头将搜索请求发送到索引器，并将合并后的结果返回给用户。该拓扑结构对于横向扩展特别有用。要超出部门级别扩展您的部署，您将可能采用分布式搜索。

有关分布式搜索的深入讨论（包括配置和详细用例），请参阅*《分布式搜索》*中的“关于分布式搜索”。

配置和数据管道

有关用于配置 Splunk Enterprise 设置的位置的指导，请参阅*《管理员手册》*中的“配置参数和数据管道”。该主题列出了配置设置及其适用的数据管道段。

如果您知道 Splunk Enterprise 拓扑结构中的哪些组件用于处理数据管道的哪些段，您可以使用该主题来确定用于配置任何特定设置的位置。例如，如果您使用搜索头来处理搜索段，您需要在搜索头上配置所有与搜索相关的设置。

相关信息

概括地说，以下是 Splunk Enterprise 分布式环境的基本组件：

- **索引器。**请参阅*《管理索引器和索引器群集》*中的索引、索引器和索引器群集。
- **转发器。**请参阅*《转发数据》*中的“关于转发和接收”。
- **搜索头。**请参阅*《分布式搜索》*中的“关于分布式搜索”。

帮助管理部署的组件

管理组件支持处理组件的活动。部署通常包括这些管理组件中的一个或多个：

- **监视控制台**执行整个部署的集中监视。
- **部署服务器**更新配置，并将应用分发给处理组件（主要是转发器）。
- **许可证主服务器**处理 Splunk Enterprise 许可授权。
- **群集主节点**或“主节点”协调**索引器群集**的活动。它也会处理索引器群集的更新。
- **Deployer** 处理**搜索头群集**的更新。

和处理组件一样，管理组件是 Splunk Enterprise 实例的专门配置版本。

根据组件及其工作负载，您经常可以在单个 Splunk Enterprise 实例上合并管理组件。在某些情况下，您可以将同一个实例中的管理组件定位为处理组件。

请参阅特定组件的文档，以了解任何共存的可能性：

- 有关监视控制台的信息，请参阅*《监视 Splunk Enterprise》*中的“哪个实例应托管控制台？”。
- 有关部署服务器的信息，请参阅*《更新 Splunk Enterprise 实例》*手册中的“计划部署”。
- 有关许可证主服务器的信息，请参阅*《管理员手册》*中的“配置许可证主服务器”。
- 有关群集主节点的信息，请参阅*《管理索引器和索引器群集》*手册中的“主节点的其他角色”。
- 有关 Deployer 的信息，请参阅*《分布式搜索》*手册中的“Deployer 要求”。

分布式部署的关键手册

所有的 Splunk Enterprise 功能在分布式部署中都可用，所以所有的 Splunk Enterprise 手册对于了解您的部署的全部潜力非常重要。然而，在您设置和配置部署时，可以参阅手册，因为其中有一小部分说明特别重要。这些手册大多按组件类型组织：

- *安装手册。*介绍如何安装 Splunk Enterprise 实例。
- *转发数据。*介绍如何安装、部署和配置任何类型的转发器。
- *管理索引器和索引器群集。*介绍如何配置索引器，以及如何部署和配置索引器群集。

- *分布式搜索。*介绍分布式搜索：设置搜索头，将索引器连接到搜索头，并部署和配置搜索头群集。
- *数据导入。*提供用于配置数据输入范围的指南。*管理员手册。*涵盖了广泛的管理相关的活动。在设置您的部署时，许可证主服务器的相关章节特别重要。
- *监视 Splunk Enterprise。*涵盖了监视控制台的设置，以及如何使用控制台来监视您的部署。
- *更新 Splunk Enterprise 实例。*介绍如何使用部署服务器来更新部署中的组件。

实现分布式部署

开始实现您的分布式部署

Splunk Enterprise 部署范围可以从单个实例部门部署（每天为数 GB 的数据创建索引并为数名搜索数据的用户提供服务），到跨多个数据中心分布的大型企业部署（要为数 TB 数据创建索引并为数百人提供搜索服务）。

Splunk Enterprise 生产部署通常要求您安装和配置各种组件，例如转发器、搜索头和索引器。本手册包含了一系列用于实现通用分布式部署方案的框架，范围大小涵盖部门部署到大型企业部署。

这些框架可用作引导实现过程的高级路线图。每个框架都介绍了一种通用部署方案。然后，它提供了实现该方案的过程概述，以及过程中每一步的详细文档链接。

选择最能反映您需求的方案，并遵循它的框架。此框架将引导您如何拥有一个正在运行的部署。此时，您准备专注于管理任务（例如设置用户，处理安全问题，以及最后，为您的最终用户创建像仪表板和搜索一样的知识对象）的范围。

Splunk Enterprise 组件和部署方案

要实现 Splunk Enterprise 生产部署，您必须安装各种 Splunk Enterprise 组件。您安装的特定组件取决于部署类型。即使是要实现单个实例的部署，在单个 Splunk Enterprise 实例既用作索引器又用作搜索头的部署中，您需要在数据生成的主机上安装转发器，来为实例提供数据。要调整超出单个实例的部署规模，您必须安装和配置几种类型的 Splunk Enterprise 组件。

您配置的组件根据您部署的大小和特定需求而有所不同。例如，确保数据高可用性的部署需要使用与不太关注高可用性的部署不同的配置。

由相同 Splunk Enterprise 软件包构建的不同组件，对于其中的大部分，使用不同的配置以满足不同的角色需求。例外是通用转发器，它使用 Splunk Enterprise 轻型软件包。

有关组件的详细介绍，请查看“使用 Splunk Enterprise 组件调整您的部署规模”。

如何开始

实施部署的过程中，您需要根据您的目标做出一系列决定。您还需要遵循众多主题（在大量文档中介绍的）中描述的程序。您执行的程序根据您部署的需求而有所不同。

要为您特定的部署需求决定正确的程序集，然后在文档中找到所有的程序，这是很困难的。本章的目的是简化这一过程。本章中的主题为您提供信息，以帮助您了解部署需求，并从一开始就做出正确的决定。

下一章“使用实现框架的典型部署方案”为几个有代表性的部署类型或方案中的每一个提供单独的主题。这些主题包含每个方案的端到端部署框架。每一个框架包括一组高级步骤（您可以遵循它们来部署方案），以及包含每一步详细程序的主题链接。

下一步要做什么

遵循以下路径：

1.请参阅“部署类型”来了解您必须作出的选择和各种类型部署的特点。

2.在“部署类型”中，阅读部署类型的“高级别”说明，以找到与您的需求相关的那一个。

3.要进行您的部署，请转到您想要实现的方案主题，并遵循其实现框架。例如，“小型企业部署：使用多个索引器的单个搜索头”。

方案主题大多假定您正在从头开始实施部署。但是，问题类似于现有部署的扩展。主题中会介绍当从较小或不同的部署类型迁移时，您特别需要注意的所有问题。

4.有关您完成初始部署之后需要执行的操作指南，请参阅“部署之后的操作”。

分布式部署类型

您可以通过各种方式来自定义您的 Splunk Enterprise 部署。然而，有一些基本分组，大多数部署都会分入其中。本主题介绍了各种类型部署的一些关键特性和注意事项。

