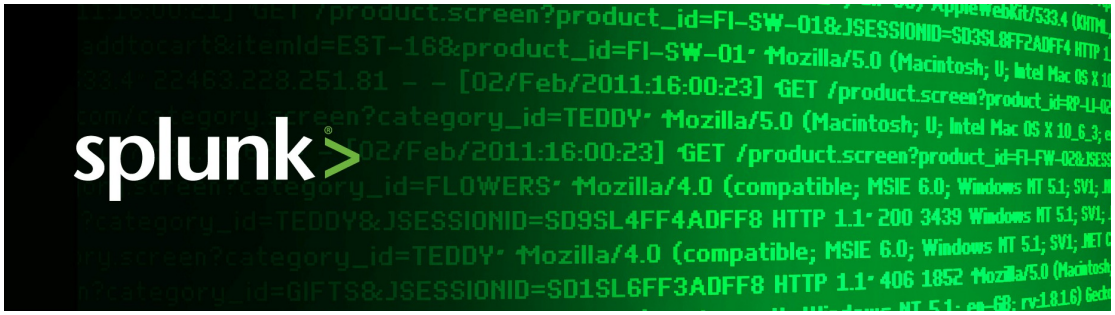


Splunk® Enterprise 6.5.0

分布式搜索

生成时间：2016 年 9 月 26 日，下午 10:22

Table of Contents

分布式搜索概述 **4**
关于分布式搜索 4
搜索头发送到搜索节点的内容 5

部署分布式搜索 **6**
部署分布式搜索环境 6
分布式搜索的系统要求和其他部署考虑 7
添加搜索节点到搜索头 8
最佳做法：将搜索头数据转发到索引器层 10

管理分布式搜索 **11**
修改知识软件包 11
管理分布式服务器名称 12
创建分布式搜索组 12
删除搜索节点 13

查看分布式搜索状态 **14**
在“设置”中查看搜索节点状态 14
使用监视控制台查看分布式搜索状态 14

搜索头群集化概述 **15**
关于搜索头群集化 15
搜索头群集化架构 15

部署搜索头群集化 **20**
搜索头群集的系统要求和其他部署注意事项 20
部署搜索头群集 23
集成搜索头群集和索引器群集 26
连接群集中的搜索头与搜索节点 27
添加用户到搜索头群集中 29
对搜索头群集使用负载均衡器 29
在多站点环境中部署搜索头群集 29
从搜索头池迁移到搜索头群集 31
从独立搜索头迁移到搜索头群集 33
升级搜索头群集 35

配置搜索头群集 **36**
配置搜索头群集 36
为搜索头群集选择复制因子 37
为搜索头群集设置密钥 38

更新搜索头群集成员 **39**
配置更改如何跨搜索头群集传输 39
群集复制的配置更新 40
使用 Deployer 分布应用和配置更新 42

管理搜索头群集 **49**
添加群集成员 49
删除群集成员 51
配置群集成员只运行特殊搜索 52
控制管理员职责 52
处理搜索头群集成员的故障 54
使用静态管理员，以从丧失多数优势的状态中恢复 55
重新启动搜索头群集 57

查看搜索头群集状态 **58**
使用 CLI 查看关于搜索头群集的信息 58
使用监视控制台查看搜索头群集状态和解决问题 60

搜索头群集化故障排除 **61**
部署问题 61
运行时注意事项 62
处理 Raft 问题 62

搜索头合并 **63**
搜索头合并概述 63
创建搜索头池 64
对搜索头池使用负载均衡器 66
其他合并操作 66
管理配置更改 67
部署服务器和搜索头合并 67
为配置刷新选择时间 67
升级搜索头池 67

安装知识软件包 **67**
关于安装软件包 67
配置安装软件包 69
使用带搜索头合并的安装软件包 71

运行中的分布式搜索 **72**
授权如何用于分布式搜索 72
用户如何控制分布式搜索 74

故障排除分布式搜索 **74**
使用监视控制台查看分布式搜索状态 74
一般故障排除问题 74
处理搜索节点缓慢问题 75
隔离搜索节点 75
搜索头合并配置问题 76
分布式搜索错误消息 77

分布式搜索概述

关于分布式搜索

阅读本手册之前，请参阅*《分布式部署手册》*。该手册介绍 Splunk Enterprise 分布式部署的基础，并显示分布式搜索如何分发到全部部署。

分布式搜索提供一种调整部署的方式，方法为将搜索管理和显示层从索引和搜索检索层分离。

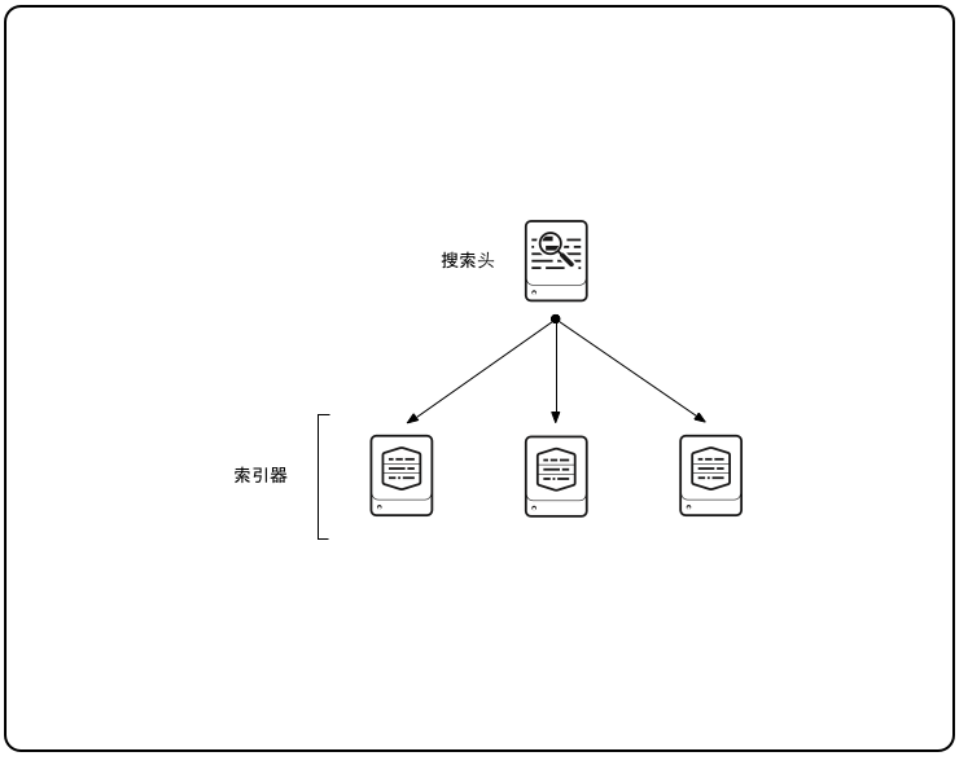
使用案例

这里是分布式搜索的一些主要使用案例：

- **增强性能的横向扩展。**通过提供跨多个 Splunk Enterprise 实例分发索引搜索负载的方式，分布式搜索有助于横向扩展，允许索引和搜索大量数据。
- **访问控制。**您可以使用分布式搜索控制对索引数据的访问权限。比如，安全人员等用户可能需要访问整个企业的数据，而其他人仅需访问其职能范围的数据。
- **管理地理分散数据。**分布式搜索允许本地办公室访问他们自己的数据，同时在企业级集中保留访问权限。例如，Chicago 和 San Francisco 的用户仅可查看他们自己的本地数据；而位于 New York 总部的用户可以搜索本地数据，以及在 Chicago 和 San Francisco 的数据。

分布式搜索组件

通过分布式搜索，名为**搜索头**的 Splunk Enterprise 实例将发送搜索请求给一组**索引器**或**搜索节点**，这将在它们的索引上执行实际搜索。然后，搜索头合并结果返回给用户。以下是一种基本的分布式搜索方案，其中一个搜索头在若干个索引器中管理搜索：



分布式搜索类型

对于部署分布式搜索环境，有多个基础选项：

- 使用一个或多个独立的搜索头在搜索节点中搜索。
- 可以将多个搜索头部署到一个搜索头群集。群集中的搜索头共享资源、配置和任务。这样能提供一种将对用户的部署进行透明化扩展的方式。
- 将搜索头作为索引器群集的一部分进行部署。索引器群集能够提升数据可用性和数据恢复，这是另外一个优点。索引器群集中的搜索头可以是独立的搜索头或者是搜索头群集中的成员。

在每种情况下，搜索头都只执行搜索管理和显示功能。所连接的搜索节点将对数据建立索引，并针对索引的数据进行搜索。

独立搜索头

小型分布式搜索部署有一个独立的搜索头；即，这个搜索头不属于任何群集。

要扩展单个搜索头的规模，必须部署一个搜索头群集。

搜索头群集

搜索头群集是一组搜索头，能够协同工作以提供可扩展性和高可用性。它的角色是跨搜索节点组搜索的中心资源。

在大多数情况下，群集中的搜索头是可以互换的。所有搜索头都能访问相同的搜索节点集。还可以运行或访问相同的搜索、仪表板、知识对象等。

当您需要在相同的搜索节点集中运行多个搜索头，则推荐使用搜索头群集。群集协调搜索头的活动、基于当前负载分配任务，并确保所有的搜索头访问相同的知识对象集。

请参阅"关于搜索头群集化"。

索引器群集和搜索头

索引器群集还使用搜索头以跨一组索引器或**对等节点**搜索。索引器群集中的搜索头可以是独立的搜索头或者是搜索头群集中的成员。

当作为索引器群集的一部分时，您以不同方式部署和配置搜索头：

- 关于通过索引器群集使用独立搜索头的相关信息，请参阅*《管理索引器和索引器群集》*手册中的"配置搜索头"。
- 关于通过索引器群集使用搜索头群集的相关信息，请参阅"通过索引器群集集成搜索头群集"。

搜索头发送到搜索节点的内容

当启动分布式搜索时，搜索头复制并分发其**知识对象**到它的**搜索节点**或索引器。知识对象包括保存的搜索、事件类型和其他用于跨索引搜索的实体。搜索头需要分发本材料到搜索节点，以便它们可以代表它正确执行查询。这组知识对象称为**知识包。**

知识软件包包含的内容

搜索节点使用搜索头的知识软件包代表它执行查询。当执行分布式搜索时，节点将忽略任何本地知识对象。它们仅访问搜索头的知识软件包中的对象。

软件包通常包含来自 `$SPLUNK_HOME/etc/system`、`$SPLUNK_HOME/etc/apps` 和 `$SPLUNK_HOME/etc/users` 的文件的子集（配置文件和资产）。

分发知识包流程意味着节点默认几乎收到搜索头**应用**的整个内容。如果应用包含大量不需要与节点分享的二进制文件，您可以消除软件包中的部分内容以减少软件包大小。请参阅"修改知识软件包"。

知识软件包的位置

在搜索头上，知识包驻留于 `$SPLUNK_HOME/var/run` 目录下。完整软件包使用的扩展名为 `.bundle`，而部分更新的软件包的扩展名为 `.delta`。软件包均为 tar 文件。因此，可运行 `tar tvf` 查看其内容。

知识包将被分发到每个搜索节点上的 `$SPLUNK_HOME/var/run/searchpeers` 目录。由于知识软件包在搜索节点和搜索头上的驻留位置不同，因此搜索脚本不应硬编码路径到资源。

查看复制状态

在将搜索节点添加到搜索头后，如"添加搜索节点至搜索头"中所述，可以查看知识包的复制状态：

1. 在搜索头上，在 Splunk Web 页面顶部单击**设置**。

2. 单击"分布式环境"区域中的**分布式搜索**。

3. 单击**搜索节点**。

每个搜索节点都对应一行。**复制状态**列说明搜索头是否成功将知识包复制到搜索节点。

注意：如果是**搜索头群集**，则必须通过搜索头群集管理员查看复制状态。这是因为只有管理员将知识包复制到群集中的搜索节点。其他群集成员不参与软件包的复制。如果通过非管理员成员查看搜索节点的状态，则**复制状态**列可

能会显示“初始”而非“成功”。

用户授权

分布式搜索的所有授权源自搜索头。目前，它会发送搜索请求到其搜索节点，搜索头还会分发授权信息。它会告诉搜索节点运行此搜索用户的姓名、用户角色，以及包含授权信息的分布式 `authorize.conf` 文件的位置。

部署分布式搜索

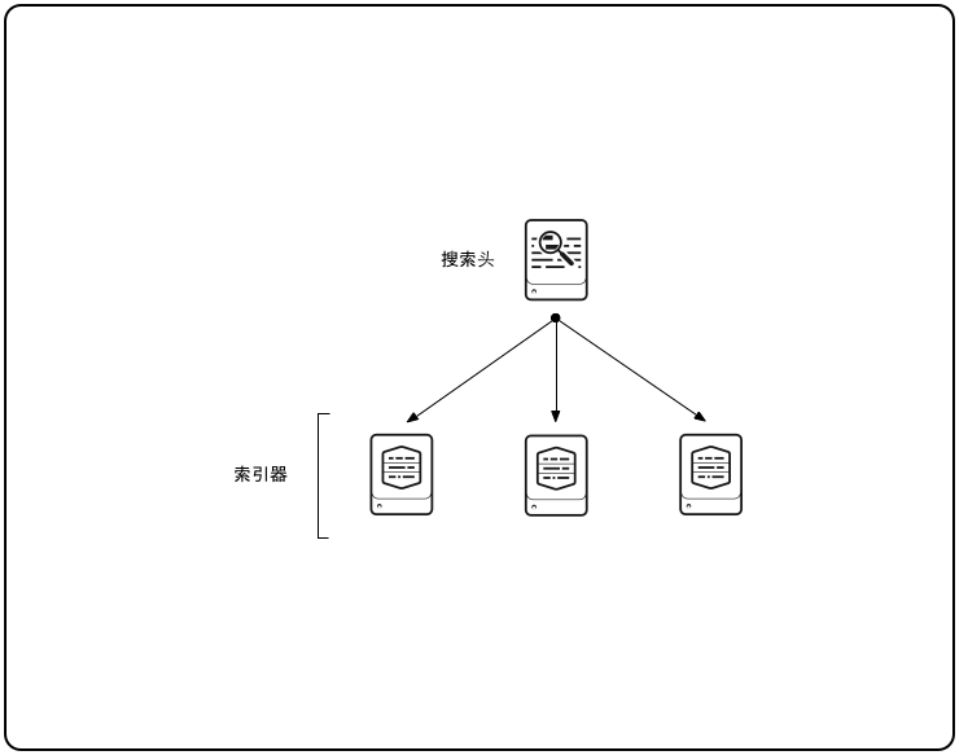
部署分布式搜索环境

重要提示：本章节中的主题说明如何部署非群集的**分布式搜索**拓扑结构。关于部署**搜索头群集**的信息，请参阅部署搜索头群集一章。

启用分布式搜索的基本配置非常简单。您可以指定一个 Splunk Enterprise 实例作为**搜索头**，并在此搜索头与一组**搜索节点**或**索引器**之间建立连接。

如果要部署多个搜索头，最佳做法是部署同一搜索头群集中的搜索头。

这是本主题所特别针对的拓扑结构类型：



搜索头连接用户，并跨索引器组管理搜索。索引器索引传入数据并搜索数据，并由搜索头定向。

部署分布式搜索

要设置由单个专用搜索头和多个搜索节点构成的简单分布式搜索拓扑结构，请执行以下步骤：

1.确定您的要求。请参阅分布式搜索的系统要求和其他部署考虑。

2.指定某个 Splunk Enterprise 实例为搜索头。由于在每个完整的 Splunk Enterprise 实例上自动启用分布式搜索，因此除了选择想要成为搜索头的实例以外，事实上此步骤不用执行任何操作。

选择并非索引外部数据的现有实例，或者安装一个新的实例。关于安装信息，请参阅特定于您操作系统的*《安装手册》*中的主题。

3.建立您希望它搜索从搜索头到所有索引器搜索的连接。这是过程中关键的一步。请参阅添加搜索节点到搜索头。

4.添加数据输入到搜索节点。按照为任意索引器添加输入相同的方式（在搜索节点上直接添加或通过连接搜索节点的转发器）添加输入。有关数据输入的信息，请参阅*《数据导入》*手册。

5. 将搜索头内部数据转发给搜索节点。请参阅最佳做法：将搜索头数据转发到索引器层。

6. 登录搜索头并执行跨所有搜索节点运行的搜索，如搜索 *。检查结果中的 `splunk_server` 字段。验证所有搜索节点列在该字段中。

7. 有关设置验证的信息，请参阅《*确保 Splunk Enterprise 安全*》手册。

若要增加索引容量，可多部署几个搜索节点。若要增加搜索管理容量，可将多个搜索头部署为同一搜索头群集的成员。

部署多个搜索头

要部署多个搜索头，最佳做法是部署同一搜索头群集中的搜索头。这种做法的好处很多，比如简化了扩展和管理。请参阅部署搜索头群集化一章。

在索引器群集中部署搜索头

Splunk **索引器群集**使用搜索头以跨一组索引器或**对等节点**搜索。当作为索引器群集的一部分时，您以不同方式部署搜索头。有关部署索引器群集中的搜索头的信息，请参阅《*管理索引器和索引器群集*》手册中的"启用搜索头"。

分布式搜索的系统要求和其他部署考虑

此主题说明当使用功能互相独立的搜索头部署基本分布式搜索拓扑结构时的关键注意事项。反之，如果您正在部署搜索头群集，请参阅"搜索头群集的系统要求和其他部署注意事项。"

分布式搜索实例的硬件要求

关于搜索头和搜索节点（索引器）的硬件要求信息，请参阅《*容量规划手册*》。

Splunk Enterprise 版本兼容性

最好同时升级搜索头和搜索节点，以充分利用最新搜索功能。如果您无法使用此功能，请遵循这些版本兼容指导原则。

搜索头与搜索节点之间的兼容性

一起应用的这两个规则定义了搜索头与搜索节点之间的兼容性要求：

- 6.x 搜索头兼容 6.x 和 5.x 搜索节点。
- 搜索头必须拥有与搜索节点相同或更高的级别。关于此上下文中"级别"的精确定义，请参阅本节后面的说明。

下面是一个非详尽的示例集，展示了兼容的组合排序：

- 6.3 搜索头兼容 5.0 搜索节点。
- 6.4 搜索头兼容 6.3 搜索节点。
- 6.4 搜索头兼容 6.4 搜索节点。

与此相反，下面是一些不兼容的组合示例：

- 5.0 搜索头不兼容 6.4 搜索节点。
- 6.3 搜索头不兼容 6.4 搜索节点。

请注意以下事项：

- 这些指导原则对于独立搜索头和参与搜索头群集活动的搜索头都有效。
- 参与索引器群集活动的搜索头具有不同的兼容性限制。请参阅《*管理索引器和索引器群集*》中的"Splunk Enterprise 版本兼容性"。
- 兼容性问题只存在主要/次要版本级别的水平上，而不是在维护级别上。例如，6.3 搜索头不兼容 6.4 搜索节点，因为 6.3 搜索头处在比 6.4 搜索节点更低的次要版本级别上。但是，6.3.1 搜索头兼容 6.3.3 搜索节点，尽管搜索头的维护版本级别较低。

混合版本分布式搜索兼容性

您可以对 5.x 搜索节点运行 6.x 搜索头，但是需要注意几个兼容性问题。要充分利用 6.x 功能集，建议您同时升级搜索头和搜索节点。

本部分介绍了兼容性问题。

混合版本部署中的 6.x 功能

当在 5.x 搜索节点上运行 6.x 搜索头时，请注意以下：

- 您可以在搜索头上使用数据模型，但仅没有报表加速。
- 您可以使用搜索头上的数据透视表。
- 您可以在搜索头上运行预测分析（`predict` 命令）。

分布式搜索的许可证

分布式搜索部署中的每个实例必须拥有对许可证池的访问权限。此规则也适用于搜索头和搜索节点。请参阅*《管理员手册》*中的“搜索头许可证”。

跨分布式搜索环境同步系统时钟

在所有参与分布式搜索活动的运行 Splunk Enterprise 实例的虚拟或物理的计算机上同步系统时钟很重要。尤其是，这表示您的搜索头和搜索节点。在搜索头合并或安装软件包的情况下，这也包括共享的存储硬件。否则，可能出现各种问题，例如软件包复制故障、搜索失败、或搜索项目的过早失效。

使用的同步方法取决于计算机的具体设置。请查阅运行 Splunk Enterprise 的特定计算机和操作系统的系统文档。对于大多数环境，网络时间协议 (NTP) 是最佳方法。

添加搜索节点到搜索头

要激活**分布式搜索**，您添加**搜索节点**或**索引器**到您指定为**搜索头**的 Splunk Enterprise 实例。您可手动指定每个搜索节点这么做。

重要提示：搜索头无法像搜索节点一样执行双重功能。唯一一个特例是监视控制台，它可以作为“搜索头的搜索头”。

此主题说明如何将搜索头连接到一组搜索节点。

如果需要将多个搜索头连接到一组搜索节点，可以分别为每个搜索头重复此流程。但是，要部署多个搜索头，最佳做法是部署同一**搜索头群集**中的搜索头。搜索头群集也可以复制一个搜索头的所有搜索节点到该群集中的其他所有搜索头，从而避免了将对等节点分别添加到每个搜索头的操作。

重要提示：群集建立搜索头和搜索节点之间的连接方式和以下主题的过程有所不同：

- **索引器群集**自动建立搜索头和索引器之间的连接，或**对等节点**。有关配置索引器群集中的搜索头的方式，请阅读*《管理索引器和索引器群集》*手册中的“配置搜索头”。
- 当连接搜索节点与搜索头时，**搜索头群集**有某些您必须考虑的限制。请参阅“连接群集中的搜索头与搜索节点”。

配置概述

要设置搜索头及其搜索节点之间的连接，请通过以下方式之一配置搜索头：

- Splunk Web
- Splunk CLI
- `distsearch.conf` 配置文件

Splunk Web 是大部分用途的最简单的方法。

在搜索头上配置。对于大部分部署，没有必要在搜索节点上进行配置。通过公共密钥验证控制对对等节点的访问权限。

先决条件

在索引器作为搜索节点之前，您必须从默认 "changeme" 更改其密码。否则，搜索头将无法对它进行验证。

使用 Splunk Web

指定搜索节点

要指定搜索节点：

1.登录搜索头上的 Splunk Web 并单击页面顶部的**设置**。

2.单击“分布式环境”区域中的**分布式搜索**。

3.单击**搜索节点**。

4.在**搜索节点**页面上，选择**新建**。

5.指定搜索节点，以及任何验证设置。

注意：必须在搜索节点的主机名称或 IP 地址前面加上 URI 方案，即 "http" 或 "https"。

6. 单击**保存**。

7. 为每个搜索头的搜索节点执行重复操作。

配置其他分布式搜索设置

要配置其他设置：

1. 登录搜索头上的 Splunk Web 并单击页面顶部的**设置**。

2. 单击“分布式环境”区域中的**分布式搜索**。

3. 单击**分布式搜索设置**。

5. 必要时更改任何设置。

6. 单击**保存**。

使用 CLI

要添加搜索节点，从搜索头上运行以下命令：

```
splunk add search-server <scheme>://<host>:<port> -auth <user>:<password> -remoteUsername <user> -remotePassword
<passremote>
```

请注意以下事项：

- <scheme> 指 URI 方案："http" 或 "https"。
- <host> 指搜索节点主机的主机名称或 IP 地址。
- <port> 指搜索节点的管理端口。
- 使用 `-auth` 标记为搜索头提供凭据。
- 使用 `-remoteUsername` 和 `-remotePassword` 标记为搜索节点提供凭据。远程凭据必须支持搜索节点上具有管理级权限的用户。

例如：

```
splunk add search-server https://192.168.1.1:8089 -auth admin:password -remoteUsername admin -remotePassword
passremote
```

每个要添加的搜索节点都必须运行此命令。

编辑 distsearch.conf

通过 Splunk Web 的可用设置，为大多数配置提供充足的选项。然而，一些高级配置设置仅可通过直接编辑 `distsearch.conf` 的方式实现。此章节仅讨论有必要将搜索头和搜索节点连接的配置设置。有关高级配置选项的信息，请参阅 distsearch.conf 规范文件。

添加搜索节点

要连接搜索节点：

1. 创建或编辑搜索头上的 `distsearch.conf` 文件。

2. 添加搜索节点组至 `[distributedSearch]` 段落作为逗号分隔值组（带有管理端口的主机名称或 IP 地址）。例如：

```
[distributedSearch]
servers = https://192.168.1.1:8089,https://192.168.1.2:8089
```

注意：必须在主机名称或 IP 地址前面加上 URI 方案，即 "http" 或 "https"。

3. 重新启动搜索头。

分布密钥文件

如果您通过 Splunk Web 或 CLI 添加搜索节点，则 Splunk Enterprise 将自动配置验证。然而，如果通过编辑 `distsearch.conf` 的方式添加对等节点，则必须手动分发密钥文件。如上所述，在添加搜索节点和重新启动搜索头后：

1. 从搜索头上复制文件 `$SPLUNK_HOME/etc/auth/distServerKeys/trusted.pem` 到每个搜索节点上的 `$SPLUNK_HOME/etc/auth/distServerKeys/<searchhead_name>/trusted.pem`。

<searchhead_name> 是搜索头的 serverName，在 server.conf 中指定。

2.重新启动每个搜索节点。

单个对等节点上多个搜索头的验证

多个搜索头可以跨单个对等节点搜索。对等节点必须存储每个搜索头证书的副本。

搜索节点在特定 $SPLUNK_HOME/etc/auth/distServerKeys/<searchhead_name> 目录中存储搜索头密钥。

例如，如果您有名为 A 和 B 的搜索头，同时它们都需要搜索一个特定的搜索节点，则执行以下操作：

1.在搜索节点上，创建 $SPLUNK_HOME/etc/auth/distServerKeys/A/ 和 $SPLUNK_HOME/etc/auth/distServerKeys/B/ 目录。

2.将 A 的 trusted.pem 文件复制到 $SPLUNK_HOME/etc/auth/distServerKeys/A/，将 B 的 trusted.pem 复制到 $SPLUNK_HOME/etc/auth/distServerKeys/B/。

3.重新启动搜索节点。

搜索节点分组

您可以将搜索节点分到分布式搜索组中。这允许您将搜索定位到搜索节点子集中。请参阅"创建分布式搜索组"。

查看搜索节点状态

请参阅在"设置"中查看搜索节点状态。

最佳做法：将搜索头数据转发到索引器层

我们认为最佳的做法是，将所有搜索头内部数据转发到搜索节点（索引器）层。这有几个优势：

- 它将所有数据累计到一个位置。这简化了管理数据的过程。您只需在一层（索引器层）管理索引和数据。
- 如果搜索头故障，它将为搜索头启用诊断。在故障之前的数据累计在索引器上，其中另一个搜索头之后可访问它。
- 通过将摘要索引搜索的结果转发到索引器层，所有搜索头都可访问它们。否则，它们只对生成它们的搜索头可用。

转发搜索头数据

首选方式是将数据直接转发到索引器，无需在搜索头上单独索引。您可通过将搜索头配置为转发器来执行此操作。下面是主要步骤：

1.确保所有必要的索引存在于索引器上。例如，S.o.S 应用使用脚本式输入（它将数据放入自定义索引）。如果您在搜索头上安装 S.o.S，则您还需要在索引器上安装 S.o.S 加载项，这样，可以针对应用生成的数据，为索引器进行必要的索引设置。另一方面，由于 _audit 和 _internal 存在于索引器以及搜索头上，所以不需要创建这些索引的单独版本以保存相应的搜索头数据。

2.将搜索头配置为转发器。在搜索头上创建 outputs.conf 文件对该搜索头进行配置，确保在整个搜索节点（索引器）集内实现负载均衡转发。您也必须关闭搜索头上的索引，这样搜索头既不在本地保留数据也不转发数据到搜索节点。

以下是一个 outputs.conf 文件示例：

```
# Turn off indexing on the search head
[indexAndForward]
index = false

[tcpout]
defaultGroup = my_search_peers
forwardedindex.filter.disable = true
indexAndForward = false

[tcpout:my_search_peers]
server=10.10.10.1:9997,10.10.10.2:9997,10.10.10.3:9997
autoLB = true
```

本示例假设每一个索引器的接收端口都配置为 9997。

有关配置 outputs.conf 的详细信息，请参阅《转发数据》手册中的"使用 outputs.conf 配置转发器"。

从搜索头群集成员转发数据

你可执行相同的配置步骤从搜索头群集成员转发数据到搜索节点集。然而，您必须确保所有成员使用相同的 `outputs.conf` 文件。如要进行此操作，不要编辑单个搜索头上的文件。相反，使用 Deployer 跨群集传输文件。请参阅"使用 Deployer 分布应用和配置更新"。

管理分布式搜索

修改知识软件包

知识包是搜索头复制并分发给每个搜索节点以启用其搜索的数据。有关本软件包的内容和用途的信息，请参阅"搜索头发送给搜索节点的内容"。

知识软件包由搜索节点一般所需的文件集组成，以便执行搜索。如有必要，您可以修改这一组文件。修改文件组的主要原因是否为：

- **作为应用开发人员，**您想要根据应用的需要自定义文件。这种情况往往涉及到操作复制白名单。您还可以为此使用复制黑名单。
- **作为管理员，**您需要限制知识包的大小。这种情况一般不常见，因为 Splunk Enterprise 使用基于 delta 的复制内容以保持软件包紧凑，同时搜索头往往只是将软件包已更改部分复制至其搜索节点。这种情况需要您识别多余文件并通过复制黑名单将其筛选出来。也可以为此使用白名单，虽然这种方法不怎么普遍。

关于本主题讨论的设置详细信息，请参阅*《管理员手册》*中的 distsearch.conf。

为某个应用自定义软件包

系统会查看 `distsearch.conf` 中的两个段落，以确定待包含在软件包的 `*.conf` 文件，查看顺序为：

1. `[replicationWhitelist]`
2. `[replicationSettings:refineConf]`

您通常只需编辑 `[replicationSettings:refineConf]` 段落以自定义应用软件包，但在极少数情况下，您可能还需修改 `[replicationWhitelist]` 段落。

由于系统启动时会先检查 `[replicationWhitelist]` 段落，所以此讨论话题也包含这一内容。

编辑 replicationWhitelist 段落

`[replicationWhitelist]` 段落（位于 `distsearch.conf` 系统默认版本中）将 `*.conf` 文件（在 `[replicationSettings:refineConf]` 段落中指定）都列为白名单。因此，为了从软件包添加或删除 `*.conf` 文件，请不要修改此段落。相反，可以更改 `[replicationSettings:refineConf]` 段落中指定的文件组，如下一部分"编辑 replicationSettings:refineConf 段落"中所述。

修改 `[replicationWhitelist]` 段落的主要原因是将用于自定义搜索命令的某些特殊类型的文件包含在软件包中。这是一个比较少见的情况。

如果需要更改白名单，您可以创建 `[replicationWhitelist]` 段落的版本（位于 `$SPLUNK_HOME/etc/apps/<appname>/default/distsearch.conf` 中），从而覆盖系统默认白名单：

```
[replicationWhitelist]
<name> = <whitelist_regex>
...
```

知识包将包含满足白名单正则表达式和 `[replicationSettings:refineConf]` 中指定的所有文件。如果指定了多个正则表达式，则软件包将包含这些文件的并集。

在本例中，知识软件包将包含具有 ".conf" 或 ".spec" 扩展名的所有文件：

```
[replicationWhitelist]
allConf = *.conf
allSpec = *.spec
```

allConf 和 allSpec 等名称仅用于分层。也就是说，如果您同时有 `distsearch.conf` 全局和本地的副本，则可以配置本地副本，这样它就能覆盖其中一个正则表达式。例如，假设上面显示的例子就是全局副本，然后您在本地副本中指定一个白名单，像这样：

```
[replicationWhitelist]
allConf = *.foo.conf
```

两个 conf 文件将分层，本地副本优先。由此，搜索头将仅分发满足这两个正则表达式的文件：

```
allConf = *.foo.conf
allSpec = *.spec
```

