



# Splunk® Enterprise 6.5.0

## 安装手册

生成时间：2016 年 9 月 26 日，下午 10:23

# Table of Contents

<b>欢迎使用 Splunk Enterprise 安装手册</b>	<b>4</b>
本手册包含哪些内容	4
<b>计划您的 Splunk Enterprise 安装</b>	<b>4</b>
安装概述	4
本地使用 Splunk Enterprise 的系统要求	4
Splunk Enterprise 架构和流程	8
有关其他随 Splunk Enterprise 分发的 Windows 第三方二进制文件的信息	10
安装说明	11
<b>确保您的 Splunk Enterprise 安装</b>	<b>11</b>
关于确保 Splunk Enterprise 安全	11
您安装 Splunk Enterprise 前确保系统安全	11
安全安装 Splunk Enterprise	12
确保 Splunk Enterprise 安全的更多方法	12
<b>在 Windows 上安装 Splunk Enterprise</b>	<b>13</b>
选择 Splunk Enterprise 应以其身份运行的 Windows 用户	13
将为网络或域用户准备用于安装的 Windows 网络	14
在 Windows 上安装	18
使用命令行在 Windows 上安装	21
更改 Windows 安装期间选择的用户	24
<b>在 Unix、Linux 或 Mac OS X 上安装 Splunk Enterprise</b>	<b>25</b>
在 Linux 上安装	25
在 Solaris 上安装	26
在 Mac OS X 上安装	27
在 FreeBSD 上安装通用转发器	29
在 AIX 上安装通用转发器	30
在 HP-UX 上安装通用转发器	30
以其他或非 root 用户身份运行 Splunk Enterprise	31
<b>使用 Splunk Enterprise 启动</b>	<b>32</b>
首次启动 Splunk Enterprise	32
接下来呢？	34
了解有关 Splunk Enterprise 的可访问性	34
<b>安装 Splunk Enterprise 许可证</b>	<b>35</b>
关于 Splunk Enterprise 许可证	35
安装许可证	35
<b>升级或迁移 Splunk Enterprise</b>	<b>36</b>
如何升级 Splunk Enterprise	36
关于升级到 6.5 - 首先阅读此主题	37
如何升级分布式 Splunk Enterprise 环境	43
从版本 5 至版本 6 的 Splunk Web 程序有何更改	45

	Splunk 应用开发人员的更改	46
	在 UNIX 上升级到 6.5	47
	在 Windows 上升级到 6.5	48
	迁移 Splunk Enterprise 实例	48
	迁移到新的 Splunk Enterprise 许可证	50
<b>卸载</b>	<b>Splunk Enterprise</b>	<b>51</b>
	卸载 Splunk Enterprise	51
<b>参考</b>		<b>53</b>
	PGP 公共密钥	53

# 欢迎使用 Splunk Enterprise 安装手册

## 本手册包含哪些内容

在《安装手册》中，您可以找到安装完整 Splunk Enterprise 所需的信息：

- [系统要求](#)
- [许可授权信息](#)
- [安装程序](#)
- [从之前版本升级的程序](#)

以及其他相关内容。

## 安装通用转发器

要安装 Splunk 通用转发器，请参阅《通用转发器》手册中的“安装通用转发器软件”。通用转发器是独立的可执行文件，有自己的一套安装过程。有关转发器的介绍，另请参阅《转发数据》手册中的“关于转发和接收”。

# 计划您的 Splunk Enterprise 安装

## 安装概述

在主机上安装 Splunk Enterprise 是实现您数据价值的第一步。安装之前请先阅读本主题和本章内容。

### 安装基础知识

1. 请参阅安装的[系统要求](#)。基于安装 Splunk Enterprise 的操作系统，以及使用 Splunk Enterprise 的方式可能会适用其他要求。
2. （可选）有关 Splunk Enterprise 的生态系统，请参阅“Splunk Enterprise 部署的各个组件”，有关安装程序在计算机上所安装内容的信息，请阅读[Splunk 架构和流程](#)。
3. 请参阅“[确保您的 Splunk Enterprise 安装安全](#)”，并根据实际情况为您计划安装 Splunk Enterprise 的主机提供安全防护。
4. 从 Splunk Enterprise 下载页面为您的系统下载安装软件包。
5. 使用操作系统的[安装说明](#)进行安装。
6. （可选）如果您是首次安装 Splunk Enterprise，请参阅[搜索教程](#)，了解如何将数据索引到 Splunk 并使用 Splunk Enterprise 的搜索语言搜索该数据。
7. （可选）安装 Splunk Enterprise 后，计算数据占用的空间量。请参阅“评估存储要求”。
8. 要在生产环境中运行 Splunk Enterprise 并了解这样的环境需要多少硬件，请参阅《容量规划手册》。

### 升级或迁移 Splunk Enterprise 实例

要从早期 Splunk Enterprise 版本升级，请参阅本手册中的“[如何升级 Splunk Enterprise](#)”以获得信息和特定说明。有关从一个版本迁移到另一个版本的提示，请参阅“有关升级 - 首先阅读此主题”了解您希望升级到的版本。该主题位于本手册中的“升级或迁移 Splunk Enterprise”一章。

要从一个主机移动 Splunk Enterprise 实例到另一个主机，请参阅本手册中的“[迁移 Splunk 实例](#)”。

## 本地使用 Splunk Enterprise 的系统要求

在下载并安装 Splunk Enterprise 以供本地使用之前，请了解有关 Splunk 支持的计算环境。有关要下载的最新版本，请参阅[下载 Splunk Enterprise](#)。有关已知和已解决问题的详细信息，请参阅[发行说明](#)。

有关部署的硬件规划讨论，请参阅《容量规划》中的“适用于 Splunk Enterprise 的容量规划介绍”。

如果您对新功能有任何想法或需求，并且您当前拥有 Splunk 合同，可与 Splunk 支持团队提出请求。

### 支持的服务器硬件架构

Splunk 在一些平台上提供支持 32 和 64 位架构。

### 支持的操作系统

下表列出了 Splunk Enterprise 的可用计算平台。第一个表格列出了 \*nix 操作系统的可用性，第二个表格列出了 Windows 操作系统的可用性。使用这些表确定 Splunk Enterprise 是否可用于您的平台。

每个表都有一系列框，这些框定义了不同的计算平台（操作系统和架构）以及 Splunk 软件类型。计算平台和 Splunk 软件类型相交的方框中的 '✓'（对勾标记）意味着该 Splunk 软件可用于该平台和类型。

方框空白意味着 Splunk 软件不可用于该平台和类型。

如果列表中未找到您要找的操作系统或架构，则软件对该平台或架构不可用。这可能表示，Splunk 已终止对该平台的支持。请参阅发行说明中的“弃用功能”里面的已弃用和移除计算平台列表。

某些方框可能使用其他字符。请参阅每张表格的下方，了解字符含义及字符将如何对安装造成潜在影响。

#### 确认支持您的计算平台

1. 在“操作系统”列查找您希望安装 Splunk Enterprise 的操作系统。
2. 在“架构”列找出匹配环境的计算架构。
3. 找出想要使用的 Splunk 软件版本：Splunk Enterprise、Splunk Free、Splunk Trial 或 Splunk 通用转发器。
4. 如果针对您希望使用的计算平台和软件类型的 Splunk 软件可用，则可以前往下载页面获取。

#### Unix 操作系统

操作系统	架构	Enterprise	Free	Trial	通用转发器
Solaris 10 和 11	x86 (64 位)	D	D	D	✓
	SPARC				✓
Linux 2.6 及更新版本	x86 (64 位)	✓	✓	✓	✓
	x86 (32 位)				D
Linux 3.x 及更新版本	x86 (64 位)	✓	✓	✓	✓
	x86 (32 位)				D
PowerLinux 2.6 及更新版本	PowerPC				✓
zLinux 2.6 及更新版本	s390x				✓
FreeBSD 9	x86 (64 位)				✓
FreeBSD 10	x86 (64 位)				✓
Mac OS X 10.10 和 10.11	Intel		✓	✓	✓
AIX 7.1 和 7.2	PowerPC				✓
AIX 6.1	PowerPC				D
HP/UX† 11i v3	Itanium				✓
ARM Linux	ARM				A

A 该平台的软件可从 [splunk.com](http://splunk.com) 下载，但没有对该平台的官方支持。

D Splunk 支持此平台和架构，但可能会在将来的版本中移除支持。有关弃用的信息，请参阅“发行说明”中的“弃用功能”。

您必须使用 `gnu tar` 解压缩 HP/UX 安装归档。

#### Windows 操作系统

下表列出了 Splunk Enterprise 支持的 Windows 计算平台。

操作系统	架构	Enterprise	Free	Trial	通用转发器
Windows Server 2008 R2	x86 (64 位)	D	D	D	D
Windows Server 2012 和 Server 2012 R2	x86 (64 位)	✓	✓	✓	✓
	x86 (64 位)		✓	✓	✓

Windows 8、8.1 及 10					
	x86 (32 位)		***	***	✓

D Splunk 支持此平台和架构，但可能会在将来的版本中移除支持。有关弃用的信息，请参阅“发行说明”中的“弃用功能”。

\*\*\* Splunk 支持，但是不建议在本平台和架构上使用 Splunk Enterprise。

## 操作系统说明

### Windows

Windows 上的某些 Splunk Enterprise 部分需要提升的用户权限才能正常运行。有关需要提升权限的组件以及如何在 Windows 上配置 Splunk Enterprise 的信息，请参阅以下主题：

- [Splunk 架构和流程](#)。
- [选择 Splunk 应以其身份运行的用户](#)
- “有关确定如何监视远程 Windows 数据的注意事项”（《数据导入》）。

### 支持分布式管理控制台 (DMC) 的操作系统

Splunk Enterprise DMC 仅能在 Linux、Solaris 和 Windows 的某些版本上工作。有关支持 DMC 的平台架构的信息，请参阅《故障排除手册》中的“支持的平台”。要了解 DMC 的其他先决条件，请参阅《分布式管理控制台》中的 DMC 先决条件。

### 已弃用操作系统和功能

随着 Splunk 产品的开发，我们将弃用并移除对旧操作系统的支持。有关已弃用或完全删除的平台和功能的信息，请参阅发行说明中的“已弃用功能”。

### 已终止对某些 \*nix 操作系统的支持

随着此版本 Splunk Enterprise 的发布，Splunk 已终止对 FreeBSD、AIX、HP-UX 和 32 位版本 Linux kernel 上的 Splunk Enterprise 的支持。仍有针对这些平台的通用转发器包，并且已对安装说明进行了更新，以便为这些系统安装通用转发器。

- [在 FreeBSD 上安装通用转发器](#)
- [在 AIX 上安装通用转发器](#)
- [在 HP-UX 上安装通用转发器](#)

### 在操作系统上创建和编辑不使用 UTF-8 字符集编码的配置文件

Splunk Enterprise 预计配置文件使用 ASCII 或 8 位通用字符集转换格式 (UTF-8)。如果您在操作系统上编辑或创建不使用 UTF-8 字符集编码的配置文件，则确保您使用的编辑器能以 ASCII 或 UTF-8 格式保存。

### IPv6 平台支持

所有支持 Splunk 的操作系统平台都可使用 IPv6 网络配置，以下除外：

- AIX
- PA-RISC 架构上的 HP/UX

有关 Splunk Enterprise 中 IPv6 支持的详细信息，请参阅《管理员手册》中的“为 IPv6 配置 Splunk”。

### 支持的浏览器

Splunk Enterprise 支持以下浏览器：

- Firefox (最新)
- Internet Explorer 11
- Safari (最新)
- Chrome (最新)

### 建议的硬件

要为生产部署进行 Splunk Enterprise 评估，请使用生产环境的典型硬件。本硬件应满足或超过建议的硬件容量规格。

有关生产部署的硬件规划讨论，请参阅《容量规划》中的“适用于 Splunk Enterprise 的容量规划介绍”。

### Splunk Enterprise 和虚拟机

如果您在任何平台上的虚拟机 (VM) 中运行 Splunk Enterprise，性能将会降低。这是因为虚拟化的工作方式是将系统上的硬件提取到资源池。系统上定义的 VM 将从这些资源池提取。Splunk Enterprise 的索引操作需要保持对一些资源的访问，尤其是磁盘 I/O。如果在 VM 中或与其他 VM 一起运行 Splunk Enterprise，索引和搜索性能会降低。

### 推荐的硬件容量

以下是针对单实例安装的确切要求（低级到中级不等）。对于重要的企业和分布式部署，请参阅《容量规划》。

平台	推荐的硬件容量/配置
非 Windows 平台	2x 6 核，2+ GHz CPU，12GB RAM，独立磁盘冗余阵列 (RAID) 0 或 1+0，装有 64 位操作系统。
Windows 平台	2x 6 核，2+ GHz CPU，12GB RAM，RAID 0 或 1+0，装有 64 位操作系统。

RAID 0 磁盘配置不提供故障容错。部署 Splunk Enterprise 索引器到使用 RAID 0 配置的系统之前，请确认 RAID 0 配置满足您的数据可靠性需求。

在任何 Splunk Enterprise 实例上，除了任何索引所需的空之外，您要保持至少 5GB 的可用硬盘空间（包括转发器）。关于如何评估您需要的空的过程，请参阅《容量规划》中的“评估存储要求”。无法保持该级别的可用空间会导致性能下降、操作系统故障和数据丢失。

### 通用和轻型转发器的硬件要求

通用转发器有自己的一套硬件要求。请参阅《通用转发器》手册中的相关要求。

### 支持的文件系统

如果在表未列出的文件系统上运行 Splunk Enterprise，软件可能运行名为 `locktest` 的启动实用工具，以测试文件系统可行性。如果 `locktest` 失败，则该文件系统不适合使用 Splunk Enterprise。

平台	文件系统
Linux	ext2, ext3, ext4, btrfs, XFS, NFS 3/4
Solaris	UFS, ZFS, VXFS, NFS 3/4
FreeBSD	FFS, UFS, NFS 3/4, ZFS
Mac OS X	HFS, NFS 3/4
AIX	JFS, JFS2, NFS 3/4
HP-UX	VXFS, NFS 3/4
Windows	NTFS, FAT32

### 有关网络文件系统 (NFS) 的注意事项

当使用网络文件系统 (NFS) 作为 Splunk 索引的存储介质时，考虑文件级别存储的所有后果。

使用数据块级别存储而不是文件级别存储来索引数据。

在具有可靠的、高带宽、低延迟链接的环境，或具备提供高可用性、群集网络存储的供应商的环境中，NFS 是较为合适的选择。但是，选择本策略的客户应与他们的硬件供应商紧密合作，确认他们的存储平台符合供应商性能和数据完整性方面的规格。

如果您使用 NFS，应注意以下问题：

- 不要使用 NFS 托管热或温索引数据桶，因为 NFS 故障可能导致数据丢失。NFS 与冷或冻结的数据桶搭配使用时效果最佳。
- 不要使用 NFS 共享索引器群集中的冷或冻结索引数据库，因为这样可能会创建一个单点故障。
- Splunk Enterprise 不支持“软”NFS 安装。这些安装会导致程序尝试在安装上进行文件操作以报告错误，并在故障后继续进行。
- 只有“硬”NFS 安装（客户端在故障时继续尝试联系服务器的安装）对 Splunk Enterprise 而言较为可靠。
- 禁用属性缓存。如果您有其他应用程序需要禁用或减少属性缓存，则必须为 Splunk Enterprise 提供启用属性缓存的单独安装。
- 不要在广域网 (WAN) 上使用 NFS 安装。这样做会导致性能问题，并导致数据丢失。

### 有关 \*nix 系统范围资源限制的注意事项

Splunk Enterprise 在 \*nix 系统上分配系统范围的资源（如文件描述符和用户进程），用于监视、转发、部署、搜索和其他事务。`ulimit` 命令控制对必须设置为 Splunk Enterprise 在 \*nix 系统上正常运行的可接受级别的这些

资源的访问。

下表显示了软件使用的系统范围的资源。它为不是转发器的实例（例如索引器、搜索头，群集主节点、许可证主服务器、部署服务器和监视控制台（MC））提供这些资源的最低建议设置。

系统范围资源	ulimit 调用	推荐的最小值
打开文件	<code>ulimit -n</code>	8192
用户进程	<code>ulimit -u</code>	1024
数据段大小	<code>ulimit -d</code>	1073741824

您的 Splunk Enterprise 实例执行的任务越多，它需要的资源越多。您应在看到实例出现低资源限制问题的情况下增加 `ulimit` 值。请参阅《故障排除手册》中的“我在 `splunkd.log` 中获取有关 `ulimit` 的错误”。

本注意事项不适用于基于 Windows 的系统。

#### 有关固态硬盘的注意事项

当与布隆过滤器组合使用时，固态硬盘 (SSD) 可为 Splunk 的“罕见”搜索（在大量数据中请求少量结果的搜索）提供较传统硬盘驱动器更显著的性能提升。它们还提供整体并发搜索的性能提升。

#### 有关通用互联网文件系统 (CIFS) / 服务器信息块 (SMB) 的注意事项

在仅由 Windows 主机共同托管时，对于以下目的，Splunk Enterprise 支持使用 CIFS/SMB 协议：

- **搜索头合并**（搜索头合并是弃用功能。）
- 冷或冻结的**索引数据桶**存储。

使用 CIFS 资源存储时，确认连接到文件和共享级资源的用户对于资源有写入权限。如果您使用第三方存储设备，确认其 CIFS 实现与 Splunk Enterprise 实例作为客户端运行的实现相兼容。

在 Windows 上切勿将数据索引到映射的网络驱动器（例如，“Y:\”映射到一个外部共享）。Splunk Enterprise 通过非物理驱动器 letter 禁用遇到的任何索引。

#### 有关使用透明大页面内存管理方案的环境的注意事项

如果您运行一个使用透明大内存页面的 Unix 环境，在尝试安装 Splunk Enterprise 之前请参阅“透明大内存页面和 Splunk 性能”。

本注意事项不适用于 Windows 操作系统。

## Splunk Enterprise 架构和流程

本主题介绍了高级别的 Splunk Enterprise 内部架构和流程。如果您正寻找有关用于 Splunk Enterprise 的第三方组件的信息，请参阅发行说明的信用部分。

### Splunk Enterprise 进程

Splunk Enterprise 服务器在您的主机 `splunkd` 上安装进程。

`splunkd` 是可访问、处理和索引流 IT 数据的分布式 C/C++ 服务器。它还会处理搜索请求。`splunkd` 将通过一系列管道流处理和索引数据，每个由一系列处理器组成。

- **管道**是 `splunkd` 进程内的单个线程，每个使用单个 XML 代码段配置。
- **处理器**是单独、且可重复使用的 C 或 C++ 函数，并作为通过管道的 IT 数据流进行操作。管道可以通过**队列**传输数据到另一个管道。
- 版本 6.2 中新增内容：`splunkd` 还提供 Splunk Web 用户界面。它允许用户搜索和导航数据，并通过 Web 界面管理 Splunk Enterprise 部署。通过 REpresentational State Transfer (REST) 与您的 Web 浏览器进行通信。
- `splunkd` 在端口 8089 上运行 Web 服务器，默认启用 SSL/HTTPS。
- 也会在端口 8000 上运行 Web 服务器，默认关闭 SSL/HTTPS。

`splunkweb` 只在 Windows 中作为旧服务安装。在 6.2 之前的版本中，它为 Splunk Enterprise 提供 Web 界面。现在，它将安装并运行，但是会立即退出。您可以通过更改配置参数，对其进行配置，以在“旧模式”中运行。

在 Windows 系统上，`splunkweb.exe` 是 Splunk 从 `python-service.exe` 重命名的第三方开放源代码可执行文件。因为这是重命名的文件，所以不包含其他与 Splunk Enterprise for Windows 二进制文件的相同文件版本信息。

[阅读有关 Splunk Enterprise 附带的其他 Windows 第三方二进制文件的信息。](#)



## 安全模式中的 Splunk Enterprise 和 Windows

如果 Windows 为安全模式，Splunk 服务不会启动。如果您尝试在安全模式中从“开始”菜单启动 Splunk Enterprise，Splunk Enterprise 将不会针对其服务未运行的事实发送告警。

## Windows 上的 Splunk Enterprise 的其他进程

在 Splunk Enterprise 的 Windows 实例上，除了介绍的两个服务之外，当您在 Splunk Enterprise 实例上创建特定数据导入时，Splunk Enterprise 会使用其他进程。当通过 Windows 特定数据导入的某些类型进行配置时，将会运行这些输入。

### ***splunk.exe***

`splunk.exe` 是 Windows 版本的 Splunk Enterprise 控制应用程序。它为程序提供命令行界面 (CLI)。它允许您启动、停止和配置 Splunk Enterprise，类似于 \*nix `splunk` 程序。

因为控制 `splunkd` 和 `splunkweb` 进程的方式，`splunk.exe` 二进制文件需要提升的上下文才能运行。在 Windows 系统上，如果此程序未具备适当权限，Splunk Enterprise 可能无法正常运行。如果您以本地系统用户身份安装 Splunk Enterprise，则这不会出现问题。

### ***splunk-admon***

`splunk-admon.exe` 将会运行，只要配置了 Active Directory (AD) 监视输入。`splunkd` 衍生出 `splunk-admon`，用于附加到最近的可用 AD 域控制器，并收集 AD 生成的更改事件。Splunk Enterprise 在索引中存储这些事件。

### ***splunk-perfmon***

配置 Splunk Enterprise 以监视本地 Windows 计算机的性能数据时 `splunk-perfmon.exe` 将会运行。本二进制文件将附加到性能数据助手库，这会查询系统上的性能库并提取瞬时和随时间变化的性能指标。