决定部署类型的关键因素

以下是决定部署类型和规模的主要问题：

- **索引量。**每天计划索引多少数据？要处理增加的索引负载，您可能需要多个**索引器**。
- **搜索的次数和类型。**您运行搜索（无论是计划搜索或是临时搜索）的频率如何？您将运行哪种类型的搜索？大量的搜索或频繁的过程密集型搜索，会同时占用**搜索头**和索引器资源。
- **并发用户的数量。**有多少用户会同时查看仪表板或运行搜索？要处理增加的用户数量，您可能需要添加搜索头，通常通过**搜索头群集**进行添加。
- **数据保真度要求。**如果您必须确保系统从不会丢失数据，则需要使用**索引器群集**。
- **可用性要求。**您对于数据可用性有什么要求？如果您必须一直使用完整的数据集，则可能需要同时部署索引器群集和搜索头群集。
- **灾难恢复要求。**快速的灾难恢复有多重要？**多站点索引器群集**能确保在地理上分散的数据中心之间快速切换到相同的数据集上。

在您的整体部署计划中还需要考虑其他注意事项，例如安全要求和数据的位置。

有代表性的部署类型

以下是部署的一些主要类型，基于部署的规模划分：

- **部门。**结合了索引和搜索管理功能的单个实例。
- **小型企业。**使用两或三个索引器的单个搜索头。
- **中型企业。**使用多个索引器的一个小型搜索头群集。
- **大型企业。**使用大量索引器的一个大型搜索头群集。

这些部署类型只是连续扩展过程中的一些点，范围涵盖从单实例部署到可为大量用例提供企业范围服务的部署。

此外，您可以在任何规模的企业部署中部署一个索引器群集。索引器群集提供了一些优点，例如高可用性、灾难恢复和简化的缩放能力。

它还能以各种方式组合拓扑结构。例如，您可以部署一个搜索头，它同时在索引器群集和一组独立的索引器上进行搜索。

注意：“小型企业”、“中型企业”等术语不是专指使用 Splunk 平台的企业的规模。相反，它们表示 Splunk 平台在企业中支持的功能的广度和深度。随着不断了解 Splunk 平台处理多种使用案例的值以及不断实现的成功，部署规模通常也随之增长。例如，一家财富 500 强公司可能一开始只是出于某个非常特定的用例而进行部门级的单实例 Splunk Enterprise 安装，后来随着时间的推移，逐步过渡到小型企业和中型企业部署，直到最后采用大型企业部署，为分布在整个公司内部的各组织和用例提供了重要价值。

开始您的部署

阅读本主题的其余部分，以获得对于您想要实施的部署类型的清晰认识。然后相应地转到下列主题之一：

- “部门部署：单个索引器”
- “小型企业部署：使用多个索引器的单个搜索头”
- “中到大型企业部署：使用多个索引器的搜索头群集”
- “高可用性部署：索引器群集”

这些主题为每个部署类型提供进一步详细信息，包括基本架构图。最重要的是，每个主题都包括对于实施过程端到端的高级指导，以及可遵循其来实施部署的具体程序链接。

处于代表性缩放级别的部署的主要特性

部署的特性将随着规模的增长而变化。通过下表，您可以在一定程度上了解所需要的内容，以及有关为满足需求而要部署的 Splunk 组件的信息。

	部门	小型企业	中型企业	大型企业
索引量（每日）	0-20 GB	20 GB-100 GB	100 GB-300 GB	300GB-1TB+
转发器数量	中值 < 10；最大值 100	中值为十几个；最大值 100 多	中值为十几个；最大值略多于 1000	中值为十几个；最大值 1000 多
用户数	中值 < 10	中值为十几个	中值为十几个；最大值略多于 100	中值为十位数；最大值 500 多
应用数（结合预打包的应用和客户开发的应用）	1-10	1-10	1-20+	10-50

索引层	1 个索引器	2 个至 3 个索引器，可能在一个群集中	4 个至 9 个索引器，可能在一个群集中	10 个以上的索引器，可能在一个群集中
搜索管理层	与索引器结合	1 个独立搜索头	在一个群集中的 3 个搜索头	在一个群集中 3 个以上的搜索头
配置管理功能	手动配置或部署服务器	手动配置或部署服务器	用于转发器和索引器的部署服务器或第三方工具。用于搜索头群集的 Deployer。	用于转发器和索引器的部署服务器或第三方工具。用于搜索头群集的 Deployer。

设计注意事项

设计注意事项也更改为部署规模。下表汇总了在设计部署时需要考虑的一些问题。

	部门	小型企业	中型企业	大型企业
转发器问题	管理、监视	负载均衡、管理、监视	负载均衡、管理、监视、中间转发器	负载均衡、管理、监视、中间转发器
搜索问题	用户计数、告警、应用	搜索头/索引器知识管理、用户计数	搜索头/索引器知识管理、用户计数、搜索头群集化、任务服务器	搜索头/索引器知识管理、用户计数、搜索头群集化、任务服务器
计划的搜索工作负荷	告警、应用/仪表板依赖项、摘要搜索	告警、应用/仪表板依赖项、摘要搜索	告警、应用/仪表板依赖项、摘要搜索、任务服务器	告警、应用/仪表板依赖项、摘要搜索、任务服务器、API/SDK
输入类型	网络、脚本式	网络、脚本式、批处理、集成	网络、脚本式、批处理、集成	网络、脚本式、批处理、集成
可用性	与平台相关（RAID、电源）	数据结构（转发器负载均衡、存储、索引复制）	用户界面（搜索头群集化、负载均衡器）；数据结构（转发器负载均衡、存储、索引复制）	用户界面（搜索头群集化、负载均衡器）；数据结构（转发器负载均衡、存储、索引复制）
可恢复性	备份、保存	备份、索引复制、数据桶/索引恢复	备份、索引复制、数据桶/索引恢复	备份、索引复制、数据桶/索引恢复
可访问性	本地验证与企业验证	验证方法	验证方法	验证方法
人员配备	管理员：0.5-1 人；搜索/仪表板/应用开发/知识管理员：0.25-1 人	管理员：0.5-1 人；搜索/仪表板/应用开发/知识管理员：0.5-1.5 人	管理员/架构师：1-2 人；知识管理员：0.5-2 人；搜索/仪表板/应用开发：1-3 人；程序/项目管理员：1 人	管理员：2-4 人以上；架构师：1 人以上；知识管理员：2-5 人以上；搜索/仪表板/应用开发：2-6 人以上；程序管理员：1 人；项目管理员：0.5-2 人