有关分层配置文件的属性的更多信息，请参阅《管理员手册》中的“属性优先顺序”。

警告：无论在哪里定义，复制白名单跨所有配置数据进行全局应用，并且不限定于任何特殊应用。当仅获取预期文件时需格外小心。

编辑 replicationSettings:refineConf 段落

`[replicationSettings:refineConf]` 段落（位于 `distsearch.conf` 中）指定包含在知识包中的 `*.conf` 文件和 `*.meta` 段落。如果您想要在软件包中修改文件组，请从此段落添加或删除。

系统默认 `distsearch.conf` 文件包含此段落的某一个版本，此段落将指定一般包含在知识包中的 `*.conf` 文件：

```
[replicationSettings:refineConf]
# Replicate these specific *.conf files and their associated *.meta stanzas.
replicate.app               = true
replicate.authorize         = true
replicate.collections       = true
replicate.commands          = true
replicate.eventtypes        = true
replicate.fields            = true
replicate.segmenters        = true
replicate.literals          = true
replicate.lookups           = true
replicate.multikv           = true
replicate.props             = true
replicate.tags              = true
replicate.transforms        = true
replicate.transactiontypes  = true
```

如果要复制一个 `.conf` 文件，并且不是 `[replicationSettings:refineConf]` 段落的系统默认版本，则请在 `$SPLUNK_HOME/etc/apps/<appname>/default/distsearch.conf` 中创建一个段落版本，然后指定 `*.conf` 文件。类似地，您可以通过在此段落中将其设置为 "false" 来移除文件。

限制知识软件包的大小

您还可以使用 `[replicationBlacklist]` 段落创建复制黑名单。这是限制知识软件包大小的最有用方法，尤其在超大文件无需复制到搜索节点的情况下使用。黑名单优先于任何白名单。

警告：无论在哪里定义，复制黑名单跨所有配置数据进行全局应用，并且不限定于任何特殊应用。如果您正在定义应用特定黑名单，请在限制时格外小心，以仅匹配应用程序不需要的文件。

管理分布式服务器名称

每个搜索头和搜索节点的名称由 `serverName` 属性（在 server.conf 中指定）确定。`serverName` 属性默认为服务器的机器名称。

在分布式搜索中，组中的所有搜索头和搜索节点必须具有唯一名称。`serverName` 在分布式搜索中具有三个特定用途：

- **用于验证搜索头。**当搜索节点正在验证搜索头时，它们将在 `/etc/auth/distServerKeys/<searchhead_name>/trusted.pem` 中寻找搜索头的密钥文件。
- **用于确定搜索查询中的搜索节点。**`serverName` 为 `splunk_server` 字段的值。当要查询某个特定节点时，可指定该字段。请参阅*《搜索》*手册中的 [[Documentation:Splunk:Search:Searchdistributedpeers|在一个或多个分布式搜索节点中搜索]。
- **用于确定搜索结果中的搜索节点。**`serverName` 会以 `splunk_server` 字段的形式返回。

注意：当添加搜索节点到搜索头时，将*不*使用 `serverName`。在这种情况下，您可通过其域名或 IP 地址确定搜索节点。

更改 `serverName` 的唯一理由是，如果您有多个 Splunk Enterprise 实例驻留在单个计算机上，同时它们参与同一分布式搜索组中。在这种情况下，您需要更改 `serverName` 以便对他们加以区分。

创建分布式搜索组

您可以将搜索节点分组以便于在它们子集中搜索。搜索节点分组称为“分布式搜索组”。您可在 `distsearch.conf` 文件中指定分布式搜索组。

例如，假设您有一组搜索节点在 New York，另一组在 San Francisco，您只想在单个位置上执行跨节点搜索．您可以通过创建两个搜索组 NYC 和 SF 来实现此目的。

当配置监视控制台时，分布式搜索组会特别有用。请参阅*《监视 Splunk Enterprise》*。

在 `distsearch.conf` 中，创建以下段落：

```
[distributedSearch]
# This stanza lists the full set of search peers.
servers = 192.168.1.1:8089, 192.168.1.2:8089, 175.143.1.1:8089, 175.143.1.2:8089, 175.143.1.3:8089

[distributedSearch:NYC]
# This stanza lists the set of search peers in New York.
default = false
servers = 192.168.1.1:8089, 192.168.1.2:8089

[distributedSearch:SF]
# This stanza lists the set of search peers in San Francisco.
default = false
servers = 175.143.1.1:8089, 175.143.1.2:8089, 175.143.1.3:8089
```

此例创建两个搜索组 NYC 和 SF，然后您可以在搜索中指定它们。

请注意以下事项：

- `servers` 属性按照 IP 地址和管理端口列出搜索节点组。
- 每个搜索组的服务器列表必须是通用 `[distributedSearch]` 段落中列表的子集。
- 组列表可重叠。例如，您可以添加第三个名为 "Primary_Indexers" 的组，该组包含每个位置上的一些节点。
- 如果您将某个组的 `default` 属性设为 "true"，当搜索没有指定搜索组时，就会查询该组中的对等节点。否则，如果您将所有组都设为 "false"，当搜索没有指定搜索组时，则会查询 `[distributedSearch]` 段落中的全部搜索节点。

要在搜索中使用搜索组，请如下指定搜索组：

```
sourcetype=access_combined status=200 action=purchase splunk_server_group=NYC | stats count by product
```

此搜索只针对在 NYC 位置上的节点运行。

注意：本功能对于单个站点索引器群集化无效。在索引器群集化中，群集随意跨搜索节点集或“对等节点”复制数据。您无法知晓特定数据集是否将驻留在特定节点上。

删除搜索节点

您可通过 Splunk Web 或 CLI 删除搜索头的搜索节点。正如您可以预期的那样，删除搜索头的该搜索节点知识；它不会影响对等节点本身。

通过 Splunk Web 删除搜索节点

您可以通过搜索头的 Splunk Web 的**搜索节点**页面删除搜索头的搜索节点。请参阅在“设置”中查看搜索节点状态。

注意：这仅会从搜索头删除搜索节点条目；它不会从搜索节点删除搜索头密钥。在大部分情况下，这不是一个问题同时无需进一步操作。

通过 CLI 删除搜索节点

在搜索头上，运行 `splunk remove search-server` 命令以从搜索头删除搜索节点：

```
splunk remove search-server -auth <user>:<password>  <host>:<port>
```

请注意以下事项：

- 使用 `-auth` 标记仅为搜索头提供凭据。
- <host> 指搜索节点主机的主机名称或 IP 地址。
- <port> 指搜索节点的管理端口。

例如：

```
splunk remove search-server -auth admin:password 10.10.10.10:8089
```

在删除搜索节点后显示成功的消息。

如果是搜索头群集，只有当您启用了**搜索节点复制**，删除节点操作才会复制到所有其他群集成员。否则，必须单独从每个成员中删除搜索节点。有关启用搜索节点复制的信息，请参阅在整个群集内复制搜索节点。

禁用信任关系

作为额外步骤，您可以禁用搜索节点和搜索头之间的信任关系。要实现这一点，删除 `trusted.pem` 文件（位于搜索节点上的 `$SPLUNK_HOME/etc/auth/distServerKeys/<searchhead_name>`）。

注意：`<searchhead_name>` 是搜索头的 `serverName`，如"管理分布式服务器名称"中所述。

通常无需该步骤。

查看分布式搜索状态

在"设置"中查看搜索节点状态

在将搜索节点添加到搜索头后，即可在**设置**中查看搜索节点的状态：

1. 在搜索头上，在 Splunk Web 页面顶部单击**设置**。

2. 单击"分布式环境"区域中的**分布式搜索**。

3. 单击**搜索节点**。

每个搜索节点都对应一行，所包含的列如下：

- **对等节点 URI**
- **Splunk 实例名称**
- **状态。**说明对等节点是正常还是故障。
- **复制状态。**说明搜索头和搜索节点之间的知识包的复制状态：
  - **初始。**指对等节点的默认状态，即节点从此搜索头收到第一个知识包之前的状态。对等节点在约为 `replication_period_sec`（位于 `limits.conf` 中，默认值为 60 秒）的时间内保持此状态。
  - **进行中。**软件包复制正在进行中。
  - **成功。**对等节点已经从此搜索头收到软件包。对等节点已经准备好加入分布式搜索。
  - **失败。**软件包复制过程中出现错误。
- **群集标签。**如果此节点属于一个索引器群集且此群集带有标签，则此字段中会给出一个值。请参阅*《监视 Splunk Enterprise》*中的"设置群集标签"。
- **运行状况。**当搜索头给一个对等节点发送检测信号时（默认情况下，每 60 秒发一次），则它会对此节点进行一系列运行状况检查。检查结果决定此对等节点的运行状况：
  - **健康。**在过去十分钟的时间内，对等节点通过了 50% 或以上的检测信号所进行的健康检查。
  - **不健康。**在过去十分钟的时间内，对等节点在 50% 以上的检测信号所进行的健康检查中有一次未通过。若需详细信息，请查看**运行状况检查失败**栏中的内容。
  - **隔离。**对等节点目前未参与分布式搜索。请参阅隔离搜索节点。
- **运行状况检查失败。**此列提供所有运行状况检查失败的详细信息。过去十分钟内的所有检查失败都会在此列出。由于检测信号期间所进行的一组运行状况检查会在出现第一次检查失败时即停止，所以此处只列出每个检测信号的第一次检查失败（如果有的话）。
- **状态。**启用或禁用。
- **操作。**可以将此对等节点隔离或将它从搜索头中删除。请参阅隔离搜索节点和删除搜索节点。

您还可以通过监视控制台了解搜索节点的相关信息。请参阅使用监视控制台查看分布式搜索状态。

使用监视控制台查看分布式搜索状态

您可以使用监视控制台来监视部署的大多数方面。本主题介绍可用来深入了解分布式搜索的控制台仪表板。

监视控制台的主要文档位于*《监视 Splunk Enterprise》*。

在**搜索**菜单下方有两个分布式搜索仪表板：

- 分布式搜索：实例
- 分布式搜索：部署

仪表板提供一系列问题的详细信息，例如：

- 对等节点的运行状况
- 搜索头的运行状况
- 知识包的复制过程
- 搜索头上的 dispatch 目录

自行查看仪表板的更多信息。此外，请参阅*《监视 Splunk Enterprise》*中的“分布式搜索仪表板”。

您还可以通过“设置”了解搜索节点的相关信息。请参阅在设置中查看搜索节点。

搜索头群集化概述

关于搜索头群集化

搜索头群集是一组作为搜索中心资源的 Splunk Enterprise **搜索头**。搜索头群集的**成员**本质上是可互换的。您可以从任一个群集成员上运行相同的搜索、查看相同的仪表板和访问相同的搜索结果。

为了实现这一互换性，群集中的搜索头必须共享配置和应用、**搜索项目**和任务计划。搜索头群集自动在成员间传输大多数的共享资源。

搜索头群集的好处

搜索头群集提供如下重要好处：

- **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，其他成员自动接管群集的管理。

群集架构

搜索头群集由一组称为群集成员的网状搜索头组成。一个群集成员（管理员）协调所有群集范围内的活动。如果作为管理员的成员发生故障，其他成员会取代它。

成员间共享：

- **任务计划。**群集集中管理任务计划，分配每个计划的搜索给最优的成员，此成员通常负载最小。
- **搜索项目。**群集复制搜索项目并使它们对于所有成员可用。
- **配置。**群集要求所有的成员共享相同的配置集。对于运行时更新知识对象，与更新仪表板或报表一样，群集自动将配置复制给所有成员。对于应用和一些其他配置，用户必须通过 **Deployer**（驻留在群集外的 Splunk Enterprise 实例）将配置推送给群集成员。

请参阅“搜索头群集化架构”。

如何设置群集

您可以通过配置和部署群集搜索头来设置群集。过程与您在任一分布式搜索环境中设置搜索头的方式类似。主要区别在于，您还需要将搜索头配置为群集成员。

请参阅章节“部署搜索头群集化”。

用户如何访问群集

用户访问群集的方式与它们访问任一搜索头的方式相同。它们将浏览器指向作为群集成员的任一搜索头。因为群集成员共享任务、搜索项目和配置，所以用户访问哪个搜索头都没有关系。用户拥有访问相同的仪表板集、搜索集等权限。

为实现高可用性和负载均衡的目标，Splunk 建议您在群集前面放置一个负载均衡器。这样，负载均衡器可以将用户分配给群集中的任一个搜索头，跨群集成员均衡用户负载。如果一个搜索头发生故障，负载均衡器可以将用户重新分配给余下的任一个搜索头。

搜索头群集和索引器群集

搜索头群集不同于**索引器群集**。索引器群集的主要目的是为了通过协调索引器组来提供高可用数据。索引器群集始终包括一个或多个相关搜索头来访问索引器上的数据。这些搜索头可能（但不一定）是搜索头群集的成员。

有关索引器群集中的搜索头的信息，请参阅《*管理索引器和索引器群集*》手册中的“配置搜索头”章节。

有关添加搜索头群集到索引器群集中的信息，请参阅本手册中的“通过索引器群集集成搜索头群集”主题。

搜索头群集化架构

搜索头群集是一组作为搜索中心资源的 Splunk Enterprise 搜索头。

搜索头群集的各个部分

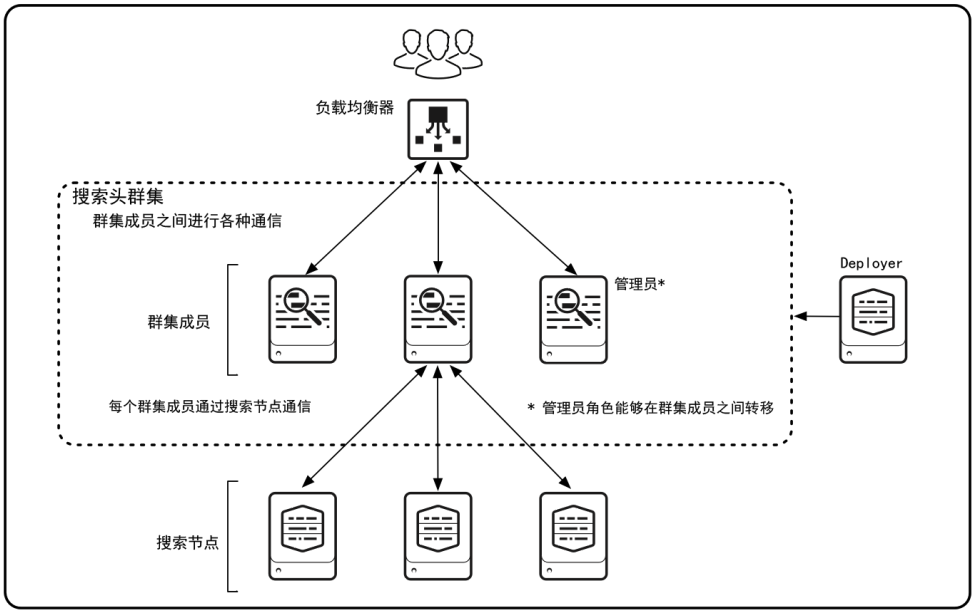
搜索头群集由一组共享配置、任务计划和**搜索项目**的**搜索头**组成。搜索头称为群集**成员**。

一个群集成员具有**管理员**角色，这意味着它会在所有成员中协调任务计划和复制活动。像其他成员一样，它也作为一个搜索头运行搜索任务、提供结果等等。随着时间的推移，管理员的角色可以在群集成员间转移。

除了组成实际群集的搜索头成员组外，一个工作中的群集还需要若干其他的组件：

- **Deployer。**这是一个给群集成员分布应用和其他配置的 Splunk Enterprise 实例。它位于群集之外，不能在与群集成员相同的实例上运行。然而，在某些情况下，它可以驻留在一些其他 Splunk Enterprise 组件相同的实例上，例如**部署服务器**或**索引器群集**主节点。请参阅"使用 Deployer 分布应用和配置更新"。
- **搜索节点。**这些是群集成员在其中运行搜索的索引器。搜索节点可以是独立索引器或索引器群集中的节点。请参阅"连接群集中的搜索头与搜索节点"。
- **负载均衡器。**这是可选择驻留在用户和群集成员间的第三方软件或硬件。通过放置的负载均衡器，用户可以通过单个界面访问搜索头集，而无需指定某个搜索头。请参阅"对搜索头群集使用负载均衡器"。

下面是一幅由三个成员组成的小型搜索头群集图：



此图显示了主要的群集相关组件和相互作用：

- 作为管理员的成员指示在群集中的各种活动。
- 成员间相互通信来在群集中计划任务、复制项目、更新配置和协调其他活动。
- 成员与搜索节点通信来完成搜索请求。
- 用户可选择通过第三方负载均衡器访问搜索头。
- Deployer 位于群集之外，并向群集成员分发更新。

注意：此图是呈现组件间一组复杂交互的极度简化版图形。例如，每个群集成员直接发送搜索请求到一组搜索节点。另一方面，只有管理员将知识包发送给搜索节点。同样的，此图并不旨在说明不同群集成员之间的信息发送。有关所有交互的详细信息，请参阅本主题的文字内容。

搜索头群集管理员

管理员是具有除所有群集成员通常搜索活动之外的其他职责的群集成员。它用于协调群集活动。任一成员都可以执行管理员角色，但是在任一时刻群集只能有一个管理员。随着时间推移，如果发生故障，管理员会更改，新成员当选为该角色。

所选举的管理员称为**动态管理员**，因为随着时间变化可能会改变。运行正常的群集使用动态管理员。在灾难恢复时期，如果群集无法选举动态管理员，则可以部署**静态管理员**作为临时解决方法。

管理员角色

管理员是群集成员，利用此身份，它可以执行任一个群集成员典型的搜索活动，同时为特殊和计划的搜索提供服务。如有必要，您可以限制管理员的搜索活动，这样它只执行特殊搜索而不执行计划的搜索。请参阅"配置管理员只运行特殊搜索"。

管理员也协调所有群集成员间的活动。它的职责包括：

- 计划任务。基于相对的当前负载，它给成员包括它自己分配任务。
- 协调告警和跨群集告警抑制。管理员跟踪每一个告警，直到成员运行一个初始化搜索将其消除。
- 将**知识包**推送到搜索节点。
- 协调项目复制。管理员确保搜索项目根据需要复制来达到**复制因子**。请参阅"为搜索头群集选择复制因子"。
- 复制配置更新。管理员将一个群集成员上的运行时更新知识对象复制到所有其他成员。这包括，例如，更新或附加到保存的搜索、查找表和仪表板。请参阅"群集复制的配置更新"。

管理员选举

搜索头群集通常使用动态管理员。这意味着作为管理员的成员可以在整个群集生命周期内更改。任一成员都能作为管理员工作。需要时，群集会进行选举，这会导致新成员接替管理员角色。

管理员选举发生在：

- 当前管理员发生故障或重新启动。
- 发生网络分区，这导致一个或多个成员与搜索头群集余下的成员分隔开。网络分区的后续修复将触发另外一个单独的管理员选举。
- 当前管理员已辞职，因为无法检测到多数成员正在参与群集活动。

注意：如果一个非群集成员的唯一故障或重新启动没有关联的网络分区，则不会触发管理员选举。

只有得到所有成员多数票的成员才能成为管理员。例如，在一个有七个成员的群集中，选举需要四票。同样，有六个成员的群集也需要四票。

"多数"必须是所有成员中的大多数人，而不是当前运行的成员。所以，如果七人成员群集中有四个成员失败，则群集无法选举新的管理员，因为剩余的三个成员人数比所要求的四个成员人数少。

选举过程涉及随机设置在所有成员上的定时器。定时器到期的成员首先参与选举并要求其他成员为其投票。通常，其他成员会同意，该成员成为新管理员。

通常在触发事件发生后的一到两分钟会选举出新管理员。在那段时间内，没有正在工作的管理员，搜索头只了解其本地环境。选举会花费这么长时间是因为每个成员在尝试成为管理员前都会等待一个最小超时周期。这些超时周期可以配置。

群集可以重新选举之前作为管理员的成员，如果它现在正在运行的话。对于支持或反对此情况发生，没有偏向。

一旦一个成员被选为管理员，它就接替管理员职责。

重要提示：多数成员必须始终运行并参与群集活动。如果管理员无法检测到多数成员，则将辞职，即废除其权限。随后将开始新管理员的选举，但是如果没有多数参与成员，则不会成功。如果在群集中失去多数人的优势，则有一个临时解决方法：部署一个静态的管理员，来替代动态管理员。静态管理员一般由管理员指定，而不是由成员选举。请参阅"使用静态管理员，以从丧失多数优势的状态中恢复"。

关于群集的管理员选举进度详情，请查看"搜索头群集化"：监视控制台中的"状态"和"配置"仪表板。请参阅"使用监视控制台查看搜索头群集状态"。

无功能群集的运行后果

如果群集中缺少多数成员而因此无法选举管理员的话，成员将继续充当独立搜索头。然而，他们只能服务于临时搜索。计划报表和警告将不再运行，因为在群集中，计划功能降级为管理员。此外，配置和搜索项目将不会在此期间复制。

要弥补此状况，您可以临时部署一个静态管理员。请参阅"使用静态管理员，以从丧失多数优势的状态中恢复"。

无功能群集的运行恢复

在群集中缺少多数成员期间，如果您无法部署静态管理员，则群集将不再运行功能，直到大多数成员再次加入群集中。当获得多数成员时，成员将选举管理员，并且群集将开始运行功能。

有两个关键用以恢复：

- 运行时间配置
- 计划报表

一旦群集开始运行功能，则它将同步成员的运行时间配置。由于当成员群集不在运行功能时成员无法独立操作，所以很有可能在此期间每个成员都开发自身独特的配置组并进行更改。例如，用户可能已经新建保存的搜索或将新的面板添加到仪表板。这些更改必须立即保持一致，并在群集中进行复制。要完成此操作，每个成员都要将其更改组报告给管理员，管理员然后协调所有更改的复制（包括其自身的更改）给成员。在此过程的末尾阶段，所有成员必须具有相同的配置组。

警告：如果管理员和每个成员仍旧在他们的更改历史中共享公共提交，则此流程只能以自动的方式处理。否则，就有必要针对管理员当前的配置组手动重新同步非管理员成员，以防成员丢失其间发生的所有更改。可配置清理限制控制更改历史。关于清理限制和重新同步过程的详情，请参阅"更新已复制的更改"。

已恢复的群集也同样再次开始处理计划报表。当群集关闭时是否尝试运行已跳过的报表，取决于计划报表的类型。大多数情况下，它只选取下一个计划运行时间的报表。然而，在群集停止运行功能之前，从上次运行的时间点开始，计划程序将运行通过报表加速和数据模型加速使用的报表。关于计划程序如何处理多种类型报表的详情，请参阅*《报表手册》*中的"配置计划报表的优先级"。

管理员选举过程影响部署

成功选举的多数票要求对部署有这些影响：

- 一个群集应该由最少三个成员组成。两个成员的群集不能容许任何节点故障。任一成员的故障都将阻止群集选举管理员和继续工作。管理员选举需要所有成员的多数 (51%) 同意，而在两个成员群集的示例中，这意味着两个节点必须都在运行。如果您将搜索头群集限制为两个成员，您会因此失去它的高可用性的好处。
- 如果您将群集部署到两个站点上，您的主要站点必须包含多数节点。如果在站点间存在网络干扰，只有具有多数节点的站点会选举新管理员。请参阅"在多个站点之间部署搜索头群集时的重要考虑事项"。

群集如何处理搜索项目

群集将大多数也称为搜索结果的搜索项目复制到多个群集成员。如果成员需要访问搜索项目，它会尽可能访问本地副本。否则，它会使用代理访问搜索项目。

项目复制

群集保留来自计划的已保存搜索的多个项目副本。复制因子用于确定群集保留的每个项目的副本数量。例如，如果复制因子是三，群集保留每个项目的三个副本：一个在生成项目的成员上，两个在其他成员上。

管理员协调向群集成员的项目复制。与任一搜索头一样，群集或非群集，当搜索完成时，其搜索项目位于生成搜索的成员的 dispatch 目录。然后管理员指示项目的复制过程，在成员间不断复制，直到副本在复制因子个数的成员上存在，包括生成成员。

接收副本的成员集对于不同的项目可以更改。即，来自相同生成成员的两个项目可以在不同成员上保留它们的复制副本。

管理员保留项目注册表，其中含有每个项目副本的位置信息。当注册表更改时，管理员向每个成员发送增量信息。

如果一个成员发生故障，那么会导致群集失去一些项目副本，管理员会协调修复活动，其目标是将群集恢复到每个项目都有复制因子个数的副本的状态。

搜索项目保留在位于 `$SPLUNK_HOME/var/run/splunk/dispatch` 下的 dispatch 目录。每个 dispatch 子目录都包含一个搜索项目。群集会复制这些子目录。

关于群集的项目复制进度详情，请查看"搜索头群集化"：监视控制台中的"项目复制"仪表板。请参阅"使用监视控制台查看搜索头群集状态"。

项目代理

群集只复制来自计划的保存的搜索的搜索项目。它不复制来自其他搜索类型的结果：

- 计划的实时搜索
- 任意种类的特殊搜索（实时或历史）

相反，如果非生成的搜索头请求它们，群集会代理这些结果。经过短暂的延时后它们会出现在请求的成员上。

另外，如果成员需要来自计划的保存的搜索的一个项目，但它本身没有该项目的本地副本，它会从有副本的成员上代理这些结果。同时，群集会将该项目的副本复制到请求的成员上，因此对于未来的任何请求它就具有本地副本了。因为是这种过程，所以一些项目可能会有超过复制因子个数的副本。

分发配置更改

除少数例外情况，所有群集成员必须使用相同的配置集。例如，如果用户在一个成员上编辑了仪表板，更新必须以某种方式传输给其他的所有成员。同样，如果您分发一个应用，您必须将其分发给所有成员。搜索头群集有方法来确保配置在群集间保持同步。

基于配置如何分发给群集成员，存在两种类型的配置更改。

- **复制更改。**群集自动将一个成员上的任意运行时知识对象更改复制到其他的所有成员。
- **部署更改。**群集依赖一个外部实例 (Deployer) 来将应用和其他非运行时配置更改推送到成员集。您必须从 Deployer 启动更改的每一次推送。

请参阅"配置更改如何跨搜索头群集传输"。

任务计划

管理员计划保存的搜索任务，根据负载为基础的启发式算法将它们分配给不同的群集成员。实际上，它试图将每一个任务分配给当前搜索负载最小的成员。

管理员可以将保存的搜索任务分配给自己。但是，它不会分配计划的实时搜索给自己。

如果一个任务在一个成员上运行失败，管理员会将它重新分配给不同的成员。管理员只重新分配任务一次，因为多次失败没有用户的干预是不可能解决的。例如，不管群集试图运行任务几次，具有不合适的搜索字符串的任务都会失败。

您可以指定成员为“仅限特殊”。在这种情况下，管理员不会给它安排任务。您也可以指定管理员的功能为“仅限特殊”。那么当前管理员将永远不会给自己安排任务。因为管理员角色会在成员间转移，该设置确保此管理员的功能不会与计划的搜索竞争。请参阅“配置群集成员只运行特殊搜索”。

注意：管理员没有深入了解每个成员计算机的实际 CPU 负载。它假定群集中的所有计算机的配置均匀，具有相同数量和类型的内核，等等。

关于群集的计划程序委派进度详情，请查看“搜索头群集化”：监视控制台中的“计划程序委派”仪表板。请参阅“使用监视控制台查看搜索头群集状态”。

群集如何处理并发搜索配额

搜索头群集，像非群集搜索头一样，强制实施两种类型的并发搜索配额：

- 用户和角色的搜索配额，通过 `srchJobsQuota` 和 authorize.conf 中的相关设置进行配置。
- 总搜索配额，通过 limits.conf 中的 `max_searches_per_cpu` 进行配置。

搜索头群集在群集范围内强制实施或对成员逐个强制实施这些配额。所选择的强制实施行为会影响这两种类型的配额：

- 如果您配置群集在群集范围内强制实施配额，则管理员将分配给用户或角色的并行搜索的基数乘以群集成员的数量来确定用户或角色的群集范围的配额。例如，在一个有五个成员的群集中，它将 `srchJobsQuota` 的值乘以 5。同样，它将全部分配的并行搜索的基数乘以成员的数量来确定所有搜索的群集范围的配额。管理员使用这些数字以确定是否允许一个新的搜索运行。

- 如果您配置群集对成员逐个强制实施配额，则每个单独的成员使用基本配额设置来确定是否允许搜索运行。搜索的群集范围报告未发生。

如何配置配额强制实施行为

您可以通过 limits.conf 中的设置来选择强制实施行为：

- `shc_role_quota_enforcement`。确定群集范围的强制实施。
- `shc_local_quota_check`。确定逐个成员的强制实施。

这些设置每个都会影响这两种类型的配额。通常情况下，您给这些设置分配相反的值。也就是说，要在群集范围内强制实施配额，使用此配置：

```
shc_role_quota_enforcement=true
shc_local_quota_check=false
```

要逐个对成员强制实施配额，使用此配置：

```
shc_role_quota_enforcement=false
shc_local_quota_check=true
```

有关这些设置的详细信息，请参阅 limits.conf。

对于默认行为的更改

在 6.5 版本中，对于强制实施基于用户和基于角色的并发搜索配额的默认行为进行了更改。

版本	默认强制实施
6.3-6.4	群集范围
6.5+	逐个成员

每一种方法都有它的优点。

群集范围强制实施的案例

当管理员分配搜索给成员时，没有考虑搜索用户。如果结合基于成员强制实施的配额，则可能会导致非预期的意外行

为。

逐个成员行为的其中一个结果是：如果管理员正好将特定用户的大部分搜索分配给一个群集成员，此成员可能会很快就达到此用户的配额上限，尽管其他成员并未达到此用户的上限。这种情况在基于角色的配额中也会出现。

例如，假设一个包含三个成员的群集对角色 X 的搜索并发配额设为 4。在某一时刻，其中两个成员正运行角色 X 的四个搜索，而另一个只运行两个。随后，计划程序要将角色 X 的一个新搜索分派给已经在运行四个搜索的其中一个成员。之后发生的动作取决于群集是对成员逐个实施还是对群集范围强制实施配额：

- 逐个对成员强制实施，成员会看到它已经达到角色 X 针对每个成员的并发上限 4。因此，该成员不会运行新的搜索。
- 对于群集范围的强制实施，成员会看到角色 X 在整个群集内的并发上限是 12（4 x 3 个成员），但目前正在运行的角色 X 的搜索只有 10（4 + 4 + 2 个）。因此，该成员会运行新的搜索。

逐个成员强制实施的案例

虽然群集范围的强制实施具有允许在群集成员集之间充分利用搜索并发配额的优势，但是它有可能会导致误判，从而引起在群集上搜索的过度订阅或订阅不足。

当管理员强制实施群集范围的用户和角色配额时，只会针对计划的搜索这样做。但是，当管理员强制实施群集范围的总搜索并发配额时，在其计算中会包括计划和临时搜索。

由于网络延迟问题可能会导致误判，因为管理员必须依靠每个成员将其正在运行的任何临时搜索通知它。如果成员对于管理员的响应很慢，管理员可能不知道有一些临时搜索，从而过度订阅群集。

同样，延迟会导致成员将搜索（计划或临时）完成通知给管理员速度很慢，导致管理员对群集订阅不足。

由于这些原因，您可能会发现，使用逐个成员强制实施的方法能更好地满足您的需求。

搜索头群集化和 KV 存储

KV 存储可以驻留在搜索头群集上。然而，搜索头群集不会协调 KV 存储数据的复制，或在 KV 存储的操作中包含它自己。有关 KV 存储的信息，请参阅*《管理员手册》*中的“关于 KV 存储”。