### ***splunk-netmon***

配置 Splunk Enterprise 以监视本地计算机的 Windows 网络信息时，`splunk-netmon` 将会运行。

### ***splunk-regmon***

配置 Splunk 的注册表监视输入时，`splunk-regmon.exe` 将会运行。首先，此输入最初将为注册表在当前状态中写入基准（如果需要），然后监视注册表随时间变化的更改。

### ***splunk-winevtlog***

您可以使用本实用工具测试定义的事件日志集合，同时它将在收集以进行调查时输出事件。Splunk Enterprise 的引擎内置 Windows 事件日志输入处理器。

### ***splunk-winhostmon***

在 Splunk 中配置 Windows 的主机监视输入时，将会运行 `splunk-winhostmon`。此输入将获得有关 Windows 主机的详细信息。

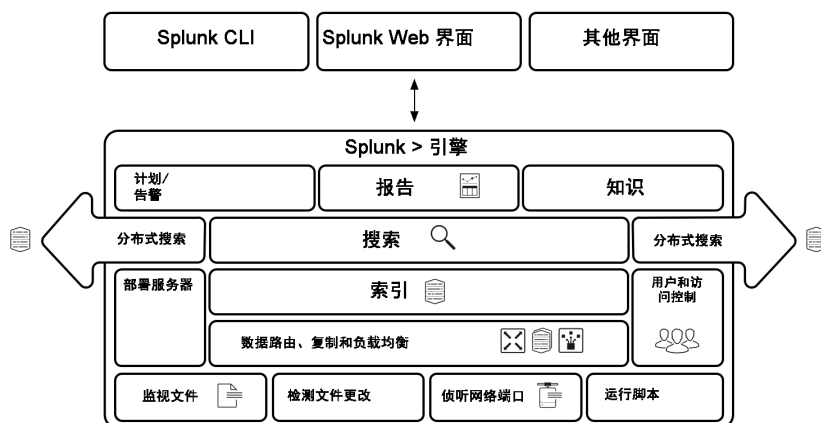
### ***splunk-winprintmon***

在 Splunk 中配置 Windows 打印监视输入时，将会运行 `splunk-winprintmon`。此输入将获得有关本地系统上 Windows 打印机和打印任务的详细信息。

### ***splunk-wmi***

当对远程计算机配置性能监视、事件日志或其他输入时，将运行本程序。根据配置输入方式的不同，它会尝试在连接网络后附加并读取 Windows 事件日志，或对指定远程计算机上的 Windows Management Instrumentation (WMI) 提供商执行 Windows Query Language (WQL) 查询。

## 架构图



## 有关其他随 Splunk Enterprise 分发的 Windows 第三方二进制文件的信息

本主题提供了 Splunk Enterprise 和 Splunk 通用转发器软件包附带的第三方 Windows 二进制文件的其他信息。

有关通用转发器的更多信息，请阅读《转发数据手册》中的“关于转发和接收数据”。

### Splunk Enterprise 附带的第三方 Windows 二进制文件

Splunk Enterprise 附带以下第三方 Windows 二进制文件。除非指定，否则仅 Splunk Enterprise 产品附带这些二进制文件。

二进制文件将为 Splunk Enterprise 提供功能，如同其各个描述所述。其中任何一个都不包含文件版本信息或认证码签名（证明二进制文件真实性的证书）。此外，Splunk Enterprise 不提供对与第三方模块相关调试符号的支持。

**注意：**仅 Splunk Enterprise 附带的第三方二进制文件、应用和脚本经测试可使用 Certified for Windows Server 2008 R2 (CFW2008R2) Windows 徽标合规性。其他二进制文件、应用或脚本，如从互联网下载的文件，未经合规性测试。

#### **Archive.dll**

Libarchive.dll 是多格式归档和压缩库。

Splunk Enterprise 和 Splunk 通用转发器都包含本二进制文件。

#### **Bzip2.exe**

Bzip2 是无专利费、高质量的数据压缩器。它通常压缩文件到最佳可用技术（统计压缩器的部分匹配预测 (PPM) 系统）的 10% 至 15% 内，同时压缩速度快约两倍，解压缩速度快六倍。

#### **Jsmine.exe**

Jsmine.exe 是删除 JavaScript 文件的空白和注释的可执行文件，减少了大小。

#### **Libexslt.dll**

Libexslt.dll 是为 libexslt（GNU 是非 Unix 网络对象模型环境 (GNOME) 项目的一部分）开发的可扩展样式表语言转换 (EXSLT) 动态链接 C 库的扩展。

Splunk Enterprise 和 Splunk 通用转发器都包含本二进制文件。

#### **Libxml2.dll**

Libxml2.dll 是可扩展标记语言 (XML) C 分析器和工具库。该库为 GNOME 项目开发，但可用在 GNOME 平台之外。

Splunk Enterprise 和 Splunk 通用转发器都包含本二进制文件。

#### **Libxslt.dll**

Libxslt.dll 是为 GNOME 项目开发的 XML 样式表语言转换 (XSLT) 动态链接 C 库。XSLT 本身是一个 XML 语言，用来定义 XML 的转换。Libxslt 基于 libxml2，为 GNOME 项目开发的 XML C 库。它还执行大部分 EXSLT 处理器便携扩展功能，以及 Saxon 的评估和表达式扩展。

Splunk Enterprise 和 Splunk 通用转发器都包含本二进制文件。

### **Minigzip.exe**

Minigzip.exe 是 'gzip' 压缩工具的最小实现。

### **Openssl.exe**

OpenSSL 项目是协作项目，用来开发强大、商业级、功能全面和开放源代码工具套件，以实现安全套接字层 (SSL v2/v3) 和传输层安全 (TLS v1) 协议以及全强度通用密码库。

Splunk Enterprise 和 Splunk 通用转发器都包含本二进制文件。

### **Python.exe**

Python.exe 是用于 Windows 的 Python 编程语言二进制文件。

### **Pythoncom.dll**

Pythoncom.dll 是封装 Python 的对象链接与嵌入 (OLE) 自动化 API 的模块。

### **Pywintypes27.dll**

Pywintypes27.dll 是为 Python 2.7 版本封装 Windows 类型的模块。

## **安装说明**

有关操作系统的详细安装说明，请选择以下选项。

- [Windows](#)
- [Windows \(来自命令行\)](#)
- [Linux](#)
- [Solaris](#)
- [Mac OS X](#)

### **在 AIX、FreeBSD 和 HP-UX 上不支持完整 Splunk Enterprise**

从版本 6.3.0 开始，Splunk Enterprise 不再可用于以下操作系统。要在这些操作系统上安装和使用 Splunk Enterprise，必须使用 6.3.0 之前的版本。

通用转发器可以在这些平台上安装。单击以下链接了解通用转发器安装说明：

- [FreeBSD](#)
- [AIX](#)
- [HP-UX](#)

## **确保您的 Splunk Enterprise 安装**

### **关于确保 Splunk Enterprise 安全**

在设置并开始使用 Splunk Enterprise 安装或升级的时候，执行一些额外步骤以确保 Splunk Enterprise 和数据安全。采取适当的步骤以确保 Splunk Enterprise 减少攻击面并缓解大多数漏洞的风险和影响。

本部分着重强调了安装前、安装期间及安装后确保 Splunk Enterprise 安全的诸多方法。《确保 Splunk Enterprise 安全》手册提供可确保 Splunk Enterprise 安全的方法相关的更多信息。

### **您安装 Splunk Enterprise 前确保系统安全**

您安装 Splunk Enterprise 前，确保操作系统安全。强化所有 Splunk Enterprise 服务器操作系统。

- 如果贵组织没有内部强化标准，请使用 CIS 强化基准。
- 至少限制对 Splunk Enterprise 服务器的 Shell 和命令行访问。
- 确保对所有 Splunk Enterprise 服务器的物理访问安全。
- 确保 Splunk Enterprise 最终用户实施物理和端点安全性。

# 安全安装 Splunk Enterprise

当您下载和安装 Splunk Enterprise 时，验证 Splunk 安装的完整性和签名。

## 验证完整性

通过使用诸如 Message Digest 5 (MD5) 和 Secure Hash Algorithm-512 (SHA-512) 等哈希函数比较哈希来验证 Splunk Enterprise 下载。使用受信任版本的 OpenSSL。

### MD5

1. [https://www.splunk.com/en\\_us/download/splunk-enterprise/thank-you-for-downloading.html](https://www.splunk.com/en_us/download/splunk-enterprise/thank-you-for-downloading.html)
2. 点击 MD5 下载链接里面的栏
3. 比较结果

### SHA512

1. 复制下载的连接名称
2. 附加 SHA512
3. <https://download.splunk.com/products/splunk/releases/6.4.3/windows/splunk-6.4.3-b03109c2bad4-x64-release.msi.sha512>

## 验证签名

通过使用 Splunk GnuPG 公共密钥来验证下载的 RPM 软件包的真实性。

1. 下载 GnuPG 公共密钥文件。（此链接通过传输层安全 (TLS)。）
2. 安装密钥。

```
rpm --import <filename>
```

3. 验证软件包签名。

```
rpm -K <filename>
```

# 确保 Splunk Enterprise 安全的更多方法

在您安装了 Splunk Enterprise 之后，有更多的选择来确保配置安全。

## 配置用户验证和基于角色的访问控制

设置用户和用户角色来控制访问权限。Splunk Enterprise 允许通过几种方法配置用户。请在《*确保 Splunk Enterprise 安全*》中参阅以下信息。

- 内置验证系统。请参阅“使用 Splunk Enterprise 本机验证设置用户验证”。
- LDAP。请参阅“设置使用 LDAP 进行的用户验证”。
- 通过外部验证系统进行脚本式验证 API，例如，Pluggable Authentication Modules (PAM) 或 Remote Access Dial-In User Server (RADIUS)。请参阅“设置使用外部系统进行的用户验证”。

配置好用户后，可分配确定并控制功能和访问级别的角色。请参阅“关于基于角色的用户访问权限”。

## 使用 SSL 证书配置加密和验证

Splunk Enterprise 提供了一组默认的证书和密钥，启用后可提供加密和数据压缩。您还可以使用自己的证书和密钥确保浏览器和 Splunk Web 之间的通信安全，以及从转发器发送到接收器（例如，索引器）的数据的安全。

请参阅本手册中的“关于使用 SSL 确保 Splunk 安全”。

## 审计 Splunk Enterprise

Splunk Enterprise 包含审计功能，可以允许您跟踪数据的可靠性。

- 《数据导入》中的“监视文件和目录”
- 《确保 Splunk Enterprise 安全》中的“搜索审计事件”

## 强化您的 Splunk Enterprise 安装

请参阅《*确保 Splunk Enterprise 安全*》中的以下主题来强化您的安装。

- 跨多个服务器部署安全密码
- 使用 Splunk Enterprise 访问控制列表
- 确保您服务帐户的安全
- 禁用多余的 Splunk Enterprise 组件
- 确保 Splunk Enterprise 在您网络上的安全

## 在 Windows 上安装 Splunk Enterprise

### 选择 Splunk Enterprise 应以其身份运行的 Windows 用户

在 Windows 上安装 Splunk Enterprise 时，该软件提供了一个选择应以其身份运行的 Windows 用户的机会。

#### 您选择的用户取决于您希望 Splunk Enterprise 监视的内容

Splunk Enterprise 以其身份运行的用户确定它可监视的内容。本地系统用户拥有对本地计算机上的所有数据而不是任何其他内容的访问权限。本地系统之外的用户拥有您希望它对任何数据的访问权限，但在安装 Splunk Enterprise 之前必须将该访问权限授予给用户。

#### 有关“本地系统”用户和其他用户选择

Windows Splunk Enterprise 安装程序提供了两种安装方式：

- 以本地系统用户身份安装。
- 以您指定的 Windows 计算机或网络上的另一个现有用户身份安装。

要使用 Splunk Enterprise 执行任何以下操作，则必须以域用户身份安装它：

- 远程读取事件日志
- 远程收集性能计数器
- 阅读网络共享的日志文件
- 使用 Active Directory 监控访问 Active Directory 架构

您指定的用户必须满足以下要求。如果用户未满足这些要求，则 Splunk Enterprise 安装可能会失败。即使安装成功，Splunk Enterprise 也可能无法正常运行。

- 是您想要监视的 Active Directory 域或林的成员（当使用 AD 时）。
- 是您安装 Splunk Enterprise 的服务器上的本地管理员组成员。
- 获得特定用户安全权限。

如果不确定应以什么用户身份运行 Splunk Enterprise，则参阅《数据导入》手册中的“决定如何监视远程 Windows 数据的注意事项”，了解有关如何为 Splunk Enterprise 用户配置所需访问权限的信息。

#### 用户帐户和密码问题

您选择运行 Splunk Enterprise 的用户也具有独特的密码要求。

如果您的 Windows 网络上有密码强制执行安全策略，则该策略控制所有密码的有效性。如果 Windows 主机或网络强制您进行密码更改，您必须采取下列措施之一以保证 Splunk Enterprise 服务运行：

- 在密码到期之前更改密码，并重新配置每台主机上的 Splunk Enterprise 服务以便使用更改的密码，然后重新启动每台主机上的 Splunk Enterprise。
- 配置帐户，以便密码不会到期。
- 使用受管服务帐户。请参阅本主题中的“在 Windows Server 2008、Server 2012、Windows 7 和 Windows 8.x 上使用受管服务帐户”。

#### 使用受管服务帐户

如果您在 Active Directory 中运行比 Windows Server 2008 更高的 Windows 服务器版本或比 Windows 7 更高的 Windows 服务器版本，同时 AD 域具有至少一个运行 Windows Server 2008 R2 或更高版本的域控制器，则可安装 Splunk Enterprise 以受管服务帐户 (MSA) 身份运行。

使用 MSA 的好处是：

- 隔离服务帐户，提高安全性。
- 管理员不再需要管理凭据或管理帐户。密码将在到期后自动更改。他们无需手动设置密码或重新启动与这些帐户关联的服务。
- 管理员可以委派这些帐户的管理给非管理员。

使用 MSA 安装 Splunk Enterprise 之前要了解的一些重要事情是：

- MSA 需要与在运行 Splunk Enterprise 的主机上的域帐户相同的权限。
- MSA 必须是运行 Splunk Enterprise 主机的本地管理员。
- 您无法在不同主机上使用同一帐户，如同域帐户一样。
- 在计算机上安装 Splunk Enterprise 之前，您必须在运行 Splunk Enterprise 的主机上正确配置和安装 MSA。请参阅 MS Technet 上的“服务帐户分步指南”(http://technet.microsoft.com/en-us/library/dd548356%28WS.10%29.aspx)。

要使用 MSA 安装 Splunk Enterprise，请参阅[“将为网络或域用户准备用于 Splunk Enterprise 安装的 Windows 网络”](#)。

## 安全与远程访问注意事项

### 最低权限要求

如果您将 Splunk Enterprise 安装为域用户，运行实例的主机需要一些默认权限更改。

使用域用户安装 Splunk Enterprise 时，`splunkd` 和 `splunkforwarder` 服务需要特定的用户权限。根据您希望监视数据来源的不同，Splunk Enterprise 用户可能需要其他权限。无法设置这些权限可能会导致 Splunk Enterprise 安装失败，或安装无法正常运行。

#### `splunkd` 或 `splunkforwarder` 服务所需的基本权限

- 完全控制 Splunk Enterprise 的安装目录。
- 对您希望索引的任何文件的读取访问权限。

#### `splunkd` 或 `splunkforwarder` 服务所需的本地/域安全策略用户权限分配

- 作为服务登录的权限。
- 作为批处理任务登录的权限。
- 更换进程级别标记的权限。
- 作为操作系统一部分的权限。
- 绕过遍历检查的权限。

## 如何分配这些权限

本部分提供安装之前，如何分配适当用户权限给 Splunk Enterprise 服务帐户的指导。有关过程，请参阅[“将为网络或域用户准备用于 Splunk Enterprise 安装的 Windows 网络”](#)。

### 使用组策略分配权限给多台计算机

要分配策略设置给 AD 域或林中的一些工作站和服务，您可以使用这些特定权限定义组策略对象 (GPO)，并跨域部署该 GPO。

创建并启用 GPO 后，您的域中的主机将在下次计划 AD 复制周期（通常为每 1.5 至 2 小时）或下次启动时间选取更改。或者，您可以使用希望更新组策略的主机上的 `GPUPDATE` 命令行实用工具强制 AD 复制。

当您使用 GPO 设置用户权限时，这些权限将覆盖主机上的相同本地安全策略权限。您无法更改本设置。要保留本地安全策略权限，您必须在 GPO 中分配这些权限。

### 故障排除权限问题

介绍的权限为 `splunkd` 和 `splunkforwarder` 服务所需。您需要访问的数据可能需要您分配其他权限。许多用户权限分配和其他组策略限制可以防止 Splunk Enterprise 运行。如果您遇到问题，考虑使用进程监视器或 `GPRESULT` 等工具故障排除环境中的 GPO 应用程序。

## 将为网络或域用户准备用于安装的 Windows 网络

您作为网络或域用户而非“本地系统”用户，准备用于 Splunk Enterprise 安装的 Windows 网络。

这些说明经测试适用于 Windows Server 2008 R2、Windows Server 2012 和 Windows Server 2012 R2，可能与 Windows 的其他版本有所不同。

您使用这些说明分配的权限是成功安装 Splunk Enterprise 所需的最低权限。您可能需要分配其他权限，无论在本地安全策略或组策略对象 (GPO)，或您创建的用户和组帐户内，以便 Splunk Enterprise 访问您需要的数据。

### 通过组策略了解更改系统默认值的安全要求和后果

此过程需要对主机和/或您希望进行 Splunk Enterprise 操作的 Active Directory 域具有完全管理访问权限。在

不具有本访问权限的情况下，不要尝试执行本程序。

由于对于 Splunk Enterprise 操作的访问权限要求较低，如果您希望以用户而不是“本地系统”用户身份来运行 Splunk Enterprise，这些更改是必要的。您必须更改 Windows 网路以完成此过程。这会构成一个重大的安全风险。

要减轻该风险，您可以阻止 Splunk Enterprise 以其身份运行的用户以交互方式登录，并限制用户可以登录的工作站数量。或者，在 Windows Server 2008 R2 及更高版本上，可以设置受管理用户帐户 (MSA)，进一步限制风险。

如果您不了解它们附带的安全风险，则不要执行这些过程。

## 将为域用户准备用于 Splunk 安装的 Active Directory

准备 Active Directory，以便以域用户身份安装 Splunk Enterprise 或 Splunk 通用转发器。

当创建用户和组时，遵照 Microsoft 的最佳实践 (<http://technet.microsoft.com/en-us/library/bb727085.aspx>)。

要使用 PowerShell 配置 Active Directory，请参阅本主题后面介绍的“使用 PowerShell 配置 AD 域”。

### 前提条件

您必须满足下列要求，才能执行此过程：

- 您的 Windows 环境运行 Active Directory。
- 您是希望配置的 AD 域的域管理员。
- 安装主机是此 AD 域的成员。

### 创建组

1. 通过选择**开始 > 管理工具 > Active Directory 用户和计算机**来运行“Active Directory 用户和计算机”工具。
2. 载入程序后，选择您希望准备用于 Splunk Enterprise 操作的域。
3. 双击现有的容器文件夹，或从**操作**菜单选择**新建 > 组**创建组织单位。
4. 选择**操作 > 新建 > 组**。
5. 键入代表 Splunk Enterprise 用户帐户的名称，例如，Splunk Accounts。
6. 确保**组范围**设置为**域本地**，同时**组类型**会设置为**安全**。
7. 单击**确定**创建组。
8. 创建第二个组，并指定代表已启用 Splunk Enterprise 计算机的名称，例如，Splunk Enabled Computers。该组包含接收了权限以域用户身份运行 Splunk Enterprise 的计算机帐户。
9. 确保**组范围**为**域本地**，同时**组类型**为**安全**。

### 分配用户和计算机给组

1. 如果您还未创建希望运行 Splunk Enterprise 所使用的用户帐户，则进行这项操作。如果没有自己的内部政策，请遵照 Microsoft 创建用户和组的最佳实践。
2. 将帐户添加到 **Splunk 帐户** 组。
3. 对于运行 Splunk Enterprise 的计算机，请将它们的帐户添加到**启用 Splunk 的计算机**组中。
4. 退出 **Active Directory 用户和计算机**。

### 定义组策略对象 (GPO)

1. 选择**开始 > 管理工具 > 组策略管理**，运行**组策略管理控制台 (GPMC)** 工具。
2. 在左侧的树视图窗格中，选择**域**。
3. 单击**组策略对象**文件夹。
4. 在**<您的域>中的组策略对象**文件夹中，右键单击并选择**新建**。
5. 键入描述分配用户权限给您应用的服务器的 GPO 名称。例如，“Splunk Access”。
6. 保持**源启动器 GPO**字段的设置为“(none)”。
7. 单击**确定**以保存 GPO。

### 添加权限到 GPO

1. 在 GPMC 时，右键单击新建的组策略对象，并选择**编辑**。
2. 在**组策略管理编辑器**中，在左窗格浏览**计算机配置 -> 策略 -> Windows 设置 -> 安全设置 -> 本地策略 -> 用户权限分配**。
  1. 在右窗格中，双击作为操作系统的一部分条目。
  2. 在打开的窗口中，选中**定义这些策略设置**复选框。
  3. 单击**添加用户或组...**
  4. 在显示的对话框中，单击**浏览...**
  5. 在打开的**选中用户、计算机、服务帐户或组**对话框中，键入您之前创建的“Splunk Accounts”组名称，然后单击**检查名称**。如果有效，Windows 将为该名称添加下划线。否则，它将告诉您无法找到对