有关培训机会和适合于您的部署规模的专业服务产品的信息，请联系您的 Splunk 销售代表。

进一步阅读

有关决定部署规模和类型的更多指导：

- 有关硬件容量规划和部署调整的详细信息，请参阅《*容量规划*》手册。
- 有关实施高可用性部署的益处和利弊的讨论，请参阅《*管理索引器和索引器群集*》手册中的“关于索引器群集和索引复制”。

使用实现框架的典型部署方案

部门部署：单个索引器

既用作索引器又用作搜索头的单个 Splunk Enterprise 实例通常能满足大型组织中单一部门的索引和搜索需求。通常您还可以在数据生成的主机上安装转发器。转发器将主机上的数据提供给索引器。

本主题描述如何实现一个部署，其包含：

- 合并的索引器/搜索头
- 多个转发器

使用案例

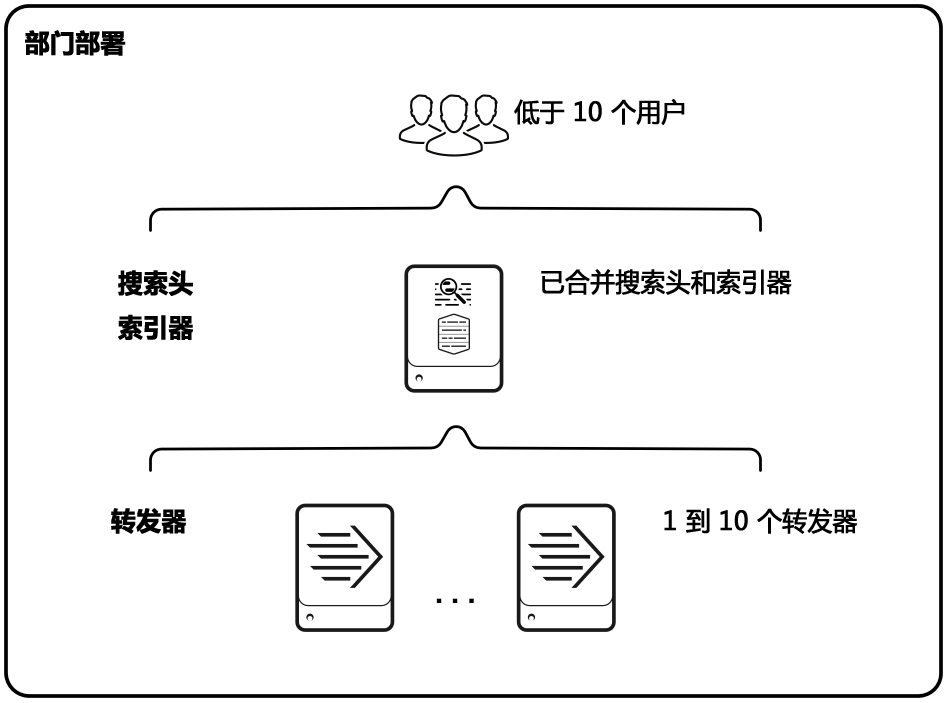
该类型的部署特性包括：

- 每天索引量不到 20 GB。
- 少数几个用户，通常不到 10 个。
- 用于向该实例发送数据的转发器，数量相对较少，通常不到 10 个，很少超过 100 个。

有关部门部署特性的详细信息，请参阅"部署类型"。

架构

本图显示了该类型部署架构的高级视图：



从底部开始，该图说明了处理的层：

- **数据导入。**数据通过**转发器**进入系统，转发器获取外部数据，对于数据进行少量的预处理，然后将数据转发到索引器。在一个部门的部署中，通常只有少于十个转发器，虽然对于一些使用案例，可能会有多达 100 个转发器。
- **索引和搜索（已合并）。**单个**索引器**接收、索引和存储来自转发器的传入数据。索引器也可兼任**搜索头**。在该容量中，它处理搜索请求，例如来自用户的临时请求和保存的搜索请求。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。

实现框架

要实现该类型方案：

1.安装一个 Splunk Enterprise 实例来用作合并的索引器/搜索头。有关安装说明，请参阅*《安装手册》*中的"安装概述"。

2.配置 Splunk Enterprise 许可证。请参阅*《管理员手册》*中的"Splunk Enterprise 许可授权如何工作"。

3.配置实例的**接收端口**。转发器将数据通过该端口发送到索引器。请参阅《*转发数据*》手册中的"启用接收器"。

4.在托管数据源的计算机上安装**通用转发器**，并配置转发器向 Splunk Enterprise 实例发送数据。您如何执行此

操作取决于您的需求和偏好，以及您正在多少个转发器上进行部署。例如：

- 您可以在多台计算机上逐个或同时安装转发器。
- 您可以先安装转发器，然后再配置它们，或者同时安装并配置转发器。
- 您可以手动或者通过部署服务器或第三方软件的方式来配置转发器。

有关安装和配置通用转发器的信息，请参阅*《Splunk 通用转发器手册》*中的“安装通用转发器软件”。

5.将输入配置为转发器，以便数据开始进入系统。请参阅*《数据导入》*手册中的“配置输入”。

后续步骤

一旦您已经启动并运行 Splunk Enterprise 实例，您可以进一步优化您的系统，并准备数据和其演示，使终端用户能够受益。有关您现在需要执行的操作类型的汇总，请参阅“部署之后的操作”。

要进一步调整规模

要提高索引和搜索容量，第一步是从搜索管理功能中分离索引功能。为此，增加第二个 Splunk Enterprise 实例来作为专用搜索头。一旦您有了专用搜索头，您可以通过添加更多的索引器来提高索引容量。请参阅“小型企业部署：使用多个索引器的单个搜索头”。

有关确定何时添加更多实例，以及是否只添加索引器，或者同时添加索引器和搜索头的指导，请参阅：

- 本手册中的“部署类型”。
- *《容量规划》*手册中的“性能建议摘要”。

小型企业部署：使用多个索引器的单个搜索头

要增加索引和搜索容量，使其超出某一特定值，您必须从单个 Splunk Enterprise 实例过渡到多实例部署。您可拆分搜索管理和索引功能，将它们分配给在独立的计算机上运行的单独实例。在扩展的第一级，通常部署一个能与两或三个索引器通信的单个搜索头。该类型部署的特点是多部门或小型企业解决方案。

本主题描述如何实现一个部署，其包含：

- 一个搜索头
- 多个索引器
- 多个转发器

注意：您可以部署一个**索引器群集**，而非部署多个独立的索引器。该拓扑结构非常有用，即使您不想要数据的高可用性和随附的存储开销。它仍然需要少量的开销，但它提供了简化索引器管理的好处。请参阅“高可用性部署：索引器群集”。