部署搜索头群集化

搜索头群集的系统要求和其他部署注意事项

搜索头群集**成员**的大多数系统要求与任意非群集搜索头相同。本主题详细介绍了搜索头群集的特定要求。

关键要求摘要

以下是关于群集成员配置需要注意的主要问题：

- 每个成员必须运行在它自己的计算机或虚拟机上，同时所有计算机必须运行相同的操作系统。
- 所有成员必须运行相同版本的 Splunk Enterprise。
- 所有成员必须连接到高速网络。
- 您必须部署至少与复制因子一样多的成员或者三个成员，以较大者为准。

除了群集成员之外，您需要 **Deployer** 将更新分发给成员。Deployer 必须运行在非成员实例上。在某些情况下，它可以运行在与**部署服务器**或**索引器群集**主节点相同的实例上。

关于这些和其他问题的详细信息，请参阅本主题的其余部分。

硬件和操作系统要求

群集成员的计算机要求

每个成员必须运行在它自己的、单独的计算机或虚拟机上。

计算机的硬件要求实际上与任一个 Splunk Enterprise 搜索头相同。请参阅《*容量规划手册*》中的“参考硬件”。主要的区别是需要增加存储空间来容纳更大的 dispatch 目录。请参阅“存储注意事项”。

Splunk 建议您为所有群集成员使用具有相同硬件规格的同等计算机。原因是**群集管理员**基于成员当前的工作负载给它们分配计划任务。当执行此操作时，它不会深入了解每个成员计算机的实际处理能力。相反，它假定每个计算机都是同等配置。

群集成员的操作系统要求

Splunk Enterprise 所有受支持的操作系统都能使用搜索头群集化。对于受支持的操作系统列表，请参阅*《操作手*

*册》*中的“系统要求”。

所有的搜索头群集成员和 Deployer 必须在相同的操作系统中运行。

如果搜索头群集连接至索引器群集中，则索引器群集实例必须和搜索头群集成员运行在同一个操作系统。

存储注意事项

当您为群集搜索头确定存储要求时，需要考虑为了处理**搜索项目**的复制副本而必须增加的容量。

为了实现存储评估的目的，在您的非群集环境中如果有搜索头的话，在您将其迁移到群集中之前，您可以观察其 dispatch 目录随时间的大小变化。计算跨所有非群集搜索头的 dispatch 目录的总大小，然后对于群集特定因子进行调整。

需要考虑的最重要的因子是**复制因子**。例如，如果复制因子为 3，您大约需要全部预群集存储总量的三倍，在群集成员中平均分布。

其他因子会进一步增加群集存储需求。一个关键因子是需要为节点失败进行计划。如果一个成员发生故障导致它的项目集（原始和副本）从群集中消失，进行修复活动来确保每一个项目再次拥有与复制因子匹配的全部完整的副本。在修复期间，驻留在故障成员上的副本会在剩余成员间进行复制，这增加了每个剩余成员的 dispatch 目录的大小。

其他问题也会增加每个成员基础上的存储要求。例如，群集不会确保跨成员间复制副本的绝对平等的分布。此外，对于一些搜索项目，群集可以拥有多于其复制因子数量的副本。请参阅“群集如何处理搜索项目”。

作为最佳做法，给每个成员的计算机配置实质上比预估需要的存储容量更多的容量。这样既允许未来的存储增长，也允许由故障的群集成员导致的临时存储增加。如果有任一个成员的磁盘空间不足，群集都将停止运行搜索。

Splunk Enterprise 实例要求

Splunk Enterprise 版本兼容性

您可以在版本 6.2 或更高版本的任意 Splunk Enterprise 实例组上实现搜索头群集化。

所有群集成员必须运行相同版本的 Splunk Enterprise，至少为维护等级。必须同时将所有成员升级至最新版本。例如，对于同一搜索头群集，不可以部分成员的版本为 6.3.2 而另一些成员的为 6.3.1。

注意：在搜索头群集升级期间，群集可以暂时包括运行以前版本的成员和运行新版本的成员。到升级过程结束时，所有成员必须再次运行相同的版本。只有从版本 6.4 或更高版本升级时才有效。请参阅“升级搜索头群集”。

搜索头群集可以对 5.x 或 6.x **搜索节点**运行。搜索头群集成员的级别必须高于或等于搜索节点的级别。有关搜索头和搜索节点间的版本兼容的详细信息，请参阅“版本兼容”。

重要提示：参与索引器群集活动的搜索头具有不同的兼容性限制。请参阅*《管理索引器和索引器群集》*中的“Splunk Enterprise 版本兼容性”。

许可要求

许可要求与任意搜索头的要求相同。请参阅《*管理员手册*》中的“Splunk Enterprise 许可证类型”。

所需实例数量

群集必须包含需要的最小数量成员来满足下面的两个要求：

- 三个成员，这样群集可以在一个成员发生故障时继续工作。请参阅“管理员选举过程影响部署”。
- 实例的复制因子数量。请参阅“为搜索头群集选择复制因子”。

例如，如果复制因子为 2 或 3，您需要至少三个实例。如果复制因子为 5，您需要至少五个实例。

您可以选择添加更多的成员来提高搜索和用户容量。

最大实例数量

搜索头群集化支持单个群集包含多达 50 个成员。

在多个站点中运行的搜索头群集

虽然当前对于多站点搜索头群集没有正式概念，但是您仍旧可以在多个站点中部署群集成员。

当在多个站点中部署群集时，请在站点上将您认为是主要的群集成员归为多数成员。这样就能确保只要主要站点正在运行，群集就能继续选举管理员，然后继续运行功能。请参阅“在多站点环境中部署搜索头群集。”

群集成员不能是搜索节点

群集成员不能是另一个搜索头的搜索节点。有关访问群集成员数据的推荐方法，请参阅"最佳做法：将搜索头数据转发到索引器层。"

网络要求

网络配置

所有成员都必须驻留在高速网络上，其中的每个成员都能访问任意其他成员。

这些成员不一定需要位于相同子网中，或者甚至在相同数据中心中（假定数据中心之间的连接速度很快）。您可以在 server.conf 中调整不同的搜索头群集超时设置。如在配置超时设置时需要帮助，请联系 Splunk 专业服务人员。

群集成员使用的端口

这些端口必须在每个成员上可用：

- 管理端口（默认为 8089）必须对所有其他成员可用。
- http 端口（默认为 8000）必须对所有访问成员数据的浏览器可用。
- KV 存储端口（默认为 8191）必须对所有其他成员可用。您可以使用 CLI 命令 `splunk show kvstore-port` 来确定端口号。
- **复制端口**必须对所有其他成员可用。

这些端口必须在防火墙的允许端口列表中。

警告：当任一个成员参与群集活动时，切勿更改它的管理端口。如果您需要更改管理端口，必须首先从群集中删除该成员。

跨分布式搜索环境同步系统时钟

在所有参与分布式搜索活动的运行 Splunk Enterprise 实例的虚拟或物理的计算机上同步系统时钟很重要。尤其是，这表示您的群集成员和搜索节点。否则，可能出现各种问题，例如搜索失败、搜索项目的过早失效或问题告警。

使用的同步方法取决于计算机的具体设置。请查阅运行 Splunk Enterprise 的特定计算机和操作系统的系统文档。对于大多数环境，网络时间协议 (NTP) 是最佳方法。

Deployer 要求

您需要一个作为 **Deployer** 工作的 Splunk Enterprise 实例。Deployer 更新成员配置。请参阅"使用 Deployer 分布应用和配置更新"。

重要提示：切勿将 Deployer 功能置于任一个搜索头群集成员上。Deployer 必须运行来自任何群集成员的单独实例。

虽然 Deployer 功能只用于搜索头群集，但是它内置在所有运行 6.2 或以上版本的 Splunk Enterprise 实例中。Deployer 的处理要求相对比较简单，因此您可以经常将 Deployer 功能共存于执行其他功能的实例上。对于要运行 Deployer 的实例，您有以下几个选项：

- 如果您的部署服务器仅服务少量的部署客户端（不超过 50 个），则您可以在与部署服务器相同的实例中运行 Deployer。在客户端计数较大时，Deployer 和部署服务器功能可能会互相妨碍。请参阅*《更新 Splunk Enterprise 实例》*中的"部署服务器配置"。
- 如果您正在运行一个索引器群集，则可以在与索引器群集主节点相同的实例上运行 Deployer，这取决于主节点负载。此选项是否适用于您取决于主节点的负载。有关群集主节点负载限制的信息，请参阅*《管理索引器和索引器群集》*中的"主节点的其他角色"。
- 如果您有监视控制台，则您可以在相同的实例中运行 Deployer。请参阅*《监视 Splunk Enteprise》*中的"哪个实例应托管控制台？"。
- 如果没有上述枚举的实例类型，则在专用 Splunk Enterprise 实例中运行 Deployer。

一个 Deployer 只能服务一个单独的搜索头群集。如果您有多个群集，则必须为每个群集使用一个单独的 Deployer。Deployer 必须在单独的实例中运行。

其他注意事项

部署服务器和搜索头群集

切勿使用部署服务器更新群集成员。

不支持通过部署服务器将配置或应用分发到群集成员。要在成员集中分发配置，必须使用搜索头群集 deployer。请参阅"使用 Deployer 分布应用和配置更新"。

搜索头群集和搜索头合并

您不能在作为**搜索头池**一部分的实例上启用搜索头群集。有关迁移的信息，请参阅"从搜索头池迁移到搜索头群集"。

部署搜索头群集

本主题包括配置和启动搜索头群集所需要的主要步骤。

搜索头群集的各个部分

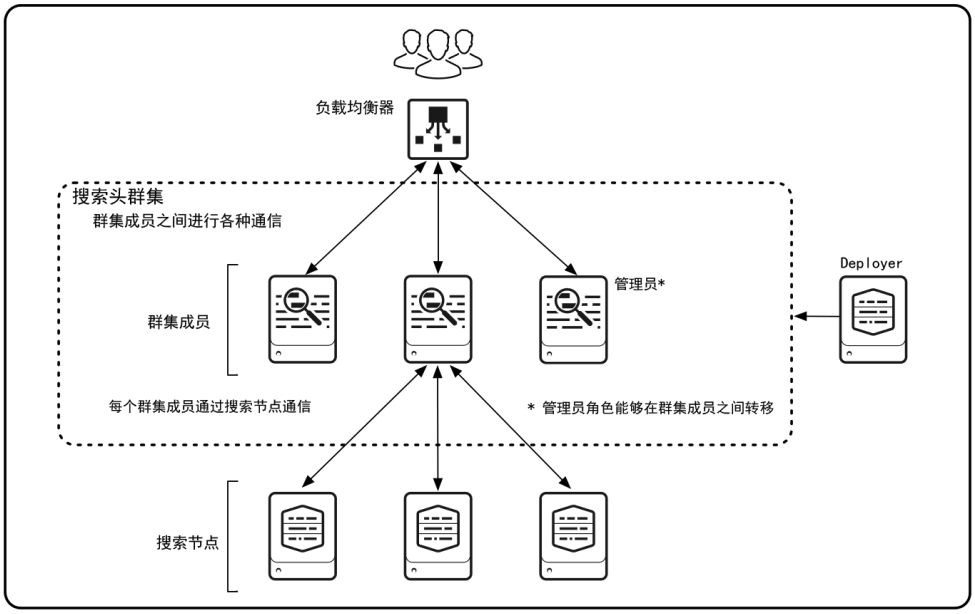
搜索头群集由一组共享配置、任务计划和**搜索项目**的**搜索头**组成。搜索头称为**群集成员**。

一个群集成员具有**管理员**角色，这意味着它会在所有成员中协调任务和复制活动。像其他成员一样，它也作为一个搜索头运行搜索任务、提供结果等等。随着时间的推移，管理员的角色可以在群集成员间转移。

除了组成实际群集的搜索头成员组外，一个工作中的群集还需要若干其他的组件：

- **Deployer。**这是一个给群集成员分布应用和其他配置的 Splunk Enterprise 实例。它位于群集之外，不能在与群集成员相同的实例上运行。然而，在某些情况下，它可以驻留在其他 Splunk Enterprise 组件相同的实例上，例如部署服务器或索引器群集主节点。
- **搜索节点。**这些是群集成员在其中运行搜索的索引器。搜索节点可以是独立索引器或索引器群集中的节点。
- **负载均衡器。**这是可选择驻留在用户和群集成员间的第三方软件或硬件。通过放置的负载均衡器，用户可以通过单个界面访问搜索头集，而无需指定某个搜索头。

这幅小型搜索头群集（由三个成员组成）图介绍了不同的组件和它们间的关系：



本主题侧重于设置群集成员和 Deployer。本章节中的其他主题介绍如何配置搜索节点、与索引器群集连接和添加负载均衡器。

部署群集

以下是部署群集的主要步骤：

1.确定您的要求。

2.设置 Deployer。

3.安装 Splunk Enterprise 实例。

4.初始化群集成员。

5.启动群集管理员。

6.执行部署后设置。

1.确定您的要求

a. 确定群集大小，即想在群集中包含的搜索头数量。通常，明智的做法是将您所有的搜索头置于单个群集中。影响群集大小的因子包括预计的搜索负载和并发用户的数量，以及可用性和故障转移需求。请参阅"关于搜索头群集化"。

b. 决定您要实现的**复制因子**。复制因子是指群集保留的搜索项目副本的数量。优化复制因子取决于环境的特定因素，但实际上涉及故障容错与存储容量的权衡。较高的复制因子表示更多的搜索项目副本将驻留在更多的群集成员上，因此您的群集可以容许更多的成员故障，而不需要使用代理来访问搜索项目。但还表示您将需要更多的存储来处理其他副本。请参阅"为搜索头群集选择复制因子"。

c. 确定搜索头群集是否针对独立索引器组或索引器群集运行。有关索引器群集的信息，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"。

d. 学习"搜索头群集的系统要求和其他部署注意事项"主题，以了解有关其他关键问题的信息。

2.设置 Deployer

建议您现在选择 Deployer 作为群集设置的一部分，因为在您对于群集成员分发应用和更新配置之前您需要位置就绪的 Deployer。

a. 为 Deployer 功能选择 Splunk Enterprise 实例。

此实例不能是搜索头群集的成员，但是在一些情况下，它可以是用作其他目的的 Splunk Enterprise 实例。如有必要，安装新的 Splunk Enterprise 实例作为 Deployer。请参阅"Deployer 要求"。

如果您有多个群集，则必须为每个群集使用一个单独的 Deployer，除非您在所有的群集之间部署相同的配置。请参阅"部署到多个群集"。

在所有 Splunk Enterprise 实例上自动启用 Deployer 功能。主要配置步骤是指定 Deployer 的安全密钥，具体会在下一步中介绍。在部署过程的后续部分，您可以在此 Deployer 实例中指定群集成员，这样它们就可以访问此实例。

有关如何使用 Deployer 给群集成员分布应用的信息，请参阅"使用 Deployer 分布应用和配置更新"。

b. 配置 Deployer 的安全密钥。

请参阅"为搜索头群集设置安全密钥"。

Deployer 使用安全密钥对与群集成员的通信进行验证。群集成员也使用它来相互验证。您必须在所有群集成员和 Deployer 上为密钥设置相同的值。在初始化群集成员的时候在其上设置密钥。

要设置 Deployer 的密钥，指定 `pass4SymmKey` 属性（在 `[general]` 或 `[shclustering]` 段落中指定；该段落位于 Deployer 的 `server.conf` 文件中）。例如：

```
[shclustering]
pass4SymmKey = yoursecuritykey
```

c. 在 Deployer 上设置搜索头群集标签。

搜索头群集标签用于确认监视控制台中的群集。此参数可选，但是如果您在某一个成员中将其配置，则必须在所有成员中，以及 Deployer 里面使用相同的数值配置。

要设置标签，指定 `shcluster_label` 属性（在 `[shclustering]` 段落中指定；该段落位于 Deployer 的 `server.conf` 文件中）。例如：

```
[shclustering]
shcluster_label = shcluster1
```

请参阅《*监视 Splunk Enterprise*》中的"设置群集标签"。

d. 重新启动 Deployer 激活配置更改。

3.安装 Splunk Enterprise 实例

安装将用作群集成员的 Splunk Enterprise 实例。有关所需成员的最小数量，请参阅"所需实例数量"。

警告：始终使用新实例。向搜索头群集中添加实例的过程会覆盖当前驻留在实例上的任意配置或应用。

有关如何安装 Splunk Enterprise 的信息，请阅读《*安装手册*》。

重要提示：您必须更改每一个实例的管理员密码。用来配置群集的 CLI 命令不能在使用默认密码的实例上执行。

4.初始化群集成员

对于想包括在群集中的每一个实例，运行 `splunk init shcluster-config` 命令并重新启动实例：

```
splunk init shcluster-config -auth <username>:<password> -mgmt_uri <URI>:<management_port> -replication_port
<replication_port> -replication_factor <n> -conf_deploy_fetch_url <URL>:<management_port> -secret <security_key> -
shcluster_label <label>

splunk restart
```

请注意以下事项：

- 此命令仅用于群集成员。请勿在 Deployer 运行此命令。
- 您只能在已启动并运行的实例上执行此命令。
- 对于此实例，`-auth` 参数指定您当前的登录凭据。此参数为必需项。
- `-mgmt_uri` 参数指定此实例的 URI 和管理端口。必须使用完全限定域名。此参数为必需项。
- `-replication_port` 参数指定实例用于侦听来自其他群集成员的搜索项目流的端口。您可指定任一一个可用的、未使用的端口作为复制端口。请勿重复使用实例的管理或接收端口。此参数为必需项。
- `-replication_factor` 参数确定群集保留的每个搜索项目副本的数量。所有群集成员必须使用相同的复制因子。此参数可选。如果未显式设置，复制因子默认为 3。
- `-conf_deploy_fetch_url` 参数指定 Deployer 实例的 URL 和管理端口。此参数在初始化期间是可选项，但是在您使用 Deployer 功能之前需要设置它。请参阅"使用 Deployer 分布应用和配置更新"。
- `-secret` 参数指定用于验证群集成员间和每个成员与 Deployer 间通信的安全密钥。所有群集成员和 Deployer 的密钥必须相同。请参阅"为搜索头群集设置安全密钥"。

  重要提示：

- `-shcluster_label` 参数用于确认监视控制台中的群集。此参数可选，但是如果您在某一个成员中将其配置，则必须在所有成员中，以及 Deployer 里面使用相同的数值配置。请参阅*《监视 Splunk Enterprise》*中的"设置群集标签"。

例如：

```
splunk init shcluster-config -auth admin:changed -mgmt_uri https://sh1.example.com:8089 -replication_port 34567 -
replication_factor 2 -conf_deploy_fetch_url https://10.160.31.200:8089 -secret mykey -shcluster_label shcluster1

splunk restart
```

警告：要在步骤 5 中引导管理员之后添加更多成员，您必须遵照"添加群集成员"中的程序执行操作。

5.启动群集管理员

a. 选择初始化实例之一作为首个群集管理员。选择哪个实例作为此角色都没有关系。

b. 在所选择的实例上运行 `splunk bootstrap shcluster-captain` 命令：

```
splunk bootstrap shcluster-captain -servers_list "<URI>:<management_port>,<URI>:<management_port>,..." -auth
<username>:<password>
```

请注意以下事项：

- 此命令将指定的实例作为首个群集管理员。
- 仅在单个实例上运行此命令。
- `-servers_list` 参数包含群集成员的逗号分隔的列表，表中包括您正在运行命令的成员。成员通过 URI 和管理端口进行标识。此参数为必需项。
- **重要提示：**在 `-servers_list` 中指定的 URI 必须与您之前初始化每个成员时在 `-mgmt_uri` 参数中指定的值完全相同。例如，不能在初始化期间使用 `https://foo.example.com:8089` 而这里使用 `https://foo.subdomain.example.com:8089`，即使他们会解析到相同的节点。

下面是一个 bootstrap 命令的示例：

```
splunk bootstrap shcluster-captain -servers_list
"https://sh1.example.com:8089,https://sh2.example.com:8089,https://sh3.example.com:8089,https://sh4.example.com:8089"
-auth admin:changed
```

6.执行部署后设置

要完成设置，执行下面额外的步骤（如有必要）：

a. 连接搜索头群集与搜索节点。需要此步骤。它根据搜索节点是否驻留在索引器群集中而有所不同：

- 要连接搜索头群集与索引器群集，请参阅"通过索引器群集集成搜索头群集"。

- 要连接搜索头群集与非群集索引器，请参阅“连接群集中的搜索头与搜索节点”。

b. 添加用户。需要此步骤。请参阅“添加用户到搜索头群集中”。

c. 在搜索头前面安装负载均衡器。本步骤可选。请参阅“对搜索头群集使用负载均衡器”。

d. 使用 Deployer 为搜索头分布应用和配置更新。在升级配置组之前必须执行此步骤。请参阅“使用 Deployer 分布应用和配置更新”。

检查搜索头群集状态

要检查搜索头群集的总体状态，对于任意成员运行此命令：

```
splunk show shcluster-status -auth <username>:<password>
```

此命令返回管理员和群集成员的基本信息。它指示每个成员的状态（正常或故障）。

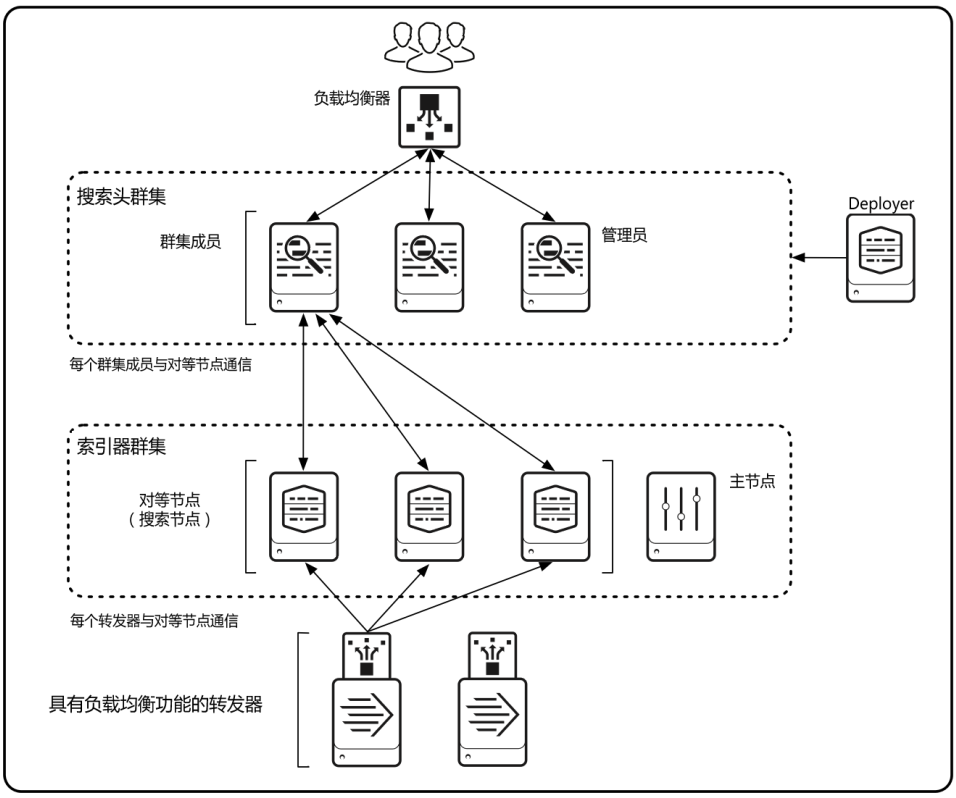
您还可以通过监视控制台了解群集状态的更多信息。请参阅“使用监视控制台查看搜索头群集状态和解决问题”。

集成搜索头群集和索引器群集

要集成搜索头群集和**索引器群集**，您必须配置搜索头群集的每个成员作为索引器群集的搜索头。在执行此操作之后，搜索头会从索引器群集的主节点上获得**搜索节点**列表。

您可以通过单站点或者多站点索引器群集来集成搜索头群集。

本图中搜索头群集在单站点索引器群集中执行搜索：



使用单站点索引器群集以集成

将每个搜索头群集成员配置为索引器群集中的搜索头。使用 CLI `splunk edit cluster-config` 命令。例如：

```
splunk edit cluster-config -mode searchhead -master_uri https://10.152.31.202:8089 -secret newsecret123

splunk restart
```

该示例指定：

- 此实例是索引器群集中的搜索头。
- 索引器群集的主节点驻留在 `10.152.31.202:8089` 上。
- 密钥为 "newsecret123"。您必须在索引器群集和搜索头群集的所有节点上使用相同的密钥。

必须为搜索头群集的每个成员执行此操作。

这是所有您需要的基本配置。搜索头现在针对索引器群集上的搜索节点运行搜索。

使用多站点索引器群集以集成

在**多站点索引器群集**中，每个搜索头和索引器都有已分配的站点。多站点索引器群集提升灾难恢复的功能，因为数据在多个站点之间分配。比如，您可能配置两个站点，一个在 Boston，另一个在 New York。如果一个站点故障，则数据仍旧可以通过另外一个站点访问。请参阅“多站点索引器群集”。

注意：虽然搜索头群集能够参与多站点索引器群集，但是搜索头群集本身没有站点意识。请参阅“在多站点环境中部署搜索头群集。”

配置成员

要使用多站点索引器群集来集成搜索头群集成员，请将每个成员配置为索引器群集中的搜索头，如单站点示例中所述。唯一的差别就是您必须还要为每个成员指定站点。这一般应该是 "site0"，所以群集中所有的搜索头都在相同的一组索引器之间执行它们的搜索。例如：

```
splunk edit cluster-config -mode searchhead -site site0 -master_uri https://10.152.31.202:8089 -secret newsecret123

splunk restart
```

相关信息

有关索引器群集中的搜索头配置的更多信息，请参阅《*管理索引器和索引器群集*》手册中的“配置搜索头”章节。此章节也包括更复杂情况的配置，例如混合搜索（搜索头跨索引器群集和非群集索引器搜索）。

连接群集中的搜索头与搜索节点

在群集中的搜索头运行搜索之前，它们需要了解索引器或**搜索节点**的标识符。群集的所有成员必须访问相同的搜索节点集。

搜索头如何找到它们的搜索节点取决于搜索头群集是否是**索引器群集**的一部分。需要考虑两种情况：

- 搜索头群集在索引器群集上运行。
- 搜索头群集在单个的非群集索引器上运行。

重要提示：群集成员不能给其他群集成员分发搜索。换句话说，群集成员不能是群集的搜索节点。

索引器群集上的搜索头群集

如果搜索头群集与索引器群集连接，索引器群集的主节点给搜索头提供能运行搜索的对等节点列表。

在您配置搜索头群集成员以便它们参与索引器群集活动之后，您不需要为搜索头执行任何进一步的配置来了解它们的搜索节点。请参阅通过索引器群集集成搜索头群集。

即使您不需要索引复制的益处，您仍然可以利用这个简单的方法来配置搜索节点集。仅整合您的索引器集与复制因子为 1 的索引器群集。从管理的角度看，这种拓扑结构还提供了许多其他好处。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”。

非群集索引器上的搜索头群集

有两种方式可以添加非群集搜索节点：

- 分别添加搜索节点到每个成员。
- 添加搜索节点到一个成员，然后让群集复制此对等节点配置到其他所有群集成员。这个过程称为**“搜索节点复制”**。

在 Splunk Enterprise 6.4 版本之前，可用的方式只有一种。您必须为每个成员分别添加搜索节点。从 6.4 版本开始，您可以只为一个成员添加搜索节点，然后让群集将此对等节点配置复制到其他成员。

复制的方式一般来说更为可取，因为：

- 过程更简单快捷。
- 可确保所有成员均能访问所有对等节点。
- 如果您后续添加新成员到群集时，它会自动获取完整的对等节点集。

较适用于为单个成员添加节点的主要场景是，您已经有了一个群集，而且已经采用自动添加搜索节点到每个成员的方式。

您可随时切换为复制方式。已经分别添加到单个成员的节点配置仍会保留。当后续添加新成员时，它会获取完整的对等节点集，而不管这些节点最初添加到群集时采用的是哪种方式。

注意：复制方式使用的并不是群集复制的配置更新中所描述的配置复制方式。而是使用 Raft 状态机将所有变更复制到所有活跃的成员。这种方式使所有活跃的成员同时接收到添加请求，确保所有成员都可以访问同一个搜索节点集。

在整个群集内复制搜索节点

1.为每个成员启用搜索节点复制。

在每个成员的 `server.conf` 文件中，配置 `[raft_statemachine]` 段落，如下所示：

```
[raft_statemachine]
disabled = false
replicate_search_peers = true
```

2.重新启动每个搜索头群集成员。

3.通过 CLI 添加搜索节点到一个成员。这里选择对哪个成员执行此操作都没有关系。

在一个成员上，运行以下命令，一次针对一个搜索节点：

```
splunk add search-server <scheme>://<host>:<port> -auth <user>:<password> -remoteUsername <user> -remotePassword
<passremote>
```

请注意以下事项：

- <scheme> 是访问该搜索节点的 URI 方案："http" 或 "https"。
- <host> 指搜索节点主机的主机名称或 IP 地址。
- <port> 指搜索节点的管理端口。
- `-auth` 提供该成员的凭据。
- `-remoteUsername` 和 `-remotePassword` 提供该搜索节点的凭据。远程凭据必须支持搜索节点上具有管理级权限的用户。

例如：

```
splunk add search-server https://192.168.1.1:8089 -auth admin:password -remoteUsername admin -remotePassword
passremote
```

当添加一个搜索节点到一个群集成员时，此群集会快速复制此操作到其他的成员。这些成员随后会一起提交更改。

重要提示：要通过复制添加对等节点，必须要有一个运行状况良好的群集。在所有活跃的成员成功提交更改之前，扮演管理员角色的成员须保持不变。如果遇到问题或更改没能通过当前管理员成功提交，纠正措施很简单：只要重新运行 `splunk add search-server` 命令。

4.为每个搜索节点重复运行 `splunk add search-server` 命令。

注意：也可以通过复制方式将搜索节点从群集成员中删除。请参阅通过 CLI 删除搜索节点。

分别添加搜索节点到每个成员

要将搜索节点分别添加到每个搜索头，使用 CLI。有每个搜索头上，为要添加的每个搜索节点调用 `splunk add search-server` 命令：

```
splunk add search-server <scheme>://<host>:<port> -auth <user>:<password> -remoteUsername <user> -remotePassword
<passremote>
```

您必须在每个搜索头上为每个搜索节点重复一次此过程。例如，对一个有三个成员、五个搜索节点的群集，必须一共运行此命令 15 次。

警告：所有搜索头必须使用相同的搜索节点集。

通过 Splunk Web 添加搜索节点

除了 CLI 之外，您还可以通过 Splunk Web 添加搜索节点：

1.取消隐藏搜索头的隐藏设置，如设置菜单中所述。

2.遵循使用 Splunk Web 中的说明。

如果启用了搜索节点复制，您可以将搜索节点只添加到其中一个群集成员。如果没有启用搜索节点复制，则必须将他们添加到每一个群集成员。

通过直接编辑 distsearch.conf 的方式添加搜索节点

如果没有使用搜索节点复制，您可以直接编辑 `distsearch.conf` 并通过 Deployer 分发配置文件，以这种方式来添加搜索节点。此方式要求您也要手动将密钥文件从每个搜索头分发到每个搜索节点。请参阅编辑 distsearch.conf。

由于需要手动分发密钥文件，此方式与搜索节点复制不兼容。

将搜索头数据转发给搜索节点

我们认为最佳的做法是，将所有搜索头内部数据转发到搜索节点（索引器）层。在您连接搜索头与搜索节点之后，请遵循最佳做法：将搜索头数据转发到索引器层。

添加用户到搜索头群集中

在搜索头群集中，所有群集成员应保持相同的用户集和相同的角色集。

要添加用户到搜索头群集，可以采用任意一种可用的验证方式：Splunk Enterprise 内置验证、LDAP、SAML 或脚本式验证。有关详细信息，请参阅*《确保 Splunk Enterprise 安全》*手册中有关验证的章节。