- 象，并提示您再次键入对象名称。
- 6. 单击“确定”关闭“选择用户...”对话框。
- 7. 单击“确定”关闭“添加用户或组”对话框。
- 8. 再次单击“确定”关闭权限属性对话框。
- 3. 为以下其他权限重复步骤 2a-2h：
  - **绕过遍历检查**
  - **作为批处理任务登录**
  - **作为服务登录**
  - **更换进程级别标记**

### 更改每个主机的管理员组成员

此程序限制您应用该 GPO 主机上管理员组成员。

**警告：**请确认需要访问每个主机上管理员组的所有帐户已添加到限制组策略设置。否则您无管理权限访问应用该 GPO 的主机。

1. 在“组策略管理编辑器”窗口中，在左窗格浏览**计算机配置 -> 策略 -> Windows 设置 -> 安全设置 -> 限制组**。
  1. 在右窗格中，右键单击并选择弹出菜单中的**添加组...**。
  2. 在显示的对话框中，键入**管理员**并单击“确定”。
  3. 在显示的属性对话框中，单击**本组成员**：旁边的**添加**按钮。
  4. 在显示的**添加成员**对话框中，单击**浏览...**。
  5. 在打开的**选中用户、计算机、服务帐户或组**对话框中，键入您之前创建的“Splunk Accounts”组名称，然后单击**检查名称**。如果有效，Windows 将为该名称添加下划线。否则，它将告诉您无法找到对象，并提示您再次键入对象名称。
  6. 单击“确定”关闭**选择用户...**对话框。
  7. 单击“确定”关闭“添加用户或组”对话框。
  8. 再次单击“确定”关闭组属性对话框。
2. 为以下其他用户或组重复步骤 1a-1h：
  - 域管理员
  - 需要成为应用 GPO 的各个主机上管理员组成员的任何其他用户。
3. 关闭“组策略管理编辑器”窗口以保存 GPO。

### 限制 GPO 应用程序以选择计算机

1. 在 GPMC 时，如果还未选定，在 GPMC 左窗格选择您创建的 GPO 并添加权限。GPMC 将在右窗格显示有关 GPO 的信息。
2. 在右窗格中，**安全过滤**下，单击**添加...**
3. 在显示的**选择用户、计算机或组**对话框中，键入“Splunk Enabled Computers”（或代表您之前创建的已启用 Splunk 计算机的组名称。）
4. 单击**检查名称**。如果该组有效，Windows 将为该名称添加下划线。否则，它将告诉您无法找到对象，并提示您再次键入对象名称。
5. 单击“确定”返回 GPO 信息窗口。
6. 重复步骤 2-5 以添加“Splunk Accounts”组（代表您之前创建的 Splunk 用户帐户的组。）
7. 在**安全过滤**下，单击**验证用户**条目以突出显示。
8. 单击**删除**。GPMC 将从“安全过滤”字段删除“验证用户”条目，仅留下“Splunk Accounts”和“启用 Splunk 的计算机”。

### 应用 GPO

Active Directory 控制出现组策略更新的时间，同时 GPO 将应用到域中的主机。正常情况下，每 90-120 分钟复制一次。您必须等这段时间跑完，才能尝试以域用户身份安装 Splunk，或在想要更新其组策略的主机上，通过命令提示符运行 `GPUPDATE /FORCE` 来强制进行组策略更新。

1. 在 GPMC 时，在 GPMC 左窗格选择您希望应用到创建的 GPO 的域。
2. 右键单击该域，并在弹出的菜单中选择**链接现有 GPO...**。  
**注意：**如果您仅希望 GPO 对您之前创建的 OU 产生影响，那么选择 OU，然后右键单击显示弹出菜单。
3. 在显示的**选择 GPO**对话框中，选择您创建和编辑的 GPO 并单击**确定**。GPMC 将应用 GPO 到选定域。
4. 从 GPMC 菜单选择**文件 > 退出**关闭 GPMC 菜单。

### 使用受管系统帐户安装 Splunk

或者，您可以使用受管系统帐户安装 Splunk Enterprise。

您可以使用本主题之前的“将为域帐户准备用于 Splunk Enterprise 安装的 Active Directory”分配适当安全策略权限和组成员资格给 MSA。

安装后，向 MSA 授予文件权限时，您可能需要将 NTFS 权限继承与 Splunk Enterprise 安装目录以上的母目录分开，并明确分配该目录和所有子目录的权限。

如果使用“服务”控制面板进行 Splunk 服务更改，Windows 将自动向 MSA 授予“作为服务登录”权限。



1. 创建和配置您计划用于监视 Windows 数据的 MSA。
2. 从[命令行安装 Splunk](#) 并使用 `LAUNCHSPLUNK=0` 标记防止 Splunk Enterprise 在安装完成后运行。
3. 安装完成后，使用“Windows 资源管理器”或 `ICACLS` 命令行实用工具以便向 Splunk Enterprise 安装目录及其子目录授予 MSA“完全控制”权限。
4. 更改 `splunkd` 和 `splunkweb` 服务帐户的默认用户名，如本手册“[修正 Windows 安装期间选择的用户](#)”主题所述。  
注意：完成此步骤后，您必须在用户名末尾附加美元符号 (\$) 以便 MSA 运行。例如，如果 MSA 是 `SPLUNKDOCS\splunk1`，则必须在适当的服务对话框的适当字段中输入 `SPLUNKDOCS\splunk1$`。您必须同时为 `splunkd` 和 `splunkweb` 服务执行这项操作。
5. 确认 MSA 拥有“作为服务登录”权限。
6. 启动 Splunk Enterprise。它以上述配置的 MSA 运行，同时可以访问 MSA 拥有访问权限的所有数据。

## 使用 PowerShell 配置您的 AD 域

您还可以使用 PowerShell 为 Splunk Enterprise 服务配置 Active Directory 环境。

### 创建 Splunk 用户帐户

1. 打开 PowerShell 窗口。
2. 如果需要，则导入 ActiveDirectory PowerShell 模块：

```
> Import-Module ActiveDirectory
```

3. 创建新用户：

```
> New-ADUser -Name <user> `
-SamAccountName <user> `
-Description 'Splunk Service Account' `
-DisplayName 'Service:Splunk' `
-Path '<organizational unit LDAP path>' `
-AccountPassword (Read-Host -AsSecureString 'Account Password') `
-CannotChangePassword $true `
-ChangePasswordAtLogon $false `
-PasswordNeverExpires $true `
-PasswordNotRequired $false `
-SmartcardLogonRequired $false `
-Enabled $true `
-LogonWorkstations '<server>' `
```

在本例中：

- 命令创建一个其密码不会变更的帐户，该密码不会在首次登录后强制变更，也不会到期。
- `<user>` 是您希望创建的用户名称。
- `<organizational unit LDAP path>` 是放置新用户的组织单元名称，指定格式为 X.500，例如：CN=Managed Service Accounts,DC=splk,DC=com。
- `<server>` 是单个主机或逗号分隔的列表，指定了帐户可登录的主机。

**注意：**不需要 `LogonWorkstations` 参数，但您可以限制受管服务帐户可以登录域的工作站。

### 配置 Splunk Enterprise 服务器

一旦您配置了用户帐户，使用 PowerShell 以帐户正确的权限配置服务器，以运行 Splunk Enterprise。

**警告：**这是一个高级程序。对您的 AD 的不当更改可能会使其无法使用。只有在您认为适当并了解所产生的后果（包括由于拼写错误和格式不正确文件而造成的问题）时才能执行这些步骤。

在下例中：

- `<user>` 是您创建将运行 Splunk Enterprise 的用户名称。
- `<domain>` 是用户驻留的域。
- `<computer>` 是您希望进行变更而连接到的远程计算机。

要从 PowerShell 配置本地安全策略：

1. 连接到您希望配置的主机。
  - 如果使用本地主机，请登录并打开 PowerShell 提示符（如果未执行此操作）。
  - 如果连接到远程主机，在远程主机上创建一个新的 `PSession`，如下示例所示。
  - 您可能需要在能够进行远程连接之前禁用 Windows Firewall。要这样做，请阅读 MS TechNet（Windows Server 至 Server 2008 R2 版本）中“需要禁用 Windows 防火墙”，以及 MS TechNet 中“Windows PowerShell 高级安全管理防火墙”。

```
> Enter-PSession -Computename <computer>
```

2. 将服务帐户添加到本地管理员组。

```
> $group = [ADSI]'WinNT://<server>/Administrators,group'
> $group.Add('WinNT://<domain>/<user>')
```

3. 在本地计算机上创建一个包含用户权限设置当前状态的备份文件。

```
> secedit /export /areas USER_RIGHTS /cfg OldUserRights.inf
```

4. 使用备份创建新用户权限信息文件，以在导入时为 Splunk Enterprise 用户分配提升的权限。

```
> Get-Content OldUserRights.inf `
| Select-String -Pattern `
'(SeTcbPrivilege|SeChangeNotify|SeBatchLogon|SeServiceLogon|SeAssignPrimaryToken|SeSystemProfile)' `
| %{ '$_,<domain>\<user>' }
| Out-File NewUserRights.inf
```

5. 为新策略信息文件创建一个标头并将标头和新信息文件连接在一起。

```
> ( '[Unicode]', 'Unicode=yes' ) | Out-File Header.inf
> ( '[Version]', 'signature=' '$CHICAGO`$`', 'Revision=1' ) | Out-File -Append Header.inf
> ( '[Privilege Rights]' ) | Out-File -Append Header.inf
> Get-Content NewUserRights.inf | Out-File -Append Header.inf
```

6. 查阅策略信息文件，确保标头书写恰当且文件无语法错误。

7. 将文件导入主机中的本地安全策略数据库。

```
> secedit /import /cfg Header.inf /db C:\splunk-lsp.sdb
> secedit /configure /db C:\splunk-lsp.sdb
```

## 为 Splunk Enterprise 安装准备本地计算机或非 AD 网络

如果未使用 Active Directory，遵照这些说明，在希望安装 Splunk Enterprise 的主机上，对希望 Splunk Enterprise 以其身份运行的用户授予管理访问权限。

1. 添加用户到本地管理员组，以便为 Splunk Enterprise 应以其身份运行的用户授予管理员权限。
2. 选择**开始 > 管理工具 > 本地安全策略**，启动本地安全策略。将启动本地安全策略，并显示本地安全设置。
3. 在左窗格中，展开**本地策略**，然后单击**用户权限分配**。
  1. 在右窗格中，双击**作为操作系统的一部分**。
  2. 单击**添加用户或组...**
  3. 在显示的对话框中，单击**浏览...**
  4. 在打开的**选中用户、计算机、服务帐户或组**对话框中，键入您之前创建的 "Splunk Computers" 组名称，并单击**检查名称...**如果有效，Windows 将为该名称添加下划线。否则，它将告诉您无法找到对象，并提示您再次键入对象名称。
  5. 单击“确定”关闭“选择用户...”对话框。
  6. 单击“确定”关闭“添加用户或组”对话框。
  7. 再次单击“确定”关闭右侧属性对话框。
4. 为以下其他权限重复步骤 3a-3g：
  - **绕过遍历检查**
  - **作为批处理任务登录**
  - **作为服务登录**
  - **更换进程级别标记**

完成这些步骤后，您可以以所需用户身份[安装 Splunk Enterprise](#)。

## 在 Windows 上安装

您可以使用基于图形用户界面 (GUI) 的安装程序或从命令行在 Windows 上安装 Splunk Enterprise。如果从命令行安装，有更多选项（如静默安装）可用。有关从命令行安装过程的信息，请参阅[从命令行在 Windows 上安装](#)。

在 64 位 Windows 系统上，不能再安装或运行 Splunk Enterprise 的 32 位 Windows 版本。也不能在运行不支持的 OS 的计算机上（例如，在运行 Windows Server 2003 的计算机上）安装 Splunk Enterprise。请参阅[系统要求](#)。如果您尝试以这种方式运行安装程序，它会警告您并阻止安装。

### 安装通用转发器

要安装 Splunk **通用转发器**，请参阅《[通用转发器](#)》手册中的“通过安装程序安装 Windows 通用转发器”。通用转发器是独立于 Splunk Enterprise 安装程序的一个安装程序。

### 升级？

如果您计划升级 Splunk Enterprise，请在继续之前查看“如何升级 Splunk Enterprise”以了解说明和迁移注意事项。

### 安装之前

**选择 Splunk 应以其身份运行的 Windows 用户**

安装之前，请务必阅读“[选择 Splunk 应以其身份运行的 Windows 用户](#)”，确定 Splunk 应以其身份运行的用户帐户以满足特定需求。所选用户将承担安装软件前所必须执行操作的相应后果，同时可在此找到更多详细信息。

### 如果可以，禁用或限制防病毒软件

Splunk Enterprise 的索引子系统需要高磁盘吞吐量。设备驱动程序在 Splunk Enterprise 和操作系统之间的任何软件都会限制 Splunk Enterprise 的处理能力，导致缓慢甚至未响应系统。这包括防病毒软件。

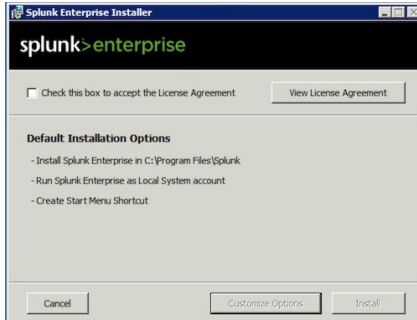
您必须配置此类软件，以避免在启动 Splunk Enterprise 安装之前访问扫描 Splunk 安装目录和进程。

## 通过 GUI 安装程序安装 Splunk Enterprise

Windows 安装程序是 MSI 文件。

### 开始安装

1. 要启动安装程序，请双击 `splunk.msi` 文件。安装程序运行并显示 **Splunk Enterprise 安装程序** 面板。



2. 要继续安装，请选中“选中此框以接受许可协议”复选框。这样就能激活“自定义安装”和“安装”按钮。
3. （可选）如果您希望查看许可证协议，点击“查看许可证协议”。

### 安装选项

Windows 安装程序为您提供两个选项：使用默认安装设置进行安装，或在安装前配置所有设置。

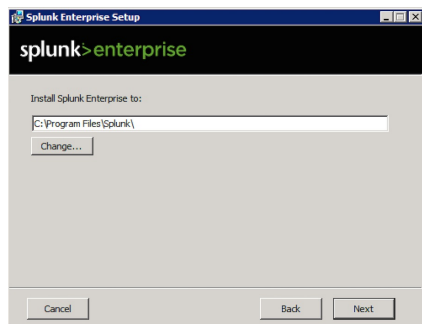
当您选择使用默认设置进行安装时，安装程序将执行以下操作：

- 在系统驱动器（启动您的 Windows 系统的驱动器）上的 `\Program Files\Splunk` 中安装 Splunk Enterprise。
- 安装 Splunk Enterprise 到默认管理和 Web 端口上。
- 以“本地系统”用户身份配置 Splunk Enterprise。
- 为软件创建“开始菜单”快捷方式。

如果您希望更改任何默认安装设置，点击“自定义选项”按钮并按此主题中的“自定义选项”说明进行操作。或者，单击“安装”按钮，以默认值安装软件并按本主题后面介绍的“完成安装”继续操作。

### 在安装期间自定义选项

您可以在安装期间自定义几个选项。当您选择自定义选项时，安装程序将显示“将 Splunk Enterprise 安装到”面板。



默认情况下，安装程序将 Splunk Enterprise 放到系统驱动器的 `\Program Files\Splunk` 中。在整个文档集中，Splunk Enterprise 的安装目录称为 `$SPLUNK_HOME` 或 `%SPLUNK_HOME%`。

Splunk Enterprise 将安装并运行两个 Windows 服务：`splunkd` 和 `splunkweb`。`splunkd` 服务处理所有的 Splunk Enterprise 操作，安装的 `splunkweb` 服务仅在旧模式下运行。

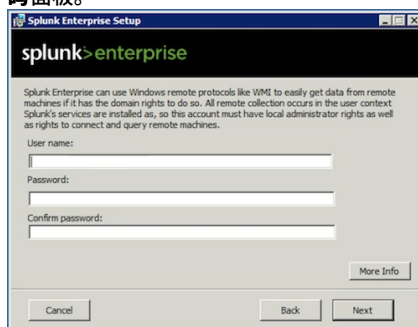
这些服务以您在“选择 Splunk Enterprise 应以其身份运行的 Windows 用户”面板中指定的用户身份安装及运行。您可以选择以本地系统用户或其他用户身份运行 Splunk Enterprise。

当安装程序询问您要安装 Splunk Enterprise 的用户身份时，必须以 `domain\username` 格式指定用户名。该用户必须是安全上下文的有效用户，同时必须是 Active Directory 域的启用成员。Splunk Enterprise 必须在 Local System 帐户或拥有有效密码和本地管理员权限的有效用户帐户下运行。未包含具有用户的域名将导致安装失败。

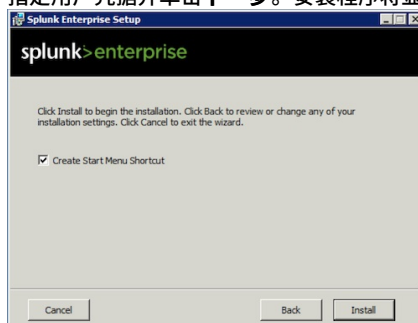
1. 单击“更改...”指定其他安装 Splunk Enterprise 的位置，或单击“下一步”接受默认值。安装程序显示“选择 Splunk Enterprise 应以其身份运行的用户”面板。



2. 选择用户类型并单击下一步。
3. 如果您选择的是 Local System 用户，请继续到步骤 5。否则，安装程序将显示登录信息：指定用户名和密码面板。



4. 指定用户凭据并单击下一步。安装程序将显示安装摘要面板。



5. 单击“安装”以继续安装。

## 完成安装

安装程序运行，安装软件并显示**安装完成**面板。



如果在安装程序期间指定了错误的用户，则会看到两个用来介绍的弹出窗口错误。如果出现这种情况，Splunk

Enterprise 将默认以“本地系统”用户身份安装。在这种情况下，Splunk Enterprise 不会自动启动。您可以继续安装到最后面板，但取消选中“使用 Splunk 启动浏览器”复选框以防止浏览器启动。然后，在启动 Splunk 之前，使用[这些说明](#)切换到适当的用户。

1. （可选）选中**使用 Splunk 启动浏览器和创建开始菜单快捷方式**。
2. 单击**完成**。如果选中适当复选框，安装完成时，Splunk Enterprise 将会启动，并且会在支持的浏览器中启动。

## 在 Splunk Web 中避免 Internet Explorer 增强安全弹出窗口

如果使用 Internet Explorer 访问 Splunk Web，添加以下 URL 到允许的内网组或完全受信组，避免收到“增强安全”弹出窗口：

- [quickdraw.splunk.com](http://quickdraw.splunk.com)
- 您 Splunk Enterprise 实例的 URL

## 安装或升级许可证

如果这是 Splunk Enterprise 的新安装或从一种许可证类型切换到另一种类型，则必须安装或更新许可证。请参阅“安装许可证”。

## 后续步骤

现在您已安装 Splunk Enterprise，可以了解如何开始使用 Splunk Enterprise。请参阅[接下来呢？](#)

或者，您可以在《[数据导入](#)》中查看以下主题以获取有关添加 Windows 数据的帮助：

- 监视 Windows 事件日志数据
- 监视 Windows 注册表数据
- 监视基于 WMI 的数据
- 决定如何监视远程 Windows 数据的注意事项。

## 使用命令行在 Windows 上安装

您可在 Windows 上通过命令行安装 Splunk Enterprise。

不要在 64 位系统中运行 32 位安装程序。如果您尝试这样做，安装程序将警告您并阻止安装。

要通过命令行安装 Splunk **通用转发器**，请参阅《[通用转发器](#)》手册中的“通过命令行安装 Windows 通用转发器”。

## 何时从命令行安装？

您可以从命令提示符或 PowerShell 窗口，在单个计算机上手动安装 Splunk Enterprise。这里是从命令行安装非常有用的一些方案：

- 您希望安装 Splunk Enterprise，但不希望立即启动它。
- 您希望使用脚本自动化 Splunk Enterprise 的安装。
- 您希望在稍后复制的系统上安装 Splunk Enterprise。
- 您希望使用部署工具，如组策略或系统中心配置管理器。
- 您希望在运行 Windows Server Core 版本的系统上安装 Splunk Enterprise。

## 使用 PowerShell 安装

您可以从 PowerShell 窗口安装 Splunk Enterprise。所需步骤与通过命令提示符进行安装所需步骤相同。

## 升级？

要升级 Splunk Enterprise，请查看“如何升级 Splunk”以了解说明和迁移注意事项。

Splunk Enterprise 不支持在升级期间更改管理或 Splunk Web 端口。

## 安装之前

### **选择 Splunk Enterprise 应以其身份运行的 Windows 用户**

安装之前，请参阅“[选择 Splunk Enterprise 应以其身份运行的 Windows 用户](#)”，确定 Splunk Enterprise 应以其身份运行的用户帐户以满足您的数据集合需求。安装软件之前，您选择的用户具有所需操作的特定后果。

### **将为域用户准备用于 Splunk Enterprise 安装的域**

在安装之前，请参阅“[将为网络或域用户准备用于 Splunk Enterprise 安装的 Windows 网络](#)”了解如何配置您的域以运行 Splunk Enterprise 相关的说明。

**如果可以，禁用或限制防病毒软件**

Splunk Enterprise 的索引子系统需要高磁盘吞吐量。设备驱动程序在 Splunk Enterprise 和操作系统之间的任何软件都会限制 Splunk Enterprise 的处理能力，导致缓慢甚至未响应系统。这包括防病毒软件。