使用案例

该**分布式搜索**方案提供了第一级的横向扩展。它允许用户跨一组索引器运行搜索。随着您需求的进一步提高，您可以添加更多的索引器。

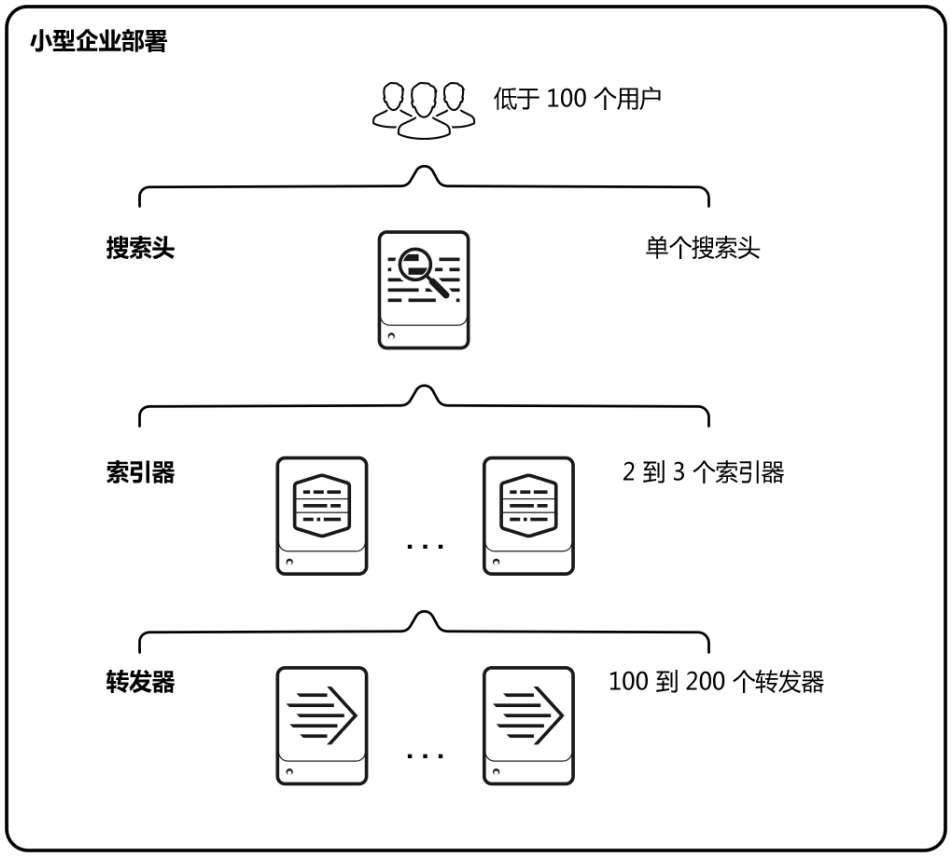
该类型的部署特性包括：

- 每天索引量介于 20GB 到 100GB 之间。
- 介于 10 到 100 个用户之间。
- 最多数百个转发器，用于向索引器提供数据。转发器通常利用负载均衡将数据分布在一组索引器中。

有关小型企业部署特性的详细信息，请参阅“部署类型”。

架构

本图显示了该类型部署架构的高级视图：



从底部开始，该图说明了处理的三层：

- **数据导入。**数据通过**转发器**进入系统，转发器获取外部数据，对于数据进行少量的预处理，然后将数据转发到索引器。您通常可配置转发器使用其内置的负载均衡能力，将数据分散到一组索引器上。
- **索引。**两个或三个**索引器**接收、索引和存储来自一组转发器的传入数据。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**执行搜索管理功能。它会处理搜索请求，例如来自用户的临时请求和保存的搜索请求，并将请求分布到一组索引器上，这些索引器对于它们的本地数据执行实际搜索。搜索头然后合并索引器的结果，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。

迁移问题

本主题假定您正在从头开始实施该部署。如果不是如此，反之您正在扩展现有的单实例部署，则过程类似，但有几个其他的问题需要注意：

- 在新的部署中，将您当前的单实例部署作为索引器而非搜索头。该实例可能更适合配置用于一个索引器的需求。已经在实例上的数据将能继续在新的部署中进行搜索。
- 将独立实例的应用和知识对象转移到新的搜索头实例。
- 配置您的许可证以容纳其他实例。

实现框架程序包括处理这些问题的步骤。

实现框架

要实现该类型方案：

1.为索引器和搜索头安装 Splunk Enterprise 实例。例如，要部署带有两个索引器的单个搜索头，则安装三个实例。有关安装说明，请参阅*《安装手册》*中的“安装概述”。

注意：搜索头和索引器有不同的硬件要求。关于为您的实例配置硬件的信息，请参阅*《容量规划》*手册中的“参考硬件”。

2.（仅迁移）如果您是从一个独立的实例迁移，则使用该实例作为其中一个索引器。已经在实例上的数据在新的环境中继续可用。

3.（仅迁移）如果您是从一个独立的实例迁移，则将现有的知识对象和应用集转移到新的搜索头实例：

a. 如有必要，更新之前的独立实例，以便它与新的搜索头实例运行相同的版本。

b. 将独立实例的 `$SPLUNK_HOME/etc/apps` 和 `$SPLUNK_HOME/etc/users` 目录内容复制到搜索头上的相同位置。

c. 重新启动搜索头。

4.在您选择作为搜索头的实例上，配置索引器实例作为实例的**搜索节点**。此步骤正式声明实例的相应角色（索引器、搜索头）。请参阅*《分布式搜索》*手册中的"添加搜索节点到搜索头"。

5.配置 Splunk Enterprise 许可证。如果您现有一个许可证，请确保它涵盖了新的实例。请参阅*《管理员手册》*中的"Splunk Enterprise 许可授权如何工作"。

6.在每个索引器上，配置**接收端口**。转发器将数据通过该端口发送到索引器。请参阅*《Splunk 通用转发器》*手册中的"启用接收器"。

7.在托管数据源的计算机上安装**通用转发器**，并配置转发器向一组索引器发送数据。您如何执行此操作取决于您的需求和偏好，以及您正在多少个转发器上进行部署。例如：

- 您可以在多台计算机上逐个或同时安装转发器。
- 您可以先安装转发器，然后再配置它们，或者同时安装并配置转发器。
- 您可以手动或者通过部署服务器或第三方软件的方式来配置转发器。

有关安装和配置通用转发器的信息，请参阅*《通用转发器手册》*中的"如何转发数据至 Splunk Enterprise"。

建议您配置转发器在一组索引器间对于数据进行负载均衡，而不是只向单个索引器发送数据。请参阅*《转发数据》*手册中的"设置负载均衡"。

（仅迁移）如果在以前的部署中已经有一些转发器，则重新配置它们在所有的索引器之间进行负载均衡。

8.将输入配置为转发器，以便数据开始进入系统。请参阅*《数据导入》*手册中的"配置输入"。

后续步骤

一旦您已经启动并运行 Splunk Enterprise 实例，而且它们能彼此通信，则您可以进一步优化您的系统，并准备数据和其演示，使终端用户能够受益。有关您现在需要执行的操作类型的汇总，请参阅"部署之后的操作"。