大部分情况下，群集会自动在成员组内同步用户配置。群集通过配置复制来做到这一点。请参阅"群集复制的配置更新"。

使用 Splunk Enterprise 内置验证

对于 Splunk Enterprise 内置验证，您可以使用 Splunk Web 或 CLI 来添加用户和映射角色。在任意一个群集成员上执行此操作。然后，此群集会通过复制 `$SPLUNK_HOME/etc/passwd` 文件自动将更改分发给所有成员。

验证限制

搜索头群集化对于如何配置验证有一些限制：

- 只有当您通过 Splunk Web、CLI 或 REST 端点配置了验证，群集才会自动复制配置变更。相反，如果您是通过直接编辑配置文件的方式，则必须使用 Deployer 将配置文件分发给所有群集成员。
- 即使您通过 Splunk Web、CLI 或 REST 端点配置了验证，群集也只会复制基本配置文件，以及 `$SPLUNK_HOME/etc/passwd` 文件（仅对于内置验证）。如果所采用的验证方式要求任何其他相关的非配置文件，则必须使用 Deployer 将这些文件分发给群集成员。例如：
  - 对于 SAML，必须使用 Deployer 推送证书。
  - 对于脚本式验证，必须使用 Deployer 推送脚本。您必须使用 Deployer 来推送 `authentication.conf`，因为通过直接编辑 `authentication.conf` 的方式只能配置脚本式验证。

如何使用 Deployer 推送验证文件

要通过 Deployer 推送任意文件组，如 SAML 证书，您需要创建一个应用目录来专门存放这些文件。

有关如何使用 Deployer 推送文件的详细信息，请参阅"使用 Deployer 分布应用和配置更新"。

对搜索头群集使用负载均衡器

Splunk 建议您在群集的搜索头集的前面运行第三方硬件或软件负载均衡器。通过这种方式，用户可以通过单个界面访问搜索头集，而无需指定某个搜索头。

有多种第三方负载均衡器可用于此目的。选择采用 7 层（应用程序级别）处理的负载均衡器。

配置负载均衡器，以便用户会话"粘住"或"持续"。这可确保用户在整个会话期间保持在单个搜索头上。

在多站点环境中部署搜索头群集

您可以在多个物理站点之间部署搜索头群集成员。您可以将群集成员集成至多站点索引器群集中。然而，搜索头群集并没有站点意识。

在多个物理站点之间部署搜索头群集

对于群集成员可以驻留的位置没有限制。然而，如果站点之间出现较长的网络延迟，则您可能会发现 UI 响应能力变

得缓慢。

群集成员在网络中互相传输的数据量很难量化，具体取决于因素的种类，如用户数量、用户活动量、正在运行的搜索数量和类型等等。

通过多站点索引器群集以集成搜索头群集

您可以将搜索头群集成员集成至多站点索引器群集中。多站点索引器群集在您部署时具有重要的优势。最重要的是它能够增强部署的高可用性和灾难恢复能力。请参阅*《管理索引器和群集》*手册中的“多站点索引器群集”。

要通过多站点索引器群集以集成搜索头群集，请将每个成员配置为多站点群集中的搜索头。请参阅“使用多站点索引器群集以集成。”

建议您将搜索头的 `site` 属性设置为 "site0"，以禁用**搜索相关性**。当禁用搜索相关性时，搜索头跨所有站点在索引器之间运行其搜索。除了可用索引器组的更改，搜索头每次都会在相同组的主要数据桶副本之间运行其搜索。

通过将所有搜索头设置为 "site0"，可确保为终端用户提供无缝体验，因为所有搜索头都使用同样一组主要数据桶副本。相反，如果您将不同的搜索头设置为不同的站点，则终端用户可能在获取某些结果时注意到延迟时间，具体取决于正好运行特殊搜索的搜索头是哪个。

如果您对于搜索相关性具有覆盖需求，则可以将搜索头分配到特定站点。

搜索头群集并没有站点意识

和索引器群集不同的是，搜索头群集缺乏站点意识：

- 您无法按站点逐个配置项目复制。
- 群集无法保证每个搜索项目的副本存在于每个站点中。

对于搜索头群集，站点意识没有像索引器群集那样关键。如果搜索头群集成员丢失搜索项目的复制副本，则群集会从驻留在相同站点或不同站点的其他成员中将其代理。请参阅“群集如何处理搜索项目”。即使因站点故障导致某些搜索项目所有副本的损失，这里还有其他可以管控的情形，即您可以通过再次运行搜索对此进行恢复等。

注意：如有必要，这边还有几个解决站点意识缺乏的方法。比如，如果您的搜索头群集由四个搜索头构成，并且在两个站点中进行平均分配，则您可以将复制因子设置为 3，因而确保每个站点对于每个搜索项目至少具有一个副本。

在多个站点之间部署搜索头群集时的重要考虑事项

在多个站点之间部署搜索头群集时，您所作出的选择对于这些故障方案具有重要的影响：

- 站点故障
- 网络中断

特别是，如果遇到双站点群集时，您应当将多数成员置于您认为是主要的站点上。

为何多数成员应该位于主要站点

当在两个站点之间部署群集时，请将多数群集成员置于您认为是主要的站点上。这样就能确保只要站点正在运行，群集就能继续运行功能。

在某些情况下，如当成员离开或加入群集时，群集会进行选举，以选择新的管理员。为了保证此选举过程能够成功，需要所有群集成员的大多数人能够同意新管理员。因此，群集的功能正常运行需要多数成员能够一直保持运行状态。请参阅“管理员选举”。

当群集在两个站点之间运行，如果其中一个站点故障，则只要另外一个站点具有大多数成员，则就能选举一个新的管理员。类似地，如果在站点间存在网络干扰，只有具有多数节点的站点会选举新管理员。通过将多数成员分配至您的主要站点，您可以最大化其可用性。

当具有多数成员的站点故障会发生什么情况

如果具有多数成员的站点故障，则具有少数成员的站点无法选举新管理员。管理员选举需要多数成员的投票，但只有少数成员正在运行。群集无法运行功能。请参阅“无功能群集的运行后果”。

要矫正此状况，您可以在具有少数成员的站点上临时部署一个**静态管理员**。一旦多数成员站点返回，则应该将少数成员站点转换为**动态管理员**。请参阅“使用静态管理员，以从丧失多数优势的状态中恢复。”

当两个站点之间网络中断时会发生什么情况

如果两个站点之间的网络故障，则每个站点上的成员将尝试选举一名管理员。然而，只有具有大多数成员的站点才能成功。该站点可以继续无限期地充当群集。

在此期间，其他站点的成员能够继续充当独立的搜索头。然而，他们只能服务于临时搜索。计划报表和警告将不再运行，因为在群集中，计划功能降级为管理员。

当其他站点重新连接到多数成员站点，则他们的成员将重新加入群集中。关于当成员重新加入群集中时将发生的情况，请参阅"当成员重新加入群集中时"。

带有两个以上站点的群集

如果站点超过两个，则只有当站点之间的多数成员仍旧可以通信并选举管理员时，群集才能运行功能。比如，如果您的站点 1 有五位成员，站点 2 有八位成员，站点 3 有四位成员，则上述站点中的任何一个损失都不会影响到群集，因为您在剩余两个站点中仍旧有一个多数成员（至少是九位成员）。然而，如果站点 1 有六位成员，站点 2 有两位成员，而站点 3 有三位成员，则只要站点 1 仍旧处于活动状态，群集就仍旧能够运行功能，因为您至少需要六位成员来构建一个多数成员群体。

从搜索头池迁移到搜索头群集

您可以从搜索头池将设置迁移到搜索头群集。然而，您不能迁移搜索头实例本身。当启用搜索头群集成员的时候，您必须使用新的实例。

迁移过程会稍有不同，这取决于您是向新群集还是运行中的群集中迁移。

要迁移的对象类型

要迁移的对象有两种类型：

- 自定义应用配置。这些都将在搜索头池的共享存储区域中的 `etc/apps` 下面生成。
- 专属用户配置。这些都将在搜索头池的共享存储区域中的 `etc/users` 下面生成。

在这两种情况下，您将相关目录从搜索头池的共享存储区域复制到搜索头群集的 Deployer。然后您可以使用 Deployer 来将这些目录传输给群集成员。

Deployer 针对每个类型使用不同的方法将配置推送到群集中。迁移后，应用配置遵照来自用户配置的不同规则。

关于已部署设置在群集成员中驻留的位置信息，请参阅"已部署配置在群集成员的位置"。

自定义应用配置

当迁移一个应用自定义设置时，Deployer 将其置于群集成员的默认目录中。这就包含应用在搜索头池中运行时的任何运行时更改。

因为用户无法在默认目录中更改设置，所以这就意味着用户无法在这些已迁移实体中执行某些运行时操作：

- 删除。用户无法删除任何已迁移实体。
- 移动。用户无法将这些设置从一个应用移动到另外一个。
- 更改共享等级。用户无法更改共享等级。比如，用户无法将共享从应用等级更改为专属。

群集用户可以通过在相应位置编辑实体来覆盖现有属性。运行时更改将会放入群集成员的本地目录中。本地目录覆盖默认目录，因而更改也将覆盖默认设置。

专属用户配置

Deployer 将仅复制用户配置到管理员。然后管理员将通过一般复制配置的方式将设置复制到所有群集成员，如"群集复制的配置更新"中所述。

与自定义应用配置不同的是，用户配置驻留在群集成员的标准用户位置，并且能够在未来删除、移动和进行其他操作。他们的行为只是如同通过 Splunk Web 群集用户所创造的任何运行时设置。

当您将用户配置迁移到现有的搜索头群集中时，Deployer 将正确处理已存在于群集中的段落。它不会覆盖任何现有的段落。

比如，假设群集成员已经具有包含此段落的文件 `$SPLUNK_HOME/etc/users/admin/search/local/savedsearches.conf`：

```
[my search]
search = index=_internal | head 1
```

同时在 Deployer 中也有包含这些段落的文件 `$SPLUNK_HOME/etc/shcluster/users/admin/search/local/savedsearches.conf`：

```
[my search]
search = index=_internal | head 10
enableSched = 1
```

```
[my other search]
search = FOOBAR
```

这将为以下成员提供最终合并配置：

```
[my search]
search = index=_internal | head 1

[my other search]
search = FOOBAR
```

如果各成员已经具有 `[my search]` 段落，则此段落保持现有设置，而不采用迁移过来的设置。如果各成员还没有 `[my other search]` 段落，则此段落会添加到文件中。

注意：Splunk 并不支持针对每个用户搜索历史文件的迁移。

请勿迁移默认应用

当您将应用迁移到搜索头群集时，不会迁移任何默认应用，即 Splunk Enterprise 附带的应用，例如搜索应用。如果您将默认应用推送给群集成员，会覆盖驻留在成员上的那些应用的版本，您不会希望执行此操作。

然而，您可以通过移动并全局导出的方式将自定义设置动默认应用迁移到新应用。

本主题中每个迁移程序都包含迁移默认应用自定义设置的步骤。

向新搜索头群集迁移

从搜索头池将设置迁移到新的搜索头群集：

1.遵循部署任一个新搜索头群集的过程。在您初始化群集成员的时候指定 Deployer 位置。请参阅"部署搜索头群集"。

警告：您必须部署新实例。您不能重复使用现有的搜索头。

2.将搜索头池中的共享存储位置上的 `etc/apps` 和 `etc/users` 目录复制到 Deployer 实例上的分发目录。分发目录位于 `$SPLUNK_HOME/etc/shcluster` 中。

有关分发目录文件结构的详细信息，请参阅"如何放置 Deployer 的配置软件包"。

3.如果您想要将自定义设置从默认应用中迁移，则您可以将其移动到新应用并全局导出。比如，要从搜索应用中迁移设置 ：

a. 将分发目录中的 `.../search/local` 目录复制到新应用目录，如分发目录中的 `search_migration_app`。**不要对此新应用"搜索"进行命名。**

b. 全局导出这些设置并使它们对所有应用可用，包括搜索应用。要实现这一点，请创建一个 `.../search_migration_app/metadata/local.meta` 文件并使用如下内容进行填充：

```
[]
export=system
```

详细信息请参阅 default.meta 规范文件。

4.如果 `$SPLUNK_HOME/etc/shcluster/apps` 包含任何默认应用，例如搜索应用，则必须马上删除。切勿将它们推送给群集成员。如果推送了默认应用，它们会覆盖已经在成员上运行的那些应用的版本。

5.在 Deployer 中运行 `splunk apply shcluster-bundle` 命令以推送配置软件包到群集中。请参阅"推送配置软件包"。

Deployer 直接将 `etc/apps` 推送到群集成员。它将 `etc/users` 推送给管理员，然后管理员将设置异步复制给其他群集成员。

注意：如果您在之前搜索头池使用的相同搜索节点集上指定群集成员，群集需要重新构建驻留在搜索节点上的报表加速摘要或数据模型摘要。此操作会自动执行。然而，不会自动删除旧的摘要集。

向现有搜索头群集迁移

要将设置从搜索头池迁移到现有的搜索头群集：

1.将搜索头池中的共享存储位置上的 `/etc/apps` 和 `etc/users` 目录复制到可编辑的临时目录。

2.如果您想要将自定义设置从默认应用中迁移，则您可以将其移动到新应用并全局导出。比如，要从搜索应用中迁移设置 ：

a. 将临时目录中的 `.../search/local` 目录复制到新应用目录，如临时目录中的 `search_migration_app`。**不要对此新应用“搜索”进行命名。**

b. 全局导出这些设置并使它们对所有应用可用，包括搜索应用。要实现这一点，请创建一个 `.../search_migration_app/metadata/local.meta` 文件并使用如下内容进行填充：

```
[]
export=system
```

详细信息请参阅 default.meta 规范文件。

3. 在临时目录中，删除这些子目录：

- 任何默认应用，例如搜索应用。切勿将默认应用推送给群集成员。如果推送了默认应用，它们会覆盖已经在成员上运行的那些应用的版本。
- 已经在 Deployer 分发目录中存在的任何应用。否则，搜索头池上运行的版本会覆盖已经在成员上运行的版本。

4. 将余下的子目录从临时位置复制到位于 `$SPLUNK_HOME/etc/shcluster` 的 Deployer 的分发目录。保持已经在分发目录中存在的子目录不变。

有关分发目录文件结构的详细信息，请参阅“如何放置 Deployer 的配置软件包”。

5. 在 Deployer 中运行 `splunk apply shcluster-bundle` 命令以推送配置软件包（包括迁移设置）到群集中。请参阅“推送配置软件包”。

Deployer 直接将 `etc/apps` 推送到群集成员。它将 `etc/users` 推送给管理员，然后管理员将设置异步复制给其他群集成员。

注意：如果您在之前搜索头池使用的相同搜索节点集上指定群集成员，群集需要重新构建驻留在搜索节点上的报表加速摘要或数据模型摘要。此操作会自动执行。然而，不会自动删除旧的摘要集。

搜索头群集和安装软件包

对于大多数部署类型（包括搜索头群集），Splunk 建议您使用普通软件包复制，而不是带有共享存储的安装软件包。

作为 5.0 timeframe 中对软件包复制的更改结果，如基于 Delta 复制的引入和流中的改进，安装软件包的实际用例当前受到极大的限制。在大多数情况下，安装软件包在网络流量方面或软件包更改分发到搜索节点的速度方面的差别微乎其微。同时，添加重要的管理复杂性，尤其是与共享存储结合时。由于这是基于 Delta 的复制，因此即使您的配置包含大型文件，只要这些文件没有变化，普通软件包复制就几乎不会包含连续的复制成本。

从独立搜索头迁移到搜索头群集

您可以将设置从现有的独立搜索头迁移到搜索头群集中的所有成员。

重要提示：您不能迁移搜索头实例本身，只能迁移它的设置。您只能向搜索头群集中添加清理的新的 Splunk Enterprise 实例。

要迁移的对象类型

要迁移的对象有两种类型：

- 自定义应用配置。这些将在独立搜索头上的 `etc/apps` 下生成。
- 专属用户配置。这些将在独立搜索头上的 `etc/users` 下生成。

在这两种情况下，您将相关目录从搜索头复制到搜索头群集的 Deployer。然后您可以使用 Deployer 来将这些目录传输给群集成员。

Deployer 针对每个类型使用不同的方法将配置推送到群集中。后迁移应用配置遵照来自用户配置的不同规则。

关于已部署设置在群集成员中驻留的位置信息，请参阅“已部署配置在群集成员的位置”。

自定义应用配置

当迁移一个应用自定义设置时，Deployer 将其置于群集成员的默认目录中。这就包含应用在独立搜索头中运行时的任何运行时更改。

因为用户无法在默认目录中更改设置，所以这就意味着用户无法在这些已迁移实体中执行某些运行时操作：

- 删除。用户无法删除任何已迁移实体。

- 移动。用户无法将这些设置从一个应用移动到另外一个。
- 更改共享等级。用户无法更改共享等级。比如，用户无法将共享从应用等级更改为专属。

群集用户可以通过在相应位置编辑实体来覆盖现有属性。运行时更改将会放入群集成员的本地目录中。本地目录覆盖默认目录，因而更改也将覆盖默认设置。

专属用户配置

Deployer 将仅复制用户配置到管理员。然后管理员将通过一般复制配置的方式将设置复制到所有群集成员，如"群集复制的配置更新"中所述。

与自定义应用配置不同的是，用户配置驻留在群集成员的标准用户位置，并且能够在未来删除、移动和进行其他操作。他们的行为只是如同通过 Splunk Web 群集用户所创造的任何运行时设置。

当您将用户配置迁移到现有的搜索头群集中时，Deployer 将正确处理已存在于群集中的段落。它不会覆盖任何现有的段落。

比如，假设群集成员已经具有包含此段落的文件 `$SPLUNK_HOME/etc/users/admin/search/local/savedsearches.conf`：

```
[my search]
search = index=_internal | head 1
```

同时在 Deployer 中也有包含这些段落的文件 `$SPLUNK_HOME/etc/shcluster/users/admin/search/local/savedsearches.conf`：

```
[my search]
search = index=_internal | head 10
enableSched = 1

[my other search]
search = FOOBAR
```

这将为以下成员提供最终合并配置：

```
[my search]
search = index=_internal | head 1

[my other search]
search = FOOBAR
```

如果各成员已经具有 `[my search]` 段落，则此段落保持现有设置，而不采用迁移过来的设置。如果各成员还没有 `[my other search]` 段落，则此段落会添加到文件中。

注意：Splunk 并不支持针对每个用户搜索历史文件的迁移。

请勿迁移默认应用

当您将应用迁移到搜索头群集时，不会迁移任何默认应用，即 Splunk Enterprise 附带的应用，例如搜索应用。如果您将默认应用推送给群集成员，会覆盖驻留在成员上的那些应用的版本，您不会希望执行此操作。

然而，您可以从默认应用中迁移自定义设置：

- 您可以迁移任何默认应用相关的专用对象。专用对象位于目录 `etc/users` 下，而不在 `etc/apps` 之下。
- 您可以通过将默认设置移动到新应用并全局导出，将应用中的默认设置进行迁移。本主题的迁移程序包括此步骤。

向搜索头群集迁移设置

注意：此程序假设您已部署搜索头群集。请参阅"部署搜索头群集"。

要迁移设置：

1.将独立搜索头上的 `$SPLUNK_HOME/etc/apps` 和 `$SPLUNK_HOME/etc/users` 目录复制到 Deployer 上的可编辑临时目录。

2.如果您想要将自定义设置从默认应用中迁移，则您可以将其移动到新应用并全局导出。比如，要从搜索应用中迁移设置 ：

> **a.** 将临时目录中的 `.../search/local` 目录复制到新应用目录，如临时目录中的 `search_migration_app`。**不要对此新应用"搜索"进行命名。**

b. 全局导出这些设置并使它们对所有应用可用，包括搜索应用。要实现这一点，请创建一个 `.../search_migration_app/metadata/local.meta` 文件并使用如下内容进行填充：

```
[]
export=system
```

详细信息请参阅 default.meta 规范文件。

3. 在临时目录中，删除这些子目录：

- 任何默认应用，例如搜索应用。切勿将默认应用推送给群集成员。如果推送了默认应用，它们会覆盖已经在成员上运行的那些应用的版本。
- 已经在 Deployer 分发目录中存在的任何应用。否则，独立搜索头上运行的版本会覆盖已经在成员上运行的版本。

4. 将余下的所有子目录从临时位置复制到位于 `$SPLUNK_HOME/etc/shcluster` 的 Deployer 的分发目录。保持已经在分发目录中存在的子目录不变。

有关分发目录文件结构的详细信息，请参阅"如何放置 Deployer 的配置软件包"。

5. 如果您需要添加新的群集成员，您必须部署干净的实例。您不能重复使用现有的搜索头。有关添加群集成员的信息，请参阅"添加群集成员"。

6. 在 Deployer 中运行 `splunk apply shcluster-bundle` 命令以推送配置软件包（包括迁移设置）到群集中。请参阅"推送配置软件包"。

Deployer 直接将 `etc/apps` 推送到群集成员。它将 `etc/users` 推送给管理员，然后管理员将设置异步复制给其他群集成员。

注意： 如果您在之前独立搜索头使用的相同搜索节点集上指定群集成员，群集需要重新构建驻留在搜索节点上的报表加速摘要或数据模型摘要。此操作会自动执行。然而，不会自动删除旧的摘要集。

升级搜索头群集

本主题介绍搜索头群集的升级方式。此过程和维护及主要版本升级的过程相同。

从版本 6.5 开始，您可以执行滚动升级。这允许群集在升级过程中继续运行。要使用滚动升级过程，您必须从版本 6.4 或更高版本升级。

从版本 6.4 或更高版本升级

从版本 6.4 或更高版本升级时，您可以执行滚动升级。

1. 升级一个成员，并使其成为管理员：
    1. 停止成员。
    2. 升级成员。
    3. 启动成员，并等待它加入群集。
    4. 将管理员职责转换给已升级的成员。请参阅"转换管理员职责"。
2. 对于每个额外的成员，逐个：
    1. 停止成员。
    2. 升级成员。
    3. 启动成员。
3. 升级 Deployer：
    1. 停止 Deployer。
    2. 升级 Deployer。
    3. 启动 Deployer。

请注意以下事项：

- 群集正在持续进行期间不支持混合版本的群集。因此，在滚动升级过程中必须快速移动，首先升级一个成员，然后立即升级下一个，依此类推，直到完成所有成员的升级。
- 到升级结束时，所有成员必须运行相同版本的 Splunk Enterprise（至少为维护等级）。
- 您可以对 5.x 或 6.x 搜索节点运行搜索头群集成员，所以没有必要同时升级索引器。请参阅"Splunk Enterprise 版本兼容性"。

从版本 6.3 或更早版本升级

要升级搜索头群集，请执行这些步骤：

1. 停止所有群集成员。
2. 升级所有成员。
3. 停止 Deployer。

4. 升级 Deployer。
5. 重新启动 Deployer。
6. 重新启动成员。
7. 请等待一到两分钟，以完成管理员选举。随后群集将开始运行功能。

请注意以下事项：

- 所有群集成员必须运行相同版本的 Splunk Enterprise（至少为维护等级）。
- 您可以对 5.x 或 6.x 搜索节点运行搜索头群集成员，所以没有必要同时升级索引器。请参阅"Splunk Enterprise 版本兼容性"。

Deployer 在 post-6.2.6 升级之后重新启动

与 6.2.6 及以下版本相比，Deployer 在处理 6.2.6 以上的版本时用户配置会有所不同。由于这一变化，当升级群集至 6.2.6 以上的版本时，如果您是首次使用 Deployer 分发更新，则 Deployer 必须对所有群集成员进行滚动重新启动。

升级后，当您首次运行 `splunk apply shcluster-bundle` 命令时会触发重新启动。只有您使用 Deployer 将用户配置推送到 6.2.6 或以下版本才能重新启动。

用户配置部署中的此更改意味着此类配置不再驻留于群集成员的默认目录。这将在配置中启用某些运行时操作。尤其是，您现在可以删除或移动某些配置或更改共享等级。关于 6.2.6 之后版本中 Deployer 如何处理用户配置的更多信息，请参阅"用户配置"。

针对基于用户和基于角色的搜索配额所修改的行为

处理基于用户和基于角色的并发搜索配额的默认行为在 6.5 版本中有所变化。

在版本 6.3 和 6.4 中，默认是在整个群集成员组内强制实施配额。从 6.5 版本开始，默认是逐个对成员强制实施配额。

如有必要，您可以更改配额强制实施行为。请参阅"任务计划"。

配置搜索头群集

配置搜索头群集

本主题介绍如何配置搜索头群集自身的行为。它没有介绍如何配置群集成员的搜索时环境，例如成员能访问的保存的搜索、仪表板和应用。有关配置搜索时环境的信息，请参阅"更新搜索头群集成员"章节。

成员将群集配置存储在本地的 `server.conf` 文件（位于 `$SPLUNK_HOME/etc/system/local/` 下）。有关所有可用的配置属性的详细信息，请参阅 server.conf 规范文件。

关键信息

当阅读本主题时记住下面的关键点：

- 基本配置发生在部署过程中您初始化每个成员的时候。
- 搜索头群集具有大量可用的配置设置。除少数例外情况，没有 Splunk 支持的指导您不应该更改这些设置的初始或默认值。
- 除了特别指出的设置，您必须在所有成员间保持完全相同的设置。
- 当您在所有成员间更改设置时，您必须在近似相同的时刻重新启动所有成员。

初始化时配置

当您初始化每个成员的时候，可以在部署过程中设置所有基本配置。以下是在初始化期间您可以或必须为每个群集成员设置的关键配置属性：

- 成员的 URI。请参阅"部署搜索头群集"。
- 成员的复制端口。请参阅"部署搜索头群集"。
- 群集的复制因子。请参阅"为搜索头群集选择复制因子"。
- 群集的密钥。请参阅"为搜索头群集设置安全密钥"。
- Deployer 位置。请参阅"给 Deployer 指定群集成员"。
- 群集的标签。请参阅"部署搜索头群集"。

警告：强烈建议您在初始化期间设置所有这些属性，之后不要更改它们。请参阅"部署搜索头群集"。

初始化后配置更改

初始化后可以自行安全执行的主要的配置更改是特殊搜索设置。存在两种类型：一种是指定是否特定成员只能运行特殊搜索，另一种是指定是否当前作为管理员的成员只能运行特殊搜索。管理员不会将计划的搜索分配给特殊成员。请

参阅"配置群集成员只运行特殊搜索"。

作为灾难恢复的解决方法之一，您可以临时切换到**静态管理员**。请参阅"使用静态管理员，以从丧失多数优势的状态中恢复。"

警告：请勿编辑 `id` 属性（位于 `[shclustering]` 段落中）。系统会自动将其设置。此属性必须符合有效的 GUID 要求。

设置搜索头群集标签

在部署群集时，一般通过 `splunk init` 命令来设置群集标签。如果在部署时没有进行此设置，也可以稍后在任意一个成员上运行以下命令来为群集完成此设置：

```
splunk edit shcluster-config -shcluster_label <label>
```

设置此标签后，您不用重新启动成员。

注意：如果您在一个群集成员中设置了标签，则也必须在 Deployer 中进行设置。请查阅"配置 Deployer"。

`-shcluster_label` 参数用于确认监视控制台中的群集。请参阅*《监视 Splunk Enterprise》*中的"设置群集标签"。

在所有成员间保持相同的配置设置

搜索头群集的 `server.conf` 属性在所有成员间必须具有相同的值，但以下情况除外：

- `mgmt_uri`
- `adhoc_searchhead`
- `[replication_port://<port>]`

如果这些配置值之外的其他配置值在成员间不同，那么群集行为的更改将取决于当前哪个成员作为管理员。您不会希望发生此情况。

配置方法

大多数配置在初始群集部署期间发生，通过 CLI 命令 `splunk init` 进行。之后要执行进一步的配置，有以下两种选择：

- 使用 CLI `splunk edit shcluster-config` 命令。
- 直接编辑 `[shclustering]` 段落（位于 `server.conf`）。

通常使用 CLI 更简单。

警告：您必须在所有成员上进行相同的配置更改，然后在近似相同的时刻重新启动它们。因为在所有成员间保持完全相同的设置非常重要，不要使用 `splunk rolling-restart` 命令来重新启动，除非是要按"配置群集成员只运行特殊搜索"中所述来更改 `captain_is_adhoc_searchhead` 属性。相反，在每个成员上运行 `splunk restart` 命令。

使用 CLI 配置搜索头群集

您可以使用 CLI 命令 `splunk edit shcluster-config` 来编辑 `[shclustering]` 段落（位于 `server.conf`）。将每个属性和它的配置值指定为关键值对。

例如，要编辑 `adhoc_searchhead` 属性：

```
splunk edit shcluster-config -adhoc_searchhead true -auth <username>:<password>
```

CLI 确认操作成功并指示您重新启动 `splunkd`。

请注意以下事项：

- 您可以使用此命令来编辑 `[shclustering]` 段落中除 `disabled` 属性（用于启动或关闭搜索头群集）之外的任何属性。
- 只能在已经初始化的成员上使用此命令。对于初始配置，可使用 `splunk init shcluster-config`。

通过编辑 server.conf 配置搜索头群集

您也可通过直接编辑 `server.conf` 的方式来更改属性。搜索头群集属性位于 `[shclustering]` 段落中，除了一种情况：要修改复制端口，使用 `[replication_port]` 段落。

为搜索头群集选择复制因子

复制因子确定群集保留的每个搜索项目或搜索结果的副本数量。复制只发生在来自计划的保存的搜索的项目上。群集不会从特殊搜索或实时搜索中复制结果。

复制因子的影响

群集可以容许（复制因子 - 1）个成员出现故障而不会丢失任何搜索项目。例如，要确保系统可以处理两个成员出现故障而不会丢失搜索项目，必须将复制因子配置为 3，这意味着群集会存储每个搜索项目的三个副本，每个副本存储在不同的成员上。如果其中两个成员故障，第三个成员上的项目仍是可用的。

复制因子的默认值是 3。这个数量足够满足大部分需求。

即便是对于一个大型群集，假设有 50 个搜索头，您不需要设一个相应大的复制因子。只要您没有丢失复制因子个数的成员，那么每个搜索项目至少仍有一个副本存在于群集的某处，而且所有群集成员都可访问该副本。群集中的任意搜索头都可以通过存储了搜索项目副本的搜索头作为代理访问任意搜索项目。代理操作速度很快，不可能阻碍对于来自任何搜索头的搜索结果的访问。

注意：复制因子只确定群集保留的搜索项目副本的数量。它不会影响运行时配置更改的复制，例如新的保存的搜索。这些更改通过不同的过程复制到所有群集成员。如果您有 50 个搜索头，那么 50 个中的每个搜索头都会获得这些配置更改的一个副本。请参阅"群集复制的配置更新"。

复制因子配置

所有群集成员必须使用相同的复制因子。确定复制因子 `server.conf` 的属性是 `replication_factor`。

作为成员初始化的一部分，在群集部署期间指定复制因子。请参阅"初始化群集成员"。

如有必要，在部署后您可以更改复制因子，但是建议您在执行此操作之前咨询 Splunk 支持。如果您在一个成员上更改了复制因子，您必须在所有成员上更改它。有关修改配置值的信息，请参阅"配置搜索头群集"。

相关信息

有关群集如何复制搜索项目的信息，请参阅"群集如何处理搜索项目"。该子主题介绍了在下列情况中有关项目复制的若干关键点：

- 在一些情况下，对于一个搜索项目，群集可能复制多于其复制因子数目的副本。
- 如果没有项目副本的成员需要访问该项目，就会发生项目代理以及额外的复制。
- 如果一个成员发生故障，群集会替代存储在该成员上的项目副本。

请参阅"列出搜索项目"以了解如何查看群集和单个成员上的项目集。

为搜索头群集设置密钥

安全密钥验证所有群集成员间的通信，以及验证成员和 Deployer 实例间的通信。

有关搜索头群集配置的概述，请参阅"配置搜索头群集"。

密钥必须在所有节点上一致

您必须在所有成员和 Deployer 上为密钥设置相同的值。

如果搜索头群集是索引器群集的一部分，在两种群集类型间必须使用相同的密钥。

在部署期间设置密钥

使用 `-secret` 参数和 CLI 命令 `splunk init shcluster-config` 在初始部署期间设置密钥。请参阅"部署搜索头群集"。

在部署后设置密钥

如果您在部署过程中忘了设置密钥，在部署之后可通过在每个群集成员和 Deployer 上配置 `server.conf` 中的 `pass4SymmKey` 属性来设置密钥。将属性放在 `[shclustering]` 或 `[general]` 段落下。例如：

```
[shclustering]
pass4SymmKey = yoursecuritykey
```