您配置此类软件，以避免在启动 Splunk Enterprise 安装之前访问扫描 Splunk 安装目录和进程

**从命令行安装 Splunk Enterprise**

调用 `msiexec.exe` 以通过命令行或 PowerShell 提示符安装 Splunk Enterprise。

对于 32 位平台，使用 `splunk-<...>-x86-release.msi`：

```
msiexec.exe /i splunk-<...>-x86-release.msi [<flag>]... [/quiet]
```

对于 64 位平台，使用 `splunk-<...>-x64-release.msi`：

```
msiexec.exe /i splunk-<...>-x64-release.msi [<flag>]... [/quiet]
```

`<...>` 的值因特定版本而异；例如，`splunk-6.3.2-aaff59bb082c-x64-release.msi`

命令行标记允许您在安装时配置 Splunk Enterprise。使用命令行标记，您可以指定一些设置，包括但不限于：

- 要索引的 Windows 事件日志。
- 要监视的 Windows 注册表单元。
- 要收集的 Windows Management Instrumentation (WMI) 数据。
- Splunk Enterprise 以其身份运行的用户。有关您的 Splunk 实例应以其身份安装的用户类型信息，请参阅“[选择 Splunk Enterprise 应以其身份运行的 Windows 用户](#)”。
- 启用 Splunk 的附带应用程序配置（如轻型转发器）。
- Splunk Enterprise 是否应在安装完成后自动启动。

**支持的标记**

以下是通过命令行安装 Splunk Enterprise for Windows 时可用的标记列表。

Splunk 通用转发器是单独的可执行文件，带自己的安装标记。有关通用转发器支持的安装标记的信息，请参阅《[通用转发器](#)》手册的“通过命令行部署 Windows 通用转发器”。

标记	用途	默认
AGREETOLICENSE=Yes No	使用本标记以同意 EULA。对于静默安装，本标记必须被设置为 <code>Yes</code> 。	No
INSTALLDIR="<directory_path>"	使用本标记指定要安装的目录。在整个文档集中，Splunk 的安装目录被称为 <code>\$SPLUNK_HOME</code> 或 <code>%SPLUNK_HOME%</code> 。	C:\Program Files\Splunk
SPLUNKD_PORT=<port number>	使用这些标记指定 <code>splunkd</code> 和 <code>splunkweb</code> 要使用的替代端口。  如果指定端口，同时该端口不可用，则 Splunk 将自动选择下一个可用端口。	8089
WEB_PORT=<port number>	使用这些标记指定 <code>splunkd</code> 和 <code>splunkweb</code> 要使用的替代端口。  如果指定端口，同时该端口不可用，则 Splunk 将自动选择下一个可用端口。	8000
WINEVENTLOG_APP_ENABLE=1/0  WINEVENTLOG_SEC_ENABLE=1/0  WINEVENTLOG_SYS_ENABLE=1/0  WINEVENTLOG_FWD_ENABLE=1/0	使用这些标记指定 Splunk 是否应索引特定 Windows 事件日志。您可以指定多个标记：  应用程序日志  安全日志  系统日志  转发器日志	0（关闭）



WINEVENTLOG_SET_ENABLE=1/0	设置日志	
REGISTRYCHECK_U=1/0 REGISTRYCHECK_BASELINE_U=1/0	<p>使用这些标记指定 Splunk 是否应从中索引事件</p> <p>捕获 Windows 注册表用户单元 (HKEY_CURRENT_USER) 的基准快照。</p> <p><b>注意：</b>您可以同时设置这两个动作。</p>	0 (关闭)
REGISTRYCHECK_LM=1/0 REGISTRYCHECK_BASELINE_LM=1/0	<p>使用这些标记指定 Splunk 是否应从中索引事件</p> <p>捕获 Windows 注册表用户单元 (HKEY_LOCAL_MACHINE) 的基准快照。</p> <p><b>注意：</b>您可以同时设置这两个动作。</p>	0 (关闭)
WMICHECK_CPUTIME=1/0 WMICHECK_LOCALDISK=1/0 WMICHECK_FREEDISK=1/0 WMICHECK_MEMORY=1/0	<p>使用这些标记指定 Splunk 应索引哪个基于 WMI 的流行性能指标：</p> <p>CPU 使用情况</p> <p>本地磁盘使用情况</p> <p>可用磁盘空间</p> <p>内存统计数据</p> <p><b>注意：</b>如果需要本 Splunk 实例以监视远程 Windows 数据，则还必须指定 LOGON_USERNAME 和 LOGON_PASSWORD 安装标记。Splunk 无法收集任何没有明确访问权限的远程数据。此外，您指定的用户需要特定权限、管理权限和其他权限，您必须在安装之前配置。有关所需凭据的其他信息，请阅读本手册的<a href="#">“选择 Splunk 应以其身份运行的 Windows 用户”</a>。</p> <p>Splunk 可以索引更多基于 WMI 的指标。有关特定信息，请参阅《数据导入手册》中的“监视 WMI 数据”。</p>	0 (关闭)
LOGON_USERNAME="<domain\username>" LOGON_PASSWORD="<pass>"	<p>为用户使用这些标记提供 Splunk 以其身份运行用户的 domain\username 和密码信息。使用这些凭据配置 splunkd 和 splunkweb 服务。对于 LOGON_USERNAME 标记，您必须使用 "domain\username" 格式指定用户名的域：</p> <p>如果希望本 Splunk Enterprise 安装监视任何远程数据，则需要强制使用这些标记。有关要使用凭据的其他信息，请阅读本手册的<a href="#">“选择 Splunk 应以其身份运行的 Windows 用户”</a>。</p>	无
SPLUNK_APP="<SplunkApp>"	<p>使用本标记指定为本次 Splunk 安装后用的附带 Splunk 应用程序配置。目前，&lt;SplunkApp&gt; 的支持的选项是：SplunkLightForwarder 和 SplunkForwarder。这将指定本 Splunk 实例分别作为轻型转发器或重型转发器。有关更多信息，请参阅《转发数据手册》中的“关于转发和接收”主题。</p> <p>如果在此指定 Splunk 转发器或轻型转发器，则还必须指定 FORWARD_SERVER="&lt;server:port&gt;"。</p> <p>要安装不带任何应用程序的 Splunk Enterprise，请忽略本标记。</p> <p><b>注意：</b>完整版本的 Splunk 不会启用通用转发器。通用转发器是可单独下载的可执行文件，带自己的安装标记。</p>	无

FORWARD_SERVER="<server:port>"	仅在您使用 <code>SPLUNK_APP</code> 标记启用 Splunk 重型或轻型转发器时，使用本标记。指定本转发器将发送数据的服务器和 Splunk 服务器端口。	无
DEPLOYMENT_SERVER="<host:port>"	使用本标记指定推送配置更新的部署服务器。输入部署服务器的名称（主机名或 IP 地址）和端口。	无
LAUNCHSPLUNK=0/1	使用本标记指定 Splunk 是否应在系统启动后自动启动。  <b>注意：</b> 如果使用 <code>SPLUNK_APP</code> 标记启用 Splunk 转发器，则安装程序将配置 Splunk 为自动启动并忽略本标记。	1（打开）
INSTALL_SHORTCUT=0/1	使用本标记指定安装程序是否应在桌面和开始菜单创建 Splunk 快捷方式。	1（打开）

## 静默安装

要静默运行安装，添加 `/quiet` 到安装命令字符串的末尾。如果您的系统已开启用户访问控制（有些系统默认开启），则必须以管理员身份运行安装。为此：

- 当打开命令提示或 PowerShell 窗口时，右键单击应用图标并选择“以管理员身份运行”。
- 使用命令窗口运行静默安装命令。

## 示例

以下是使用不同标记的一些示例。

### 以本地系统用户身份静默安装 Splunk Enterprise

```
msiexec.exe /i Splunk.msi /quiet
```

### 启用 Splunk 重型转发器并为 Splunk Enterprise 以其身份运行的用户指定凭据

```
msiexec.exe /i Splunk.msi SPLUNK_APP="SplunkForwarder" FORWARD_SERVER="<server:port>" LOGON_USERNAME="AD\splunk" LOGON_PASSWORD="splunk123"
```

### 启用 Splunk 重型转发器，启用 Windows 系统事件日志的索引并以静默模式运行安装程序

```
msiexec.exe /i Splunk.msi SPLUNK_APP="SplunkForwarder" FORWARD_SERVER="<server:port>" WINEVENTLOG_SYS_ENABLE=1 /quiet
```

其中，"`<server:port>`" 是本计算机应发送数据的服务器和 Splunk 服务器端口。

## 避免 Internet Explorer (IE) 增强安全弹出窗口

要避免 IE 增强安全弹出窗口，将下列 URL 添加到允许的内网组或 IE 中的完全受信组：

- `quickdraw.splunk.com`
- 您 Splunk 实例的 URL

## 后续内容是什么？

安装好 Splunk Enterprise 后，[后续内容是什么？](#)

您还可以参阅《数据导入手册》中的本主题，了解有关如何监视 Windows 数据的注意事项。

## 更改 Windows 安装期间选择的用户

您可以在首次启动软件之前更改 Splunk Enterprise 或通用转发器以其身份安装的 Windows 用户。

有几种方案对于执行此任务是有帮助的。

- 如果在 Splunk Enterprise 安装期间选择了“域用户”，同时该用户不存在或者可能您键入了错误信息。
- 如果需要受管系统帐户 (MSA) 安装 Splunk Enterprise 实例。
- 如果从 ZIP 压缩文件安装软件，并希望从默认的系统用户更改 Splunk Enterprise 服务的 Windows 用户。

您必须在启动 Splunk Enterprise 之前执行此过程。如果已经启动了 Splunk Enterprise，则停止、卸载并重新安装。



1. 在**控制面板 > 管理工具 > 服务**中，找到 `splunkd` 和 `splunkweb`（或通用转发器的 `splunkforwarder`）服务。不能启动这些服务。默认情况下，本地系统用户拥有这些服务。
2. 右键单击每个服务，并选择**属性**。
3. 单击**登录**选项卡。
4. 单击**本帐户**按钮，并填写正确的域\用户名和密码。
5. 单击**应用**。
6. 单击**确定**。
7. （可选）如果您在传统模式下运行 Splunk Enterprise，为第二个服务重复步骤 2 至 6。
8. 从服务管理器或命令行界面启动 Splunk Enterprise 服务。

# 在 Unix、Linux 或 Mac OS X 上安装 Splunk Enterprise

## 在 Linux 上安装

您可以在 Linux 上使用 RPM 或 DEB 软件包或 tar 文件安装 Splunk Enterprise，具体取决于主机运行的 Linux 版本。

要安装 Splunk **通用转发器**，请参阅《通用转发器》手册中的“安装 \*nix 通用转发器”。通用转发器是独立的可执行文件，有自己的一套安装过程。

### 升级？

如果正在升级，请在升级之前查看“如何升级 Splunk”以了解说明和迁移注意事项。

### Tar 文件安装

Tar 文件是手动安装形式。使用 tar 文件安装 Splunk Enterprise 时：

- `tar` 的一些非 GNU 版本可能没有 `-C` 参数。在这种情况下，要安装到 `/opt/splunk`（无论是 `cd` 至 `/opt`），或在运行 `tar` 命令之前，将 tar 文件放入 `/opt`。这种方法适用于您的主机文件系统上的任何可访问目录。
- Splunk Enterprise 不会创建 `splunk` 用户。如果希望 Splunk Enterprise 以特定用户身份运行，您必须在安装之前手动创建用户。
- 确保磁盘分区拥有足够空间可容纳您计划保留索引的未压缩数据量。

要在 Linux 系统上安装 Splunk Enterprise，使用 `tar` 命令展开 tar 文件到相应目录：

```
tar xvzf splunk_package_name.tgz
```

默认安装目录是当前工作目录中的 `splunk`。要安装到 `/opt/splunk`，使用以下命令：

```
tar xvzf splunk_package_name.tgz -C /opt
```

### RedHat RPM 安装

Red Hat、CentOS 和类似的 Linux 版本有可用的 RPM 软件包。

确保您想要的 RPM 软件包可在目标主机本地使用。确认 Splunk Enterprise 用户可以读取并访问文件。

1. 如果需要，可更改下列文件权限。

```
chmod 744 splunk_package_name.rpm
```

2. 调用下列命令，以在默认目录 `/opt/splunk` 下安装 Splunk Enterprise RPM。

```
rpm -i splunk_package_name.rpm
```

3. （可选）要在其他目录安装 Splunk，使用 `--prefix` 标记。

```
rpm -i --prefix=/opt/new_directory splunk_package_name.rpm
```

**注意：**在升级时，`rpm` 可执行文件不提供安全 `net`。您可以使用 `--prefix` 标记将其安装到不同目录，如果您用标记指定的目录不匹配初始安装软件的目录，升级可能出现问题。

### 使用 RPM 软件包替换现有的 Splunk Enterprise 安装

- 运行 `rpm`（使用引用现有 Splunk Enterprise 目录的 `--prefix` 标记）。

```
rpm -i --replacepks --prefix=/splunkdirectory/ splunk_package_name.rpm
```

### 使用 Red Hat Linux Kickstart 自动化 RPM 安装

- 如果希望使用 Kickstart 自动化 RPM 安装，请编辑 kickstart 文件并添加以下内容。

```
./splunk start --accept-license  
./splunk enable boot-start
```

**注意：**enable boot-start 行为可选项。

## Debian .DEB 安装

### 安装前提条件

- 只能将 Splunk Enterprise Debian 软件包安装到默认位置，即 /opt/splunk。
- 此位置必须为常规目录，非符号链接。
- 要安装软件包，您必须具有根用户的访问权限或具有 sudo 权限。
- 软件包不会创建环境变量来访问 Splunk Enterprise 安装目录。您必须自己设置这些变量。

如果需要将 Splunk Enterprise 安装到别处，或如果为 /opt/splunk 使用符号链接，则使用 tar 文件来安装软件。

- 运行使用 Splunk Enterprise Debian 软件包名称作为参数的 dpkg 安装程序。

```
dpkg -i splunk_package_name.deb
```

### 安装项目

Splunk 软件包状态：

```
dpkg --status splunk
```

列出所有软件包：

```
dpkg --list
```

## 后续步骤

安装 Splunk Enterprise 后，若其尚未启动，

- 则可以将其[启动](#)。
- 了解后续内容。请参阅[了解后续内容？](#)

## 卸载 Splunk Enterprise

有关如何卸载 Splunk Enterprise 的信息，请阅读[卸载 Splunk Enterprise](#)。

## 在 Solaris 上安装

您可以使用 PKG 软件包或 tar 文件在 Solaris 上安装 Splunk Enterprise。

要安装 Splunk [通用转发器](#)，请参阅《[通用转发器](#)》手册中的“安装 \*nix 通用转发器”。通用转发器是独立的可执行文件，有自己的一套安装过程。

### 升级？

如果正在升级，请在继续之前查看“如何升级 Splunk”以了解说明和迁移注意事项。

## 安装 Splunk

Splunk Enterprise for Solaris 可作为 PKG 文件或 tar 文件。

### PKG 文件安装

PKG 安装软件包包含要求您在 Splunk 安装之前回答一些问题的请求文件。

```
pkgadd -d ./splunk_product_name.pkg
```

显示了可用软件包列表。

- 选择您希望处理的软件包（默认是 "all"）。

然后，安装程序将提示您指定基本安装目录。

- 要安装到默认目录 `/opt/splunk`，保留为空白。

## **tar 文件安装**

Tar 文件是手动安装形式。使用 tar 文件安装 Splunk Enterprise 时：

- tar 的一些非 GNU 版本可能没有 `-c` 参数。在这种情况下，如果希望安装到 `/opt/splunk`（无论是 `cd` 至 `/opt`），或在运行 `tar` 命令之前，将压缩包放入 `/opt`。这种方法适用于您的计算机文件系统上的任何可访问目录。
- 如果 `gzip` 二进制文件不在您的系统上，则可改用 `uncompress` 命令。
- Splunk Enterprise 不会自动创建 `splunk` 用户。如果希望以特定用户身份运行，您必须在安装之前手动创建用户。
- 确保磁盘分区拥有足够空间可容纳您计划保留索引的未压缩数据量。

要在 Solaris 系统上安装 Splunk Enterprise，使用 `tar` 命令展开 tar 文件到适当目录：

```
tar xvzf splunk_package_name.tar.Z
```

默认安装目录是当前工作目录中的 `splunk`。要安装到 `/opt/splunk`，使用以下命令：

```
tar xvzf splunk_package_name.tar.Z -C /opt
```

## **安装项目**

要了解有关 Splunk Enterprise 软件包及它所安装内容的更多详细信息，运行下列命令：

```
pkginfo -l splunk
```

要列出主机上安装的所有软件包：

```
pkginfo
```

## **后续内容是什么？**

安装 Splunk Enterprise 后，若其尚未启动，

- 则可以将其[启动](#)。
- 了解[后续内容](#)。

## **卸载 Splunk Enterprise**

有关如何卸载 Splunk Enterprise 的信息，请阅读本手册中的[卸载 Splunk Enterprise](#)。

## **在 Mac OS X 上安装**

您可以使用 DMG 软件包或 tar 文件在 Mac OS X 上安装 Splunk Enterprise。

要安装 Splunk **通用转发器**，请参阅《**通用转发器**》手册中的“安装 \*nix 通用转发器”。通用转发器是独立的可执行文件，有自己的一套安装过程。

## **升级？**

如果正在升级，请在继续之前查看“如何升级 Splunk Enterprise”以了解说明和迁移注意事项。

## **安装选项**

Mac OS 版本有两种格式：DMG 软件包和 tar 文件。

如果需要在同一主机的不同位置进行两次安装，则使用 tar 文件。pkg 安装程序无法安装第二个实例。如果存在一

个实例，将在成功安装第二个实例后删除第一个。

### 图形安装

#### 1. 双击 DMG 文件。

将打开包含 splunk.pkg 的**查找器**窗口。

#### 2. 在查找器窗口中，双击 splunk.pkg。

将打开安装程序，并显示**简介**，其中列出了版本和版权信息。

#### 3. 单击**继续**。

将打开**选择目标**窗口。

#### 4. 选择 Splunk Enterprise 的安装位置。

- 要在默认目录 `/Applications/splunk` 中安装，单击硬盘驱动器图标。
- 要选择其他位置，单击**选择文件夹...**

#### 5. 单击**继续**。

将显示预安装摘要。如需更改，

- 单击**更改安装位置**以选择一个新文件夹，或者
- 单击**返回**以返回上一个步骤。

#### 6. 单击**安装**。

安装开始。这可能需要几分钟的时间才能完成。

#### 7. 您的安装完成时，单击**结束**。安装程序会在桌面上放置一个快捷方式。

### 命令行安装

为从命令行在 Mac OS X 上安装 Splunk Enterprise，您必须使用 root 用户，或使用 `sudo` 命令升级权限。**如果您使用 `sudo`，您的帐户必须是管理级帐户。**

#### 1. To mount the dmg:

```
sudo hddid splunk_package_name.dmg
```

查找器将磁盘映像安装在桌面。可使用 `/Volumes/SplunkForwarder <版本>` 下的映像（注意这里有空格）。

#### 2. 要安装

- 至 root 卷：

```
cd /Volumes/SplunkForwarder\ <version>
sudo installer -pkg .payload/splunk.pkg -target /
```

**注意：**磁盘映像的名称中有一个空格。使用反斜杠转义空格或使用引号使磁盘映像名称换行。

- 至其他磁盘分区：

```
cd /Volumes/SplunkForwarder\ <version>
sudo installer -pkg .payload/splunk.pkg -target /Volumes\ Disk
```

**注意：**磁盘映像的名称中有一个空格。使用反斜杠转义空格或使用引号使磁盘映像名称换行。

`-target` 将指定目标卷，如另一个磁盘，其中 Splunk 将安装到 `/Applications/splunk`。

要安装到任何卷的 `/Applications/splunk` 之外的目录，使用如上所述的图形安装程序。

### tar 文件安装

Tar 文件是手动安装形式。使用 tar 文件安装 Splunk Enterprise 时：

- Splunk Enterprise 不会自动创建 `splunk` 用户。如果希望以特定用户身份运行，您必须在安装之前手动创建用户。
- 确保磁盘分区拥有足够空间可容纳您计划保留索引的未压缩数据量。

要在 Mac OS X 系统上安装 Splunk Enterprise，使用 `tar` 命令展开 `tar` 文件到适当目录：

```
tar xvzf splunk_package_name.tgz
```

默认安装目录是当前工作目录中的 `splunk`。要安装到 `/Applications/splunk`，使用以下命令：

```
tar xvzf splunk_package_name.tgz -C /Applications
```

## 后续内容是什么？

安装 Splunk Enterprise 后，若其尚未启动，

- 则可以将其[启动](#)。
- 了解[后续内容](#)。

## 卸载 Splunk Enterprise

有关如何卸载 Splunk Enterprise 的信息，请阅读本手册中的[卸载 Splunk Enterprise](#)。

## 在 FreeBSD 上安装通用转发器

**重要提示：**Splunk 不提供针对在 FreeBSD 上安装 Splunk Enterprise 的软件包，但提供针对 FreeBSD 版本 9 和 10 的通用转发器安装软件包。这些说明详细介绍了在这些版本的 FreeBSD 中安装通用转发器的方法。

要在 FreeBSD 中使用 Splunk Enterprise，您必须下载较早版本的 Splunk 软件。

### 基本安装

**注意：**这些说明仅供安装通用转发器使用。当前无适用于 FreeBSD 的 Splunk Enterprise 版本可用。

此过程在默认目录 `/opt/splunkforwarder` 下安装通用转发器。如果 `/opt` 不存在或您未创建，可能收到错误消息。

FreeBSD 的最佳实践保留小型 `root` 文件系统。您可能想要创建至其他文件系统的符号链接并在那里安装 Splunk，而不是尝试在 `/opt` 中安装。