要进一步调整规模

要提高索引和搜索容量，第一步是添加更多的索引器。为此，安装另一个 Splunk Enterprise 实例，并配置搜索头将其视为搜索节点。

要服务更多的用户，并增加搜索容量，使其超过一定的等级，最终您必须添加更多的搜索头。通常，部署多个搜索头的最佳方法是部署一个搜索头群集。请参阅"中到大型企业部署：使用多个索引器的搜索头群集"。

有关确定何时添加更多实例，以及是否只添加索引器，或者同时添加索引器和搜索头的详细信息，请参阅：

- 本手册中的"部署类型"。
- *《容量规划》*手册中的"性能建议摘要"。

中到大型企业部署：使用多个索引器的搜索头群集

从小型企业过渡到中型企业部署，您需要同时提高索引和搜索容量。为提高索引容量，您可以继续添加索引器。为提高搜索容量，您可以添加搜索头来服务更多的用户和进行更多的搜索操作。

部署多个搜索头的推荐方法是将搜索头组合到**搜索头群集**中。搜索头群集允许用户和搜索在一组搜索头之间共享资源。它们也比单独搜索头的组更容易管理。搜索头群集要求至少有三个搜索头。

中型和大型企业部署之间的差异主要是扩展和管理问题。基本部署的拓扑结构是类似的。它们都采用带有多个索引器的搜索头群集。

本主题描述如何实现一个部署，其包含：

- 一个搜索头群集，包含多个搜索头
- 多个索引器
- 多个转发器

注意：您可以部署一个**索引器群集**，而非部署多个独立的索引器。该拓扑结构非常有用，即使您不想要数据的高可用性和随附的存储开销。它仍然需要少量的开销，但它提供了简化索引器管理的好处。请参阅"高可用性部署：索引器群集"。

中型企业部署用例

中型企业部署比小型企业部署提供更大的横向扩展。它为大量的用户和搜索提供服务。随着您的需求不断增加，您可以继续添加索引器和搜索头。

该类型的部署特性包括：

- 每天索引量介于 100 GB 到 300 GB 之间。
- 用户数量可能达 100 个或更多。
- 最多数千个转发器，用于向索引器提供已经过负载均衡的数据。

有关中型企业部署特性的详细信息，请参阅“部署类型”。

大型企业部署用例

大型企业部署甚至提供更大的横向扩展。

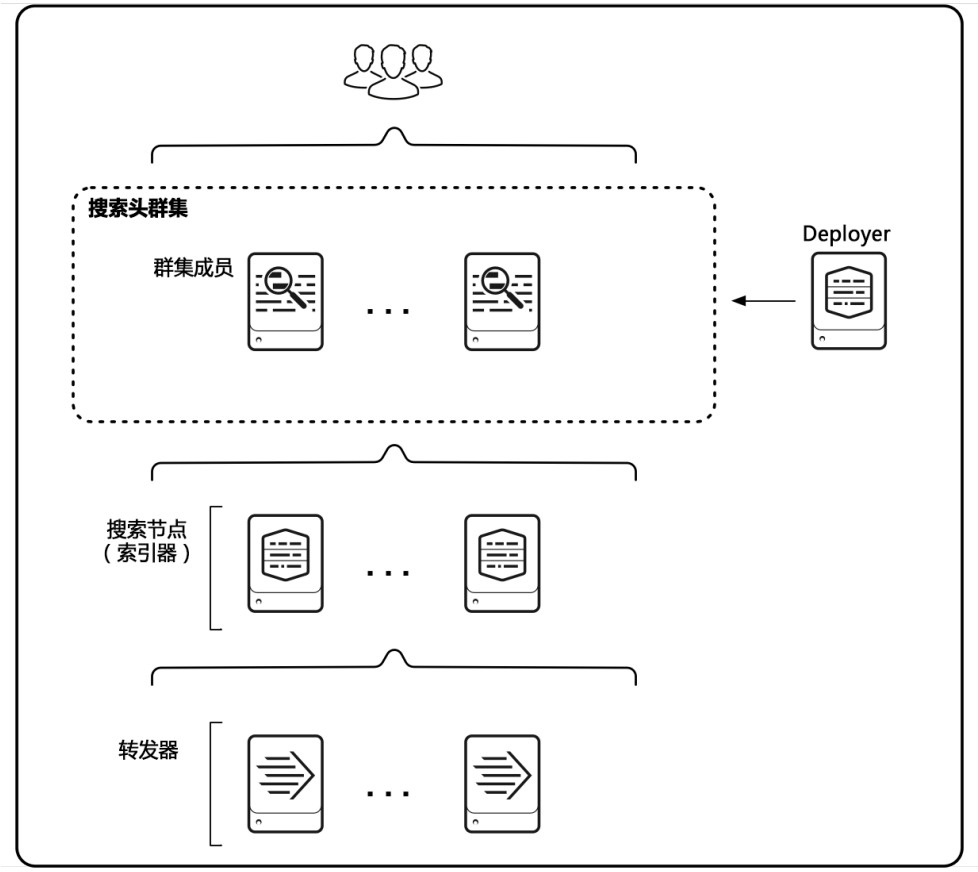
该类型的部署特性包括：

- 每天索引量介于 300 GB 到数 TB 之间。
- 大量用户，数量可能达数百个。
- 数千个转发器。

有关大型企业部署特性的详细信息，请参阅“部署类型”。

架构

本图显示了中型或大型企业部署架构的高级视图：



从底部开始，该图说明了处理的三层：

- **数据导入。**数据通过**转发器**进入系统，转发器获取外部数据，并将数据转发到索引器。您可配置转发器使用其内置的负载均衡能力，将数据分散到一组索引器上。
- **索引。索引器**接收、索引和存储来自转发器的传入数据。
- **搜索管理。**搜索头群集，由三个或多个搜索头成员组成，执行搜索管理功能。群集中的搜索头会协调它们的活动来处理搜索请求，例如来自用户的临时请求和保存的搜索请求，并将请求分布到一组索引器上。**Deployer** 将应用分发给搜索头群集成员。

迁移问题

本主题假定您正在从头开始实施搜索头群集部署。如果不是如此，反之您正在扩展现有的非群集部署，则过程类似，但有几个其他的问题需要注意：

- 您必须为群集中的每个搜索头使用新的 Splunk Enterprise 实例。您可以将当前搜索头的设置和应用迁移到搜索头群集，但您不能重新使用搜索头本身。请参阅*《分布式搜索》*手册中的“从独立搜索头迁移到搜索头群集”。
- 您必须配置您的许可证以容纳其他实例。