如果搜索头群集是索引器群集的一部分，在 `[general]` 段落中设置密钥，这样实例在它的两种角色（搜索头群集成员和索引器群集节点）下都会使用相同的密钥。

必须重新启动每个实例使密钥生效。有关部署后配置的更多信息，请参阅"配置方法"。

保存密钥副本

您应该在一个安全的地方保存密钥的一份副本。一旦开始运行一个实例，安全密钥就从明文变为加密形式，无法再从 `server.conf` 中恢复。如果之后您想添加一个新成员，您将需要使用明文形式来设置密钥。

更新搜索头群集成员

配置更改如何跨搜索头群集传输

首先阅读

在阅读本主题前，请参阅：

- 《*管理员手册*》中的“使用配置文件管理 Splunk Enterprise”。该章节中的主题提供了有关配置文件的重要背景信息。

搜索头群集中配置文件的重要性

配置文件中的设置选项控制搜索头（包括**知识对象集**）的功能。例如，有为**保存的搜索**、**事件类型**和**工作流动作**提供设置的配置文件。其他配置文件为非搜索功能（例如数据输入和索引）提供设置。请参阅《*管理员手册*》中的“配置文件列表”。

除了配置文件，其他文件对于搜索时功能很重要。例如，静态**查找**表、**仪表板**和**数据模型**使用不同的文件作为它们定义的一部分。

为了使搜索头群集能正常工作，它的成员必须全部使用相同的搜索相关配置集。例如，群集中的所有搜索头需要访问相同的保存的搜索集。因此，它们必须使用相同的 `savedsearches.conf` 设置。

成员也须使用相同一组用户相关设置。请参阅“添加用户到搜索头群集中”。

在群集中的所有搜索头间应用也必须完全相同。一个应用实际上只是一个配置集。

配置更改如何在搜索头群集中传输

搜索头群集使用两种方式来确保配置在其成员间一致：自动复制和 Deployer。

复制更改

群集自动将一个群集成员上的任意运行时知识对象更改复制到其他的所有成员。这包括，例如，更新或附加到保存的搜索、查找表和仪表板。例如，当 Splunk Web 的用户定义字段提取的时候，群集将该字段提取复制到群集中的所有其他搜索头。

此外，群集也会复制少量其他运行时更改，比如对用户和角色的更改。

请参阅“群集复制的配置更新”。

部署更改

群集不会复制所有的配置更改，而是在运行时通过 Splunk Web、CLI 或 REST API 所进行的特定更改，主要是知识对象。对于其他配置更改和添加，您必须明确地将更改推送给所有群集成员。您可以通过称为 **Deployer** 的特殊 Splunk Enterprise 实例来执行此操作。

需要使用 Deployer 的更改（包括您可以直接编辑的任何配置文件）的示例。例如，如果您在 `limits.conf` 中进行了更改，必须通过 Deployer 推送此更改。同样，如果您直接编辑知识对象配置文件，例如 `savedsearches.conf`，也必须使用 Deployer 将其分发给群集成员。此外，必须使用 Deployer 将新的或升级的应用推送给群集成员。

您也可以使用 Deployer 将应用和用户设置从现有的搜索头池或独立搜索头迁移到搜索头群集中。

请参阅“使用 Deployer 分布应用和配置更新”。

添加非群集搜索节点到搜索头群集

添加非群集搜索节点（即，索引器不属于任何索引器群集）到搜索头群集是群集不会自动复制配置更改的其中一种场景。但是同时，以使用 Deployer 推送更新后的 `distsearch.conf` 这一方式来添加搜索节点可能也并不简便，因为 Deployer 随后会对所有群集成员进行滚动重新启动。

要避免群集成员的重新启动，可以使用 CLI 命令 `splunk add search-server` 将对等节点分别添加到每一个群集成员。有关详细信息，请参阅“连接群集中的搜索头与搜索节点”。

警告：快速对所有群集成员进行此操作，以便所有成员都保持同一个搜索节点集。

“设置”菜单

Splunk Web 中的“设置”菜单将设置分为若干个组，包括一个称为“知识”的组，它包含知识对象设置。搜索头群集在每个成员的“设置”菜单中默认隐藏大部分的非“知识”组。例如，隐藏数据输入和分布环境的设置。如有必要，您可以取消隐藏已隐藏的组。

隐藏非“知识”设置的原因是群集只复制某些设置更改，主要是“知识”类别中的设置更改。如果您将一个成员更改为非知识类别中的设置，除少数例外情况，群集不会自动将该更改复制到其他成员。这可能导致成员相互之间不同步。

如果您需要访问一个成员的隐藏设置，您可以取消隐藏这些设置：

1. 单击 Splunk Web 右上角的**设置**。出现主要限制为“知识”组的设置列表。

2. 单击列表底部的**显示全部设置**按钮。出现一个对话框提醒您隐藏的设置将不会被复制。

3. 要继续，单击对话框中的**显示**。出现设置的完整列表（取决于您的角色权限）。

现在对于具有查看设置权限的所有用户，通常是所有的管理员用户，设置都取消隐藏了。要重新隐藏设置，您必须重新启动实例。

重要提示：如果您对于隐藏设置进行了更改，更改的配置将只存在于进行更改的群集成员上。如果您希望其他成员也获得该更改，必须使用 Deployer 推送该设置的基本配置文件。

CLI 命令和群集成员

大多数一般的 CLI 命令以及和搜索相关的 CLI 命令可以用于群集成员。如果您在某一个成员中运行命令，则群集将结果配置更改复制到其他成员中。

然而，对于活跃的群集成员，不管是哪种变体，不要运行 `splunk clean` 命令。比如，`splunk clean all` 命令应该只能在从群集中删除成员时才能使用，因为该命令会删除 `_raft` 文件夹和 `/etc/passwd` 等内容。同样，如果您在一个成员上运行 `splunk clean userdata`，则只有这个成员上的用户数据会被清除。这一更改不会复制到其他的成员，导致成员间的用户/角色信息不一致。

关于复制更改的更多信息，请参阅“群集复制的配置更新”。

群集复制的配置更新

群集自动将用户对某个群集成员所做的运行时配置更改复制到其他的所有成员。

注意：群集将配置更改复制到所有的群集成员。群集的复制因子只适用于搜索项目复制。请参阅“为搜索头群集选择复制因子”。

群集复制的更改

以下是群集会复制的配置更改的主要类型：

- 对**知识对象**的运行时更改或附加内容，例如**保存的搜索**、**查找**表和**仪表板**。例如，当 Splunk Web 的用户定义**字段提取**的时候，群集将该字段提取复制到群集中的所有搜索头。
- 对用户和角色的运行时更改。请参阅“添加用户到搜索头群集中”。

复制在以下约束条件下运行：

- 群集只复制运行时通过特定配置方法所进行的更改。
- 白名单确定群集会复制的更改的具体类型。

触发复制的配置方法

群集复制通过这些方法进行的更改。

- Splunk Web
- Splunk CLI
- REST API

群集一般不会复制任何您手动进行的配置更改，如对于配置文件的直接编辑。

例如，如果在一个群集成员上一个用户在 Splunk Web 中创建了一个保存的搜索，群集将该保存的搜索复制给所有群集成员。然而，如果您作为管理员通过直接编辑群集成员上的 `savedsearches.conf` 文件添加一个保存的搜索，群集不会将该保存的搜索复制到其他的群集成员。必须使用 **Deployer** 将保存的搜索推送给所有群集成员。

复制白名单

群集使用白名单来确定要复制的更改。此白名单可通过 `conf_replication_include` 属性集（在 `server.conf` 的默认版本中，位于 `$SPLUNK_HOME/etc/system/default`）进行配置。

您可以通过编辑成员的 `server.conf` 文件（位于 `$SPLUNK_HOME/etc/system/local`）从列表中添加或删除条目。如果您更

改了白名单，必须在所有群集成员上进行相同的更改。

有关白名单中条目的综合列表，请查阅 `server.conf` 的默认版本。这是白名单条目的近似集：

```
alert_actions
authentication
authorize
datamodels
event_renderers
eventtypes
fields
html
literals
lookups
macros
manager
models
multikv
nav
panels
passwd
passwords
props
quickstart
savedsearches
searchbnf
searchscripts
segmenters
tags
times
transforms
transactiontypes
ui-prefs
user-prefs
views
viewstates
workflow_actions
```

群集将更改复制到白名单条目相关的所有文件。除了配置文件自身之外，这包括仪表板和导航 XML、查找表文件、数据模型 JSON 文件，等等。群集也会复制存储在 *.meta 文件中的权限。

以下是对于不同白名单条目复制文件的类型示例：

```
# escape-hatch HTML views
conf_replication_include.html = true
# lookup table files
conf_replication_include.lookups = true
# manager XML
conf_replication_include.manager = true
# datamodel JSON files
conf_replication_include.models  = true
# nav XML
conf_replication_include.nav = true
# view XML
conf_replication_include.views = true
```

群集忽略的更改

群集忽略不在白名单中的任何条目的配置更改。示例包括索引时间设置，例如定义数据输入或索引的设置。

此外，群集只复制通过 Splunk Web、Splunk CLI 或 REST API 进行的更改。如果您直接编辑配置文件，群集不会复制它。相反，必须使用 Deployer 将文件分发给所有群集成员。

群集也不会复制新安装的或升级的应用。

有关如何通过 Deployer 分发配置更改的信息，请参阅“使用 Deployer 分布应用和配置更新”。

注意：Deployer 一般与群集复制结合使用，以将用户（非应用）配置迁移到群集成员。典型使用案例是将用户设置从现有的搜索头池或独立搜索头迁移到搜索头群集中。您将推送想要在 Deployer 中迁移的用户配置。Deployer 将其推送到管理员，然后管理员将其复制到其他群集成员。关于详细信息，请参阅“用户配置”。

复制如何工作

当用户对于群集成员搜索头进行配置更改的时候，成员将更改保存到本地的文件或文件集，也将更改发送给管理员。大约每五秒钟，每个群集成员都会联系管理员并提取自上次提取更改之后到达的任何更改。然后每个群集成员在本地应用更改。

例如，假设群集成员上的一个用户使用 Splunk Web 来创建新的字段提取。Splunk Web 将字段提取保存到该成员的本地文件中。然后成员将文件更改发送给管理员。当每个群集成员下次联系管理员的时候，它会提取更改以及任何其他最近的更改，并在本地应用它们。在几秒钟内，所有群集成员都有了新的字段提取。

注意：在群集成员集之间，用这种方式复制和更新的文件具有相等的语义和功能。然而，在所有成员上的文件可能不是完全相同。例如，根据情况（如更改到达管理员的次序），在 `props.conf` 中更新的设置可能在不同的成员上出现在文件的不同位置。

关于群集的配置复制进度的详细信息，请查看“搜索头群集”：监视控制台中的“配置复制”仪表板。请参阅“使用监视控制台查看搜索头群集状态”。

当发生复制时

复制的目的是为在所有群集成员间保持搜索相关配置的同步。要确保实现此目的，复制会在不同的时间发生，这取决于成员状态：

- **每个活跃的群集成员**每五秒钟会联系管理员并提取自上次提取更改之后到达的任何更改。
- **当新成员加入到群集中时**，它会联系管理员并下载包含当前复制配置集的压缩包，其包括在群集生存期间进行的所有更改。它在本地应用压缩包。
- **当成员重新加入群集时**。首先，遵循“添加之前从群集中删除的成员”中列出的过程，在您将实例重新添加到群集中之前清理该实例。然后成员联系管理员并下载压缩包，方式与新成员加入的时候相同。
- **在群集恢复期间**。有关详细信息，请参阅下面的部分。

查看复制状态

DMC 包含了关于配置复制状态的丰富信息。请参阅“使用 DMC 查看搜索头群集状态和解决问题”。

要查看成员上次是何时从管理员提取一组配置更改，可从任意成员运行 `splunk show shcluster-status` 命令。

```
splunk show shcluster-status
```

对于每个成员，该命令的输出包括字段 `last_conf_replication`。它指示上一次成员从管理员成功提取一组更新配置的时间。

有关命令的一般信息，请参阅“显示群集状态”。

复制如何处理灾难恢复问题

通常群集持续将更改复制到所有的群集成员。然而，当群集从停机时间中恢复时，或当故障成员重新加入群集中时，必须再次进行其他的复制操作，以确保所有成员共享同一组复制更改，包括停机期间的任何更改。

有关成员意外发生故障的情况，请参阅“处理搜索头群集成员的故障”。在一些情况下，成员会下载中间的更改集并应用它们。在其他情况下，您可能需要运行 `splunk resync shcluster-replicated-config` 命令来应用此压缩包。

关于整个群集恢复期间，复制如何运行功能的信息，请参阅“无功能群集的运行恢复”。

使用 Deployer 分布应用和配置更新

Deployer 是您用于将应用和某些其他配置更新分发给搜索头群集成员的 Splunk Enterprise 实例。Deployer 分发的一组更新被称为**配置软件包**。

Deployer 响应您的命令来分发配置软件包。当有成员加入或重新加入群集时，Deployer 都会分发此软件包。

警告：您必须使用 Deployer 而不是部署服务器来分发应用给群集成员。Deployer 的使用消除了与运行时更新（群集通过“群集复制的配置更新”中介绍的机制自动复制）发生冲突的可能性。

关于群集的应用部署进度详情，请查看“搜索头群集”：监视控制台中的“应用部署”仪表板。请参阅“使用监视控制台查看搜索头群集状态”。

Deployer 管理的是哪些配置？

Deployer 具备以下主要角色：

- 它还要管理应用和用户配置从非群集实例和搜索头池到搜索头群集中的迁移。
- 它将基线应用配置部署到搜索头群集成员。
- 它提供了将非复制、非运行时配置更新分发给所有搜索头群集成员的方法。

请勿使用 Deployer 将搜索相关的运行时配置更改从一个群集成员分发到其他成员。相反的是，群集通常自动将此类更改复制到所有的群集成员。例如，如果成员上一个用户创建了一个保存的搜索，群集将其自动复制给所有其他成员。请参阅"群集复制的配置更新"。要分发所有其他的更新，您需要 Deployer。

配置从 Deployer 到成员移动只能是一个方向。成员绝不可将配置上传到 Deployer。您同样没有必要通过从群集中手动复制文件到 Deployer 来强制进行此操作，因为成员会在它们之间持续复制所有的运行时配置。

Deployer 处理的更新类型

以下是需要 Deployer 更新的特定类型：

- 新的或升级的应用。
- 您直接编辑的配置文件。
- 非搜索相关更新，甚至那些通过 CLI 或 Splunk Web 配置的更新，例如对于 `indexes.conf` 或 `inputs.conf` 的更新。
- 需要从搜索头池或独立的搜索头迁移的设置。这些设置可以是应用或用户设置。

注意：您可使用 Deployer 来只部署配置更新。不能用于搜索头群集的初始配置或成员运行其上的 Splunk Enterprise 实例的版本升级。

Deployer 无法处理的更新类型

请勿使用 Deployer 将特定运行时更改从一个群集成员分发到其他成员。这些更改通过配置复制进行自动处理。请参阅"配置更改如何跨搜索头群集传输"。

由于 Deployer 只是管理配置的子集，因此请注意以下内容：

- Deployer 并非为群集中的所有配置代表"Truth 的单独数据来源"。
- 您无法使用 Deployer 通过自身将最新状态还原到群集成员。

应用升级和运行时更改

由于配置文件优先顺序有它的工作方式，所以用户在运行时对应用所做的更改将通过后续升级保存在应用中。

比如说您部署的是某些应用的 1.0 版本，然后有一个用户修改应用的仪表板。当您稍后部署应用的 1.1 版本时，用户修改内容会在应用的 1.1 版本中继续留存。

如"群集复制配置更新"中所述，群集将大部分运行时更改自动复制到所有成员。那些运行时更改后续不会上传到 Deployer，但是由于配置分层有它的工作方式，所以这些更改的优先顺序将超过通过 Deployer 分发的非修改应用中的配置。要了解详情中的此问题，请阅读该主题的其余部分，以及*《管理员手册》*中的主题"配置文件优先顺序"。

Deployer 何时分发配置给成员？

Deployer 在以下情形下将应用配置分发给群集成员：

- 当您调用 `splunk apply shcluster-bundle` 命令时，Deployer 将所有更新或更改的配置推送到成员。请参阅"分发配置软件包"。
- 当成员加入或重新加入群集中时，会检查 Deployer 是否有应用更新。任何时候只要成员重新启动，也会检查更新。如有任何更新的可用，它就会将其从 Deployer 推送出去。

只有当您调用 `splunk apply shcluster-bundle` 命令时，Deployer 才会将用户配置分发给管理员。管理员随后将那些配置复制到成员。

配置 Deployer

注意：本小节的操作集成到部署搜索头群集（在"部署搜索头群集"主题中介绍）的过程中。如果您已经在搜索头群集的初始部署期间设置了 Deployer，可以跳过此部分。

选择一个实例作为 Deployer

每个搜索头群集都需要一个 Deployer。Deployer 必须运行在搜索头群集之外的 Splunk Enterprise 实例上。

根据您的 Splunk Enterprise 环境的特定组件，Deployer 可能可以运行在具有其他职责的现有 Splunk Enterprise 实例上，例如部署服务器或索引器群集的主节点。否则，您可以在专用实例上运行它。请参阅"Deployer 要求"。

部署到多个群集

Deployer 将相同的配置软件包发送给它服务的所有群集成员。因此，如果您有多个搜索头群集，仅当群集都采用完全相同的配置、应用等等的时候，您可以给所有的群集使用相同的 Deployer。

如果您预计随着时间的变化群集可能需要不同的配置，则为每个群集设置独立的 Deployer。

在 Deployer 上设置密钥

您必须在 Deployer 和所有搜索头群集成员上配置密钥。Deployer 使用该密钥对与群集成员的通信进行验证。要设置密钥，指定 `pass4SymmKey` 属性。可选择在 `[general]` 或 `[shclustering]` 段落中（位于 Deployer 的 `server.conf` 文件中）指定此属性。例如：

```
[shclustering]
pass4SymmKey = yoursecretkey
```

所有群集成员和 Deployer 的密钥必须相同。您可以在初始化期间在群集成员上设置密钥。

必须重新启动 Deployer 实例使密钥生效。

注意：如果群集成员与 Deployer 上的 `pass4SymmKey` 值不匹配（例如，您在成员上设置了该值却忘了在 Deployer 上设置它），当 Deployer 试图推送配置软件包时您会收到一条错误消息。消息与下面的相似：

```
Error while deploying apps to first member: ConfDeploymentException: Error while fetching apps baseline on
target=https://testitls11:8089: Non-200/201 status_code=401; {"messages":[{"type":"WARN","text":"call not properly
authenticated"}]}
```

在 Deployer 上设置搜索头群集标签。

搜索头群集标签用于确认监视控制台中的群集。此参数可选，但是如果您在某一个成员中将其配置，则必须在所有成员中，以及 Deployer 里面使用相同的数值配置。

要设置标签，指定 `shcluster_label` 属性（在 `[shclustering]` 段落中指定；该段落位于 Deployer 的 `server.conf` 文件中）。例如：

```
[shclustering]
shcluster_label = shcluster1
```

请参阅*《监视 Splunk Enterprise》*中的“设置群集标签”。

给 Deployer 指定群集成员

每个群集成员都需要了解 Deployer 的位置。Splunk 建议您在成员初始化期间指定 Deployer 位置。请参阅“部署搜索头群集”。

如果您没有在初始化期间设置 Deployer 位置，在使用 Deployer 之前您必须在每个成员的 `server.conf` 文件中添加此位置：

```
[shclustering]
conf_deploy_fetch_url = <URL>:<management_port>
```

`conf_deploy_fetch_url` 属性指定 Deployer 实例的 URL 和管理端口。

如果之后您向群集中添加新成员，在添加到群集之前您必须在成员上设置 `conf_deploy_fetch_url`，这样它可以立即联系 Deployer 来获得当前配置软件包（如果有）。

配置软件包包含的内容

配置软件包是 Deployer 分发给群集的一组文件。索引由两种类型的配置组成：

- 应用配置。
- 用户配置。

将应用或其他配置拷贝到 Deployer 上面的位置，确定配置软件包的内容。

Deployer 将配置软件包推送到群集中，具体方法取决于配置为应用还是用户。在群集成员中，应用配置遵照来自用户配置的不同规则。请查看“已部署配置在群集成员的位置”。

Deployer 将配置软件包作为一组压缩包（其中每个应用对应一个，整个用户目录又对应一个）推送给群集。

配置软件包在 Deployer 的位置

在 Deployer 上，配置软件包驻留于 `$SPLUNK_HOME/etc/shcluster` 目录下。该目录下的一组文件组成配置软件包。

此目录的结构如下所示：

```
$SPLUNK_HOME/etc/shcluster/
     apps/
          <app-name>/
          <app-name>/
          ...
     users/
```

请注意以下一般要点：

- 无论是在 `/apps` 还是在 `/users` 之下，配置软件包必须至少包含一个子目录。如果您尝试推送不含应用或用户子目录的配置软件包，则 Deployer 会出现错误。
- Deployer 仅推送 `shcluster` 下子目录的内容。在 `shcluster` 下的任何独立文件都不会直接推送。例如，它不会推送文件 `/shcluster/file1`。要部署独立文件，在 `/apps` 下创建新应用目录并将文件放入本地子目录中。例如，将 `file1` 放到 `$SPLUNK_HOME/etc/shcluster/apps/newapp/local` 下。
- `shcluster` 位置仅供待分发给群集成员的文件使用。Deployer 不会使用该目录中的文件来解决其自己的配置需求。

请注意以下有关应用的要点：

- 将每个应用放入 `/apps` 下各自的子目录中。您必须解压应用。
- 在部署后，放在默认和本地子目录下的所有文件都合并到成员的默认子目录中（仅针对应用目录）。请查看"应用配置"。
- 配置软件包必须包含所有之前推送的应用，以及任何新应用。如果您从软件包中删除了一个应用，在下次您推送软件包的时候，应用会从群集成员中删除。
- 要更新群集成员上的应用，请将更新的版本放入配置软件包。只覆盖应用的现有版本。
- 要删除您之前推送的应用，请从配置软件包中删除它。当您下次推送软件包的时候，每个成员都将从它自己的文件系统中删除它。
- 当 Deployer 推送软件包的时候，它会推送自上次推送之后已经更改的所有应用的全部内容。即使应用的唯一更改是一个单独文件，它仍旧会推送整个应用。如果应用没有更改，Deployer 不会再次推送它。
- **警告：**如果配置软件包中的应用具有与群集成员上默认应用相同的名称，则将覆盖该应用。例如，如果您在配置软件包中创建了一个称为"搜索"的应用，它将覆盖 Splunk Enterprise 附带的默认搜索应用。您希望发生此情况的可能性极小。

请注意以下有关用户设置的要点：

- 要推送用户特定文件，将文件放入您希望驻留在成员上的 `/users` 子目录下。
- 如果内容中包括至少一个配置文件，Deployer 将只推送 `/shcluster/users` 下的内容。例如，如果您在一些用户子目录下放置了专用查找表或视图，则只有当 `/shcluster/users` 下也有至少一个配置文件时，Deployer 才会进行推送。
- 接下来您无法通过从 Deployer 删除文件然后再次推送软件包的方式删除用户设置。在这一方面，用户设置和应用设置的表现有所不同。

已部署配置在群集成员的位置

在群集成员上，部署的应用和用户配置分别驻留在 `$SPLUNK_HOME/etc/apps` 和 `$SPLUNK_HOME/etc/users` 下。

应用配置

部署应用时，Deployer 将应用配置置于群集成员的默认目录。

Deployer 永远不会将文件部署到成员的本地应用目录 `$SPLUNK_HOME/etc/apps/<app_name>/local`。相反，它将来自配置软件包的本地和默认设置部署到成员的默认应用目录 `$SPLUNK_HOME/etc/apps/<app_name>/default`。这确保部署的设置永远不会覆盖成员上的本地或复制运行时设置。否则，例如，应用升级会去掉运行时更改。

在推送配置软件包之前发生的分段过程中，Deployer 会将配置软件包复制到它文件系统上的分段区域，在该区域它会将 `/shcluster/apps/<appname>/local` 中文件的所有设置合并到 `/shcluster/apps/<appname>/default` 的相应文件中。然后 Deployer 只推送合并的默认文件。

在合并过程中，本地目录中的设置优先于任何相应的默认设置。例如，如果您有一个 `/newapp/local/inputs.conf` 文件，Deployer 从该文件中提取设置并将它们与 `/newapp/default/inputs.conf` 中的任意设置合并。如果一个特定属性在两处都进行了定义，合并的文件会保留本地目录中的定义。

用户配置

Deployer 将仅复制用户配置到管理员。然后管理员将通过一般复制配置的方式将设置复制到所有群集成员，如"群集复制的配置更新"中所述。

与应用配置不同的是，用户配置驻留在群集成员的标准用户位置，并且不会迁移到默认的目录中。他们的行为只是如

同通过 Splunk Web 群集用户所创造的任何运行时设置。

用户配置部署主要对从独立搜索头或搜索头池到搜索头群集的迁移设置颇具价值。请查看"从搜索头池迁移到搜索头群集"。

当您将用户配置迁移到现有的搜索头群集中时，Deployer 将正确处理已存在于群集中的段落。它不会覆盖任何现有的段落。

比如，假设群集成员已经具有包含此段落的文件 `$SPLUNK_HOME/etc/users/admin/search/local/savedsearches.conf`：

```
[my search]
search = index=_internal | head 1
```

同时在 Deployer 中也有包含这些段落的文件 `$SPLUNK_HOME/etc/shcluster/users/admin/search/local/savedsearches.conf`：

```
[my search]
search = index=_internal | head 10
enableSched = 1

[my other search]
search = FOOBAR
```

这将为以下成员提供最终合并配置：

```
[my search]
search = index=_internal | head 1

[my other search]
search = FOOBAR
```

如果各成员已经具有 `[my search]` 段落，则此段落保持现有设置，而不采用迁移过来的设置。如果各成员还没有 `[my other search]` 段落，则此段落会添加到文件中。

应用级知识对象的管理

在您部署一个应用到成员后，后续不能通过 Splunk Web、CLI 或 REST API 删除应用的基础知识对象。您也不能移动、共享或取消共享这些知识对象。

此限制仅适用于应用的基础知识对象 - 那些从 Deployer 分发到成员的知识对象。它不适用于应用的运行时知识对象，如果有的话。例如，如果您部署一个应用，然后后续使用 Splunk Web 在应用中创建一个新的知识对象，您可以使用 Splunk Web 或任何其他的常用方法来管理该对象。

管理基础知识对象的限制适用于查找表、仪表板、报表、宏、字段提取等。这个规则的唯一例外是在 default.meta 中没有权限段落的应用级的查找表文件。可以通过成员的 Splunk Web 删除这样的查找文件。

删除一个应用级的基础知识对象的唯一方法是重新部署不包括该知识对象的应用的更新版本。

注意：本条款不适用于由 Deployer 推送的用户级的知识对象。用户级的对象可以通过所有常用的方法管理。

管理基础知识对象的限制是由于 Deployer 将应用推送给成员之前，它会将所有本地应用配置移动到默认目录的这一事实。默认配置不能移动或以其他方式管理。另一方面，任何运行时知识对象驻留在应用的本地目录，因此可以正常的方式管理。有关部署的配置驻留何处的更多信息，请参阅"应用配置"。

Deployer 发送给群集的确切内容？

Deployer 将配置软件包作为一组压缩包（每个应用一个压缩包）推送给成员。此外，它还将整个 `$SPLUNK_HOME/etc/shcluster/users` 目录所构成的一个压缩包推送到管理员。

初次推送到一组新成员时，Deployer 会将整个一组应用压缩包分发到每个成员。在后面的推送过程中，它只会分发新应用或自上次推送以来已更改的应用。如果在应用中有一个单独文件已修改，则 Deployer 会重新分发整个应用。但它不会重新分发未更改的应用。

如果您在 `users` 目录中更改一个单独文件，则 Deployer 会将整个用户压缩包重新部署到管理员。这是由于通常只有在升级或迁移期间，`users` 目录才会修改和重新部署，而不像 `apps` 目录可能会在群集的生存期内就能看到常规更新。

警告：如果试图推送一个非常大的压缩包 (>200 MB)，此操作可能由于各种超时而失败。如可行，从压缩包的应用中删除一些内容并再次尝试。

部署配置软件包

要部署配置软件包，您需要将软件包从 Deployer 推送到群集成员。

推送配置软件包

要将配置软件包推送给群集成员：

1.将子目录中的应用和其他配置更改放在 Deployer 的 `shcluster/` 下。

2.解压任何应用。

3.在 Deployer 上运行 `splunk apply shcluster-bundle` 命令：

```
splunk apply shcluster-bundle -target <URI>:<management_port> -auth <username>:<password>
```

请注意以下事项：

- `-target` 参数为群集的任一成员指定 URI 和管理端口，例如，`https://10.0.1.14:8089`。您仅指定一个群集成员但是 Deployer 会推送给所有成员。此参数为必需项。
- `-auth` 参数为 Deployer 实例指定凭据。

作为对 `splunk apply shcluster-bundle` 的响应，Deployer 会显示下面的消息：

```
Warning: Depending on the configuration changes being pushed, this command
might initiate a rolling-restart of the cluster members. Please refer to the
documentation for the details.  Do you wish to continue? [y/n]:
```

有关哪个配置更改会触发重新启动的信息，请参阅 `$SPLUNK_HOME/etc/system/default/app.conf`。它列出了更改时不会触发重新启动的配置文件。所有其他配置的更改都会触发重新启动。

4.要继续进行，需要以 `y` 响应此消息。

注意：通过将 `--answer-yes` 标记附加到 `splunk apply shcluster-bundle` 命令，您可以删除此消息：

```
splunk apply shcluster-bundle --answer-yes -target <URI>:<management_port> -auth <username>:<password>
```

如果您要将命令包含在脚本中或自动化该过程，则非常有用。

群集如何应用配置软件包

Deployer 和群集成员执行以下命令：

1.Deployer 将配置软件包放在其文件系统上的独立位置 (`$SPLUNK_HOME/var/run/splunk/deploy`) 中，然后将应用目录推送给每个群集成员。配置软件包通常由若干个压缩包组成，每个应用一个压缩包。Deployer 只推送更新或已更改的应用。

2.如果自上次推送以来有任何用户配置更改，则 Deployer 单独将用户压缩包推送到管理员。

3.管理员将任何已更改用户配置复制到其他群集成员。

4.每个群集成员都在本地将应用压缩包进行应用。如果确定需要滚动重新启动，则大约有 10% 的成员在同一时刻重新启动，直到所有成员都重新启动。

在滚动重新启动期间，所有成员包括当前管理员都会重新启动。管理员的重新启动会触发选举过程，这会导致产生新的管理员。在最后一个成员重新启动之后，群集需要大约 60 秒来达到稳定。在此间隔期间，可能会出现错误消息。您可以忽略这些消息。在 60 秒后它们应该会停止。有关滚动重新启动过程的更多信息，请参阅"重新启动搜索头群集"。

控制重新启动过程

通常需要让群集在必要时自动触发所有的滚动重新启动。但是，如果您需要保持对重新启动过程的控制，则可以运行某个版本的 `splunk apply shcluster-bundle` 使重新启动在开始前及时停止。进行此操作后，必须自行重新启动。配置软件包更改在成员重新启动后才会生效。

若需确保运行 `splunk apply shcluster-bundle` 命令不会导致重新启动，使用以下版本的命令：

```
splunk apply shcluster-bundle -action stage && splunk apply shcluster-bundle -action send
```