**1. 确认** `/opt/splunkforwarder` 目录是否存在。如果不存在，则创建目录或从那里链接到其他文件系统。

**2. 使用 Intel 安装程序在 FreeBSD 上安装通用转发器：**

```
pkg_add splunkforwarder-intel.tgz
```

要在其他目录中安装 Splunk Enterprise：

```
pkg_add -v -p /usr/splunk splunkforwarder-intel.tgz
```

### Tar 文件

Tar 文件是手动安装形式。

这些说明仅供安装通用转发器 `tar` 文件使用。当前无适用于 FreeBSD 的 Splunk Enterprise 版本可用。

使用 `tar` 文件安装通用转发器时：

- `tar` 的一些非 GNU 版本可能没有 `-c` 参数。在这种情况下，如果希望安装到 `/opt/splunkforwarder`（无论是 `cd` 至 `/opt`），或在运行 `tar` 命令之前，将压缩包放入 `/opt`。这种方法适用于您的计算机文件系统上的任何可访问目录。
- 转发器不会自动创建 `splunk` 用户。如果希望 Splunk Enterprise 以特定用户身份运行，您必须在安装之前手动创建用户。
- 确保磁盘分区拥有足够空间可容纳您计划保留索引的未压缩数据量。

用 `tar` 命令将通用转发器 `tar` 文件扩展到相应的目录。默认安装目录是当前工作目录中的 `splunkforwarder`。

```
tar xvzf splunkforwarder.tgz
```

要安装到 `/opt/splunkforwarder`，执行：

```
tar xvzf splunkforwarder.tgz -C /opt
```

## 安装后

要确保转发器在 FreeBSD 上正常运行，必须在安装后执行一些其他活动，包括设置流程和虚拟内存限制。

以下数字表示 2 GB 物理内存的主机。如果主机内存不足 2 GB，则相应减少值。

### 1. 将以下内容添加到 `/boot/loader.conf` 中

```
kern.maxdsiz="2147483648" # 2GB
kern.dfdsiz="2147483648" # 2GB
machdep.hlt_cpus=0
```

### 2. 将以下内容添加到 `/etc/sysctl.conf` 中：

```
vm.max_proc_mmap=2147483647
```

### 3. 重新启动 FreeBSD 使更改生效。

## 后续内容是什么？

安装 Splunk 通用转发器后，可访问《通用转发器》手册以：

- 了解如何对其进行配置，以及它如何获取和转发数据。
- 了解您可以向其发出哪些命令。

## 在 AIX 上安装通用转发器

**重要提示：**Splunk 不提供针对在 AIX 上安装 Splunk Enterprise 的软件包，但提供针对 AIX 版本 6.1 和 7.1 的通用转发器安装软件包。这些说明详细介绍了在这些版本的 AIX 中安装通用转发器的方法。

要在 AIX 中使用 Splunk Enterprise，您必须下载较早版本的 Splunk 软件。

### 前提条件

Splunk 以安装通用转发器的身份运行的用户必须拥有读取 `/dev/random` 和 `/dev/urandom` 的权限，否则安装将失败。

### 基本安装

AIX 通用转发器安装程序使用 tar 文件形式。无适用于 AIX 的 Splunk Enterprise 当前版本可用。

使用 tar 文件安装时：

- Splunk Enterprise 不会自动创建 `splunk` 用户。如果希望 Splunk Enterprise 以特定用户身份运行，您必须手动创建用户。
- 确保磁盘分区拥有足够空间容纳您计划索引的未压缩数据量。
- 我们建议您使用 GNU tar 解压缩 tar 文件，因为 AIX tar 无法解压缩长文件名，无法覆盖文件并存在其他问题。如果必须使用系统 tar，请务必检查输出以查看错误消息。GNUtar 通常作为 Linux 应用程序包 `/opt/freeware/bin/tar` 的 AIX 工具箱的一部分安装。

要在 AIX 系统上安装通用转发器，展开 tar 文件到适当目录。默认安装目录是 `/opt/splunkforwarder`。

### 后续内容是什么？

安装 Splunk 通用转发器后，可访问《通用转发器》手册以：

- 了解如何对其进行配置，以及它如何获取和转发数据。
- 了解您可以向其发出哪些命令。

## 在 HP-UX 上安装通用转发器

**重要提示：**Splunk 不提供针对在 HP-UX 上安装 Splunk Enterprise 的软件包，但提供针对 HP-UX 版本 11i v3 的通用转发器安装软件包。这些说明详细介绍了在这些版本的 HP-UX 中安装通用转发器的方法。

要在 HP-UX 中使用 Splunk Enterprise，您必须下载较早版本的 Splunk 软件。

### 基本安装

要在 HP-UX 系统上安装通用转发器，使用 GNU tar 展开 tar 文件到适当目录。默认安装目录是

/opt/splunkforwarder

使用 tar 文件安装时：

- 转发器不会自动创建 `splunk` 用户。如果希望转发器以特定用户身份运行，您必须手动创建用户。
- 确保磁盘分区拥有足够空间容纳您计划索引的未压缩数据量。

## 后续内容是什么？

安装 Splunk 通用转发器后，可访问《通用转发器》手册以：

- 了解如何对其进行配置，以及它如何获取和转发数据。
- 了解您可以向其发出哪些命令。

## 以其他或非 root 用户身份运行 Splunk Enterprise

**重要提示：**本主题仅用于非 Windows 操作系统。有关使用非管理员用户身份在 Windows 上安装 Splunk Enterprise 的信息，请阅读本手册中的[选择 Splunk Enterprise 应以其身份运行的 Windows 用户](#)。要了解如何更改 Splunk Enterprise 服务使用的 Windows 用户，请参阅本手册中的[更改 Windows 安装期间选择的用户](#)。

您可以以本地系统上的任何用户身份运行 Splunk Enterprise。如果以非 root 用户身份运行它，确保它拥有适当权限以：

- 读取配置为要监测的文件和目录。一些日志文件和目录可能需要 root 或超级用户访问权限才能索引。
- 写入 Splunk Enterprise 目录并执行任何配置为用于告警或脚本式输入的脚本。
- 绑定它正侦听的网络端口。小于 1024 的网络端口是仅 root 用户可以绑定的预留端口。

**注意：**由于小于 1024 的端口仅预留用于 root 访问，因此如果以 root 用户身份运行，Splunk Enterprise 仅能侦听端口 514 (syslog 的默认侦听端口)。但是，您可以安装另一个实用工具（如 syslog-ng）以写入 syslog 数据到文件，并让 Splunk 监视该文件。

### 说明

要以非 root 用户身份运行 Splunk Enterprise，您需要首先以 root 身份安装 Splunk Enterprise。然后，在**首次启动 Splunk Enterprise 之前**，更改 `$SPLUNK_HOME` 目录的所有权为所需用户。以下是安装 Splunk Enterprise 并以非 root 用户身份 `splunk` 运行的说明。

在以下示例中，`$SPLUNK_HOME` 代表至 Splunk Enterprise 安装目录的路径。

1. 作为 root 用户，创建用户和组 `splunk`。

**在 Linux、Solaris 和 FreeBSD 中：**

```
useradd splunk
groupadd splunk
```

**在 Mac OS X 上：**

您可以使用**系统首选项 > 帐户**面板添加用户和组。

2. 以 root 用户身份并使用软件包之一，或最好是 tar 文件来运行安装。

**注意：**仍不要启动 Splunk Enterprise。

3. 作为 root 用户，调用 `chown` 命令更改 `splunk` 目录和其中的所有内容的所有权为所需用户。

```
chown -R splunk:splunk $SPLUNK_HOME
```

**注意：**如果您系统的 `chown` 二进制文件不支持更改文件的组所有权，则可使用 `chgrp` 命令进行更改。有关更改组所有权的其他信息，请参阅系统 `man` 主页。

4. 要变成非 root 用户，或者通过注销 root 帐户并作为非 root 用户登录，或者通过使用 `su` 命令来变成非 root 用户。

5. 作为非 root 用户，启动 Splunk Enterprise。

```
$SPLUNK_HOME/bin/splunk start
```

同时，如果希望在以其他用户身份登录时使用 `splunk` 用户身份启动 Splunk Enterprise，则可以使用 `sudo` 命令：

```
sudo -H -u splunk $SPLUNK_HOME/bin/splunk start
```

本示例命令假定：

- 如果在替代位置安装 Splunk Enterprise，则相应更新命令中的路径。
- 您的系统可能还未安装 `sudo`。如果出现这种情况，则可使用 `su`。
- 如果正在使用 `tar` 文件安装，并希望 Splunk Enterprise 以某个用户身份运行（如 `splunk`），则必须手动创建该用户。
- `splunk` 用户必须能够访问 `/dev/urandom` 为产品生成证书。

## Solaris 10 权限

当以 `splunk` 用户身份在 Solaris 10 上安装 Splunk Enterprise 时，您必须设置其他权限以启动 `splunkd`，并绑定到预留端口。

要在 Solaris 10 上以 `splunk` 用户身份启动 `splunkd`，运行：

```
# usermod -K defaultpriv=basic,net_privaddr,proc_exec,proc_fork splunk
```

要允许 `splunk` 用户绑定到 Solaris 10 上的预留端口，请以 `root` 身份运行：

```
# usermod -K defaultpriv=basic,net_privaddr splunk
```

# 使用 Splunk Enterprise 启动

## 首次启动 Splunk Enterprise

### 重要安全提示

开始使用新的 Splunk Enterprise 升级或安装之前，您应花些时间确保软件 and 您的数据是安全的。有关更多信息，请阅读《确保 Splunk Enterprise 安全》手册中的“强化标准”。

要启动 Splunk Enterprise：

## 在 Windows 上

您可以使用命令行或“服务”控制面板，在 Windows 上启动 Splunk Enterprise。使用命令行提供更多选项。在命令提示符窗口中，转到 `C:\Program Files\Splunk\bin` 并键入：

```
splunk start
```

（对于 Windows 用户：在后续示例和信息中，如果已在默认位置安装了 Splunk，使用 `C:\Program Files\Splunk` 替换 `$SPLUNK_HOME`。您还可以使用“系统属性”对话框的“高级”选项卡，将 `%SPLUNK_HOME%` 作为整个系统环境的变量进行添加。）

## 在 UNIX 上

使用 Splunk Enterprise 命令行界面 (CLI)：

```
<Splunk Enterprise installation directory>/bin/splunk start
```

然后，Splunk Enterprise 会显示许可协议，并提示您先接受许可证再继续启动序列。

您可以选择将 `SPLUNK_HOME` 环境变量设置为 Splunk Enterprise 安装目录，以便您可以按如下方式启动软件：

```
export SPLUNK_HOME=<Splunk Enterprise installation directory>
$SPLUNK_HOME/bin/splunk start
```

设置环境变量允许您稍后参考安装目录，而不必记住其确切位置。

## 在 Mac OS X 上

### 从查找器启动 Splunk Enterprise

要从查找器启动 Splunk Enterprise，双击桌面上的 **Splunk** 图标启动名为 "Splunk's Little Helper" 的帮助应用程序。



第一次运行帮助应用程序时，它会通知您需要执行一个简单的初始化。单击**确定**，允许 Splunk 初始化并设置 Trial 许可证。

帮助应用程序加载后，会显示一个提供多个选项的对话框：

- **启动并显示 Splunk**：该选项会启动 Splunk Enterprise 并在您的 Web 浏览器中打开 Splunk Web 页面。
- **仅启动 Splunk**：该选项会启动 Splunk Enterprise，但不会在浏览器中打开 Splunk Web。
- **取消**：告知帮助应用程序退出。这不会影响 Splunk Enterprise 实例本身，只会影响帮助应用程序。

做出选择后，帮助应用程序会执行请求的应用程序并终止。您可以再次运行帮助应用程序来显示 Splunk Web 或停止 Splunk Enterprise。

还可以使用帮助应用程序来停止 Splunk Enterprise（如果已在运行）。

### 从命令行启动 Splunk Enterprise

要从命令行界面启动 Splunk Enterprise，从 `$SPLUNK_HOME/bin`（其中 `$SPLUNK_HOME` 是您安装 Splunk 的目录，默认 `/Applications/splunk`）目录运行以下命令：

```
./splunk start
```

如果默认管理和 Splunk Web 端口已被使用（或者不可用），则提示 Splunk Enterprise 使用下一个可用端口。您可以接受该选项或指定一个要使用的端口。

### 其他启动选项

要在首次启动 Splunk Enterprise 时自动接受许可证，添加 `accept-license` 选项到 `start` 命令：

```
$SPLUNK_HOME/bin/splunk start --accept-license
```

将显示启动序列：

```
Splunk> All batbelt. No tights.

Checking prerequisites...
  Checking http port [8000]: open
  Checking mgmt port [8089]: open
  Checking appserver port [127.0.0.1:8065]: open
  Checking kvstore port [8191]: open
  Checking configuration... Done.
  Checking critical directories... Done
  Checking indexes...
    Validated: _audit _blocksignature _internal _introspection _thefishbucket history main msad
msexchange perfmon sf_food_health sos sos_summary_daily summary windows wineventlog winevents
    Done
  Checking filesystem compatibility... Done
  Checking conf files for problems...
    Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done

[ OK ]

Waiting for web server at http://127.0.0.1:8000 to be available... Done

If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://localhost:8000
```

共有两个其他 `start` 选项：`no-prompt` 和 `answer-yes`：

- 如果您运行 `$SPLUNK_HOME/bin/splunk start --no-prompt`，Splunk Enterprise 将继续启动，直到要求您回答问题。然后，它将显示问题，退出原因并退出。
- 如果您运行 `$SPLUNK_HOME/bin/splunk start --answer-yes`，Splunk Enterprise 将继续启动并对所有是/否问题自动回答“是”。显示问题并在回答后继续。

如果您在一行启动所有三个选项，例如：

```
$SPLUNK_HOME/bin/splunk start --answer-yes --no-prompt --accept-license
```

- Splunk 不会要求您接受许可证。
- Splunk 将对所有是/否问题回答“是”。
- Splunk 会在遇到非是/否问题时退出。

## 更改 Splunk Enterprise 启动的位置和方式

要了解如何更改控制 Splunk Enterprise 启动和运行方式的系统环境变量，请参阅《管理员手册》中的“设置或更改环境变量”。

## 启动 Splunk Web

通过支持的 web 浏览器，导航至：

```
http://<host name or ip address>:8000
```

使用您在安装期间选择的主机和端口。

当您首次登录到 Splunk Enterprise 时，默认的登录信息为：

**用户名 - admin**  
**密码 - changeme**

## 接下来呢？

在一台服务器上安装了 Splunk Enterprise 后，您可以通过如下链接开始入门：

- 了解 Splunk Enterprise 是什么，它的功能和它有何不同。
- 了解如何添加数据到 Splunk Enterprise。
- 添加和管理用户。
- 评估您需要多少空间以存储您的数据。
- 计划您的 Splunk Enterprise 部署，从每天数 GB 到数 TB。
- 了解如何搜索、监视、报告等等。
- Splunk Enterprise 与传统技术的最大差别之一是，它**可在搜索时分类和解释数据**。了解其含义以及如何使用它。

如果下载附带**应用**的 Splunk Enterprise（例如，Splunk + WebSphere），转到 Splunk Web 并在启动器中选择一个应用以直接转到应用的设置页面。有关附带应用的设置和安装部署的更多信息，请在 Splunkbase 上搜索应用名称。

## 了解有关 Splunk Enterprise 的可访问性

Splunk 专注于保持并增强辅助技术 (AT) 用户的可访问性和可用性，无论是 1973 年《美国康复法》第 508 节还是最佳可用性做法。本主题介绍了 Splunk 如何在产品为 AT 用户提供可访问性。

### Splunk Web 和 CLI 的可访问性

Splunk Enterprise 命令行界面 (CLI) 可完全访问，并包含 Splunk Web 的功能超集。CLI 旨在让所有用户都可使用，无论可访问性需求，因此 Splunk 建议 AT 用户使用 CLI（专门用于低视力或盲人，或存在行动障碍的用户）。

Splunk 还知道使用 GUI 偶尔会是首选，即使对于盲人用户。由此，Splunk Web 提供以下可访问性功能：

- 表单字段和对话框具有焦点屏幕显示，如同 Web 浏览器支持的方式。
- 没有浏览器实现视觉焦点的链接、按钮或其他元素无法实现其他屏幕焦点。
- 一致适当地标记表单字段，同时 ALT 文本介绍了功能性元素和图像。
- Splunk Web 不会覆盖用户定义的样式表。
- Splunk Web 的数据可视化通过鼠标悬停提供基本数据，或作为数据表格输出，以便使用颜色传递的信息不需颜色即可传递。
- 必要时，使用 HTML 实现的大部分数据表格使用标头和标记确定数据。
- 以 Flash 显示的数据表格将以视觉化方式显示标头。使用逗号分隔值 (CSV) 格式的基本数据输出具有适当的标头以确定数据。

### 可访问性和实时搜索

Splunk Web 不包含任何闪光或闪烁的组件。但是，使用实时搜索会导致页面更新。可轻松禁用实时搜索，无论在部署还是用户/角色级别。为获得最大便利和可用性，Splunk 建议 AT 用户使用禁用实时功能的 CLI（尤其是屏幕阅读器）。有关禁用实时搜索的详细信息，请参阅《搜索手册》中的“如何限制实时搜索的使用情况”。

## 使用 Firefox 和 Mac OS X 进行键盘导航

要启用 Mac OS X 上的 Firefox 的 Tab 键导航，使用系统首选项而不是浏览器首选项。要启用键盘导航：

1. 在菜单栏中，单击 **[Apple icon] > 系统首选项 > 键盘** 打开键盘首选项对话框。
2. 在键盘首选项对话框中，单击顶部的**键盘快捷方式**按钮。
3. 在对话框底部附近，其中显示**完整键盘访问**，单击**所有控制**单选按钮。
4. 关闭键盘首选项对话框。
5. 如果已经运行 Firefox，退出并重新启动浏览器。

# 安装 Splunk Enterprise 许可证

## 关于 Splunk Enterprise 许可证

Splunk Enterprise 从您指定的来源获取数据并加以处理，以便您进行分析。我们将此过程称为建立索引。有关建立索引过程的信息，请参阅《数据导入》手册中的“Splunk Enterprise 如何处理您的数据”。

Splunk Enterprise 许可证指定您每天可以索引的数据量。

有关 Splunk 许可证的更多信息，请从阅读以下开始：

- 《管理员》手册中的“Splunk 许可授权如何工作”。
- 《管理员》手册中的“Splunk Enterprise 许可证类型”。
- 《管理员》手册中的“有关 Splunk Free 的更多信息”。

## 安装许可证

安装 Splunk Enterprise 后，必须在 60 天内安装许可证以继续使用该产品的所有功能。

在您继续之前，您可能需要阅读这些有关许可证的主题：

- 请参阅《管理员手册》中的“Splunk 许可授权如何工作”以获得有关 Splunk 许可授权的简介。
- 请参阅《管理员手册》中的“组、堆叠、池和其他术语”以获得有关 Splunk 许可证术语的详细信息。
- 请参阅《管理员手册》中的 Splunk 软件许可证的类型，以比较许可证类型并了解哪些许可证可以组合，而哪些不能。

## 添加新许可证

如果您安装具有 Enterprise 许可证的开发/测试许可证，则会替换 Enterprise 许可证文件。

1. 导航到**设置 > 许可证**。
2. 单击**添加许可证**。



3. 单击**选择文件**并导航到您的许可证文件，然后选择该文件，或者单击**直接复制并粘贴许可证 XML...**并将许可证文件的文本粘贴到所提供的字段中。
4. 单击**安装**。Splunk Enterprise 安装您的许可证。
5. 如果您安装的第一份 Enterprise 许可证，则重新启动 Splunk Enterprise。

## 许可证违规

当您超过您的许可证所允许的每日最大索引量时，将发生许可证违规问题。如果您在任意一个日历日超过您的日许可量，您将收到违规警告。该警告将持续 14 天。如果您在过去的 30 天内，导致 Enterprise 许可证收到 5 次或更多警告，Free 许可证收到 3 次警告，您的许可证即出现违规问题。

除非您有 Splunk Enterprise 6.5.0 或更高版本的“无强制执行”许可证，否则 Splunk Enterprise 将禁用对违规

的许可证池的搜索。如果您在先前的 30 天内收到的警告次数小于 5 次 (Enterprise) 或 3 次 (Free)，或者如果您应用临时重置许可证（仅可用于 Enterprise），则恢复搜索功能。要获得重置或“无强制执行”许可证，请与您的销售代表联系。

摘要索引量不计入您的许可证。

如果您收到违规警告，直到午夜前（使用许可证主服务器上的时间计算），您都可解决此问题，否则警告将计入过去 30 天内的警告总数中。

在许可证违规期间：

- Splunk 永不停止对数据建立索引。Splunk 仅在超过许可量时阻止搜索。
- Splunk 至 `_internal` 索引的搜索不会禁用。这意味着，您仍可访问“索引状态”仪表板，或者您仍可对 `_internal` 运行搜索以诊断许可问题。

如果您出现许可证违规，请阅读《管理员手册》中的“关于许可证违规”或 Splunk 社区 Wiki 的“故障排除索引的数据量”。

《管理员手册》中的“管理 Splunk 许可证”一章提供了更多许可授权信息。

# 升级或迁移 Splunk Enterprise

## 如何升级 Splunk Enterprise

升级单个 Splunk Enterprise 实例非常简单。许多情况下，您可安装最新软件包到现有安装以升级该软件。当您在 Windows 系统上升级时，安装程序软件包将检测您之前安装的版本，并主动为您提供升级选项。