实现框架程序涵盖了这些问题。

实现框架

要实现一个带有索引器和转发器的搜索头群集：

1.安装和部署搜索头群集。请参阅*《分布式搜索》*手册中的“部署搜索头群集”。

2.（仅迁移）如果您是从一个由独立搜索头组成的较小型部署迁移，则您可以迁移原有搜索头的设置。请参阅*《分布式搜索》*手册中的“从独立搜索头迁移到搜索头群集”。

3.安装您计划用作索引器的实例。有关安装说明，请参阅*《安装手册》*中的“安装概述”。

（仅迁移）如果您是从一个较小型部署迁移，则您可继续使用现有的索引器。需要时您也可以添加新的索引器实例。

4.将搜索头连接到索引器（也称为**搜索节点**）。请参阅*《分布式搜索》*手册中的“连接群集中的搜索头与搜索节点”。

5.配置 Splunk Enterprise 许可证。如果您现有一个许可证，则必须确保它涵盖了所有新的实例。请参阅*《管理员手册》*中的“Splunk Enterprise 许可授权如何工作”。

6.在每个新的索引器上，配置**接收端口**。转发器将数据通过该端口发送到索引器。请参阅《*转发数据*》手册中的“启用接收器”。

7.在托管数据源的计算机上安装**通用转发器**，并配置转发器向一组索引器发送数据。有关安装和配置通用转发器的信息，请参阅*《通用转发器》*手册中的“安装通用转发器软件”。

建议您配置转发器在一组索引器间对于数据进行负载均衡。请参阅*《转发数据》*手册中的“设置负载均衡”。

（仅迁移）如果在以前的部署中已经有了转发器，并且您在步骤 3 中添加了索引器，则重新配置现有的转发器在整个索引器组（包括新的索引器）间进行负载均衡。

8.将输入配置为转发器，以便数据开始进入系统。请参阅*《数据导入》*手册中的“配置输入”。

后续步骤

一旦您已经启动并运行 Splunk Enterprise 实例，而且它们能彼此通信，则您可以进一步优化您的系统，并准备数据和其演示，使终端用户能够受益。有关您现在需要执行的操作类型的汇总，请参阅“部署之后的操作”。

要进一步调整规模

需要时您可以继续调整您的部署规模。要提高索引和搜索容量，第一步是添加更多的索引器。为此，安装另一个 Splunk Enterprise 实例，并配置搜索头和转发器与其相连。

要服务更多的用户，并继续增加搜索容量，使其超过一定的等级，您必须添加另一个搜索头到群集中。请参阅*《分布式搜索》*手册中的“添加群集成员”。

有关确定何时添加更多实例，以及是否只添加索引器，或者同时添加索引器和搜索头的详细信息，请参阅：

- 本手册中的“部署类型”。
- *《容量规划》*手册中的“性能建议摘要”。

高可用性部署：索引器群集

要确保数据的高可用性，您可以部署一个**索引器群集**。索引器群集是配置为复制彼此数据的一组索引器，这样系统便会保留所有数据的多个副本。此过程称为**索引复制**。索引器群集能够阻止数据丢失，同时还便于数据搜索。管理索引器群集也比管理单个索引器的组更简单。

使用索引器群集需要权衡的是，您需要额外的存储来处理复制的副本。您可以控制索引复制的程度，并因此控制存储需求，以匹配您企业的可用性需求。

有关索引器群集化的介绍，以及益处和利弊的更多详细信息，请参阅*《管理索引器和索引器群集》*手册中的“关于索引器群集和索引复制”。

您可以在任何规模的企业部署中使用索引器群集化。

当您的搜索需求增长时，您可以将索引器群集与**搜索头群集**结合起来。

本主题描述如何实现一个部署，其包含：

- 一个或多个单独的搜索头，或一个搜索头群集
- 一个索引器群集
- 多个转发器

高可用性用例

索引器群集的主要用例是企业部署，该部署要求数据的高可用性，并且愿意分配额外所需的磁盘空间来存储数据的多个副本。

简化管理用例

您也可以实现一个不使用复制的索引器群集。当您去除了复制功能，您就失去了索引器群集的一个关键优势，例如数据的可用性和数据恢复，但是您仍然获得了简化管理多个索引器的优势。请参阅《*管理索引器和索引器群集*》手册中的“使用索引器群集调整索引”。