成员会收到软件包，但不会重新启动。Splunk Web 会显示一条消息"更改必须在 Splunk 重新启动后才会生效 "。

要稍后执行滚动重新启动，从管理员调用 `splunk rolling-restart` 命令：

```
splunk rolling-restart shcluster-members
```

应用升级过程中维护查找文件

使用查找表的任何应用通常与表格文件的存根一并提供。一旦应用在搜索头中使用，则将填充表格作为运行时处理（如搜索）结果。当您以后升级应用时，默认情况下填充的查找表将被来自最新版本应用的存根文件覆盖，从而您会丢失表格中的数据。

要避免此问题，您可以规定已升级应用中的存根文件不会覆盖群集成员上任何相同名称的表格文件。在 Deployer 上运行 `splunk apply shcluster-bundle` 命令，将 `-preserve-lookups` 标记设置为 "true"：

```
splunk apply shcluster-bundle -target <URI>:<management_port> -preserve-lookups true -auth <username>:<password>
```

请注意以下事项：

- `-preserve-lookups` 默认值为 "false"。换句话说，默认情况下，当升级时已填充的查找表会被覆盖。

注意：要确保存根继续留存在成员中，只需确保现有的成员中不存在相同名称的表格文件，此功能可以临时通过 `.default` 扩展名重新命名表格文件。（例如，`lookup1.csv` 变为 `lookup1.csv.default`。）因此，如果您一直通过 `.default` 手动重命名表格文件，则您可能在使用该功能时发现这种问题。您应当在继续进行操作之前联系支持小组。

Deployer 故障的后果和纠正措施

Deployer 在以下情形下将应用配置软件包分发给群集成员：

- 当您调用 `splunk apply shcluster-bundle` 命令时，Deployer 会将应用配置推送到成员，并将用户配置推送到管理员。
- 当成员加入或重新加入群集中时，会检查 Deployer 是否有应用更新。任何时候只要成员重新启动，也会检查更新。如有任何应用更新可用，它就会将其从 Deployer 推送出去。

这意味着如果 Deployer 出现故障时：

- 您无法将新配置推送到成员。
- 加入或重新加入群集中的成员，或者重新启动的成员无法推送最新一组应用压缩包。

因此，已故障的 Deployer 的含义取决于群集成员的状态。以下是需要考虑的主要问题：

- Deployer 出现故障但群集成员小组仍然稳定。
- Deployer 出现故障但有成员尝试加入或重新加入群集中。

Deployer 出现故障但群集成员小组仍然稳定

如果 Deployer 出现故障时没有成员加入或重新加入群集中，则运行群集功能的后果一般不会很严重。所有的成员配置仍旧处于同步状态，而群集继续正常地运转。唯一的显著后果是，您无法在此期间将新配置推送到成员。

Deployer 出现故障但有成员尝试加入或重新加入群集中

如果 Deployer 故障时某成员尝试加入或重新加入群集中，有可能成员的应用配置与其他群集成员的应用配置不同步：

- 新成员将无法提取当前一组应用压缩包。
- 如果某成员在 Deployer 故障之前离开群集，或者 Deployer 故障之后重新加入群集中，则在成员故障而 Deployer 仍旧运行的时候无法将任何更新提取到软件包的应用部分。

在这些情形中，正在加入及重新加入的成员的应用配置小组将会与其他群集成员的有所不同。根据软件包更改的性质，那样可能会导致重新加入的成员表现和其他成员有所不同。这样一来可能整个群集会出现故障。因此，您必须确保这种情形不会继续发展。

如何纠正 Deployer 故障

纠正主要是如下两个方面：

1.阻止 Deployer 故障期间任何成员加入或重新加入群集中，除非您确定正在加入的成员上的配置组与其他成员的相同（比如，如果重新加入的成员紧接着 Deployer 产生故障）。

2.建立新 Deployer：

a. 创建新的 Deployer 实例。

b. 将 `$SPLUNK_HOME/etc/shcluster` 内容从备份存储到新实例。

c. 如有必要，请在所有搜索头群集成员上更新 `conf_deploy_fetch_url` 数值。

d. 通过运行 `splunk apply shcluster-bundle` 命令，将已存储软件包内容推送到所有成员。

管理搜索头群集

添加群集成员

您可能需要添加到群集的成员有若干个类别。

- **新成员。**在这种情况下，您希望通过添加新成员来扩展群集。
- **之前从群集中删除的成员。**在这种情况下，您使用 `splunk remove` 命令删除了成员，现在希望将其添加回来。
- **没有被删除却离开群集的成员。**如果，例如，实例意外关闭的时候，会发生此种情况。

本主题通过一组高级程序分别处理每个类别，其中每个程序参考一个或多个详细的步骤。

添加新成员

这些程序用于之前不属于群集的 Splunk Enterprise 实例。

重要提示：建议您始终使用新安装的实例。

添加新安装的实例

要添加新安装的 Splunk Enterprise 实例（之前没有作为搜索头工作）：

1. 初始化实例。请参阅"初始化实例"。

2. 添加实例到群集。请参阅"添加实例"。

添加现有实例

要添加现有的 Splunk Enterprise 实例，必须先删除所有非默认设置：

1. 如果实例以前是另一个搜索头群集的成员，在将它添加到该群集之前要从那个群集中删除和禁用该成员。请参阅"删除群集成员"。

2. 清理实例以移除任何会妨碍群集的现有配置。请参阅"清理实例"。

3. 初始化实例。请参阅"初始化实例"。

4. 添加实例到群集。请参阅"添加实例"。

添加之前从群集中删除的成员

这些程序用于之前为群集成员但是用 `splunk remove shcluster-member` 命令删除的 Splunk Enterprise 实例。请参阅"删除群集成员"。

添加已删除的成员

要添加已删除的成员：

1. 清理实例来删除任何现有会妨碍群集的配置。请参阅"清理实例"。

2. 添加实例到群集。请参阅"添加实例"。

添加既被删除又被禁用的成员

要添加既被删除又被禁用的成员：

1. 清理实例来删除任何现有会妨碍群集的配置。请参阅"清理实例"。

2. 初始化实例。请参阅"初始化实例"。

3. 添加实例到群集。请参阅"添加实例"。

添加没有被删除却离开群集的成员

归入此类别的成员通常是因为群集成员的临时故障。

对于没有被明确删除却离开群集的成员：

1. 使用 `splunk start` 命令启动实例。

2. 您可能需要运行 `splunk resync shcluster-replicated-config` 命令来下载当前的配置集，具体取决于成员的关闭时长。

请参阅"处理群集成员的故障"以了解有关 `splunk resync shcluster-replicated-config` 命令的信息，以及与处理故障成员相关的其他问题的讨论。

详细步骤

添加群集成员的高级程序使用此部分描述的详细步骤。取决于您正在处理的特定情况，您可能只需要使用这些步骤的子集。请参阅本主题前面提到的高级程序来确定您的情况需要使用哪些详细步骤。

清理实例

注意：如果您正在添加的新实例只包含默认的配置集，则不需要执行此步骤。

如果您正在向群集中添加一个现有实例，必须首先停止该实例并运行 `splunk clean all` 命令：

```
splunk stop

splunk clean all

splunk start
```

`splunk clean all` 命令会删除配置更新，这些更新可能妨碍跨所有群集成员间保持必要的完全相同的配置和应用的目的。它不会删除 `[shclustering]` 段落（位于 `server.conf`）下的任何现有设置。

警告：此步骤会删除之前在实例上配置的大多数设置。

有关必须在所有成员间共享的配置的讨论，请参阅"配置更改如何跨搜索头群集传输"。

有关 `splunk clean` 命令的更多信息，请访问在线 CLI 帮助：

```
splunk help clean
```

初始化实例

如果对于群集来说是新成员，在将它添加到群集之前必须先初始化。

```
splunk init shcluster-config -auth <username>:<password> -mgmt_uri <URI>:<management_port> -replication_port
<replication_port> -replication_factor <n> -conf_deploy_fetch_url <URL>:<management_port> -secret <security_key> -
shcluster_label <label>

splunk restart
```

请注意以下事项：

- 请参阅"部署搜索头群集"以了解 `splunk init shcluster-config` 命令的详细信息，包括不同参数的含义。
- `conf_deploy_fetch_url` 参数指定 Deployer 实例的 URL 和管理端口。当向现有群集添加新成员的时候您必须设置 Deployer，这样成员可以立即联系 Deployer 以获得最新配置软件包（如果有）。请参阅"使用 Deployer 分布应用和配置更新"。

此步骤仅用于新成员。切勿在重新加入群集的成员上运行它。

添加实例

最后一步是向群集中添加实例。您可以在新成员或者群集的任何当前成员上运行 `splunk add shcluster-member` 命令。命令会需要不同的参数，具体取决于您运行命令的位置。

当在新成员自身上运行 Splunk 添加命令的时候，请使用以下版本的命令：

```
splunk add shcluster-member -current_member_uri <URI>:<management_port>
```

请注意以下事项：

- `current_member_uri` 是该节点正在加入的群集上的任何当前成员的管理 URI 和端口。此参数允许新节点与群集通信。

当在当前群集成员上运行 Splunk 添加命令的时候，请使用以下版本的命令：

```
splunk add shcluster-member -new_member_uri <URI>:<management_port>
```

请注意以下事项：

- `new_member_uri` 是您正要添加到群集中的新成员的管理 URI 和端口。此参数必须与您初始化该成员时指定的 `-mgmt_uri` 值一致。

添加后的活动

在成员加入或重新加入群集之后，它会应用所有复制和部署的配置更新：

1. 它会联系 Deployer 来获得配置软件包。

2. 它会联系管理员，下载复制的配置压缩包。

请参阅"配置更改如何跨搜索头群集传输"。

删除群集成员

要从群集中删除成员，可在任一个群集成员上运行 `splunk remove shcluster-member` 命令。

重要提示：您必须使用这里介绍的程序来从群集中删除成员。切勿只停止成员。

要禁用一个成员以便您随后可以重新使用实例，您也必须运行 `splunk disable shcluster-config` 命令。

之后要将成员重新加入到群集中，请参阅"添加之前从群集中删除的成员"。确切的过程取决于您只是从群集中删除成员，还是既删除又禁用成员。

删除成员

警告：在从群集中删除成员之前切勿停止它。

1. 删除成员。

若要在待删除的成员上运行 `splunk remove` 命令，请使用以下版本：

```
splunk remove shcluster-member
```

若要在另一个成员上运行 `splunk remove` 命令，请使用以下版本：

```
splunk remove shcluster-member -mgmt_uri <URI>:<management_port>
```

请注意以下事项：

- `mgmt_uri` 是正从群集中删除的成员的管理 URI。

2. 停止成员。

在删除成员之后，等待约两分钟等配置跨群集更新，然后停止实例：

```
splunk stop
```

通过停止实例，您可以阻止关于删除成员的错误消息出现在管理员上。

通过从搜索头群集中删除实例，您将自动将其从 KV 存储中删除。要确认此实例已从 KV 存储中删除，在任意剩余群集成员上运行 `splunk show kvstore-status`。实例不应出现在结果集中。如果它确实出现了，则您的搜索头群集的运行状况可能有问题。

删除和禁用成员

如果您想要保持实例处于活动状态以用于一些其他功能，则必须在移除之后禁用它：

警告：切勿首先停止成员。

1. 删除成员：

```
splunk remove shcluster-member
```

2. 禁用成员：

```
splunk disable shcluster-config
```

配置群集成员只运行特殊搜索

通常上，群集中的搜索头既服务于来自用户的特殊搜索请求，又服务于由管理员分配的计划的搜索。您可以将群集成员限制为只用于特殊搜索请求。如果您指定一个成员作为特殊搜索头，管理员将不会给它分配任何计划的搜索。

您可以用两种方式指定特殊搜索头：

- 您可以指定特定的成员始终只运行特殊搜索。
- 您可以指定成员在作为管理员时只运行特殊搜索。

注意：尽管您可以指定成员只运行特殊搜索，但您不能指定它只运行计划的搜索。任何群集成员都可以始终运行特殊搜索。当然，您可以通过任何方式来阻止用户访问搜索头。

配置成员只运行特殊搜索

您可能希望预留仅用于特殊使用的某些搜索头，具体取决于您的特定部署。特殊搜索头将永远不会运行计划的搜索。要指定特殊搜索头，设置 `adhoc_searchhead` 属性（位于成员的 `server.conf` 文件中）：

```
[shclustering]
adhoc_searchhead = true
```

必须重新启动实例使更改生效。

配置管理员只运行特殊搜索

您可以指定管理员成员作为特殊搜索头。这会阻止成员作为管理员工作的时候运行计划的搜索，这样管理员可将它的资源专用于控制群集的活动。当管理员角色移动到另一个成员的时候，之前的管理员将继续运行计划的搜索，而新管理员现在将只运行特殊搜索。

重要提示：在所有群集成员上进行此更改，这样不管哪个成员作为管理员，群集行为都会保持一致。

要指定管理员作为特殊搜索头，在每个成员上设置 `captain_is_adhoc_searchhead` 属性（位于 `server.conf`）：

```
[shclustering]
captain_is_adhoc_searchhead = true
```

必须重新启动每个成员使更改生效。不同于搜索头群集化相关的大多数配置更改，您可使用 `splunk rolling-restart` 命令来重新启动所有成员。请参阅“重新启动搜索头群集”。

有关搜索头群集配置的概述，请参阅“配置搜索头群集”。

控制管理员职责

通过以下方法，您可以很大程度控制哪个成员成为管理员：

- 您可以指定成员为“首选管理员”或“非首选管理员”。当群集分配管理员职责时，它会试图将其分配给具有首选管理员指定条件的成员。
- 您可以将管理员职责从一个成员转换到另外一个成员。

使用案例

对于控制管理员职责来处理许多情况很有用。例如：

- 您有一个一直想用作管理员的成员。或者相反，您有一个永不想用作管理员的成员。
- 您不想让管理员执行任何用户启动的特殊任务。实现方法是将某一个特定成员指定为管理员，然后使第三方负载平衡器忽略该成员。
- 您想要修复群集的状态。一个较为快捷的方法是切换到一个新管理员，因为成员们都是在清除的状态下加入新管理员。

首选管理员职责和管理员职责转换的双工具允许您在需要时灵活控制管理员职责。虽然无法保证您总是可以完全控制您的管理员定位准确性，但是至少可以减少不合适的成员充当管理员角色的可能性。并且管理员职责转换提供了根据需要将管理员转换到新成员的功能。

指定管理员职责的首选顺序

您可以指定一些成员作为首选管理员，其他成员作为非首选管理员。当群集分配管理员职责时，它会试图将其分配给

具有首选管理员指定条件的成员。

指定管理员职责的首选顺序

要指定管理员职责的成员首选顺序，设置 `preferred_captain` 属性（位于成员的 `server.conf` 文件中）：

```
preferred_captain = true|false
```

此属性默认为 true，这意味着，默认情况下，所有成员都是首选管理员。

要限制群集将管理员职责分配给一个特定成员的可能性，将该成员的 `preferred_captain` 属性设为 false：

```
preferred_captain = false
```

群集试图遵守管理员职责的首选顺序。

管理员职责首选顺序的限制

群集尝试使用 `preferred_captain=true` 将管理员职责分配给一个成员。但是，它不可能总是将管理员职责分配给一个首选管理员的成员。例如，如果在网络上没有任何首选管理员的成员可用，那么管理员职责可能会被分配给一个 `preferred_captain=false` 的成员。

在新管理员选举期间，非首选管理员成员在管理员职责转换到首选管理员成员之前可以暂时成为管理员。如果无可用首选管理员成员，则非首选管理员成员仍然是管理员，直到一个首选管理员成员变为可用。

转换管理员职责

您可以将管理员职责从一个成员转换到另外一个成员。

管理员职责转换的使用不会影响一般管理员选举进程，因为一般管理员选举进程都要响应"管理员选举"中所述的各种情形。如果选举已经开始，但是最终管理员并非您想要驻留的那个，您随后还可以调用管理员职责转换以重新定位管理员。

更改管理员

想要将管理员职责转换到其他成员，请从当前管理员运行此命令：

```
splunk transfer shcluster-captain -mgmt_uri <URI>:<management_port> -auth <username>:<password>
```

请注意以下事项：

- `-mgmt_uri` 参数为您想要将管理员职责转换给其的成员指定 URI 和管理端口。必须使用完全限定域名。
- 您可在当前管理员中运行此命令。如果您在任何其他成员（如预备管理员）中运行此命令，则您可能会得到一个错误信息。
- 运行命令后，您不用重新启动成员。

如要确定管理员职责转换已成功，请从任何成员运行 `splunk show shcluster-status` 命令：

```
splunk show shcluster-status -auth <username>:<password>
```

在其他已返回的信息中，此命令识别的是当前管理员。

在脚本中采用管理员职责转换的一些方法

`splunk transfer shcluster-captain` 命令能够用于运行某些群集行为的脚本。例如：

- 要确保通过特殊成员保留管理员职责，您可以执行一个 Cron 任务，以定期监视管理员。如果此检查检测到管理员的某一个更改，该检查可以自动运行 `splunk transfer shcluster-captain` 命令以将管理员职责返回给首选的成员。
- 要执行"滚动-重新启动-样式"功能（比如说，通过某个第三方工具部署群集更新），您可以在重新启动当前管理员之前将管理员职责转换到另外一个成员。

管理员职责转换和滚动-重新启动

自 6.3 版本起，滚动-重新启动流程自动调用管理员职责转换，以防止在重新启动过程中更改管理员职责。正因为如此，重新启动之前就是管理员的成员一般在重新启动之后仍旧是管理员。请参阅"重新启动搜索头群集"。

管理员职责转换和静态管理员

管理员职责转换只能通过**动态管理员**进行。关于通过**静态管理员**进行灾难恢复的相关信息，请参阅"使用静态管理员，以从丧失多数优势的状态中恢复"。

处理搜索头群集成员的故障

当成员发生故障的时候，群集通常可以承受此故障并能继续正常工作。

当故障成员重新启动并重新加入群集时，群集往往自动完成此过程。然而，在一些情况下需要您的干预。

当成员发生故障时

如果一个搜索头群集成员因为任意原因发生故障并意外地离开群集，通常群集可以继续工作而不发生中断：

- 群集的高可用性功能确保群集可以继续工作，只要大多数（至少 51%）的成员仍在运行。例如，如果您有一个配置有七个成员的群集，只要至少有四个成员保持正常运行，群集就能工作。如果大多数成员发生故障，群集不能成功选举出新管理员，这会导致整个群集的故障。请参阅"搜索头群集管理员"。
- 驻留在故障成员上的所有搜索项目仍然可以通过其他的搜索头来使用，只要故障的计算机数量少于复制因子。如果故障成员的数量等于或超过复制因子，有可能一些搜索项目对于剩余成员将不再可用。
- 如果故障成员正作为管理员工作，剩余节点会选举另一个成员作为管理员。由于成员间共享配置，新管理员可立即进行全部的工作。
- 如果您在搜索头前面采用了负载均衡器，负载均衡器应该能自动将故障成员上的用户重新路由到可用的搜索头上。

当成员重新加入群集时

如果故障成员的实例成功地重新启动，它会自动重新加入群集。当此情况发生的时候，它的配置需要立即更新，这样它们就匹配其他群集成员的配置。成员需要更新两组配置：

- 从管理员获得的复制更改。请参阅"更新复制更改。"
- 从 Deployer 获得的部署更改。请参阅"更新部署更改。"

有关配置如何在群集成员间共享的信息，请参阅"配置更改如何跨搜索头群集传输"。

更新复制更改

当成员重新加入群集的时候，它联系管理员请求其间发生的复制更改集。接下来发生什么取决于成员和管理员是否在他们的更改历史中共享公共提交：

- 如果管理员和成员仍旧共享一个公共提交，则成员自动从管理员下载中间更改，然后将其应用于它的脱机前配置。成员同样将其中间更改（如有）推送到管理员，管理员将其复制到其他成员。
- 如果管理员和成员没有共享公共提交，则在没有您干预的前提下，他们无法正常同步。如要更新成员配置，您必须指示成员从管理员那里下载整个配置压缩包，如"更新如何进行"里面说明的那样。压缩包覆盖成员的现有一组配置，从而失去任何本地更改的机会。

更改会基于可配置清理限制，随着时间的变化从更改历史中清理掉。

清理限制

清理配置更改历史由 `server.conf` 中的以下属性来确定：

- `conf_replication_purge.eligibile_count`。默认值为 20,000 次更改。
- `conf_replication_purge.eligibile_age`。默认值为一天。

当成员中两个限制都已超过，则成员开始从最早的更改开始，从更改历史中清理。

关于清理限制属性的更多信息，请参阅 server.conf 规范文件。

更新如何进行

当重新加入群集的时候，成员尝试从管理员那里应用中间的复制更改集。如果更改集超过清理限制，并且成员和管理员不再共享一个公共提交时，则一个横幅消息会出现在成员的 UI 上，文本类似于：

```
Error pulling configurations from the search head cluster captain; consider performing a destructive configuration
resync on this search head cluster member.
```

消息也会出现在成员的 `splunkd.log` 文件中。

如果出现这条消息，这意味着成员不能通过配置更改增量来更新配置，而必须应用整个的配置压缩包。不会自动执行此操作。相反，此操作等待您的干预。

然后您必须启动下载过程，通过在成员上运行此 CLI 命令应用压缩包。

```
splunk resync shcluster-replicated-config
```

运行命令后，您不用重新启动成员。

警告：此命令会导致覆盖成员整个的搜索相关配置集，这会引起所有本地更改的丢失。

更新部署的更改

当成员重新加入群集的时候，为了获得最新的配置软件包它会自动联系 Deployer。然后成员应用自上次下载软件包之后发生的任何更改或新增项。

请参阅"使用 Deployer 分布应用和配置更新"。

使用静态管理员，以从丧失多数优势的状态中恢复

群集一般使用**动态管理员**，并且会随着时间的变化更改。动态管理员通过定期选举来选择，并且所有群集成员的大多数人必须同意该管理员。请参阅"管理员选举"。

如果某个群集失去其成员的大多数优势，则它无法选举管理员，也无法继续运行功能。要解决此问题，您可以重新配置群集，使用**静态管理员**来代替动态管理员。

静态管理员无法随着时间的变化而更改。和动态管理员不同的是，群集无法进行选举来选择静态管理员。反之，您可以指定某一个成员为静态管理员，并且该成员将一直是管理员，直到您将另外一个成员指定为管理员。

静态管理员的缺点

静态管理员的主要缺点是：容易成为群集中的单点故障。如果管理员出现故障，则群集也出现故障。群集自身无法取代静态管理员。而且，需要手动干预。

正因为这样，所以 Splunk 建议您只有在灾难恢复时使用静态管理员操作。您可以专门采用静态管理员以从丧失多数优势的状态中恢复，但这样一来群集就无法选举动态管理员。

另外，静态管理员无法检查是否有足够的成员正在运行，以满足复制因子的要求。这意味着在某些条件下，您可能没有完整的搜索项目副本。

注意：您应当只有在绝对需要时再采用静态管理员。转换为静态管理员的过程一般比较通畅和快速，而稍后返回到动态管理员可能会受阻。

静态管理员用例

还有一些在某些情况下切换到静态管理员的明智做法：

- 单个站点群集失去其成员的大多数优势。您可以通过指定其中一位成员为静态管理员，从而恢复群集功能。
- 群集一般在两个站点之间部署。多数成员的站点出现故障。如果没有多数成员，则第二部分的成员，即少数成员的站点无法选举管理员。您可以通过指定少数成员站点中的一位成员为静态管理员，从而恢复群集功能。

在所有情况下，一旦解决沉淀问题，您就应该将群集转换为使用动态管理员。

警告：网络中断一般会中止两个站点之间的通信，但请勿使用静态管理员来解决这一问题。在网络中断期间，由于带有大多数成员的站点可以根据需要选举动态管理员，因此它能够和正常时一样，继续运行功能。然而，带有少数成员的站点无法选举管理员，因而无法作为群集运行功能。如果您尝试配置少数成员站点，然后通过静态管理员将其恢复的话，您将有两个群集，一个带有动态管理员，另外一个带有静态管理员。当网络恢复正常时，您将无法在保持两个站点之间的配置一致性。

切换到静态管理员

要切换到静态管理员，需要重新配置每个群集成员使用静态管理员：

1.在您想要指定为管理员的成员上运行此 CLI 命令：

```
splunk edit shcluster-config -mode captain -captain_uri <URI>:<management_port> -election false
```

2.在每个非管理员成员上运行此 CLI 命令：

```
splunk edit shcluster-config -mode member -captain_uri <URI>:<management_port> -election false
```

请注意以下事项：

- `-mode` 参数指定此实例作为管理员还是只作为一般成员。管理员的功能总是同时以管理员和成员的身份运行。
- `-captain_uri` 参数指定管理员实例的 URI 和管理端口。
- `-election` 参数表示此群集使用的管理员类型。如果 `-election` 设置为 "false"，表示群集使用的是静态管理员。

在运行这些命令后，不需要重新启动管理员或任何其他的成员。管理员将立即控制群集。

要确认群集是否正在通过一个静态管理员运行，可以从以下任何成员中运行此 CLI 命令：

```
splunk show shcluster-status -auth <username>:<password>
```

`dynamic_election` 标记将设置为 0。

转换为动态管理员

当沉淀问题解决后，您应该将群集改为通过单个动态管理员控制。要切换到动态管理员，您可以将之前配置为静态管理员的所有成员进行重新配置。具体做法可以参照您从中进行恢复的方案类型。

本主题提供两个主要方案的转换程序：

- 失去其成员大多数优势的单个站点群集，其中您将其余成员转换为使用静态管理员。一旦群集重新获得多数成员优势，您就应该将成员们回转到动态。
- 双站点群集，其中多数成员站点出现故障，您将少数站点成员转化到使用静态管理员。一旦多数成员站点返回时，您应该将所有成员转化到动态。

返回单个站点群集到动态管理员

失去其成员大多数优势的单个站点群集方案中，一旦群集重新获得成员大多数优势，您就应该将其转化为动态模式：

1. 当成员恢复联机时，将其逐一指向静态管理员：

```
splunk edit shcluster-config -election false -mode member -captain_uri <URI>:<management_port>
```

请注意以下事项：

- `-captain_uri` 参数指定静态管理员实例的 URI 和管理端口。

运行命令后，您不用重新启动成员。

当您将每个重新加入的成员指向静态管理员时，它将下载复制 Delta。如果已经超过清理限制，则系统就会提示您根据"更新如何进行"中说明的那样执行手动重新同步。

警告：完成此程序的其余步骤期间，您的用户不应该进行任何的配置更改。

2. 一旦群集重新获得其大多数成员优势，请将所有成员转化为动态管理员使用。当前的静态管理员应当最后一个转化。要完成此任务，请在每个成员上运行此命令：

```
splunk edit shcluster-config -election true -mgmt_uri <URI>:<management_port>
```

请注意以下事项：

- `-election` 参数表示此群集使用的管理员类型。如果 `-election` 设置为 "true"，表示群集使用的是动态管理员。
- `-mgmt_uri` 参数指定此成员实例的 URI 和管理端口。必须使用完全限定域名。该值与您首次通过 `splunk init` 命令部署成员时所指定的数值相同。

运行命令后，您不用重新启动成员。

3. 启动其中一个成员。该成员随后成为第一个动态管理员。建议您启动的是之前角色为静态管理员的成员。

```
splunk bootstrap shcluster-captain -servers_list "<URI>:<management_port>,<URI>:<management_port>,..." -auth
<username>:<password>
```

关于这些参数的信息，请参阅"启动群集管理员"。

返回双站点群集到动态管理员

失去其成员大多数优势的双站点群集方案中，一旦群集重新获得成员大多数站点优势，您就应该将其转化为动态模

式：

1. 当多数成员站点联机返回时，请将其成员转化为使用静态管理员。将每个多数成员站点成员指向静态管理员：

```
splunk edit shcluster-config -election false -mode member -captain_uri <URI>:<management_port>
```

请注意以下事项：

- `-captain_uri` 参数指定静态管理员实例的 URI 和管理端口。

运行命令后，您不用重新启动成员。

当您将每个重新加入的成员指向静态管理员时，它将下载复制 Delta。如果已经超过清理限制，则系统就会提示您根据"更新如何进行"中说明的那样执行手动重新同步。

2. 等待所有多数成员站点成员获得来自静态管理员的复制配置。这通常需要几分钟的时间。

警告： 完成此程序的其余步骤期间，您的用户不应该进行任何的配置更改。

3. 将所有成员回转到动态管理员使用。当前的静态管理员应当最后一个转化。要完成此任务，请在每个成员上运行此命令：

```
splunk edit shcluster-config -election true -mgmt_uri <URI>:<management_port>
```

请注意以下事项：

- `-election` 参数表示此群集使用的管理员类型。如果 `-election` 设置为 "true"，表示群集使用的是动态管理员。
- `-mgmt_uri` 参数指定此成员实例的 URI 和管理端口。必须使用完全限定域名。该值与您首次通过 `splunk init` 命令部署成员时所指定的数值相同。

运行命令后，您不用重新启动成员。

4. 启动其中一个成员。该成员随后成为第一个动态管理员。建议您启动的是之前角色为静态管理员的成员。

```
splunk bootstrap shcluster-captain -servers_list "<URI>:<management_port>,<URI>:<management_port>,..." -auth
<username>:<password>
```

关于这些参数的信息，请参阅"启动群集管理员"。

重新启动搜索头群集

使用 `splunk rolling-restart` 命令重新启动整个群集。该命令将执行所有群集成员的分阶段重新启动，以便整个群集可以在重新启动过程期间继续执行其功能。

在分发配置软件包到成员后，Deployer 还在必要时自动启动滚动重新启动。有关该流程的详细信息，请参阅"推送配置软件包"。

警告： 在大部分情况下，当更改 `[shcluster]` 段落（位于 `server.conf`）中的配置设置时，您必须几乎同时重新启动所有成员，以确保所有成员保持一致的设置。为此，除非是配置 `splunk rolling-restart` 属性的时候，在类似配置更改后切勿使用 `captain_is_adhoc_searchhead` 命令重新启动成员。相反，在每个成员上运行 `splunk restart` 命令。请参阅"配置搜索头群集"。

启动滚动重新启动

从管理员调用 `splunk rolling-restart` 命令：

```
splunk rolling-restart shcluster-members
```

监控重新启动过程

要检查滚动重新启动的进度，请从管理员中运行 `splunk rolling-restart` 命令的变体：

```
splunk rolling-restart shcluster-members -status 1
```

该命令返回已开始或结束重新启动过程的任何成员的状态。例如：

```
Peer | Status | Start Time | End Time | GUID
1. server-centos65x64-4 | RESTARTING | Mon Apr 20 11:52:21 2015 | N/A | 7F10190D-F00A-47AF-8688-8DD26F1A8A4D
```

```
2. server-centos65x64-3 | RESTART-COMPLETE | Mon Apr 20 11:51:54 2015 | Mon Apr 20 11:52:16 2015 | E78F5ECF-1EC0-4E51-9EF7-5939B793763C
```

您可以在重新启动过程中多次运行 `splunk rolling-restart` 命令以查看重新启动的当前状态。当管理员在过程末尾时重新启动，则命令将会出现故障。管理员重新启动之后，您可以在管理员的 `audit.log` 文件中查看重新启动的最后状态：

```
index=_audit rolling-restart
```

滚动重新启动如何工作

滚动重新启动的运行方式是：管理员一次发送重新启动消息给约 10%（默认）的成员。这些成员重新启动并与管理员联系之后，管理员会向另一个 10% 的成员发出重新启动消息，依此类推，直到所有成员（包括管理员）都已重新启动。