必须使用具有管理权限并且可写入实例目录及其所有子目录的用户帐户来升级 Splunk Enterprise。

### 6.5 的新功能？

有关 6.5 版本可用的全新功能的完整列表，请参阅发行说明中的“认识 Splunk Enterprise 6.5”。

有关本版本的问题和解决方案列表，请阅读发行说明中的已知问题。

### 备份您的现有部署

进行任何升级或迁移之前，一律备份现有 Splunk Enterprise 部署。

通过使用允许您恢复 Splunk Enterprise 安装和数据到升级之前状态的技术，您可以管理升级风险，无论是外部备份、磁盘或文件系统快照还是其他方式。当备份 Splunk Enterprise 数据时，请考虑 `$SPLUNK_HOME` 目录和它之外的任何索引。

有关备份 Splunk Enterprise 部署的更多信息，请参阅《管理员》手册中的“备份配置信息”和《管理索引器和群集手册》中的“备份索引数据”。

### 基于环境选择适当的升级程序

您升级 Splunk Enterprise 方式的区分基于您是否有单独的 Splunk Enterprise 实例或多个共同连接的实例。如果您已经配置了实例群集，则区别会很显著。

#### 升级分布式环境

如果您想要升级分布式 Splunk Enterprise 环境，包括存在一个或多个[搜索头合并](#)的环境，请参阅[如何升级分布式 Splunk Enterprise 部署](#)。

#### 升级群集环境

对于升级索引器群集或搜索头群集，存在特殊要求。本手册的以下主题中包含代替该说明的升级说明。

- 要升级索引器群集，请参阅《管理索引器和群集手册》中的“升级索引器群集”。
- 要升级搜索头群集，请参阅《分布式搜索手册》中的“升级搜索头群集”。

### 重要升级信息和更改

请参阅[“关于升级到 6.5：首先阅读此主题”](#)，了解升级时可能影响您的特定迁移提示和信息。

### 从 6.0 和更高版本升级

Splunk Enterprise 支持从 6.0 和更高版本直接升级到 6.5 版本。

- 在 \*nix 上升级到 6.5
- 在 Windows 上升级到 6.5

## 从 5.0 和更早版本升级

不正式支持从 5.0 和更早版本直接升级到 6.5 版本。

- 如果您运行 5.0 版，尝试升级到 6.5 版之前首先升级到 6.3 版。
- 如果您运行 4.3 版，尝试升级到 6.5 版之前首先升级到 6.0 版。
- 如果您运行 4.3 版之前的版本，在最终尝试升级到 6.5 版之前首先升级到 4.3 版，然后升级到 6.0 版。有关如何升级到 4.3 版的特定信息，请阅读“关于升级到 4.3 首先阅读此主题”。

## 获取并安装新的“无强制执行”许可证

Splunk 已创建一个新的许可证类型，在许可证发生违规后不再阻止搜索。

此许可证为 Splunk Enterprise 所有新安装的标准配置。如果要在升级后使用此许可证类型，则必须单独获取并安装在 Splunk Enterprise 实例上。这些实例必须运行 Splunk Enterprise 6.5.0 或更高版本。如果您有分布式部署，作为您的许可证主服务器的 Splunk Enterprise 实例必须运行 6.5.0 或更高版本。您与 Splunk 之间的合同必须保持在正常状态内，才能利用此新许可证类型。

有关新许可证的其他信息，请参阅《*管理手册*》中的“Splunk 软件许可证类型”。

1. 将 Splunk Enterprise 环境（单个部署或分布式部署）升级到 6.5.0 或更高版本。
2. 请联系您的销售代表，他们将向您确认详细信息并向您发出“无强制执行”许可证密钥。
3. 将该密钥应用于 Splunk Enterprise 实例，或者在分布式部署的情况下，将该密钥应用于您的许可证主服务器实例。
4. 在单个主机或许可证主服务器上重新启动 Splunk Enterprise，新许可证才能生效。

## 升级通用转发器

升级通用转发器使用与升级完整 Splunk Enterprise 不同的进程。升级通用转发器之前，请参阅您操作系统的相应升级主题：

- 升级 Windows 通用转发器
- 升级 \*nix 系统的通用转发器

有关索引器和转发器的互操作性和兼容性信息，请阅读《*转发数据手册*》的“索引器和通用转发器兼容性”。

## 关于升级到 6.5 - 首先阅读此主题

在升级之前请阅读本主题，以了解有关从早期版本升级到 6.5 版的过程的重要信息和提示。

## Splunk 应用和加载项兼容性

并非所有 Splunk 应用和加载项都与 Splunk Enterprise 6.5 兼容。如果您计划升级到本版本，请访问 Splunkbase 确认您的应用与 Splunk Enterprise 6.5 兼容。

## 升级群集环境

要升级索引器群集，请参阅《*管理索引器和群集*》手册中的“升级索引器群集”。这些说明代替本手册中升级材料。

要升级搜索头群集，请参阅《*分布式搜索*》手册中的“升级搜索头群集”。这些说明代替本手册中升级材料。

## 升级路径

Splunk Enterprise 支持至软件 6.5 版本的以下升级路径：

- 从完整 Splunk Enterprise 6.0 版本或更高版本升级至 6.5 版本。
- 从 Splunk 通用转发器 5.0 版本或更高版本升级至 6.5 版本。

如果您运行 6.0 之前的 Splunk Enterprise 版本，首先升级至 6.0，然后升级至 6.5。Splunk Enterprise 5.0 的用户在升级至 6.5 之前，也可选择升级至 6.0 至 6.3 版本。有关如何将您的实例迁移到 6.0 版的提示，请阅读“关于升级到 6.0 - 首先阅读此主题”。

## 重要升级信息和更改

在安装新版本时，您应记住几件事情：

**在索引操作期间索引器上的内存使用增加**

当您升级到 Splunk Enterprise 6.5 版本时，索引器在索引操作期间使用的内存量会增加。如果已使用并行化（多个索引管道）配置了索引器，则使用率的增加可能很大。

已使用单个索引管道（Splunk Enterprise 安装的默认值）配置的索引器可以看到内存使用率增加高达 10%。有两个管道集的索引器可以看到内存使用率增加高达 15%。已经配置了四个索引管道的索引器可以看到内存使用率增加高达 25%。

在执行升级之前，请确认您的索引器达到或超过《容量规划》手册详细说明的最低硬件规格。有关每个主机的内存详细信息，请参阅“参考硬件”。

### ***Splunk 的免费版本现在包括“应用键值存储”***

当您升级到 Splunk Enterprise 6.5 版本时，Splunk Enterprise 的免费版本可访问“应用键值存储”功能。

此更改将导致支持“应用键值存储”的进程在主机上运行。这些进程可能会导致额外的内存或磁盘空间使用量。

### ***工具功能添加了一个新的内部索引，并可能增加磁盘空间使用量***

Splunk Enterprise 的工具功能（允许您在选择启用后与 Splunk 共享 Splunk Enterprise 性能统计信息），包括一个新的内部索引，这可能会导致在您升级的主机上使用磁盘空间。您可以按照《管理员手册》中“共享性能数据”中的说明不要选择共享性能数据。

### ***分布式搜索现已默认为单个协议***

为减少搜索头连接到搜索节点时出现潜在问题，已在控制该进程的 `distsearch.conf` 中添加或更改了几个变量。

- `trySSLFirst` 属性在搜索头至搜索节点连接上下文中不再有任何意义。
- 新属性 `defaultUriScheme` 控制搜索头连接搜索节点所使用的协议，可设置为 `http` 或 `https`。设置属性后，该属性用作对于添加至搜索头任何对等节点的默认连接方案。

升级后，查看 `distsearch.conf` 确认已使用新变量更新文件。

该更改于 Splunk Enterprise 6.4 推出，但为了那些从早期版本升级到 6.5 的用户，我们在此处保留它。

### ***增加了某些 JSChart 限制，这可能会降低旧版浏览器的性能***

增加了 JSChart 图表元素可以显示的系列、结果和数据点的数量。

系列的数量从 50 翻倍到 100。可以显示的结果数量从 1,000 增加到了 10,000。并且总数据点的数量从 20,000 增加到了 50,000。

如果您还未更改这些 JSChart 元素的默认值，那么升级后您将在 JSChart 元素上看到更多的数据点。如果使用旧版浏览器与 Splunk Enterprise 进行交互，则可能会看到性能略有降低。

### ***添加了新的功能 'deleteIndexesAllowed'（禁止索引删除）***

添加了新的用户功能，需要非管理员用户角色来保存它，才能删除索引。升级后，必须将此功能分配给任何非管理员用户角色，然后才能删除任何索引。

用户角色还必须具有 "delete\_by\_keyword" 功能。

### ***如果数据模型或报表加速摘要较多，迁移时间可能会显著增加***

升级至 6.5 版本 Splunk Enterprise 时，软件生成数据模型和报表加速摘要校验和，作为迁移的一部分。此操作目的是更好地实现索引器群集上的索引兼容性，但在所有部署中都会进行此操作。如果您的部署中有大量现有数据模型或报表加速摘要，校验和生成过程可能需要很长时间。Splunk Enterprise 在下列进程期间在 `migration.log` 中生成条目：

```
Generating checksums for datamodel and report acceleration bucket summaries for all indexes.  
If you have defined many indexes and summaries, summary checksum generation may take a long time.  
Processed 1000 out of 10007 configured indexes.  
Processed 2000 out of 10007 configured indexes.  
[...]  
Processed 10000 out of 10007 configured indexes.  
Finished generating checksums for datamodel and report acceleration bucket summaries for all indexes.
```

该更改于 Splunk Enterprise 6.4 推出，但为了那些从早期版本升级到 6.5 的用户，我们在此处保留它。

### ***Inputcsv、outputcsv 和 streamedsrv 搜索命令的工作目录已更改***

`inputcsv`、`outputcsv` 和 `streamedsrv` 搜索命令的工作目录已更改。升级后执行这些搜索命令时，Splunk Enterprise

会从 `$SPLUNK_HOME/var/run/splunk/csv` 存储和读取它们创建的文件，而不是从 `$SPLUNK_HOME/var/run/splunko`

升级过程将所有现有工作文件移动至新目录并将下列消息记录到 `migration.log`：

```
Creating $SPLUNK_HOME/var/run/splunk/csv and moving inputcsv/outputcsv files into the created directory.
```

请注意以下迁移问题：

- 升级时，因为更改了目录位置，使用命令的应用、加载项或脚本或者对旧工作目录的引用将受到不良影响。
- 您必须手动迁移与 `inputcsv` 结合使用的任何文件，这些文件不以 `.csv` 文件扩展名结尾或位于子目录中。
- 如果您有一个使用 `outputcsv` 命令的 Splunk Enterprise 外部组件，则必须手动更新使用该命令的组件中任何文件或脚本的路径。
- 此外，如果组件包含 `outputcsv` 生成的文件，并且这些文件不以 `.csv` 结尾或位于子目录中，则必须手动将这些文件迁移到新的工作目录。

该更改于 Splunk Enterprise 6.4 推出，但为了那些从早期版本升级到 6.5 的用户，我们在此处保留它。

### **仅在用户上下文中存在的搜索命令将不再执行**

如果您有在特定 Splunk Enterprise 用户的上下文中运行的任何搜索命令（意味着仅在该用户的 `commands.conf` 中定义的命令，例如，`$SPLUNK_HOME/etc/users/alice/local/commands.conf`），那么在升级后这些命令将不再可用于执行。

要解决此问题，请将命令配置移动到应用级别（将配置放入 `$SPLUNK_HOME/etc/apps/<app_name>/local/commands.conf`）或系统级别（`$SPLUNK_HOME/etc/system/local/commands.conf`）。

该更改于 Splunk Enterprise 6.4 推出，但为了那些从早期版本升级到 6.5 的用户，我们在此处保留它。

### **确认 `introspection` 目录有正确的权限**

如果您作为非 root 用户在 Linux 上运行 Splunk Enterprise 并使用 RPM 来升级，RPM 将 `$SPLUNK_HOME/var/log/introspection` 目录写为 root 用户。当您之后试图启动实例的时候这会产生错误。要防止出错，在升级后重新启动 Splunk Enterprise 前，将 `$SPLUNK_HOME/var/log/introspection` 目录 `chown` 为 Splunk Enterprise 运行时所使用的用户。

该更改于 Splunk Enterprise 6.4 推出，但为了那些从早期版本升级到 6.5 的用户，我们在此处保留它。

### **Splunk Web 可视化编辑器的更改优先于单值可视化的现有 '`rangemap`' 配置**

如果您使用 `rangemap` 搜索命令来定义仪表板上单值可视化的范围和颜色，升级时则改为使用“格式”编辑器。使用“格式”编辑器对于这些可视化进行的更改会覆盖 `rangemap` 配置。继续，通过使用不包含 `rangemap` 命令的查询来生成新的单值可视化，然后使用“格式”编辑器来配置范围、颜色或任何其他设置。

您使用编辑器对于由 `= rangemap` 生成的单值可视化进行的任何更改，会覆盖您对于 `range map` 命令的编辑。另外，当编辑器尝试保存现有配置时，它不再将 `rangemap` 识别为生成这些可视化类型的有效命令。

该更改于 Splunk Enterprise 6.4 推出，但为了那些从早期版本升级到 6.5 的用户，我们在此处保留它。

### **Splunk Enterprise 现已限制添加时滞较大的搜索节点**

升级至 Splunk Enterprise 6.5 后，可能无法使用 Splunk Web 从添加节点的搜索头添加时滞超过 10 分钟的搜索节点。

可通过在搜索头上编辑 `limits.conf` 并将 `addpeer_skew_limit` 设置为低于默认值 600（秒）的正整数来进行更改。

该更改于 Splunk Enterprise 6.4 推出，但为了那些从早期版本升级到 6.5 的用户，我们在此处保留它。

### **Splunk Enterprise 支持在单个进程中运行多个搜索可能增加内存使用率**

自 6.5 版起，Splunk Enterprise 可以在 \*nix 主机上的单个进程中启动多个搜索。

升级时，您可以看到改进的搜索性能，但也可能看到内存使用量有所增加。

此变化不适用于 Splunk Enterprise 的 Windows 实例。

该更改于 Splunk Enterprise 6.4 推出，但为了那些从早期版本升级到 6.5 的用户，我们在此处保留它。

### **已移除对于部署监视器应用的支持**

已移除对于 Splunk 部署监视器应用的支持。当您升级至 Splunk Enterprise 6.5 时，改用监视控制台来监视您的分布式部署。请参阅 *监视 Splunk Enterprise*。

该更改于 Splunk Enterprise 6.3 推出，但为了那些从早期版本升级到 6.5 的用户，我们在此处保留它。

## 数据块签名已删除

数据块签名已从 Splunk Enterprise 中删除。此功能已弃用一段时间。

该更改于 Splunk Enterprise 6.3 推出，但为了那些从早期版本升级到 6.5 的用户，我们在此处保留它。

## 升级时将重新构建加速的自定义数据模型摘要

当您升级至 Splunk Enterprise 6.5 时，目前在实例上的任何加速的自定义数据模型摘要 - 例如由 Splunk App for Enterprise Security 创建的这些摘要 - 将被重新构建。这是因为对于已经进行的数据模型搜索的优化，会使得搜索与先前生成的摘要不兼容。

在重新构建过程中，索引器上摘要使用的 CPU、内存和磁盘 I/O 都将显著增加。依赖于这些数据模型摘要的搜索将会非常缓慢，可能无法正常工作。

如果您需要预防 Splunk Enterprise 升级时自动重新构建这些摘要，则在开始升级之前对于 Splunk Enterprise 配置进行如下更改：

在 `datamodels.conf` 中：

```
acceleration.manual_rebuilds = true
```

在 `limits.conf` 中：

```
[tstats]
allow_old_summaries = true
```

此更改于 Splunk Enterprise 6.3 版本中推出，但也可以在从 6.3 版本升级到 6.5 版本时发生。但为了那些从早期版本升级到 6.5 版本的用户，我们在此处保留它。

## 现在对于学习来源类型的数量存在限制

在所有版本的 Splunk Enterprise 中，对于实例在监视和索引文件的过程中能学习的来源类型的数量存在限制。

为了减少在这样的操作过程中 CPU 和内存使用量达到高峰的情况，创建了一个新的属性来控制实例在监视文件和分析文件内容时学习的来源类型数量。限制值为 1,000，您可通过编辑 `limits.conf` 中的以下属性并重新启动 Splunk Enterprise 来更改该设置：

```
learned_sourcetypes_limit = <number>
```

该设置应能预防内存和 CPU 使用量达到高峰，同时继续使用 `props.conf` 和 `inputs.conf` 来定义并应用来源类型。

该更改于 Splunk Enterprise 6.3 推出，但为了那些从早期版本升级到 6.5 的用户，我们在此处保留它。

## 已启用数据模型摘要的并行摘要

Splunk 平台每次运行来为数据模型生成摘要文件的搜索数量已更改。

当您升级至 Splunk Enterprise 6.5 时，软件会运行两个并发搜索任务（而非一个）来生成摘要文件。该更改称为“并行摘要”。当搜索任务运行时，它可能会导致在包含数据模型的实例上 CPU 和内存使用量的增加，但是也会导致可更快使用数据模型摘要。

您可以为个别数据模型将此设置改回之前的默认值。请参阅《*知识管理器手册*》中的“并行摘要”。

该更改于 Splunk Enterprise 6.3 推出，但为了那些从早期版本升级到 6.5 的用户，我们在此处保留它。

## 现在您必须启用对于 Splunk Enterprise 调试端点的访问

默认情况下，Splunk Enterprise 过去一向允许访问调试端点。现在已不再如此。升级时，您将不能访问调试端点，直到您对于 `web.conf` 进行更改并重新启动 Splunk Enterprise：

```
[settings]
enableWebDebug = true
```

该更改于 Splunk Enterprise 6.3 推出，但为了那些从早期版本升级到 6.5 的用户，我们在此处保留它。

## 从搜索头合并迁移到搜索头群集

如果您想从独立的搜索头或从已弃用的搜索头合并迁移至搜索头群集，则必须按照特定说明进行操作，并使用新的针



对搜索头群集成员的 Splunk Enterprise 实例。有关迁移至搜索头群集的更多信息，请参阅《分布式搜索》手册中的下列主题：

- 从独立搜索头迁移
- 从搜索头合并迁移

### **搜索头群集现已遵守基于用户和角色的搜索配额**

升级至 Splunk Enterprise 6.5 后，您部署的所有搜索头群集都将遵守并强制实行针对用户和角色的搜索配额。这可能导致不执行某些搜索，取决于活动的并发搜索数量。要弥补此功能，在 `limits.conf` 中设置下列属性：

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

该更改于 Splunk Enterprise 6.3 推出，但为了那些从早期版本升级到 6.5 的用户，我们在此处保留它。

### **新“应用键值存储”服务可能会增加磁盘空间使用量**

“应用键值存储 (KV 存储)”服务（通过在其中存储和检索数据来提供一种保留应用程序状态的方式）可能导致实例上的磁盘使用量的增加，这取决于您运行了多少应用。您可以通过编辑 `server.conf` 更改 KV 存储服务放置数据的位置，使用 `splunk clean` CLI 命令恢复 KV 存储使用的数据。请参阅《管理员手册》中的“关于应用键值存储”。

该更改于 Splunk Enterprise 6.2 推出，但为了那些从早期版本升级到 6.5 的用户，我们在此处保留它。

### **Splunk Enterprise 现在可以识别对性能造成不良影响的搜索命令**

为提高安全性和性能，已对一些搜索处理语言 (SPL) 命令进行了变量标记，这些变量可在您将其用于搜索查询时提示 Splunk Enterprise 向您发出性能影响警告。升级后，您可能会看到一个警告消息，阐明您运行的搜索中包含可能带来风险的命令。

### **现在未加速数据模型的结果与加速数据模型的结果相匹配**

未加速数据模型查询事件索引的方式已更改。

这些模型现在查询所有的索引，而不仅是默认的索引。这意味着，您看到的未加速数据模型的结果数量现在应该与您看到的加速数据模型的结果数量相匹配。

在升级后，您可能会看到未加速数据模型比升级之前更多的结果。

该更改于 Splunk Enterprise 6.2 推出，但为了那些从早期版本升级到 6.5 的用户，我们在此处保留它。

### **新安装的服务打开额外的网络端口**

Splunk Enterprise 将安装并运行两个新服务：“应用键值存储”和“应用服务器”。这会在本地计算机上默认打开两个网络端口。8065（用于 Appserver）和 8191（用于“应用键值存储”）。确保您在计算机上运行的任何防火墙软件不会阻止这些端口。“应用键值存储”服务也启动一个额外的过程 `mongod`。如果需要，您可以通过编辑 `server.conf` 和更改 `dbPath` 属性到 Splunk Enterprise 实例能到达的文件系统的有效路径来禁用“应用键值存储”。请参阅《管理员手册》中的“关于应用键值存储”。

该更改于 Splunk Enterprise 6.2 推出，但为了那些从早期版本升级到 6.5 的用户，我们在此处保留它。

### **已更改单值可视化格式**

单值可视化格式更改，因为这些可视化已经过重新设计，以保证从远处看尽量能够看清楚。升级时，可能会有非常大的字母或数字影响使用这些可视化的仪表板。

要解决这个问题，可以：

- 如果您显示可随时间查询的数字值，可利用新的时间上下文。
- 使用单个 XML 将单值面板高度从默认值 115 像素降低。或，
- 用自定义 HTML 面板替换单值面板。