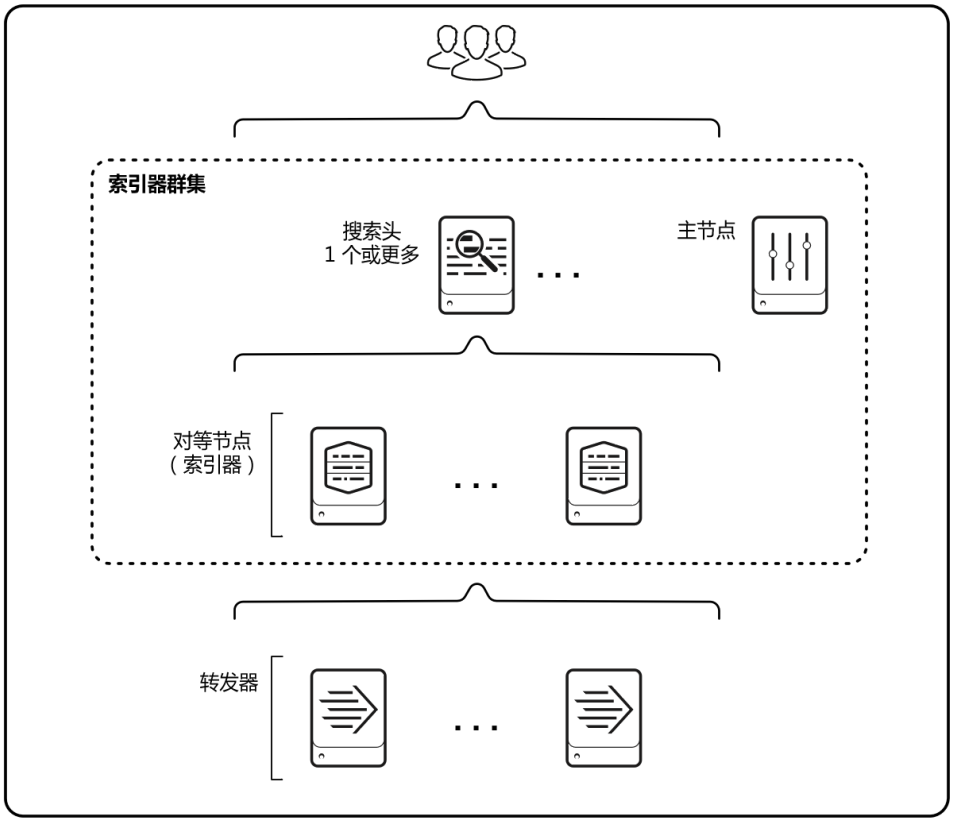
架构

索引器群集架构的主要类型有：

- 使用一个或多个单独搜索头的索引器群集
- 使用搜索头群集的索引器群集

使用单独搜索头的索引器群集

本图显示了使用一个或多个单独搜索头的索引器群集架构的高级视图：



从底部开始，该图说明了处理的三层：

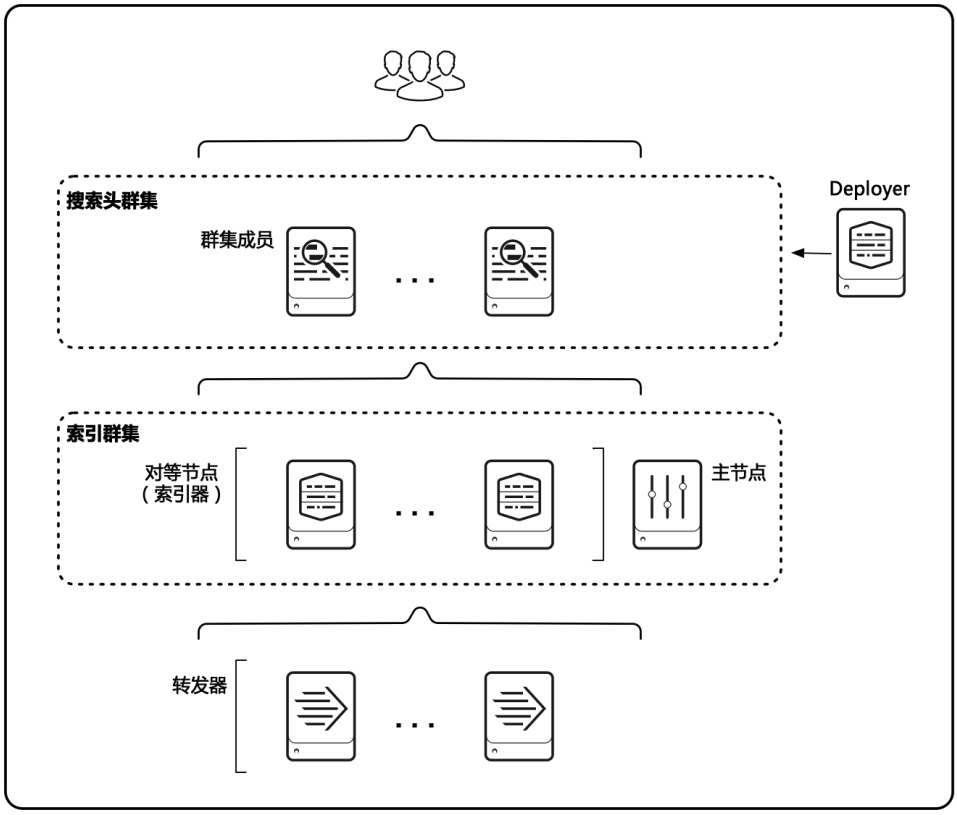
- **数据导入。**数据通过**转发器**进入系统，转发器获取外部数据，并将数据转发到索引器。您可配置转发器使用其内置的负载均衡能力，将数据分散到一组索引器上。
- **索引。**索引器或者群集**对等节点**接收、索引和存储来自转发器的传入数据。

- **搜索管理。**一个或多个单独的搜索头执行搜索管理功能。

主节点调整群集节点的功能，但是不会索引、存储或搜索数据。

使用搜索头群集的索引器群集

您可以将索引器群集与搜索头群集结合起来。如果您需要部署多个搜索头，这是推荐做法：



与以前的架构相比，主要区别是搜索头群集取代了单独搜索头。索引器群集与搜索头群集的主要交互方式和其与单独搜索头的交互方式相同。

迁移问题

本主题假定您正在从头开始实施索引器群集部署。如果不是如此，反之您正在扩展一组非群集索引器，则可以将现有索引器整合到群集中，但有几个问题需要注意：

- 已经在单独索引器上的数据仍然可用于搜索，但它不会被复制。
- 您再也不能使用部署服务器来管理您的应用。您必须改用内置在索引器群集中的**配置软件包**方法。这会要求您将应用迁移到群集中。

有关这些问题和其他问题的详细信息，请参阅：

- *《管理索引器和索引器群集》*手册中的“群集和非群集索引器部署之间的关键差异”。
- 请参阅《*管理索引器和索引器群集*》手册中的“将非群集索引器迁移到群集环境”。

实现框架程序简要介绍了迁移问题。

实现框架

要实现索引器群集：

1.安装需要的 Splunk Enterprise 实例，并部署索引器群集。请参阅*《管理索引器和索引器群集》*手册中的“索引器群集部署概述”。

2.（仅迁移）如果您是从一个由一个或多个独立索引器组成的部署迁移，还可阅读*《管理索引器和索引器群集》*手册中的“将非群集索引器迁移到群集环境”。

3.如果您想要实现用于搜索层的搜索头群集，请参阅*《分布式搜索》*手册中的“部署搜索头群集”和“集成搜索头群集和索引器群集”。

4.配置 Splunk Enterprise 许可证。如果您现有一个许可证，则必须确保它涵盖了所有新的实例。请参阅*《管理员手册》*中的“Splunk Enterprise 许可授权如何工作”。还可参阅*《管理索引器和索引器群集》*手册的“索引器群集的系统要求和其他部署注意事项”中有关许可授权信息的部分。

5.在托管数据源的计算机上安装**通用转发器**（如果未执行此操作）。请参阅*《通用转发器》*手册中的“如何安装通用转发器”。

6.将对等节点连接到转发器：

a. 决定要使用的方法。请参阅*《管理索引器和索引器群集》*手册中的“使用转发器在索引器群集中获取数据”。

b. 根据您的决定，遵循*《管理索引器和索引器群集》*手册中的“使用索引器发现来连接转发器与对等节点”或者“直接连接转发器与对等节点”。

7.将输入配置为转发器，以便数据开始进入系统。请参阅*《数据导入》*手册中的“配置输入”。

后续步骤

一旦您已经启动并运行 Splunk Enterprise 实例，而且它们能彼此通信，则您可以进一步优化您的系统，并准备数据和其演示，使终端用户能够受益。有关您现在需要执行的操作类型的汇总，请参阅“部署之后的操作”。

要进一步调整规模

需要时您可以调整群集规模。要提高索引和搜索容量，第一步是添加另一个索引器。为此，启用新的 Splunk Enterprise 实例作为对等节点。

要服务更多的用户，并继续增加搜索容量，使其超过一定的等级，您必须添加更多的搜索头。在索引器群集中包含多个搜索头的推荐做法是在搜索头群集中部署它们。请参阅*《分布式搜索》*手册中的“从独立搜索头迁移到搜索头群集”。