注意：如果群集中的成员少于 10 个，则管理员会一次对一个成员发起重新启动。

管理员是最后一个重新启动的成员。管理员成员重新启动之后，它将继续以管理员身份运行功能。

在所有成员都重新启动后，群集需要大约 60 秒达到稳定。在此间隔期间，可能会出现错误消息。您可以忽略这些消息。它们应该在 60 秒内停止。

注意：在滚动重新启动期间，无法保证所有的知识对象对于所有成员可用。

配置同时重新启动的成员数量

默认情况下，管理员将一次发出重新启动命令给 10% 的成员。然而，该百分比可以通过 `percent_peers_to_restart` 属性（位于 `[shcluster]` 段落，在 `server.conf` 中）配置。为方便起见，您可以使用 CLI 命令 `splunk edit shcluster-config` 配置本属性。例如，要更改重新启动行为以便管理员一次重新启动 20% 的对等节点，使用本命令：

```
splunk edit shcluster-config -percent_peers_to_restart 20
```

警告：切勿设置大于 20% 的值。否则，在管理员选举过程中会出现问题。

在更改 `percent_peers_to_restart` 属性后，您仍需要运行 `splunk rolling-restart` 命令以真正开始重新启动。

如果群集无法维持大多数成员优势，则重新启动出现故障

带有**动态管理员**的群集需要多数成员能够一直保持运行状态。请参阅“管理员选举”。此要求将扩展到滚动重新启动过程。

如果下一组成员（由 `percent_peers_to_restart` 属性控制）重新启动时导致活跃的成员数量降到 51% 以下（比如，由于某些其他成员出现故障所导致），则重新启动过程将停止，以确保大多数成员都处于活跃状态。然后管理员将多次尝试重新启动流程，以防其他成员重新加入过渡期间的群集中。在 `restart_timeout` 时段（默认为 10 分钟）结束之前，这些尝试操作都将持续进行。此时，管理员不再进行更多的尝试，同时其余成员也不会再查看滚动重新启动过程。

`restart_timeout` 属性可以在 `server.conf` 中进行设置。

查看搜索头群集状态

使用 CLI 查看关于搜索头群集的信息

一些 CLI 命令提供搜索头群集的状态信息。

您还可以使用监视控制台以获得更多关于群集的信息。请参阅“使用监视控制台查看搜索头群集状态和解决问题”。

显示群集状态

要检查搜索头群集的总体状态，在任意成员上运行此命令：

```
splunk show shcluster-status -auth <username>:<password>
```

此命令返回管理员和群集成员的基本信息。所提供的关键信息包括：

- （管理员部分。）`dynamic_captain` 字段表示群集是否使用**动态管理员**。数值为 1 指定的是动态管理员。
- （管理员部分。）`id` 字段指定的是群集 GUID。此 GUID 与任何群集成员（包括管理员）的 GUID 都不同。
- （管理员部分。）`label` 字段指定群集标签。监视控制台使用的是标签标识符。
- （每个成员的部分。）`status` 字段指示每个成员的状态：正常、故障、滞留或重新启动。以下状态数值需要说

明：

  - **滞留。**当群集成员磁盘空间耗尽的时候，它进入滞留状态。当在滞留状态的时候，管理员将不会给它分配计划的搜索或项目副本。要修复的话，您必须增加实例可用的磁盘空间。
  - **故障。**当一个成员由于某些故障退出群集或您手动将其从群集中删除时，该成员会进入故障状态。当您运行此命令时，管理员会注意这点并报告成员状态为“故障”。然而，如果稍后管理员职责有所转换，则新管理员不会有任何成员离开群集的记录。当您对新管理员运行此命令时，它不会返回关于故障成员的任何信息。
  - **待定。**这表示该成员正尝试重新加入群集中。这是一种过渡状态。当成员成功地重新加入群集后，其状态会变为**正常**。

- （每个成员的部分。）`last_conf_replication` 字段指示成员上一次是何时从管理员上提取了一组配置。请参阅“查看复制状态”。

显示成员配置

要检查群集成员的配置，可在成员自身上运行此命令：

```
splunk list shcluster-config -auth <username>:<password>
```

或者，您可以在另一个成员上运行下面的命令变体：

```
splunk list shcluster-config -uri <URI>:<management_port> -auth <username>:<password>
```

请注意以下事项：

- `-uri` 参数为要检查其配置的成员指定 URI 和管理端口。

群集成员列表

要获得所有群集成员的列表，请从任一成员上运行以下命令：

```
splunk list shcluster-members -auth <username>:<password>
```

此命令返回群集的所有成员，以及它们的配置。

注意：此命令继续列出离开群集的成员，直到管理员职责有所转换。

成员信息列表

要列出成员的信息，可在成员自身上运行此命令：

```
splunk list shcluster-member-info -auth <username>:<password>
```

或者，您可以在另一个成员上运行下面的命令变体：

```
splunk list shcluster-member-info -uri <URI>:<management_port> -auth <username>:<password>
```

请注意以下事项：

- `-uri` 参数为您希望了解配置的成员指定 URI 和管理端口。

列出搜索项目

要列出存储在群集上的项目集，可在管理员上运行此命令：

```
splunk list shcluster-artifacts
```

要列出存储在特定成员上的项目集，可在成员自身上运行此命令：

```
splunk list shcluster-member-artifacts
```

列出计划程序任务

要列出计划程序任务集，可在管理员上运行此命令：

```
splunk list shcluster-scheduler-jobs -auth <username>:<password>
```

使用监视控制台查看搜索头群集状态和解决问题

您可以使用监视控制台来监视部署的大多数方面。本主题讨论的是提供搜索头群集洞察的控制台仪表板。

监视控制台的主要文档位于*《监视 Splunk Enterprise》*。

监视控制台中的“搜索头群集化”仪表板

在**搜索**菜单下面有若干搜索头群集化仪表板：

- 搜索头群集化：状况和配置
- 搜索头群集化：配置复制
- 搜索头群集化：项目复制
- 搜索头群集化：计划程序委派
- 搜索头群集化：应用部署

这些仪表板提供关于搜索头群集的大量信息，如：

- 群集成员实例名称和状况
- 当前管理员识别和管理员选举活动
- 配置复制性能
- 项目复制详情
- 计划程序活动
- Deployer 活动

自行查看仪表板的更多信息。此外，请参阅*《监视 Splunk Enterprise》*中的“搜索头群集化仪表板”。

注意：您还可以使用 CLI 以获得更多关于群集的信息。请参阅“使用 CLI 查看关于搜索头群集的信息”。

搜索头群集故障排除

作为搜索头群集连续监视的一部分，监视控制台提供了用于故障排除的各种信息。例如：

- 搜索头群集化：“状态”和“配置”仪表板显示：
  - 各种类型搜索的搜索并发，带有关于运行与限制的详细信息：
  - 状态，包括管理员职责和状态
  - 检测信号信息（在本主题中其他部分讨论）
  - 配置基线一致性（在本主题中其他部分讨论）
  - 项目计数
  - 选举活动
- 搜索头群集化：“配置复制”仪表板显示：
  - 警告和错误模式
  - 配置复制活动
- 搜索头群集化：“项目复制”仪表板显示：
  - 警告和错误模式
  - 项目复制活动
- 搜索头群集化：“计划程序委派”仪表板显示：
  - 计划程序委派活动
- 搜索头群集化：“应用部署”仪表板显示：
  - 应用部署的状态

故障排除检测信号问题

搜索头群集化：“状态”和“配置”仪表板有助于了解群集成员发送给管理员的检测信号。具体地说，它为每个成员显示：

- 成员上一次发送检测信号给管理员的时间
- 管理员上一次收到成员的检测信号的时间

这些时间应该是相同的或几乎相同。发送和接收时间的显着差异表明可能存在问题。

您也可以通过 REST API 来访问检测信号信息。有关 shcluster/captain/members/{name}，请参阅 REST API 文档。

检测信号的角色

成员定期向管理员发送检测信号。默认情况下，成员每五秒发送一次检测信号。

频率通过每个成员上 `server.conf` 的 `[shclustering]` 段落中的 `heartbeat_period` 属性来定义。所有成员必须将此属性设置为相同的值。

检测信号是从成员到管理员的基础通信。这表示该成员处于活动状态，并且是群集的一部分。检测信号也包含了多种信息，如：

- 搜索项目
- 已派遣搜索
- 告警和抑制
- 已完成的摘要任务
- 成员负载信息

当管理员收到检测信号时，它注意到该成员处于 "up" 状态。

在管理员从每个节点都接收到检测信号之后，它将所有的发送信息合并，并且反过来向成员发送信息，例如：

- 搜索项目日志
- 全部的告警和抑制列表
- 已派遣搜索

检测信号故障的影响

管理员期望定期从每个成员收到检测信号，如 `server.conf` 的 `[shclustering]` 段落中的 `heartbeat_timeout` 属性所指定的。

默认情况下，超时设为 60 秒。

管理员只能通过成员的检测信号知道它的存在。如果它从未收到检测信号，它将不知道成员存在。

如果在指定的超时时间内，管理员没有从之前发送检测信号的成员收到检测信号，则管理员将该成员标记为 "down"。管理员不会向处于 "down" 状态的成员分发新的搜索。

检测信号故障的原因

如果管理员没有收到成员的检测信号，通常表示下列情况之一：

- 成员出现故障或不可用。
- 管理员和成员之间的网络分区。
- HTTP 请求失败。这些在管理员的 `splunkd_access.log` 中可见。

注意：默认情况下，Splunk Enterprise 只在 `splunkd_access.log` 中记录检测信号故障。要同样为检测信号成功启用日志记录，在管理员上配置 `server.conf` 的 `[shclustering]` 段落中的 `access_logging_for_heartbeats=true`。如果您想要该配置更改在管理员职责转换中存在，请对所有成员进行更改，而不只是当前管理员。

配置基线一致性故障排除

搜索头群集化：“状态”和“配置”仪表板包括配置基线的一致性的信息。此信息有助于确定是否在群集成员集间正确地复制了配置更改。

要查找此信息，转到仪表板的“快照”部分并查看“状态”表。每个成员都对应一行。该表包括与基线一致性有关的两列：

- **配置基线一致性**。此列包含一个比较每个成员的基线与所有其他成员的基线一致性的比率。有关更多详细信息，请单击比率。右边的一个表针对每个单独的成员比较成员的基线一致性。
- **未发布的更改数目**。此列指示成员上是否有任何尚未被复制到管理员的配置更改集。特别是，它会注释一个成员是否与管理员不同步。

当检测到基线不匹配时，至少有一个成员需要采取显式操作以恢复基线一致性。检查一致性比较表，以确定与其他大多数成员不同步的成员。要恢复一致性，在成员上运行 `splunk resync shcluster-replicated-config`。请参阅“更新复制更改”。

关于配置复制的介绍，请参阅“群集复制的配置更新”。

搜索头群集化故障排除

部署问题

当添加新成员的时候崩溃

如果在您添加成员到群集中时成员崩溃，请确定此实例是否之前是另一个群集的成员。如果是这样，您可能没有从之前的群集中正确地删除此成员。

当添加成员到群集中时，建议您始终使用新实例，但是如果您选择重新使用一个实例，必须遵循“添加新成员”中的说明。

运行时注意事项

由于群集成员间协调导致的延迟

管理员与其他群集成员间的协调有时会产生最多 1.5 分钟的网络延迟。例如，当您保存搜索任务时，Splunk Web 短时间内可能不会更新任务状态。同样，管理员需要一分钟或更多的时间来精心安排任务的完整删除。

此外，当一个事件触发新管理员的选举时，到选举完成时将会有一到两分钟的间隔。在此期间，搜索头仅服务于特殊任务请求。

限制活动告警的数量

搜索头群集可处理大约 5000 个活动的未过期的告警。要保持在此界限内，使用告警限制或限制告警保存时长。请参阅*《告警手册》*。

站点故障会阻止管理员选举

如果群集部署在两个站点上，拥有多数成员的站点发生故障或者不可访问，则群集不能选举出新管理员。

要修正此状况，您可以临时部署一个**静态管理员**。请参阅"使用静态管理员，以从丧失多数优势的状态中恢复。"

处理 Raft 问题

如果成员上的搜索头群集的基础 Raft 元数据进入错误状态，您可以通过清理成员的 `var/run/splunk/_raft` 文件夹来纠正这个问题。请参阅"修复成员上的 Raft 问题"。

如果由于 Raft 问题，群集无法选举出管理员并保持正常运行状态，您可以清理所有成员的 Raft 文件夹，然后启动群集。请参阅"修复整个群集"。

修复成员上的 Raft 问题

Raft 问题的主要症状是，当您在管理员上运行 `splunk show shcluster-status` 时，成员的状态显示为 "down"。要确认 Raft 问题，在成员的 `splunkd.log` 文件中查找以字符串 "ERROR SHCRaftConsensus" 开始的错误消息。

成员的 `_raft` 文件夹中的文件被破坏是 Raft 问题的常见原因。您可以通过清理成员上的文件夹来解决这个问题。然后从管理员填充文件夹。

要修复 Raft 问题，清理成员的 `_raft` 文件夹。在成员上运行 `splunk clean raft` 命令：

1. 停止成员：

   ```
   splunk stop
   ```
2. 清理成员的 Raft 文件夹：

   ```
   splunk clean raft
   ```
3. 启动成员：

   ```
   splunk start
   ```

然后从管理员填充 `_raft` 文件夹。

修复整个群集

如果即使大多数成员都可用，管理员选举仍然失败，则 Raft 元数据被破坏是一个可能的原因。要确认，您可以检查成员的 `splunkd.log` 文件中是否有以字符串 "ERROR SHCRaftConsensus" 开始的错误。

您可以通过清理所有成员的文件夹然后启动群集来解决问题：

1. 停止所有成员。
2. 在每个成员上运行 `splunk clean raft`：

   ```
   splunk clean raft
   ```
3. 启动所有成员。
4. 选择一个成员作为管理员，并启动它：

   ```
   splunk bootstrap shcluster-captain -servers_list "<URI>:<management_port>,<URI>:<management_port>,..." -auth
   <username>:<password>
   ```
5. 如果您使用的是搜索节点复制，则必须将搜索节点重新添加到一个成员中。请参阅"在整个群集内复制搜索节点"。

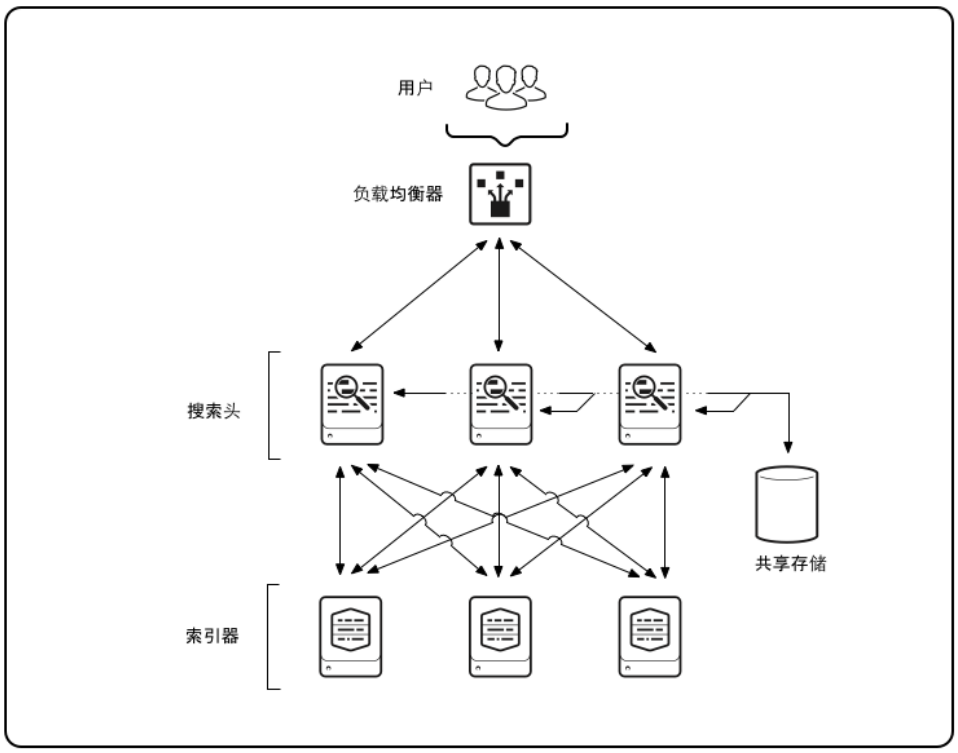
搜索头合并

搜索头合并概述

已弃用此功能。
Splunk Enterprise 6.2 版本中已弃用此功能。这意味着，尽管这将继续运行，但可能在未来版本删除。 作为替代方法，您可以部署搜索头群集化。请参阅"关于搜索头群集化"。 有关所有弃用功能的列表，请参阅《发行说明》中的主题"弃用功能"。

重要提示：搜索头合并是高级功能。建议您联系 Splunk 销售团队，在尝试实施之前讨论您的部署。

您可以设置多个搜索头，以便它们共享配置和用户数据。这被称为**搜索头合并**。拥有多个搜索头的主要原因在于，当您拥有大量用户搜索同一数据时，横向扩张变得较为容易。如果搜索头不可用，搜索头合并还可减少影响。本图提供了带搜索头合并的典型部署的概述：



您在希望包含在池中的每个搜索头启用搜索头合并，以便它们可以共享配置和用户数据。一旦启用搜索头合并，这些对象类别将作为池中的所有搜索头的通用资源：

- **配置数据** -- **配置文件**包含用于**保存的搜索**和其他**知识对象**的设置。
- **搜索项目**，特定搜索运行的记录。
- **计划程序状态**，以便仅池中的一个搜索头可以运行特定**计划的报表**。

例如，如果在搜索头上创建并保存搜索，则池中的所有其他搜索头将自动拥有对它的访问权限。

搜索头合并使得 `$SPLUNK_HOME/etc/{apps,users}` 中的所有文件可用于共享。这包括 *.conf 文件、*.meta 文件、view 文件、搜索脚本、查找表等。

主要实施问题

请注意以下事项：

- 大部分共享存储解决方案无法正常跨 WAN 执行。由于搜索头合并要求低延迟共享存储能够每秒满足大量运行，因此跨 WAN 实施搜索头合并不会得到支持。
- 池中的所有搜索头必须运行相同版本的 Splunk Enterprise。务必要立即升级所有。请查看*《安装手册》*中的"升级您的分布式 Splunk Enterprise 部署"。

- 搜索头合并的目的是简化 *专用*搜索头的组管理。不要在作为搜索头的索引器组上实施它。那是不支持的配置。*搜索头合并对索引性能具有极大影响。*
- 池中的搜索头不能是彼此的搜索节点。

搜索头合并和知识软件包

搜索头分发给其搜索节点的一组数据被称为**知识包**。有关详细信息，请参阅"搜索头发送给搜索节点的内容"。

默认情况下，仅搜索头池中的搜索头会发送知识软件包给一组搜索节点。同时，如果池中的搜索头还是彼此的搜索节点，则它们将不会发送软件包给彼此，因为它们可以访问池中的软件包。这是 4.3.2 版本引入的优化，但在 5.0 版本中成为默认。它通过 distsearch.conf 中的 `useSHPBundleReplication` 属性控制。

作为进一步优化，您可以安装知识库到共享存储，如同"关于安装软件包"所述。这样做，您无需分发软件包到搜索节点。有关如何组合搜索头合并与安装知识软件包的信息，请阅读名为"使用搜索头合并的安装软件包"的主题中的部分。

相关信息

有关搜索头合并的更多信息，请参阅本章节其他主题：

- "创建搜索头池"
- "对搜索头池使用负载均衡器"
- "其他合并操作"
- "管理配置更改"
- "部署服务器和搜索头合并"
- "为配置刷新选择时间"

问答

有什么问题吗？请访问 Splunk Answers，查看 Splunk 社区有哪些与搜索头合并相关的问题和答案。

创建搜索头池

要创建搜索头池，请遵照这些步骤：

1. 设置每个搜索头可以访问的共享存储位置。

2. 配置每个搜索头。

3. 停止搜索头。

4. 启用每个搜索头的合并。

5. 复制用户和应用目录到共享存储位置。

6. 重新启动搜索头。

以下详细介绍了操作步骤：

1.设置每个搜索头可以访问的共享存储位置

这样池中的每个搜索头可以共享配置和项目，他们需要通过共享存储访问通用文件集：

- **在 *nix 平台上，**设置 NFS 安装。
- **在 Windows 上，**设置 CIFS (SMB) 共享。

重要提示：Splunk 用户帐户需要对共享存储位置的读取/写入访问权限。*当在 Windows 上安装搜索头时，请务必作为拥有对共享存储的读取/写入访问权限的用户进行安装。本地系统用户没有本访问权限。*有关更多信息，请参阅《安装手册》中的"选择运行 Splunk 的用户"。

2.配置每个搜索头

a. 单独设置每个搜索头，以常规方式指定搜索节点。请参阅"添加搜索节点到搜索头"。

b. 确保每个搜索头在 server.conf 中配置的 `serverName` 属性唯一。有关本要求的详细信息，请参阅"管理分布式服务器名称"。如果搜索头没有唯一的 `serverName` 属性，则在启动时会生成警告。有关详细信息，请参阅"有关唯一 serverName 属性的警告"。

c. 指定必要验证。您有两个选择：

- 单独指定每个搜索头的用户验证。搜索头上的一个有效用户不会自动成为池中的另一个搜索头的用户。您可以

使用 LDAP 以集中管理用户验证，如同“使用 LDAP 设置用户验证”所述。

- 在共享存储上放置所有池成员使用的通用验证配置。在对验证进行任何更改后，您必须重新启动池成员。

注意：在单个池成员上进行的任何验证更改（例如，通过 Splunk Web）将覆盖*仅限该池成员*的共享存储上的任何配置。因此，如果共享存储已经存在通用配置，您应避免通过 Splunk Web 进行验证更改。

3.停止搜索头

在启用合并之前，必须先停止 `splunkd`。为池中的每个搜索头进行此设置。

4.启用每个搜索头的合并

使用 CLI 命令 `splunk pooling enable` 启用搜索头的合并。此命令会设置 `server.conf` 中的某些值。它还在共享存储位置内创建子目录，并验证 Splunk Enterprise 可在其中创建和移动文件。

命令语法如下：

```
splunk pooling enable <path_to_shared_storage> [--debug]
```

注意：

- 在 NFS 上，`<path_to_shared_storage>` 应是 NFS 的共享安装点。
- 在 Windows 上，`<path_to_shared_storage>` 应是 CIFS/SMB 共享的 UNC 路径。
- `--debug` 参数导致命令记录额外信息到 `btool.log`。

在池中的每个搜索头上执行本命令。

此命令会设置 `[pooling]` 段落中的值。此段落属于 `server.conf` 文件（位于 `$SPLUNK_HOME/etc/system/local`）。

您还可以直接编辑 `[pooling]` 段落（属于 `server.conf`）。有关 `server.conf` 的详细信息，请查看此处。

重要提示：`[pooling]` 段落必须放在 `server.conf` 文件中。该文件位于 `$SPLUNK_HOME/etc/system/local/` 下。这意味着，您无法通过应用（无论在本地磁盘或共享存储上）部署 `[pooling]` 段落。有关详细信息，请参阅 server.conf spec 文件。

5.复制用户和应用目录到共享存储位置

复制现有搜索头上的 `$SPLUNK_HOME/etc/apps` 和 `$SPLUNK_HOME/etc/users` 目录的内容到共享存储位置的空目录 `/etc/apps` 和 `/etc/users`。这些目录在第 4 步中创建，并驻留在您当时指定的 `<path_to_shared_storage>` 下。

例如，如果您的 NFS 安装位于 `/tmp/nfs`，则复制匹配该模式的应用子目录：

```
$SPLUNK_HOME/etc/apps/*
```

到

```
/tmp/nfs/etc/apps
```

这将导致一组子目录，如：

```
/tmp/nfs/etc/apps/search
/tmp/nfs/etc/apps/launcher
/tmp/nfs/etc/apps/unix
[...]
```

类似地，复制用户子目录：

```
$SPLUNK_HOME/etc/users/*
```

到

```
/tmp/nfs/etc/users
```

重要提示：您可以选择仅复制应用子集和子目录；然而，请务必移动它们到上述的准确位置。

6.重新启动搜索头

在运行 `splunk pooling enable` 命令后，重新启动 `splunkd`。为池中的每个搜索头进行此设置。

对搜索头池使用负载均衡器

您可能希望运行搜索头前面的负载均衡器。通过这种方式，用户可以通过单个界面访问搜索头池，而无需指定某个搜索头。

使用负载均衡器的另一种原因是，如果其中一个搜索头出现故障，确保访问搜索项目和结果。通常，RSS 和电子邮件告警提供对发起搜索的搜索头的链接。如果该搜索头出现故障（同时没有负载均衡器），项目和结果将变得无法访问。然而，如果您在前面有一个负载均衡器，则可设置告警以便它们引用负载均衡器而不是某个搜索头。

配置负载均衡器

当选择和配置负载均衡器时，这里有一些问题要注意：

- 负载均衡器必须采用 7 层（应用程序级别）处理。
- 配置负载均衡器，以便用户会话"粘住"或"持续"。这可确保用户在整个会话期间保持在单个搜索头上。

生成至负载均衡器的告警链接

要生成至负载均衡器的告警链接，您必须编辑 `alert_actions.conf`：

1. 从搜索头复制 `alert_actions.conf` 到共享存储位置的适当应用目录。在大部分情况下，目录为 `/<path_to_shared_storage>/etc/apps/search/local`。

2. 编辑 `hostname` 属性以指向负载均衡器：

```
hostname = <proxy host>:<port>
```

有关详细信息，请参阅《管理员手册》中的 alert_actions.conf。

告警链接现在应指向负载均衡器，而不是单个搜索头。

其他合并操作

除了 CLI 命令 `splunk pooling enable` 之外，还有其他几个命令对于管理搜索头合并非常重要：

- `splunk pooling validate`
- `splunk pooling disable`
- `splunk pooling display`

必须先停止 `splunkd`，之后才能运行 `splunk pooling enable` 或 `splunk pooling disable`。然而，您可以运行 `splunk pooling validate` 和 `splunk pooling display`，当 `splunkd` 已经停止或正在运行的时候都可以。

验证每个搜索头拥有对共享资源的访问权限

最初设置搜索头合并时，`splunk pooling enable` 命令将验证搜索头访问权限。如果需要验证搜索头对共享资源的访问权限（例如，如果您更改 NFS 配置），则可运行 CLI 命令 `splunk pooling validate`：

```
splunk pooling validate [--debug]
```

禁用搜索头合并

您可以使用本 CLI 命令禁用搜索头合并：

```
splunk pooling disable [--debug]
```

为您需要禁用的每个搜索头禁用本命令。

重要提示：在运行 `splunk pooling disable` 命令之前，您必须先停止 `splunkd`。在运行该命令后，应重新启动 `splunkd`。

显示合并状态

您可以使用 CLI 命令 `splunk pooling display` 来确定是否在搜索头上启用合并：

```
splunk pooling display
```

本示例显示系统如何根据是否启用合并做出反应：

```
$ splunk pooling enable /foo/bar
$ splunk pooling display
```

```
Search head pooling is enabled with shared storage at: /foo/bar
$ splunk pooling disable
$ splunk pooling display
Search head pooling is disabled
```

管理配置更改

重要提示：一旦在搜索头上启用合并，您必须在直接编辑配置文件时通知搜索头。

具体来说，如果添加段落给 `local` 目录中的任何配置文件，您必须运行以下命令：

```
splunk btool fix-dangling
```

注意：如果通过 Splunk Web 或 CLI 进行更改，这将没有必要。

部署服务器和搜索头合并

通过搜索头合并，所有搜索头将访问单个配置集，以便您无需使用**部署服务器**或第三方部署管理工具，如 Puppet 以推送更新给多个搜索头。然而，您可能仍希望使用部署工具搜索头合并，以合并跨所有 Splunk Enterprise 实例的配置操作。

如果您希望使用部署服务器管理您的搜索头配置，请注意以下：

1.通过创建 `deploymentclient.conf` 文件（位于 `$SPLUNK_HOME/etc/system/local`）并指定其部署服务器，指定一个搜索头为部署客户端。您无需指定一个搜索头为部署客户端。

2.在 `deploymentclient.conf` 中，设置 `repositoryLocation` 属性为搜索头的共享存储安装点。您还必须设置 `serverRepositoryLocationPolicy=rejectAlways`，以确保本地设置的 `repositoryLocation` 会作为下载位置。

3.在部署服务器上的 `serverclass.conf` 中，定义搜索头客户端的服务器类。

有关部署服务器的详细信息，请参阅*《更新 Splunk Enterprise 实例》*手册中的"关于部署服务器"。

为配置刷新选择时间

在 5.0.2 和更早版本中，从存储位置同步的默认值被设置为非常频繁的间隔。这会导致花费过长时间读取来自池的配置更改，尤其对于具有大量用户（数百或数千）的部署。

自 5.0.3 起，默认设置被更改为更加不频繁的间隔。在 `server.conf` 中，以下设置会影响配置刷新时间：

```
# 5.0.3 defaults
[pooling]
poll.interval.rebuild = 1m
poll.interval.check = 1m
```

这些设置的之前默认值分别是 2s 和 5s。

对于旧默认值，对搜索头进行的更改将在 7 秒后对另一个搜索头可用。通常无需对此进行更新以快速传输。通过更改设置为一分钟，共享存储系统上的负载将极大减少。根据业务需求的不同，您可以设置这些值为更长的间隔。

升级搜索头池

池中的所有搜索头必须运行相同版本的 Splunk Enterprise。

有关升级程序，请参阅*《安装手册》*中的"升级您的分布式 Splunk Enterprise 部署"。在尝试升级您的搜索头池之前，请仔细阅读此程序。您必须准确地按此步骤执行，以确保池功能完全正常。

安装知识软件包

关于安装软件包

重要提示：对于大多数部署，Splunk 建议您使用普通软件包复制，而不是带有共享存储的安装软件包。作为 5.0 timeframe 中对软件包复制的更改结果，如基于 Delta 复制的引入和流中的改进，安装软件包的实际用例当前受到极大的限制。在大多数情况下，安装软件包在网络流量方面或软件包更改分发到搜索节点的速度方面的差别微乎其微。同时，添加重要的管理复杂性，尤其是与共享存储结合时。由于这是基于 Delta 的复制，因此即使您的配置包含大型文件，只要这些文件没有变化，普通软件包复制就几乎不会包含连续的复制成本。

搜索头分发给其搜索节点的一组数据被称为**知识包**。软件包内容驻留在搜索头的

`$SPLUNK_HOME/etc/{apps,users,system}` 子目录中。有关本软件包的内容和用途的信息，请参阅"搜索头发送给搜索节点的内容"。

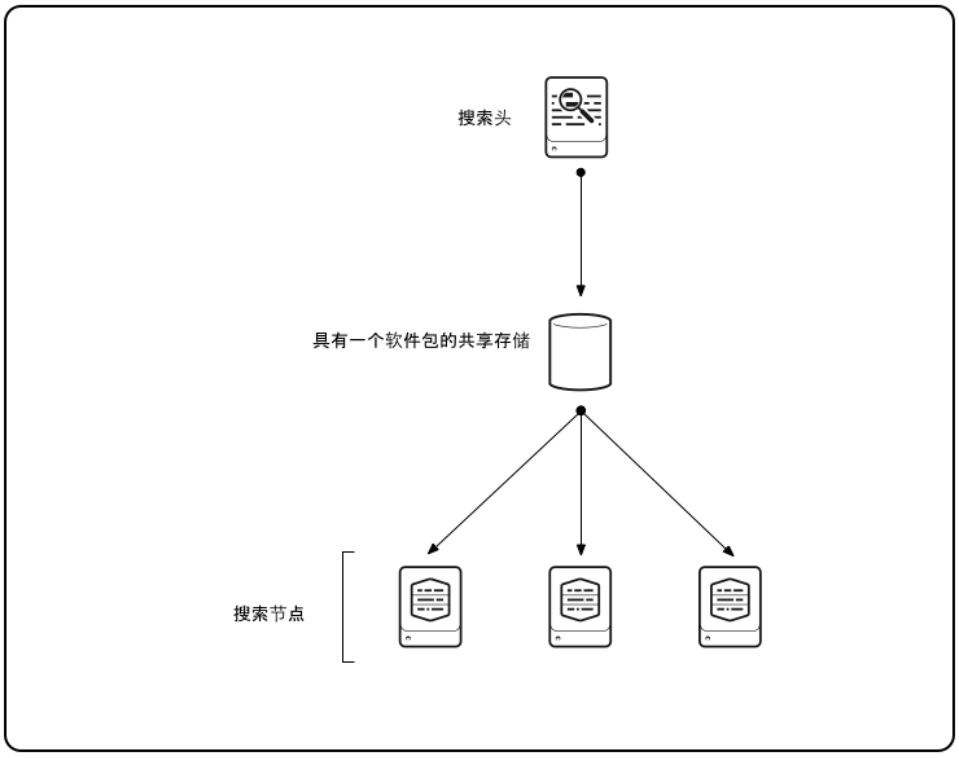
默认情况下，搜索头复制并分发知识软件包给每个搜索节点。您可以告诉搜索节点安装知识软件包的目录位置，消除软件包复制的需求。当安装知识包到共享存储时，它被称为**安装软件包**。