升级前，请参阅 Splunk Answers 中的这篇帖子了解详细信息。

该更改于 Splunk Enterprise 6.3 推出，但为了那些从早期版本升级到 6.5 的用户，我们在此处保留它。

### **一些属性的新默认值会影响 SSL 上的 Splunk 操作**

有些新默认值可能会影响在 SSL 上运行 Splunk Enterprise：

- `supportSSLv3Only` 属性（此属性控制 Splunk Enterprise 如何处理 SSL 客户端）现在的默认设置为 `true`。这意味着只有使用 SSL v3 协议的客户端才能连接到 Splunk Enterprise 实例。

- `cipherSuite` 属性（此属性控制在 SSL 连接期间使用的加密协议）现在的默认设置为 `TLSv1+HIGH:@STRENGTH`。这意味着只有拥有传输层安全 (TLS) v1 密码和“高”加密套件的客户端才能连接到 Splunk Enterprise 实例。

该更改于 Splunk Enterprise 6.3 推出，但为了那些从早期版本升级到 6.5 的用户，我们在此处保留它。

### **登录页面自定义不再可用**

登录页面自定义在 Splunk Enterprise 6.2 版本中不再可用。您只能在升级后修改登录页面的页脚。

## **Windows 特定更改**

### **已删除对 Internet Explorer 9 和 10 的支持**

Microsoft 已宣布，对于 Internet Explorer 11 版本以下的所有版本的支持已于 2016 年 1 月 12 日结束。因为该公告，Splunk 已停止对这些相同版本的 Splunk Web 的支持。这可能会导致 Internet 上不理想的浏览体验

升级时，还应将使用的 Internet Explorer 版本升级到 11 版本或更高的版本。另一种方法是使用 Splunk 支持的另一种浏览器。

### **Windows 主机监视输入不再监视应用程序状态**

已将 Windows 主机监视输入修改为不再监视已安装的应用程序状态。

由于 Splunk Enterprise 用来监视应用程序状态的系统调用中的一个 bug，“Windows 安装程序”服务会试图重新配置所有已安装的应用程序。

升级时，任何引用了“应用程序”属性的 Windows 主机监视输入段落将会失效。要获得应用程序状态数据，可使用“Windows 事件日志”监视器并搜索事件 ID 号 11707（用于安装）或 11724（用于卸载/删除）。

也可以使用 PowerShell 脚本 (`Get-WmiObject -Class Win32_Product | Format-List -Property Name,InstallDate,InstallLocation,PackageCache,Vendor,Version,IdentifyingNum`) 或 WMIC (`wmic product get name,version,installdate`)。

该更改于 Splunk Enterprise 6.3 推出，但为了那些从早期版本升级到 6.5 的用户，我们在此处保留它。

### **新的安装和升级过程**

Splunk Enterprise 的 Windows 版本使用更加简化的安装和升级工作流。安装程序现在假定特定的默认值（用于新的安装）和默认保留现有的设置（用于升级）。要对于默认安装进行任何更改，您必须检查“自定义选项”按钮。在升级期间，您唯一的选择是接受许可协议。请参阅[安装选项](#)。”

该功能于 Splunk Enterprise 6.2 推出，但为了那些从早期版本升级到 6.5 的用户，我们在此处保留它。

### **已做更改，以支持 Windows 输入的更加细致的授权**

Splunk Enterprise 已更新以允许使用 Windows 输入（如网络监视和主机监视）时有更多的控制。如果使用的 Splunk Enterprise 用户角色并非从其他角色继承，可能用户无法访问特定的 Windows 输入。

该更改于 Splunk Enterprise 6.4 推出，但为了那些从早期版本升级到 6.5 的用户，我们在此处保留它。

### **Splunk Web 服务安装但不运行**

`splunkd` 服务处理所有 Splunk Web 操作。然而，在 Windows 实例上，尽管在正常模式操作的时候 `splunkweb` 服务一启动立即退出，安装程序仍然会安装此服务。您可通过更改 `web.conf` 中的配置参数配置服务在旧模式下运行。请参阅《管理员手册》中的“在旧模式中，在 Windows 上启动 Splunk Enterprise”。

**重要提示：切勿永久在传统模式下运行 Splunk Web。** 使用传统模式临时解决由用户界面与主 `splunkd` 服务的新集成引入的问题。一旦您纠正此问题，尽快将 Splunk Web 返回到正常模式。

该更改于 Splunk Enterprise 6.2 推出，但为了那些从早期版本升级到 6.5 的用户，我们在此处保留它。

### **升级后，将不支持启用联邦信息处理标准 (FIPS)**

对于从附带启用安全套接字层 (SSL) 证书的 Splunk Enterprise 系统升级到启用 FIPS 的系统不支持升级路径。如果您需要启用 FIPS，您必须在新安装时开启。

### **监视 Windows 事件日志数据时转换安全标识符 (SID) 和全局唯一标识符 (GUID) 的默认行为已更改**

现已默认禁用所有通道的、控制 Splunk Enterprise 监视事件日志通道时是否尝试解决 SID 和 GUID 的 `etc_resolve_ad_obj` 属性。升级后，所有监视不显式定义此属性的段落的 `inputs.conf` 将不再执行此转换。

该更改于 Splunk Enterprise 6.2 推出，但为了那些从早期版本升级到 6.5 的用户，我们在此处保留它。

## 了解已知的升级问题

要了解 Splunk Enterprise 的任何其他升级问题，请参阅 *发行说明* 中的“已知问题 - 升级问题”。

## 如何升级分布式 Splunk Enterprise 环境

分布式 Splunk Enterprise 环境差异巨大。一些环境具有多个索引器或搜索头，另一些环境具有搜索头池，而其他的环境具有索引器和搜索头群集。这些类型的环境对升级单个实例安装提出了挑战。

### 确定适用于您的环境类型的升级过程

根据您拥有的分布式环境的类型，您可能需要按照单独的说明完成升级。本主题提供有关如何升级没有任何群集元素（如索引或搜索头群集）的分布式环境的指导。它还包含有关如何升级使用已弃用的**搜索头池**功能的环境的信息。具有群集元素的环境（如索引器群集和搜索头群集）在不同主题中具有不同的升级过程。

- 要升级具有搜索头池或没有任何群集元素的分布式环境，请遵循本主题中的过程。
- 要升级具有索引群集的环境，请参阅《*管理索引器和索引器群集*》中的“升级索引器群集”。
- 要升级具有搜索头群集的环境，请参阅《*分布式搜索*》中的“升级搜索头群集”。
- 如果您还有其他的分布式 Splunk Enterprise 环境升级问题，可以在 Splunk 支持门户记录相应情况。

### 分布式组件之间的跨版本兼容性

虽然各种 Splunk 软件组件之间的兼容性有一定的范围，但是当它们都处于特定版本时，它们的工作效果最好。如果必须升级分布式部署的一个或多个组件，则应确认升级的组件与您未升级的组件保持兼容。

- 有关不同版本**搜索头**和**搜索节点**（索引器）之间兼容性的信息，请参阅《*分布式搜索*》中的“分布式搜索的系统要求和其他部署考虑”。
- 有关索引器与转发器之间兼容性的信息，请参阅《*转发数据*》中的“转发器与索引器兼容性”。

### 在升级之前测试应用

在升级分布式环境之前，请确认 Splunk 应用可在您要升级到的 Splunk Enterprise 版本上运行。如果您想要升级的分布式环境包含搜索头合并，则必须测试应用，因为搜索头合并对应用和配置使用共享存储空间。

当您升级池搜索头时，迁移实用工具会警告您需要将应用复制到搜索头的共享存储。该工具不会为您复制这些应用。您必须在升级过程中手动将更新后的应用复制到共享存储，包括 Splunk Enterprise 随附的应用（例如，搜索应用）。如果不这样做，则在完成升级之后，用户界面可能会出现問題。

1. 在参考计算机上，安装当前运行的完整 Splunk Enterprise 版本。
2. 在此实例上安装应用。
3. 访问应用以确认它们如您所期望的一样运行。
4. 升级实例。
5. 再次访问应用以确认它们仍在运行。

如果应用按预期运行，则可以在升级分布式环境期间将其移到相应位置：

- 如果使用的是非池搜索头，请在每个搜索头的升级过程中将应用移到该搜索头上的 `$SPLUNK_HOME/etc/apps`。
- 如果使用的是池搜索头，请将应用移到共享存储位置，池搜索头应该在此位置查找应用。

### 升级包含多个索引器和非池搜索头的分布式环境

此过程会先升级搜索头层，然后升级索引层，以保持可用性。

#### 准备升级

1. 确认非池搜索头使用的所有应用均可在 Splunk 升级版本上运行，如本主题中的“[在升级之前测试应用](#)”。
2. （可选）如果您的环境中使用**部署服务器**，请暂时禁用该服务器。这可防止该服务器将无效配置分布到您的其他组件。
3. （可选）升级部署服务器，但不要重新启动它。

#### 升级搜索头

1. 禁用一个搜索头。
2. 升级搜索头。不要让其重新启动。
3. 在升级该搜索头之后，将经确认可以正常运行的应用放入搜索头的 `$SPLUNK_HOME/etc/apps` 目录中。
4. 重新启用并重新启动搜索头。
5. 在搜索头上测试应用的运行状况和功能。
6. 如果该搜索头没有任何问题，则逐个禁用其余搜索头并升级。重复此步骤，直到已达到您环境中的最后一个搜索头。
7. （可选）在启用每个搜索头之后测试其运行状况和功能。

8. 在升级完最后一个搜索头之后，测试所有搜索头的运行状况和功能。

### 升级索引器

1. 逐个禁用索引器并进行升级。可以在升级之后立即重新启动索引器。
2. 测试搜索头，以确保其在所有索引器中查找数据。
3. 升级所有索引器后，重新启动部署服务器。

### 升级包含多个索引器和池搜索头的分布式环境

如果您的分布式环境包含**池搜索头**，则升级此环境的过程明显变得更加复杂。如果您的组织对停机时间有限制，则使用维护窗口来执行此类升级。

以下是升级此种环境的一些重要概念。

- 池搜索头必须作为一组启用和禁用。
- 所有池搜索头上的 Splunk Enterprise 版本必须均相同。
- 在升级搜索头池之前，您必须测试搜索头使用的应用和配置。

如果您对此处所示的指导说明有其他问题，可以通过 Splunk 支持门户记录相应情况。

升级包含多个索引器和池搜索头的分布式 Splunk 环境：

### 准备升级

有关如何在每个搜索头上启用和禁用搜索头合并的说明，请参阅《[分布式搜索](#)》手册中的“配置搜索头合并”。

1. 确认池搜索头使用的所有应用均可在 Splunk Enterprise 升级版本上运行，如本主题中的[“在升级之前测试应用”](#)。
2. 如果您的环境中使用**部署服务器**，请暂时禁用该服务器。这可防止该服务器将无效配置分布到您的其他组件。
3. 升级部署服务器，但不要重新启动它。
4. 在您的搜索头池中指定一个要升级的搜索头，以测试功能和运行情况。
5. 对于这些说明的其余部分，请参阅作为“搜索头 #1”的那个搜索头。

**注意：**您必须先删除搜索头从搜索头池中删除，然后才能升级搜索头。必须执行此操作有以下几个原因：

- 防止搜索头池共享存储中托管的应用和用户对象被更改。
- 阻止本地应用和系统设置在升级期间被意外迁移到共享存储。
- 确保当升级期间发生问题时，您在回退中使用有效的本地配置。

如果升级引发了问题，则可以在非合并配置中暂时使用搜索头作为备份。

### 升级搜索头池

**警告：**升级之前，先将每个搜索头从搜索头池中删除；升级之后，将其重新添加回池中。尽管不需要确认每个搜索头的运行情况和功能，但是在升级阶段期间一次只能运行一个搜索头。

1. 关闭您环境中的所有搜索头。此时，搜索操作将不可用，直到您在升级之后重新启动所有搜索头时搜索功能才可用。
2. 将经确认可以正常运行的应用放入搜索头池的共享存储区域中。
3. 将搜索头 #1 从搜索头池中删除。
4. 升级搜索头 #1。
5. 重新启动搜索头 #1。
6. 测试搜索头的运行状况和功能。在本例中，“运行情况和功能”意味着实例启动并且您可以登录该实例。并不意味着您可以使用共享存储中托管的应用或对象。也不意味着分布式搜索将正确运行。
7. 如果升级的搜索头 #1 按预期运行，则将其关闭。
8. 将应用和用户首选项从搜索头复制到共享存储上。
9. 将搜索头添加回搜索头池中。
10. 重新启动搜索头。
11. 按照该过程逐个升级池中的其余搜索头。

### 重新启动搜索头

1. 在升级完池中的最后一个搜索头之后，重新启动所有搜索头。
2. 测试所有搜索头在搜索头池中托管的所有应用和用户对象上的运行情况和功能。
3. 在所有索引器中测试分布式搜索。

### 升级索引器

有关搜索头和索引器之间版本兼容性的信息，请参阅《[分布式搜索](#)》中的“分布式搜索的系统要求和其他部署考虑”。

1. （可选，如果没有停机时间的问题）选择一个索引器以保持运行环境，并将其指定为“索引器 #1”。

2. （可选，如果没有停机时间的问题）选择第二个索引器进行升级，并将其指定为“索引器 #2”。
3. 如果需要保持正常运行时间，则关闭除索引器 #1 之外的其他所有索引器。否则，关闭所有的索引器，并继续步骤 7。
4. 升级索引器 #2。
5. 启动索引器 #2 并测试其运行情况和功能。
6. 在确认索引器 #2 正确运行之后，关闭索引器 #1。
7. 逐个升级索引器 #1 以及所有其余索引器。可以在升级之后立即重新启动索引器。
8. 确认所有索引器的运行情况和功能。
9. 重新启动部署服务器，并确认其运行情况和功能。

## 升级转发器

升级分布式环境时，您还可以升级该环境中的所有通用转发器。但这不是必需的，您可能希望考虑是否需要这样做。转发器始终兼容最新版本的索引器。









要升级通用转发器，请参阅《通用转发器》手册中的以下主题。

- 升级 Windows 通用转发器
- 升级 \*nix 系统的通用转发器

## 从版本 5 至版本 6 的 Splunk Web 程序有何更改

本主题列出从 5.x 版本到 6.3 版本中如何使用 Splunk Web 用户界面完成任务的一些主要区别。

### 更改了什么？

程序/任务	您之前如何使用它	您现在如何使用它
首次登录 Splunk Enterprise	在 5.x 中，Splunk Enterprise 启动器具有两个选项卡：欢迎和 Splunk 主页。在“欢迎”中，您可以添加数据和启动搜索应用。 	在 6.3 中，Splunk Enterprise 通过主页启动。该主页的主要部分包括 Splunk Enterprise 导航栏、应用面板、浏览 Splunk Enterprise 面板和一个自定义的默认仪表板（这里未显示）。 
返回到主页	在 5.x 中，要返回主页/欢迎，您从应用菜单选择主页应用。 	在 6.3 中，您单击导航栏左上角的 Splunk 徽标。这样做会始终返回主页。 
编辑帐户信息	在 5.x 中，您在“管理器 > 用户和验证 > 您的帐户”下访问帐户信息（更改全名、电子邮件地址、默认应用、时区、密码）。 	在 6.3 中，您从“管理员 > 编辑帐户”下的 Splunk 导航直接访问帐户信息。 
注销 Splunk Enterprise	在 5.x 中，您单击导航栏上的“注销”按钮。 	在 6.3 中，您选择“管理员 > 注销”。（如果您未以“管理员”身份登录，Splunk Enterprise 显示已登录用户的全称。单击该名称启动“登录”菜单选项） 

管理器/设置	<p>在 5.x 中，您从管理器页面或导航栏上的“管理员”链接编辑所有对象和系统配置。</p> 	<p>在 6.3 中，您直接从“设置”菜单访问这些配置。没有单独的管理器页面。</p> 
管理应用：编辑安装的应用的权限，创建新应用或浏览 Splunk Apps 的社区应用	<p>在 5.x 中，您使用“管理器 -&gt; 应用”或从“应用”菜单选择。</p> 	<p>在 6.3 中，您使用导航栏上的“应用”菜单或主页的“应用”名称旁边的齿轮图标。</p> 
搜索	<p>摘要，搜索</p> <p>搜索和报表</p> <p>仪表板和视图</p> 	<p>搜索</p> <p>报表</p> <p>仪表板</p> 
提取字段或显示来源	<p>在搜索结果中，单击事件时间戳左侧的箭头并选择“提取字段”或“显示来源”。</p> 	<p>在搜索结果中，单击事件时间戳左侧的箭头，然后单击“事件动作”。选择“提取字段”或“显示来源”。</p> 
查找告警列表	<p>在导航栏中，您选择“告警”。</p> 	<p>在导航栏中，您选择“活动 &gt; 触发的告警”。</p> 
查找时间线	<p>在 5.x 中，在运行搜索后，时间线始终作为仪表板一部分可见。您可以隐藏时间线。</p> 	<p>在 6.3 中，您仅能在运行搜索后，在查找事件选项卡的情况下查看时间线。</p> 

## Splunk 应用开发人员的更改

如果为 Splunk 平台开发应用，请阅读本主题，了解我们对 6.5 版本的软件使用应用的方式进行的更改，以及如何迁移现有应用以使用于新版本。

### 没有重大更改

从 Splunk Enterprise 6.4 版本到 6.5 版本，没有对 Splunk 应用开发人员进行重大更改。

### 新的独立应用程序可用于检查应用



对于 Splunk Enterprise 6.5 版本，Splunk 将发布一个名为 AppInspect 的独立应用。此应用程序允许您评估您的应用，并通知您可能会阻止 Splunk 认证从 Splunkbase 下载的应用的任何问题。

要了解有关 AppInspect 的更多信息，请参阅“Splunk 开发门户”中的“Splunk AppInspect 概述”。

## 在 UNIX 上升级到 6.5

### 在升级之前

在升级之前，请参阅“关于升级到 6.5 版本：首先阅读此主题”了解从现有版本升级时，新版本中哪些更改可能会影响您的相关信息。

Splunk Enterprise 不提供恢复到旧版本的方法。如果需要转换为较早的 Splunk 版本，卸载升级的版本并重新安装想要的版本。

### 备份您的文件

执行升级之前，**备份所有文件**，包括 Splunk Enterprise 配置、索引的数据和二进制文件。

有关备份数据的信息，请参阅《*管理索引器和群集手册*》中的“备份索引数据”。

有关备份配置的信息，请参阅《*管理员手册*》中的“备份配置信息”。

### 升级如何工作

要升级 Splunk Enterprise 安装，必须直接在旧版本上安装新版本（在相同的安装目录）。当 Splunk Enterprise 在升级后启动时，它会检测到文件已更改，并询问您是否要在执行升级之前预览迁移更改。

如果您选择在继续之前查看变更，则升级脚本将建议变更写入 `$SPLUNK_HOME/var/log/splunk/migration.log.<timestamp>` 文件。

重新启动 Splunk Enterprise 后，它才会更改您的配置。

### 升级 Splunk Enterprise

1. 在具有要升级的实例的主机上打开 shell 提示符。
2. 更改为 `$SPLUNK_HOME/bin` 目录。
3. 运行 `$SPLUNK_HOME/bin/splunk stop` 命令以停止此实例。
4. 请确认没有其他进程可以自动启动 Splunk Enterprise。
5. 要升级和迁移，直接将 Splunk Enterprise 软件包安装到您的现有部署。
  - 如果您使用的是 `.tar` 文件，则将其扩展到与现有 Splunk Enterprise 实例相同的目录（具有相同所有权）中。这将覆盖并替换匹配文件，但不会删除唯一的文件。`tar xzf splunk-6.x.x-<version-info>.tgz -C /splunk/parent/directory`
  - 如果您使用的是软件包管理器（如 RPM），请键入 `rpm -U splunk_package_name.rpm`
  - 如果您使用的是 `.dmg` 文件（在 Mac OS X 上），请双击该文件并按照说明操作。指定与现有安装相同的安装目录。
6. 运行 `$SPLUNK_HOME/bin/splunk start` 命令。  
Splunk Enterprise 显示以下输出。  

```
This appears to be an upgrade of Splunk.

-----

Splunk has detected an older version of Splunk installed on this machine. To
finish upgrading to the new version, Splunk's installer will automatically
update and alter your current configuration files. Deprecated configuration
files will be renamed with a .deprecated extension.

You can choose to preview the changes that will be made to your configuration
files before proceeding with the migration and upgrade:

If you want to migrate and upgrade without previewing the changes that will be
made to your existing configuration files, choose 'y'.

If you want to see what changes will be made before you proceed with the
upgrade, choose 'n'.

Perform migration and upgrade without previewing configuration changes? [y/n]
```
7. 选择是要运行迁移预览脚本以了解现有配置文件将发生哪些更改，还是继续迁移并立刻升级。如果选择查看预期更改，脚本会提供一个列表。
8. 在查看完这些更改并准备继续迁移和升级之后，再次运行 `$SPLUNK_HOME/bin/splunk start`。

### 同时升级并接受许可协议

将新文件放入 Splunk Enterprise 安装目录后，可以在一个命令中接受许可证并执行升级。

- 是否要在继续升级之前接受许可证并查看预期的更改（回答 'n'），请使用以下命令。

```
$SPLUNK_HOME/bin/splunk start --accept-license --answer-no
```

- 是否接收许可证并开始升级而不查看更改（回答'y'）。

```
$SPLUNK_HOME/bin/splunk start --accept-license --answer-yes
```