要向现有的搜索头群集中添加更多的搜索头，请参阅*《分布式搜索》*手册中的“添加群集成员”。

有关确定何时添加更多实例，以及是否只添加索引器，或者同时添加索引器和搜索头的详细信息，请参阅：

- 本手册中的“部署类型”。
- *《容量规划》*手册中的“性能建议摘要”。

如果您的企业跨越多个站点，则您可以实现一个**多站点索引器群集**而非单站点群集。请参阅*《管理索引器和索引器群集》*手册中的“多站点索引器群集部署概述”。如果您已经有一个单站点群集，并且想将它转换为多站点群集，请参阅*《管理索引器和索引器群集》*手册中的“将索引器群集从单个站点迁移到多站点”。

管理您的部署

部署之后的操作

部署实施是一系列管理相关任务的第一步，您必须执行这些任务来充分利用 Splunk Enterprise。本主题提供了典型的部署之后任务的大纲，并提供了详细介绍这些问题的主题链接。

《分布式部署的关键手册》列出了与部署直接相关的手册。在部署过程中，您已经遇到了这些手册的部分内容。这些相同的手册涵盖了部署之后的配置和管理问题。它们将用作您微调系统时的持续不断的资源，您自己应该熟悉其内容。此外，其他手册会提供指导，以改善和扩展您的系统，并使系统符合终端用户的知识需求。

接下来执行以下操作

以下是您在完成初始部署后应该马上执行的一些任务：

- **设置用户和角色。**请参阅*《确保 Splunk Enterprise 安全》*中的“用户和基于角色的访问控制”章节。
- **阅读有关 Splunk Enterprise 安全的信息。**仔细查看*《确保 Splunk Enterprise 安全》*手册。
- **将搜索头内部数据转发给搜索节点。**请参阅最佳做法：*《分布式搜索》*中的“将搜索头数据转发到索引器层”。

增加您部署的价值

一旦您启动并运行部署，而且您已经处理了基本问题（例如安全问题），准备专注于您的数据：获取什么数据，如何获取数据，以及如何呈现数据，以便用户可以有效地使用它。

Splunk Enterprise 几乎可以处理任何种类的数据。有关数据的不同类型以及如何配置它们，包括来源类型和事件处理的重要问题，有许多内容需要了解。与数据导入相关的所有问题的详细信息，请阅读*《数据导入》*。要确保了解有关来源类型的资料，从“来源类型为何重要”开始。

接下来，您需要开发搜索、报表、仪表板等等，使您的用户能使用和访问数据。这些对象统称为**知识对象**。对于这一点，可以主要参考*《知识管理器手册》*。

Splunk 提供广泛的预先构建的应用，它们会为您完成大部分工作。他们定义数据导入、来源类型、知识对象和其他配置。对于许多常见和不常见的需求，它们为您和您的用户提供现成的解决方案。例如，有监视您的系统安全的应用，以及其他用于 IT 运营管理的应用。要了解有关预先构建的应用的更多内容，并下载这些应用，请参阅 Splunkbase。

您也可以创建自己的应用。请参阅 dev.splunk.com 以获得有关开发应用的指导。

用于管理您的部署的资源

*《管理员手册》*提供有关其他重要任务的指导。特别是，请参阅"Splunk 管理：更多内容"。它提供了各种手册中描述关键管理任务的主题链接。

监视控制台提供了您可以用来监视部署的大多数方面的各种仪表板。请参阅本手册中的监视您的分布式部署。其他信息，请参阅*《监视 Splunk Enterprise》*。

有关内部日志文件和对于部署进行故障排除的其他工具的信息，请参阅*《故障排除手册》*。

分发应用和其他配置给实例组

Splunk Enterprise 提供**部署服务器**来分发应用和其他配置集给 Splunk Enterprise 实例组。此工具对于管理转发器上的配置特别有用，而且它可以分发更新给任何 Splunk Enterprise 实例，包括索引器和搜索头。请参阅*《更新 Splunk Enterprise 实例》*。

要更新群集上的节点，不要使用部署服务器。反之，群集使用它们自己的工具：

- 在索引器群集中，群集主节点会分发更新给对等节点。请参阅*《管理索引器和索引器群集》*中的"更新通用对等节点配置和应用"。
- 在搜索头群集中，Deployer 会分发更新给群集成员。请参阅*《分布式搜索》*中的"使用 deployer 分布应用和配置更新"。

您也可以使用第三方工具来分发更新。

Splunk 世界的其余部分

Splunk Enterprise 仅是 Splunk 世界中的一个产品。其他产品包括：

- 基于云来访问 Splunk Enterprise 功能的 **Splunk Cloud**。
- 用于数据浏览、分析和 Hadoop、NoSQL 和其他数据存储可视化的 **Splunk Analytics for Hadoop**。
- 用于扩展 Splunk Enterprise 功能的**各种应用和加载项**。

有关更多信息，请访问 Splunk 文档门户和 Splunk 产品概述。

监视您的分布式部署

您可以使用监视控制台来监视部署的大多数方面。本主题介绍提供整个部署概述的控制台仪表板。

监视控制台的主要文档是*《监视 Splunk Enterprise》*。

部署级的仪表板

监视控制台包括可以总览整个部署情况的仪表板，以及其他深入到部署中、关注部署特定功能（例如索引或搜索头群集化）的仪表板。本主题介绍概述仪表板：介绍特定功能的手册涵盖了与这些功能相关的仪表板。

例如，对于单独的搜索头群集，监视控制台提供了五个仪表板，它们涵盖了例如项目复制、配置复制和应用部署之类的操作。在*《分布式搜索》*里有关搜索头群集化的文档中介绍了这些仪表板。同样地，在*《管理索引器和索引器群集》*中介绍了与索引器群集或者索引性能相关的仪表板。

提供部署级视图的仪表板或页面有三种类型：

- 概述
- 实例
- 资源使用情况

概述仪表板

提供部署概述的仪表板位于**概述**菜单下方。它们也是在您最初启动控制台的时候会出现的仪表板。有两个仪表板：

- 概述
- 拓扑结构

通过单击**概述**或**拓扑结构**按钮，您可在这些仪表板之间进行切换。

“概述”仪表板会指定索引器、搜索头、群集主节点和许可证主服务器的数量。它还包括有关使用情况和告警的信息。

“拓扑结构”仪表板显示每个组件类型的实例，以及索引器和搜索头之间的连接。它还提供有关每个实例的一些高级信息，例如索引器的索引速度以及实例是否在运行或已关闭。

实例页面

“实例”仪表板会列出部署中的所有 Splunk Enterprise 实例。对于每个实例，它也提供有关其基本特性和状态的信息。您可以通过**实例**菜单访问它。

资源使用情况仪表板

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。其他仪表板提供实例或计算机的使用信息。

请参阅*《监视 Splunk Enterprise》*中的“资源使用情况：部署”。