警告：大部分共享存储解决方案无法跨 WAN 正常运行。由于安装软件包需要共享存储，因此您通常不应跨 WAN 进行实施。

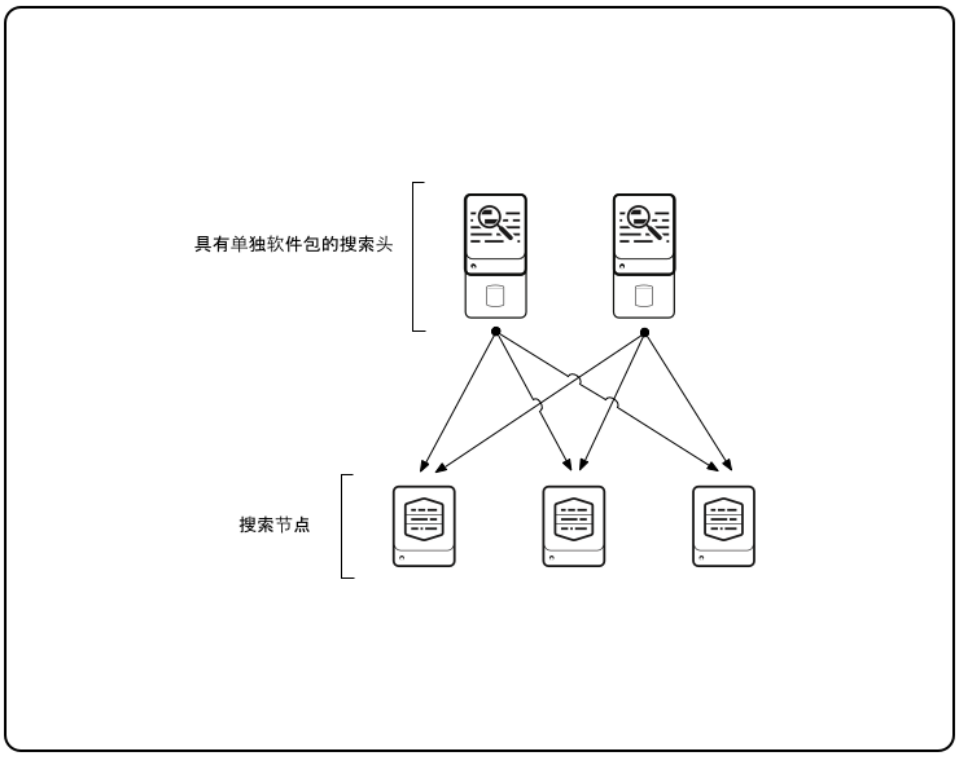
安装软件包架构

根据搜索头配置的不同，这里有一些方式来设置安装软件包。这里是一些典型的方式：

- **用于单个搜索头。**安装知识软件包到共享存储。然后，所有搜索节点访问软件包以处理搜索请求。本图介绍了在共享存储上安装软件包的单个搜索头：



- **用于多个非群集搜索头。**在每个搜索头的本地存储上保留知识软件包。在本图中，每个搜索头保留其自己的软件包，其中每个搜索节点单独安装和访问：



在每种情况下，搜索节点需要访问每个搜索头的 `$SPLUNK_HOME/etc/{apps,users,system}` 子目录。

搜索节点仅在执行搜索头的搜索请求时使用安装目录。对于索引和其他与分布式搜索不直接相关的用途，搜索节点将使用它们自己的本地 `apps`、`users` 和 `system` 目录，与其他索引器一样。

配置安装软件包

要设置安装软件包，您需要同时配置搜索头及其搜索节点。这里介绍的程序假定软件包在共享存储上，但是它们无需这样。它们仅需要在一些搜索头和搜索节点可以访问的位置。

配置搜索头

这里是配置搜索头的步骤：

1. 在共享存储上安装软件包子目录 (`$SPLUNK_HOME/etc/{apps,users,system}`)。最简单的方式是安装搜索头的整个 `$SPLUNK_HOME/etc` 目录：

- **在 *nix 平台上，**设置 NFS 安装。
- **在 Windows 上，**设置 CIFS (SMB) 共享。

重要提示：搜索头的 Splunk 用户帐户需要对共享存储位置的读取/写入访问权限。搜索节点只能具有软件包子目录的读取权限，从而避免文件锁定问题。搜索节点无需在共享存储位置中更新任何文件。

2. 在搜索头的 `distsearch.conf` 文件中，设置：

```
shareBundles=false
```

这将让搜索头停止复制软件包到搜索节点。

3. 重新启动搜索头。

配置搜索节点

对于每个搜索节点，遵照这些步骤以访问安装软件包：

1. 在搜索节点上安装软件包目录。

2. 在搜索节点上创建 `distsearch.conf` 文件（位于 `$SPLUNK_HOME/etc/system/local/`）。对于对等节点连接到的每个搜索头，使用以下属性创建 `[searchhead:<searchhead-splunk-server-name>]` 段落：

```
[searchhead:<searchhead-splunk-server-name>]
mounted_bundles=true
bundles_location=<path_to_bundles>
```

请注意以下事项：

- 搜索节点的配置文件必须仅包含 `[searchhead:<searchhead-splunk-server-name>]` 段落。`distsearch.conf` 中的其他段落仅用于搜索头。
- 要确定 `<searchhead-splunk-server-name>`，在搜索头上运行以下命令：

```
splunk show servername
```

- **重要提示：**如果搜索节点正在搜索头群集化中运行，则对等节点中的 `[searchhead:]` 段落必须指定群集中的 GUID，而不是任何群集成员的服务器名称。例如：

```
[searchhead:C7729EE6-D260-4268-A699-C1F95AAD07D5]
```

要识别 GUID，请在群集成员中运行本命令：

```
splunk show shcluster-status
```

群集 GUID 是 `id` 字段的数值，一般位于结果的管理员部分。

- `<path_to_bundles>` 需要在搜索节点而不是搜索头上指定安装点。例如，假定搜索头上的 `$SPLUNK_HOME` 是 `/opt/splunk`，同时您通过 NFS 导出 `/opt/splunk/etc`。然后，在搜索节点上，您将 NFS 共享安装于 `/mnt/splunk-head`。`<path_to_bundles>` 的值应该是 `/mnt/splunk-head`，**而不是** `/opt/splunk`。
- 如果多个非群集搜索头分发搜索给本搜索节点，则您必须为每个在搜索节点上创建单独段落。

3. 重新启动搜索节点。

注意：您可以设置到软件包子目录 (`apps`,`users`,`system`) 的符号链接，确保搜索节点仅能访问搜索头的 `/etc` 目录中的必要子目录。此操作为可选。有关该操作的详细信息，请参阅以下示例。

配置示例

这里是在共享存储上设置安装软件包的示例：

搜索头

在其 Splunk Enterprise 服务器名称是 "searcher01" 的搜索头上：

1. 安装搜索头的 `$SPLUNK_HOME/etc` 目录到具有读取/写入访问权限的共享存储。

2. 在搜索头的 `distsearch.conf` 文件中，设置：

```
[distributedSearch]
...
shareBundles = false
```

3. 重新启动搜索头。

搜索节点

对于每个搜索节点：

1. 安装搜索节点上搜索头的 `$SPLUNK_HOME/etc` 目录到：

```
/mnt/searcher01
```

2.（可选。）创建由转到软件包子目录的符号链接组成的目录：

```
/opt/shared_bundles/searcher01
/opt/shared_bundles/searcher01/system -> /mnt/searcher01/system
/opt/shared_bundles/searcher01/users -> /mnt/searcher01/users
/opt/shared_bundles/searcher01/apps -> /mnt/searcher01/apps
```

注意：本可选步骤对于确保对等节点仅访问必要子目录非常有用。

3.使用此段落在搜索节点创建 `distsearch.conf` 文件（位于 `$SPLUNK_HOME/etc/system/local/`）：

```
[searchhead:searcher01]
mounted_bundles = true
bundles_location = /opt/shared_bundles/searcher01
```

4.重新启动搜索节点。

5.为每个搜索节点重复该流程。

使用带搜索头合并的安装软件包

已弃用此功能。
Splunk Enterprise 6.2 版本中已弃用搜索头合并功能。这意味着，尽管这将继续运行，但可能在未来版本删除。 作为替代方法，您可以部署搜索头群集化。请参阅"关于搜索头群集化"。关于已安装软件包和搜索头群集化的信息，请参阅"搜索头群集化和已安装软件包"。 有关所有弃用功能的列表，请参阅《发行说明》中的主题"弃用功能"。

如果您正使用搜索头合并管理多个搜索头，则配置安装软件的流程基本上没有区别。要记住的几点是：

- 为搜索头池和安装软件包使用相同的共享存储位置。搜索头合并使用安装软件所需目录的子集。
- 搜索头合并本身仅要求您安装 `$SPLUNK_HOME/etc/{apps,users}` 目录。然而，当使用所安装的软件包时，您还必须提供已安装的 `$SPLUNK_HOME/etc/system` 目录。这不会导致搜索头之间的任何冲突，因为它们始终使用自己的 `system` 目录版本并忽略安装版本。
- 搜索节点必须为池中的每个搜索头在 `distsearch.conf` 中创建单独段落。这些段落中的每个 `bundles_location` 必须相同。

有关设置搜索头池的信息，请参阅"配置搜索头合并"。

配置示例：带安装软件包的搜索头合并

本示例显示了如何组合搜索头合并和安装软件包到一个系统。这里有示例的两个主要部分：

1.设置由两个搜索头组成的搜索头池。在这个部分，您还必须安装软件包。

2.设置搜索节点，以便它们可以从搜索头池访问软件包。

本示例假定您正在为共享存储位置使用 NFS 安装。

第 1 部分：设置搜索头池

在配置池之前，执行这些初步步骤：

1.启用两个 Splunk Enterprise 实例为搜索头。本示例假定示例被命名为 "searcher01" 和 "searcher02"。

2.设置每个搜索头可以访问的共享存储位置。本示例假设您设置了 NFS 安装点，并在搜索头上将它指定为 `/mnt/search-head-pooling`。

有关这些步骤的详细信息，请参阅"创建搜索头池"。

现在，配置搜索头池：

1.在每个搜索头上，停止 `splunkd`：

```
splunk stop splunkd
```

2.在每个搜索头上，启用搜索头合并。在本示例中，您使用 `/mnt/search-head-pooling` 的 NFS 安装作为您的共享存储位置：

```
splunk pooling enable /mnt/search-head-pooling [--debug]
```

此外，本步骤将创建空目录 `/etc/apps` 和 `/etc/users`，路径为 `/mnt/search-head-pooling`。步骤 3 使用这些目录。

3. 复制**其中一个搜索头上**的 `$SPLUNK_HOME/etc/apps` 和 `$SPLUNK_HOME/etc/users` 目录中的内容到 `/etc/apps` 和 `/etc/users` 子目录（位于 `/mnt/search-head-pooling`）：

```
cp -r $SPLUNK_HOME/etc/apps/* /mnt/search-head-pooling/etc/apps

cp -r $SPLUNK_HOME/etc/users/* /mnt/search-head-pooling/etc/users
```

4. 复制搜索头的 `$SPLUNK_HOME/etc/system` 目录到 `/mnt/search-head-pooling/etc/system`。

```
cp -r $SPLUNK_HOME/etc/system /mnt/search-head-pooling/etc/
```

5. 查看 `/mnt/search-head-pooling/etc/system/local/server.conf` 文件中的 `[pooling]` 段落。如果存在，则删除所有条目。

6.在每个搜索头上，编辑 `distsearch.conf` 文件以设置 `shareBundles = false`：

```
[distributedSearch]
...
shareBundles = false
```

7.在每个搜索头上，启动 `splunkd`：

```
splunk start splunkd
```

您的搜索头池现在即将运行。

第 2 部分：安装软件包到搜索节点

现在，安装软件包到搜索节点。

在每个搜索节点上，执行这些步骤：

1. 安装共享存储位置（之前在搜索头上设置为 `/mnt/search-head-pooling` 的相同位置），以便它在对等节点上显示为 `/mnt/bundles`。

2. 创建由转到软件包子目录的符号链接组成的目录：

```
   /opt/shared_bundles/bundles/system -> /mnt/bundles/etc/system
   /opt/shared_bundles/bundles/users -> /mnt/bundles/etc/users
   /opt/shared_bundles/bundles/apps -> /mnt/bundles/etc/apps
```

3. 在搜索节点上创建 `distsearch.conf` 文件（路径为 `$SPLUNK_HOME/etc/system/local/`），且文件要包含两个搜索头各自的段落：

```
[searchhead:searcher01]
mounted_bundles = true
bundles_location = /opt/shared_bundles/bundles

[searchhead:searcher02]
mounted_bundles = true
bundles_location = /opt/shared_bundles/bundles
```

4. 重新启动搜索节点：

```
splunk restart splunkd
```

为每个搜索节点重复该流程。

运行中的分布式搜索

授权如何用于分布式搜索

搜索节点在处理分布式搜索时使用的授权设置与用于本地活动的设置不同，如管理和本地搜索请求：

- 当处理分布式搜索时，搜索节点将使用**知识包**包含的设置，搜索头会在发送搜索请求给它们时分发给所有搜索节点。这些设置在搜索头上创建和管理。

- 当执行本地活动时，搜索节点将使用在搜索节点上本地创建和存储的授权设置。

当管理分布式搜索时，区分这两种类型的授权非常重要。当使用**搜索头合并**或**安装软件包**管理系统时，您尤为需要注意如何分发授权设置给知识包。

有关背景信息，请阅读有关这些关键概念：

- **Splunk Enterprise 授权：**《确保 Splunk Enterprise 安全》手册中的"关于基于角色的用户访问权限"主题。
- **安装软件包：**本手册中的"安装知识软件包"章节
- **搜索头合并：**本手册中的"搜索头合并"章节

管理分布式搜索的授权

所有授权设置存储在一个或多个 `authorize.conf` 文件中。这包括通过 Splunk Web 或 CLI 配置的设置。这些 `authorize.conf` 文件将从搜索头分发到搜索节点。在知识包上，文件通常位于 `/etc/system/{local,default}` 和/或 `/etc/apps/<app-name>/{local,default}`。

由于搜索节点会自动使用知识软件包中的设置，因此可正常执行操作。您为搜索头上的用户配置角色，同时搜索头将在它分发搜索本身时，自动分发这些配置给搜索节点。

然而，对于搜索头合并，必须确保搜索头和搜索节点全部使用同一组 `authorize.conf` 文件。为此，您必须确保：

- 池中的所有搜索头使用相同的一组 `authorize.conf` 文件
- 搜索头使用的一组 `authorize.conf` 文件会导入到知识包，以便分发给搜索节点。

本主题介绍了四个主要方案，基于您是否使用搜索头合并或安装软件包。它以从简单到复杂的顺序介绍方案。

四种方案

您需要对分布式搜索 `authorize.conf` 文件执行的操作取决于部署过程中是否实施搜索头合并或安装软件包。这四种方案是：

- 无搜索头合并，无安装软件包
- 无搜索头合并，安装软件包
- 搜索头合并，无安装软件包
- 搜索头合并，安装软件包

前两种方案"仅运行"，但后两种方案需要仔细计划。出于完整性的原因，本部分介绍了所有这四种方案。

注意：这些方案仅针对分布式搜索的授权设置。与本地授权设置的功能相同，不依赖于您的分布式搜索部署。

无搜索头合并，无安装软件包

您在搜索头上的任何授权设置都将被自动分发给其搜索节点，作为它们使用分布式搜索请求收到的复制知识软件包的一部分。

无搜索头合并，安装软件包

您在搜索头上的任何授权设置将自动放在安装软件包中，并在分布式搜索处理期间被搜索节点使用。

搜索头合并，无安装软件包

池中的搜索头将共享它们的 `/apps` 和 `/users` 目录，而不是 `/etc/system/local` 目录。所有 `authorize.conf` 文件（位于 `/apps` 子目录中）将被所有搜索头自动共享，并在任何搜索头分发搜索请求给搜索节点时自动包含在知识包中。

授权更改导致的问题还会保存在 `authorize.conf` 文件（位于搜索头的 `/etc/system/local` 目录）中（例如，如果您通过 Splunk Web 更新搜索头的授权设置）。本目录不会在池中的搜索头之间共享，但是它仍会作为知识软件包的一部分分发给搜索节点。由于配置系统工作的方式，`authorize.conf` 文件的所有副本（位于 `/etc/system/local` 中）将优先于 `/apps` 子目录中的副本。（有关详细信息，请参阅《管理员》手册中的"配置文件优先顺序"。）

因此，`authorize.conf` 副本（从单个搜索头的 `/etc/system/local` 目录分发到搜索节点的的副本）优先于任何从搜索头池共享目录分发的副本。除非您说明这种情况，否则搜索节点会以为不同搜索使用不同的授权设置结束，这取决于分发搜索的搜索头。对于大部分情况，这不是您希望出现的。

为避免发生这种问题，您需要确保对搜索头的 `/etc/system/local/authorize.conf` 文件的任何更改将被传输给池中的所有搜索头。处理这种情况的一种方式是将所有已更改的 `/etc/system/local/authorize.conf` 文件移动到应用子目录，因为池中的所有搜索头共享 `/apps` 目录。

搜索头合并，安装软件包

这类似于上一种方案。池中的搜索头将共享它们的 `/apps` 和 `/users` 目录，而不是 `/etc/system/local` 目录。所有

`authorize.conf` 文件（位于 `/apps` 子目录）将被所有搜索头自动共享。它还将被包含在搜索节点在处理来自任何搜索头的搜索请求时使用的安装软件包中。

然而，授权更改还会在 `authorize.conf` 文件（位于搜索头的 `/etc/system/local` 目录）中结束（例如，如果您通过 Splunk Web 更新搜索头的授权设置）。本目录不会在池中的搜索头之间自动共享。它还不会自动分发给搜索节点使用的已安装软件包。因此，您必须提供一些机制，确保所有搜索头和所有搜索节点拥有对 `authorize.conf` 版本的访问权限。

处理这种情况的最简单方式是移动所有已更改的 `/etc/system/local/authorize.conf` 文件到应用子目录，因为合并的搜索头和所有搜索节点都共享 `/apps` 目录。

用户如何控制分布式搜索

从用户的立场看，指定和运行**分布式搜索**与运行任何其他搜索本质上相同。当将结果呈现给用户时，**搜索头**在后台将查询分散到它的**搜索节点**中，并对结果进行合并。

用户可限制参与搜索的搜索节点。他们还需了解分布式搜索配置以进行故障排除。

执行分布式搜索

通常，通过与本地搜索相同的命令集指定分布式搜索。但是，多个其他命令和选项可专门用于帮助控制和限制分布式搜索。

搜索头默认跨搜索节点全集运行搜索。通过在查询中指定 `splunk_server` 字段，您可限制对一个或多个搜索节点进行搜索。请参阅*《搜索手册》*中的“从索引检索事件”。

搜索命令 `localop` 还用于定义分布式搜索。它允许您将后续命令的执行限制到搜索头。有关详细信息和示例，请参阅*《搜索参考》*中的 localop 的描述。

此外，`lookup` 命令为使用分布式搜索提供 `local` 参数。如果设置为 `true`，则查找仅限于搜索头；如果设置为 `false`，则查找范围还包括搜索节点。这对于复制查找表的脚本式查找尤为有用。有关详细信息和示例，请参阅*《搜索参考》*中对查找的描述。

故障排除分布式搜索

使用监视控制台查看分布式搜索状态

您可以使用监视控制台来监视部署的大多数方面。本主题讨论“搜索活动”：提供分布式搜索洞察的部署仪表板。

监视控制台的主要文档位于*《监视 Splunk Enterprise》*。

搜索活动：部署仪表板提供关于分布式搜索环境和过程的一系列有用信息，如：

- 每个搜索头的搜索活动
- 提供随着时间的变化搜索并发和 CPU 使用情况信息的历史图表

监视控制台为单个实例提供显示搜索活动的其他仪表板。

自行查看仪表板的更多信息。另外，请参阅*《监视 Splunk Enterprise》*中的“搜索活动：部署”。

一般故障排除问题

搜索头和搜索节点之间的时钟偏移会影响搜索行为

您必须通过 NTP（网络时间协议）或一些类似方式保持搜索头和搜索节点上的时钟同步。节点要求关闭时钟对齐，以确保时间比较在整个系统内有效。如果时钟不同步超过数秒钟，分布式搜索无法正常运行，从而导致搜索失败或搜索项目的过早失效结束。

在添加搜索节点到搜索头时，搜索头会检查时钟是否同步。该检查旨在确保分布式搜索环境中所有节点的系统时间都一致，不管处于哪个时区。如果节点不同步，搜索头会拒绝搜索节点并显示一个横幅消息，类似如下所示：

```
The time difference between this system and the intended peer at
uri=https://servername:8089/ was too big. Please bring the system
clocks into agreement.
```

注意：如果您通过直接编辑 `distseach.conf` 的方式添加搜索节点，搜索头则不会执行此检查。

如果还未将知识软件包的配置复制到搜索节点，则搜索可能失败

配置更改需要一段较短的时间从搜索头传输到搜索节点。结果是，在搜索头上进行配置更改和复制配置更改到搜索节

点期间（通常不超过几分钟），分布式搜索可能失败或基于先前配置提供结果。

可能导致搜索失败的配置更改类型指对新应用的更改，或对 `authentication.conf` 或 `authorize.conf` 的更改。示例包括：

- 为角色更改允许的索引，然后在该角色内以用户身份运行搜索
- 创建一个新应用，然后从该应用内运行搜索

任何失败将会记在搜索头的消息中。

可基于先前配置提供结果的更改类型包括更改字段提取或查找表文件。

如要修复，则再次运行此搜索。

网络问题可能会降低搜索性能

6.x 搜索头默认要求其搜索节点生成远程时间线。如果搜索头和搜索节点之间的网络不稳定，则可能会导致搜索变慢。

解决方法是添加以下设置到搜索头 上的 `limits.conf`：

```
[search]
remote_timeline_fetchall = false
```

进行更改后，您必须重启搜索头。

处理搜索节点缓慢问题

所有搜索节点返回所需要的数据之前，搜索一般会继续运行。使用大量的搜索节点（100 以上）可能会导致在部署中出现问题。在返回部分数据时如果某一个对等节点比其他对等节点明显缓慢时（如由于网络问题），则在等待该对等节点的最后结果的过程中，搜索可能仍旧会长时间异常运行。

如果出现这种问题，并且您想要为搜索性能交易数据保真度时，您可以定向搜索头以结束长时间运行的搜索，无需等待运行缓慢的对等节点来完成所有数据的发送。为此，仅需启用搜索头的 `[slow_peer_disconnect]` 段落（位于 `limits.conf`）。默认情况下，此操作处于禁用状态。您不用重新启动搜索头即可切换操作。

确定何时将搜索从一个运行缓慢的节点断开连接的启发式算法相对来说比较复杂，需要通过 `[slow_peer_disconnect]` 段落中的若干参数转换。如果您需要使用此操作，请联系 Splunk 专业服务以获得针对您特定的部署需要调整启发式算法的指导。

隔离搜索节点

您可以隔离搜索节点，以防止它参与以后的搜索。如果对等节点出现问题，例如磁盘或网卡损坏，则可进行这个操作。在升级搜索节点时将它进行隔离也是可取的做法。

通过隔离而非停止故障搜索节点的方式，您可以在节点上执行实时故障排除。

在必要时，您可以为特定搜索撤销隔离。请参阅如何撤销隔离。

隔离搜索节点的结果

在隔离一个搜索节点后，它就不会参与任何新的搜索。但会继续试着为目前正在执行的搜索提供服务。

隔离操作只会影响搜索节点和其搜索头之间的关系。搜索节点会继续扮演索引器的角色，接收传入数据并为数据建立索引。如果节点属于某个索引器群集，它也会继续复制来自其他对等节点的数据。

如果您要完全停止索引器的活动，则必须将它关闭。

如何隔离搜索节点

要隔离搜索节点，从搜索头上运行以下 CLI 命令：

```
splunk edit search-server -auth <user>:<password> <host>:<port> -action quarantine
```

请注意以下事项：

- 使用 `-auth` 标记仅为搜索头提供凭据。
- <host> 指搜索节点主机的主机名称或 IP 地址。
- <port> 指搜索节点的管理端口。

例如：

```
splunk edit search-server -auth admin:password 10.10.10.10:8089 -action quarantine
```

对于搜索头群集，此命令只会影响它所运行的搜索头。要将一个对等节点隔离于所有群集成员，则必须针对每个成员运行此命令。

您也可以通过搜索头的 Splunk Web 的**搜索节点**页面隔离搜索节点。请参阅在“设置”中查看搜索节点状态。

如何取消隔离搜索节点

要取消搜索节点的隔离，从搜索头上运行以下命令：

```
splunk edit search-server  -auth <user>:<password> <host>:<port> -action unquarantine
```

请注意以下事项：

- 使用 `-auth` 标记仅为搜索头提供凭据。
- <host> 指搜索节点主机的主机名称或 IP 地址。
- <port> 指搜索节点的管理端口。

例如：

```
splunk edit search-server -auth admin:password 10.10.10.10:8089 -action unquarantine
```

如何撤销隔离

当对等节点被隔离时，它一般不会参与到搜索中。但是，您可以按搜索撤销对该节点的隔离。要实现这一操作，该搜索必须是直接通过 `splunk_server` 字段将此对等节点指定为目标节点。例如：

```
index=_internal splunk_server=idx-tk421-03 (log_level=WARN OR log_level=ERROR)
```

注意：如果对等节点属于一个分布式搜索组，则不可通过指定该搜索组 `splunk_server_group` 字段的方式来撤销隔离。您必须直接通过 `splunk_server` 字段指定该对等节点。

搜索头合并配置问题

当实施搜索头合并时，您应注意几个潜在的问题，主要是搜索头之间的协调。

在 Splunk Web 中进行的验证和验证更改仅适用于单个搜索头

通过搜索头的 Splunk Web 进行的验证和验证更改仅适用于该搜索头，而不是池中的其他搜索头。池的每个成员在 `$SPLUNK_HOME/etc/system/local` 中保留其本地配置。要跨池共享配置，请根据“配置搜索头合并”的说明在共享存储中进行设置。

搜索头和共享存储之间的时钟偏移会影响搜索行为

很重要的是，通过 NTP（网络时间协议）或一些类似方式保持搜索头和共享存储服务器上的时钟保持同步。如果时钟不同步超过数秒钟，则您会以搜索失败或搜索项目的过早失效结束。

共享存储服务器上的权限问题会导致合并失败

在每个搜索头上，Splunk 运行的每个用户帐户必须拥有对共享存储服务器上文件的读取/写入权限。

性能分析

大量搜索头合并问题归结为性能不足。

当部署或调查搜索头合并环境时，考虑这些因素非常重要：

- **存储：**支持池的存储必须能够处理大量 IOPS。低于 1000 的 IOPS 可能永远无法正常运行。
- **网络：**后备存储器和搜索头之间的通信路径必须具有高带宽和极低延迟。这可能意味着您的存储系统应在与搜索头相同的交换机上。WAN 链接将无法使用。
- **服务器并行性：**由于搜索导致大量请求大量文件的进程，因此系统的并行性必须较高。这就需要调整 NFS 服务器以并行处理更大数量的请求。
- **客户端并行性：**客户端操作系统必须能够同时处理大量请求。

要验证环境，典型的方法是：

- 使用 Bonnie++ 等存储基准工具，同时避免使用文件存储，以验证提供的 IOPS 功能是否强大。

- 使用网络测试方法确定搜索头和存储系统之间的往返时间约为 10ms。
- 执行已知简单任务，如创建一百万个文件，然后删除它们。
- 假定以上测试未显示任何漏洞，执行某些 IO 负载生成或运行实际 Splunk Enterprise 负载，同时收集 NFS 统计数据以查看 NFS 请求所进行的操作。

NFS 客户端并行限制会导致搜索超时或搜索行为缓慢

搜索头池中的搜索性能基于共享存储和搜索工作负载的吞吐量。正在运行的并行搜索用户和并行计划的搜索的组合影响将导致共享量需要支持的总 IOP。IOP 要求还因搜索运行类型而异。为充分配置设备以在搜索头之间共享，您需要知道提交搜索的并行用户数量，以及同时执行的任务/应用数量。

如果搜索超时或缓慢运行，则您可能耗尽 NFS 客户端支持的最大并行请求数量。要解决该问题，增加您的客户端并行限制。例如，在 Linux NFS 客户端上，调整 `tcp_slot_table_entries` 设置。

大量用户计数的 NFS 延迟会导致配置访问延迟或派遣获取变缓

检测到变化时，Splunk Enterprise 将同步搜索头池存储配置状态与内存状态。实际上，它将在检测到更新时读取配置到内存。当处理超载搜索池存储或具有大量用户、应用和配置文件时，本同步流程会降低性能。为减轻这一影响，可以提高最小读取频率，如"选择配置刷新时间"所述。

有关唯一 serverName 属性的警告

池中的每个搜索头必须拥有唯一 `serverName` 属性。Splunk Enterprise 将在启动每个搜索头时验证这一条件。如果发现问题，它将生成如下错误消息：

```
serverName "<xxx>" has already been claimed by a member of this search head pool
in <full path to pooling.ini on shared storage>
There was an error validating your search head pooling configuration. For more
information, run 'splunk pooling validate'
```

本错误的最常见原因是池中的另一个搜索头已经使用当前搜索头的 `serverName`。为修复问题，在下列位置中更改当前搜索头的 `serverName` 属性（位于 `system/local/server.conf`）。

这里还有一些其他条件也会产生该错误：

- 当前搜索头的 `serverName` 已经更改。
- 当前搜索头的 GUID 已经更改。这通常是由于 `/etc/instance.cfg` 被删除。

要修复这些问题，运行

```
splunk pooling replace-member
```

这会更新 `pooling.ini` 文件，所使用的是当前搜索头的 `serverName`->GUID 映射，覆盖之前所有的映射。

升级后的项目以及 Splunk Web 中未正确显示的内容

当升级合并搜索头时，您必须在完成升级后，复制**所有**更新的应用 - 甚至那些 Splunk Enterprise 附带的应用（如搜索应用，以及作为应用实施的数据预览功能）- 到搜索头池的共享存储。如果未这么做，您可能看到一些项目，或其他在 Splunk Web 中无法正确显示的内容。

要修复问题，从升级的搜索头复制所有更新的应用到搜索头池的共享存储，要小心排除每个应用的 `local` 子目录。

重要提示：从复制流程排除每个应用的 `local` 子目录将防止使用配置文件的本地副本覆盖共享存储上的配置文件。

一旦复制应用，在池中的所有搜索头重新启动 Splunk Enterprise。

分布式搜索错误消息

本表列出了一些与分布式搜索关联的更加常见搜索时间错误消息。

错误消息	含义
`status=down`	指定远程对等节点不可用。
`status=not a splunk server`	指定远程对等节点不是 Splunk Enterprise 服务器。
`duplicate license`	指定远程对等节点正在使用重复许可证。
`certificate mismatch`	使用指定远程对等节点验证失败。