## 在 Windows 上升级到 6.5

您可以使用 GUI 安装程序升级，或运行命令行上的 `msiexec` 实用工具，如同“通过命令行在 Windows 上安装”。

Splunk 不提供恢复到旧版本的方法。

在升级 Splunk Enterprise 后，如果需要降级，您必须卸载已升级的版本，然后重新安装您之前使用的 Splunk Enterprise 早期版本。不要尝试使用先前版本的安装程序通过升级安装进行安装，因为这样会导致损坏实例和数据损失。

### 在升级之前

在升级之前，请参阅[“关于升级到 6.5 版本：”](#)有关您从现有版本升级时可能影响您的新版本中的更改的信息，[请首先阅读此主题](#)。

Splunk Enterprise 不提供恢复到旧版本的方法。如果需要转换为较早的 Splunk 版本，卸载升级的版本并重新安装想要的版本。

### Windows 域用户必须与您在安装时指定的用户相匹配

如果通过域用户安装 Splunk Enterprise，则必须在升级过程中显式指定相同的域用户。如果未指定同一用户，Splunk Enterprise 将使用“本地系统”用户身份安装升级。如果不这样做，或者在升级期间意外地指定了错误的用户，则请参阅[修正安装期间选择的用户](#)，以便在启动 Splunk Enterprise 之前切换到正确的用户。

### 不支持在升级期间更改 Splunk Enterprise 端口

Splunk Enterprise 不支持在升级期间更改管理或 Splunk Web 端口。如需更改这些端口，在升级前或升级后进行这些操作。

### 备份您的文件

执行升级之前，备份所有文件，包括 Splunk Enterprise 配置、索引的数据和二进制文件。

- 有关备份数据的信息，请参阅《[管理索引器和群集手册](#)》中的“备份索引数据”。
- 有关备份配置的信息，请参阅《[管理员手册](#)》中的“备份配置信息”。

### 保留自定义证书颁发机构证书副本

在 Windows 上升级时，安装程序将覆盖您在 `%SPLUNK_HOME%\etc\auth` 中创建的任何自定义证书颁发机构 (CA) 证书。如果拥有自定义 CA 文件，请在升级之前备份它们。升级后，可在 `%SPLUNK_HOME%\etc\auth` 中恢复它们。恢复证书后，重新启动 Splunk Enterprise。

## 使用 GUI 安装程序升级 Splunk Enterprise

1. 从 Splunk 下载页面下载新 MSI 文件。
2. 双击 MSI 文件。安装程序运行并尝试检测计算机上安装的 Splunk Enterprise 的现有版本。当它找到旧版本的时候，会显示一个窗格，请您接受许可协议。
3. 接受许可协议。然后，安装程序将安装更新的 Splunk Enterprise。此升级方法保留来自现有安装的所有参数。默认情况下，安装程序在升级完成时重新启动 Splunk Enterprise，并将升级期间对于配置文件所进行更改的日志放在 `%TEMP%` 中。

## 使用命令行升级

1. 从 Splunk 下载页面下载新 MSI 文件。
2. 按“通过命令行在 Windows 上安装”中的说明安装该软件。
  - 如果 Splunk 正以“本地系统”用户之外的用户身份运行，则通过 `USERNAME` 标记在命令行说明中指定该用户。
  - 您可以使用 `LAUNCHSPLUNK` 标记指定 Splunk Enterprise 是否应在升级完成后自动启动，但是您无法更改任何其他设置。
  - 不要在此时更改网络端口（`SPLUNKD_PORT` 和 `WEB_PORT`）。
3. 根据规格不同，Splunk Enterprise 可能在您完成安装后自动启动。

## 迁移 Splunk Enterprise 实例



**重要提示：这些迁移说明仅适用于本地 Splunk Enterprise 实例。**

如果您是 Splunk Cloud 客户或者想将数据从 Splunk Enterprise 迁移到 Splunk Cloud，切勿使用这些说明。请联系专业服务以寻求帮助。

您可以从一个服务器、操作系统、架构或文件系统迁移 Splunk Enterprise 实例到另一个服务器，且同时保留索引的数据、配置和用户的程序。迁移 Splunk Enterprise 实例与升级不同，升级只是在旧版本上安装新版本。升级是迁移的一种形式。

不要尝试使用这些说明将 Splunk Enterprise 安装迁移至 Splunk Cloud。这样做会导致数据丢失。有关信息和说明，请咨询专业服务人员或您的 Splunk Cloud 代表。

## 何时迁移

迁移 Splunk Enterprise 安装有一些原因：

- 您的 Splunk Enterprise 安装位于即将停用或重新用于其他目的的主机。
- 您的 Splunk Enterprise 安装在您组织或 Splunk 不再支持的操作系统，同时希望移动到支持的操作系统。
- 您希望切换操作系统（例如，从 \*nix 到 Windows，反之亦然）
- 您希望移动 Splunk Enterprise 安装到其他文件系统。
- 您的 Splunk Enterprise 安装位于 32 位架构，同时希望移动到 64 位架构以获得更高性能。
- 您的 Splunk Enterprise 安装位于计划不再支持的系统架构，同时希望移动到支持的架构。

## 迁移 Splunk Enterprise 的注意事项

尽管迁移 Splunk Enterprise 实例在许多情况下非常简单，但是进行迁移时仍要注意一些重要的注意事项。根据迁移相关系统类型、版本和架构的不同，您可能需要考虑不止一个项目。

迁移 Splunk Enterprise 实例时，请注意以下内容。

### 端序

如果使用 4.2 版之前的 Splunk Enterprise 版本索引数据，组成该数据的索引文件会对操作系统的端序非常敏感，这是系统组织单个二进制文件字节的方式（或其他数据结构）。

一些操作系统是大端序（意味着它们首先在计算机内存中存储单词最重要的字节），其他则是小端序（意味着它们先存储不重要的字节）。这些操作系统将创建同一端序的二进制文件。索引数据桶文件是二进制，因此对于 4.2 版之前的 Splunk Enterprise 版本来说，这是与创建它们的操作系统相同的端序。

有关处理器架构及其使用的端序的列表，请参阅 Wikipedia 上的端序文章。

当迁移 4.2 版之前的 Splunk Enterprise 实例时，为使目标系统能够读取迁移的数据，您必须在具有相同端序类型的系统之间转移索引文件（例如，同在 SPARC 处理器上运行的 NetBSD 系统与 Linux 系统之间。）

如果无法在使用同一端序的系统之间移动索引（例如，当从大端序系统移动到低端序系统时），您可以通过将数据从大端序系统转发至低端序系统而对其进行移动。然后，在转发完所有数据后，您可以停用大端序系统。

由 Splunk Enterprise 4.2 和更高版本创建的索引文件没有主机端序问题。

### Windows 和 Unix 路径分隔符的差别

\*nix 和 Windows 上的路径分隔符（用于分隔路径单个目录元素的字符）不同。在这些操作系统之间移动索引文件时，您必须确保使用的路径分隔符适用于目标操作系统。您还必须确保更新所有 Splunk 配置文件（尤其是 `indexes.conf`），以便使用正确的路径分隔符。

有关路径分隔符对 Splunk Enterprise 安装的影响的详细信息，请参阅《管理员》手册中的“在 \*nix 和 Windows 上运行 Splunk 的差异”。

### Windows 权限

当在 Windows 主机之间移动 Splunk Enterprise 实例时，确保目标主机分配得到了与源主机相同的权限。其中包括但不限于以下：

- 确保目标主机上的文件系统和共享权限正确，并允许运行 Splunk Enterprise 的用户访问。
- 如果 Splunk Enterprise 以本地系统用户之外的身份运行，则该用户是本地管理员组成员，同时拥有组策略对象分配的适当本地安全策略或域策略权限分配。

### 架构更改

如果降级 Splunk Enterprise 实例运行的架构（例如，64 位至 32 位），则可能因为 64 位操作系统和 Splunk Enterprise 实例创建的大型文件导致新主机中搜索性能下降。

## 分布式和群集 Splunk 环境

当希望迁移分布式 Splunk 实例上的数据（即，作为搜索节点组一部分的索引器，或者已配置为数据搜索索引器的搜索头），则您应在尝试迁移之前，删除分布式环境的实例。

### 数据桶 ID 和潜在数据桶冲突

如果迁移 Splunk Enterprise 实例到另一个已经拥有现有相同名称索引的 Splunk 实例，则必须确保这些索引内的单个数据桶具有不冲突的数据桶 ID。如果遇到数据桶 ID 冲突的数据桶，Splunk Enterprise 将不会启动。当复制索引数据时，您可能需要重命名复制的数据桶文件，从而防止出现这种情况。

## 如何迁移

在 \*nix 系统上迁移时，您可以将直接通过复制文件下载的 tar 文件解压缩到新系统，或使用软件包管理器以使用下载的软件包升级。在 Windows 系统上，安装程序将自动更新 Splunk 文件。

1. 停止希望迁移主机上的 Splunk Enterprise。
2. 复制旧主机中 \$SPLUNK\_HOME 目录的完整内容到新主机。
3. 安装适当版本的 Splunk Enterprise 到目标平台。
4. 确认索引配置文件 (indexes.conf) 包含任何非默认索引的正确位置和路径规格。
5. 在新实例上启动 Splunk Enterprise。
6. 使用现有凭据登录到 Splunk Enterprise。
7. 登录后，通过搜索确认您的数据完整。

## 如何从一个主机移动索引数据桶到另一个主机

如果想要停用 Splunk Enterprise 实例，并立即移动数据到另一个实例，则可在主机之间移动索引的单个数据桶，只要：

- 源和目标主机具有相同的端口。
- 您未恢复 4.2 或更高版本的 Splunk Enterprise 创建的数据桶到 4.2 版之前的 Splunk Enterprise 版本。

**注意：**当复制单个数据桶文件时，您必须确保新系统上没有数据桶 ID 冲突。否则，Splunk Enterprise 将不会启动。在从源系统移动到目标系统后，您可能需要重命名单个数据桶目录。

1. 将源主机上的任何热数据桶从热滚动到温。
2. 查看旧主机上的 indexes.conf，获得该主机上的索引列表。
3. 在目标主机上，创建与源系统相同的索引。
4. 从源主机复制索引数据桶到目标主机。
5. 重新启动 Splunk Enterprise。

## 迁移到新的 Splunk Enterprise 许可证

要了解如何将许可证配置从运行 4.2 版之前版本的 Splunk Enterprise 部署迁移到 4.2 版及较新许可证模型，请遵循本主题中的过程。

**注意：**本主题不介绍整个 Splunk Enterprise 部署的升级。在升级 Splunk Enterprise 部署之前，请阅读[“如何升级 Splunk”](#)。

继续操作前，请查看下列主题：

- 《[管理员手册](#)》中的“Splunk 许可授权如何工作”以获得有关 Splunk 许可授权的简介。
- 《[管理员手册](#)》中的“组、堆叠、池和其他术语”以获得有关 Splunk 许可证术语的详细信息。

### 旧的许可证

当您从 Splunk Enterprise 旧版本迁移时，您最有可能属于以下两种类别之一：

- 如果您运行 Splunk Enterprise 4.0 或更新版本，则您的许可证将在 4.2 和更新版本中正常工作。
- 如果您要从 Splunk Enterprise 4.0 之前的版本迁移，则必须联系您的 Splunk 销售代表以安排新的许可证。在继续迁移之前，请参阅[“升级到 4.0 版本时所期望的内容”](#)。根据 Splunk Enterprise 版本的新旧程度，您可能需要以多个步骤迁移（例如，首先迁移到 4.0，然后到 4.1、4.2，最后是 5.0+）以保留配置。

### 迁移搜索头

如果您的搜索头以前使用旧的转发器许可证，则会自动切换到 Download-trial 组中。在您继续之前，请将搜索头添加到已建立的 Enterprise 许可证池。即使还没有索引量，这仍会启用 Enterprise 功能，尤其是告警和验证。

### 迁移独立实例

如果您有一个 4.1.x Splunk Enterprise 索引器，并且该索引器上已安装一个许可证，则您可以按正常情况继续升

级。有关说明，请参阅[如何升级 Splunk](#)，并在迁移前确保阅读“首先阅读此主题”文档。

您的现有许可证将使用新的许可证，并显示为有效的堆叠，而索引器显示为默认池的成员。

## 迁移分布式索引部署

如果您有多个 4.1.x 索引器，每个索引器都装有自己的许可证，则按照以下高级步骤按顺序迁移部署：

1. 将其中一个 Splunk Enterprise 实例指定为**许可证主服务器**。**搜索头**是不错的选择（若有）。
2. 遵循本手册中的标准说明，安装或升级已选择作为许可证主服务器的 Splunk Enterprise 实例。
3. 根据需要配置许可证主服务器接受索引器的连接。
4. 按照以下步骤，依次逐个升级索引器：
  1. 遵照本手册中的指导说明，将索引器升级到 5.0。它将作为独立许可证主服务器来运行，直到您执行以下步骤。
  2. 复制索引器 Enterprise 许可证文件。可以在每个索引器的 `$SPLUNK_HOME/etc/splunk.license` 下找到 4.2 及更新版本的许可证文件。）
5. 将许可证安装到许可证主服务器，将其添加到想添加索引器的堆叠和池。
6. 将索引器配置为**许可证从服务器**，并在许可证主服务器中指向它。
7. 在许可证主服务器上，导航到 **管理器 > 许可授权** 并查看与相应池关联的索引器列表，以确认许可证从服务器已按预期连接。
8. 在您确认许可证从服务器已按预期连接之后，请按照相同的步骤，继续升级下一个索引器。

## 迁移转发器

如果您部署的是**轻型转发器**，有关信息请查阅《通用转发器》手册中的“从轻型转发器迁移”。您可以将现有的轻型转发器升级为通用转发器，因为通用转发器本身含有许可证。

如果您部署的是**重型转发器**（完整 Splunk 实例在转发到另一个 Splunk Enterprise 实例之前执行索引操作），则可以按索引器的方式来处理它-将其连同其他索引器一起添加到许可证池中。

# 卸载 Splunk Enterprise

## 卸载 Splunk Enterprise

按照本主题中的过程，了解如何从主机中删除 Splunk Enterprise。

### 前提条件

1. 如果您配置 Splunk Enterprise 开机时启动，请在卸载前将其从您的启动脚本中移除。

2. 停止 Splunk Enterprise。导航到 `$SPLUNK_HOME/bin` 并键入 `./splunk stop`（或仅在 Windows 上键入 `splunk stop`）。

## 使用软件包管理实用工具卸载 Splunk Enterprise

使用您的本地软件包管理命令卸载 Splunk Enterprise。在大部分情况下，之前未被软件包安装的文件将停用。这些文件包括安装目录下的配置和索引文件。

在这些说明中，`$SPLUNK_HOME` 指 Splunk 安装目录。在 Windows 中，默认为 `C:\Program Files\Splunk`。对于大多数 Unix 平台，默认安装目录为 `/opt/splunk`。在 Mac OS X 上，为 `/Applications/splunk`。

### RedHat Linux

```
rpm -e splunk_product_name
```

### Debian Linux

```
dpkg -r splunk
```

### 删除所有 Splunk 文件，包括配置文件

```
dpkg -P splunk
```

### FreeBSD

```
pkg_delete splunk
```

## 从不同位置卸载 Splunk Enterprise

```
pkg_delete -p /usr/splunk splunk
```

## Solaris

```
pkgrm splunk
```

## HP-UX

1. 停止 Splunk Enterprise。

```
$SPLUNK_HOME/bin/splunk stop
```

2. 如果启用了开机时启动，以 root 用户身份运行以下命令。

```
$SPLUNK_HOME/bin/splunk disable boot-start
```

3. 删除 Splunk 安装目录。

```
rm -rf $SPLUNK_HOME
```

可能希望删除的其他内容：

- 如果创建了任何索引，同时未使用 Splunk Enterprise 默认路径，则还必须删除这些目录。
- 如果为正在运行的 Splunk Enterprise 创建了用户或组，您还应删除它们。

## Windows

- 使用控制面板中的**添加或删除程序**选项。在 Windows 7、8.1、10，Windows Server 2008 R2 及 2012 R2 中，选项在**程序和功能**下可用。
- （可选）您还可以执行 Splunk Enterprise 安装程序软件包的 `msiexec` 可执行文件，从命令行卸载 Splunk Enterprise。

```
msiexec /x splunk-<version>-x64.msi
```

**注意：**在一些情况下，Microsoft 安装程序可能在卸载流程期间显示重新启动提示。您可以安全忽略本请求而不重新启动。

## 手动卸载 Splunk Enterprise

如果无法使用软件包管理命令，使用这些说明以卸载 Splunk Enterprise。

1. 停止 Splunk Enterprise。

```
$SPLUNK_HOME/bin/splunk stop
```

2. 查找并 `kill` 任何名称包含 "splunk" 的滞留进程。  
**对于 Linux 和 Solaris：**

```
kill -9 `ps -ef | grep splunk | grep -v grep | awk '{print $2;}'`
```

### 对于 FreeBSD 和 Mac OS

```
kill -9 `ps ax | grep splunk | grep -v grep | awk '{print $1;}'`
```

3. 删除 Splunk Enterprise 安装目录 `$SPLUNK_HOME`。

```
rm -rf /opt/splunk
```

在 Mac OS 中，您还可以拖动文件夹到回收站以删除安装目录。

4. 删除顶级目录之外的任何 Splunk Enterprise 数据存储区或索引。

```
rm -rf /opt/splunkdata
```

5. 删除 `splunk` 用户和组（如果存在）。  
**对于 Linux、Solaris 和 FreeBSD：**

```
userdel splunk
```

```
groupdel splunk
```

对于 Mac OS：

您可以使用**系统首选项 > 帐户**面板管理用户和组。

对于 Windows：

打开命令提示符并对您用于安装 Splunk Enterprise 的 msi 软件包运行命令 `msiexec /x0`。如果您没有此软件包，请从下载页面获取正确版本。

## 参考

## PGP 公共密钥

本主题包括 PGP 公共密钥和安装说明。也可使用 HTTPS 下载文件。

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.1 (GNU/Linux)

mQGibEBE21QRBADEMonUxCV2kQ2oxsJTjYXrYCWctH5/OnmhK5lT2TQaE9QUTs+w
nM3sVInQqRwBDH2qsHggqjJS0PIE867n+1Vuk0gSVzS5S01YzQjnSrisvyN452MF
2PgetHq8Lb884cPJnxR6xoFTHqOQueKEOXCovz1eVrjrfpnmWka/+5X8wCg/CJ7
pT7OXHFN4X0seVQabetEbWcEAIUaazF2i2x9QDJ+6twTAlX2oqAguqtBzJX5qaHn
OyRdBUE2g4ndiE3QAKybuq5f0UM7GXqdllhVUBatqafySfjlTBaMVzd4ttrDRpq
Wya4ppPMIWcnFG2CXf4+HuyTPgj2cry2oMBm2LMfGhxcqM5mpoyHqUiCn7591Ra/
J2/FA/0c2UAUh/eslOn89I6FhFoicT5RPtRpxMoEM1Di15zJ7EXY+xBVF9rutqHR
5OI9kdHibYTwf4qjOOPOA7237N1by9GiXY/8s+rDwmSNKZB+xAaLy17cDhYMv7CP
qFTutvE8BxTsF0MgRuzIHfJQE2quuxKJFs9lkSFGuZhvRuWRcrQgS2ltIFdhhGxh
Y2UgPHJlBgvhc2VAc3BsdW5rLmNvbT6lXgQTEQIAHgUCRsTbVAIbAwYLCQgHAWID
FQIDAXYCAQIEaQIXgAAKCRAPYLH9ZT+xEhsPAKDimP8sdCr2ecPm8mre/8TK3Bha
pQCg3/xEickiRKklpKnySUNLR/ZBh3m5Ag0ERSTbbRAIAIdfWi0BeCj8BqrcTXxm
6MMvdEkjdJC+4xmwaQpYmS4JKK/hJFfpyS8XUgHjBz/7zfR8Ipr2CU59Fy4vb5oU
HeOecK9ag5JfG2i/VWH/vEJAMCkbN/6aWwhHt992PUZC7EHQ5ufRdxGGap8SPZT
iIKY0OrX6Km6usoVWMTYKNm/v7my8dJ2F46YJ7wIBF7arG/voMOg1Cbn7pCwCatg
jOhgjdEXRJUEZP3AfLlc3t5iq5n5FYLGAOpT7OIroM5AkgbVLfj+cjKaGD5UZW7
S00akWhTbVHSCDJoZAGJrvJs5DHcEnCjVy9AJxTNMs9GowWaixfyQ7jgMNWKHJp+
EyMAAwYH/RLNK0HHVSBYPWnS2t5sXedIGAgm0fTHhVUCWQxN3knDIRmdkqDTnDKd
qcqYFsEljazI2kx1ZlWdUGmvU+Zb8FCH90e-j806jdFLKJa50/I/oY0+/+DRBZJG
3oKu/CK2NH2VnK1KLzAYnd2wZQAEja401CBV0hgutVf/ZxzDUAR/XqPHY5+EYg96
4Xz0PdZiZKOhJ5g4QjhhoL3jQwcBuyFbJADw8+Tsk8RjQzvHfuwPouVU+8F2vLJK
iF2HbKOUJvdH5GfFuk6o5V8nnir7xSrVj4abfP4xA6RVum3HtWoD7t//75gLcW77
kXDR8pmmnddm5VXnAuk+GTPGACj98+eISQQYEQIACQUCRsTbbQIbDAACRApYlH9
ZT+xEiVuAJ9INUCilkXSNu9p27zxTZhlkL04QCg6YfWldq/MWPCwa1PgiHrVJng
p4s=
=Mz6T
-----END PGP PUBLIC KEY BLOCK-----
```

## 安装密钥

1. 将密钥复制和粘贴到一个文件中，或使用 HTTPS 下载文件。

2. 使用以下安装密钥：

```
rpm --import <filename>
```