Splunk® Enterprise 8.2.0

安装手册

生成时间：2021 年 5 月 24 日，14:32

Table of Contents

欢迎使用 Splunk Enterprise 安装手册

本手册包含哪些内容

*安装手册*提供安装 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

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。

您可以通过两种方式安装 Splunk Enterprise：

- 下载和安装 Splunk Enterprise 安装包
- 下载 Splunk Enterprise Docker 图像并在 Docker 容器中运行 Splunk Enterprise

容器化的 Splunk Enterprise 可为您提供一种简化且一致的方式，便于您快速使用 Splunk Enterprise 并亲身体验软件。虽然 Splunk Enterprise Docker 容器可轻松跨不同的环境并允许进行复杂的可扩展部署，但是在这个版本中，对于基于容器的部署，Splunk 仅支持独立的单服务器 Splunk 拓扑。要了解有关 Docker 的信息，请参阅 Docker 文档。

使用安装包安装 Splunk Enterprise

1. 请参阅安装的系统要求。根据安装 Splunk Enterprise 的操作系统和使用 Splunk Enterprise 的方式，可能适用其他安装要求。
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，请参阅“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即将安装 Splunk Enterprise 的计算机提供安全防护。
4. 从 Splunk Enterprise 下载页面为您的系统下载安装软件包。
5. （可选）将您的 KV 存储存储引擎从内存映射（MMAP）存储引擎迁移到 WiredTiger 存储引擎，以显著减少所需的存储量并提高性能。要规划迁移，请参阅*《管理员手册》*中的“迁移 KV 存储的存储引擎”。
6. 使用适用于您的操作系统的安装说明进行安装。请参阅“安装说明”。
7. （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 软件并使用 Splunk Enterprise 的搜索语言搜索该数据。
8. （可选）安装 Splunk Enterprise 后，计算数据占用的空间量。请参阅*《容量规划手册》*中的“预估您的存储需求”。
9. 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》*。

在 Docker 容器中部署和运行 Splunk Enterprise

1. 确认您的系统符合以下基于容器的安装要求：
    1. 关于支持的操作系统，请参阅“支持的操作系统”中的“容器化的计算平台”部分。
    2. 确认您的系统是否符合或超出推荐的硬件要求。请参阅“推荐的硬件”。
    3. 确认您用于将 Splunk Enterprise 数据存储在 Docker 容器中的任何磁盘卷使用以下一种支持的文件系统。请参阅“支持的文件系统”。
2. 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 的计算机提供安全防护。
3. 为您的操作系统下载并安装 Docker Enterprise 或 Community Edition Engine 17.06.2 或更高版本。
4. 执行安装。请参阅“部署和运行 Splunk Enterprise Docker 容器”获取分步安装说明。
5. （可选）预估您的 Splunk Enterprise 数据将占用的空间量。请参阅*《容量规划手册》*中的“预估您的存储需求”。
6. 为容器新建并安装卷以存储 Splunk Enterprise 使用和产生的数据，例如索引的数据和配置文件。
   有关为数据持久性配置存储的说明，请参阅“Splunk Github 上的数据存储”。
7. 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

许多情况下，您可以在现有的版本基础上升级 Splunk Enterprise。

- 要从早期 Splunk Enterprise 版本升级，请参阅本手册中的“如何升级 Splunk Enterprise”以了解相关信息和特定说明。
- 有关从一个版本迁移到另一个版本的信息，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。
- 要将 Splunk Enterprise 实例从一个主机移到另一个主机，请参阅“迁移 Splunk 实例”。

本地使用 Splunk Enterprise 的系统要求

Splunk 支持在几个计算环境中使用 Splunk Enterprise。下载软件前，先了解受支持的环境。

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“通用转发器系统要求”。

如果您对新功能有任何想法或需求，请使用 Splunk 想法门户搜索、投票和请求任何 Splunk 解决方案的新增强功能（称为想法）。请参阅*《Splunk 社区入门》*手册中的“Splunk 想法”。

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。

每个表显示可用的计算平台（操作系统和架构）以及 Splunk 软件类型。计算平台和您想要的 Splunk 软件类型相交的方框中的粗体 **X** 表示该 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。

有些方框包含字符而不是粗体 **X**。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**列查找您希望安装的 Splunk Enterprise 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 软件类型：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 许可证	免费许可证	试用许可证	通用转发器包
Linux, kernel 5.4.x 版及更高版本	x86（64 位）	**X**	**X**	**X**	**X**
Linux，所有 3.x 和 4.x kernel 版本	x86（64 位）	**X**	**X**	**X**	**X**
Linux，所有 2.6 kernel 版本	x86（64 位）	D	D	D	**X**
AIX 7.1 和 7.2	PowerPC				**X**
ARM Linux	ARMv8（64 位）				**X**
FreeBSD 11	x86（64 位）				**X**
macOS 11	Intel				**X**
macOS 10.15	Intel		D	D	**X**
macOS 10.14	Intel		D	D	**X**
PowerLinux、Little Endian kernel 2.6 及以上版本	PowerPC				**X**
Solaris 11	x86（64 位）				**X**
	SPARC				**X**
z/Linux、kernel 3.0 及更高版本	s390x				**X**
z/Linux、kernel 版本 2.6	s390x				D

X：Splunk 件可用于该平台。
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”。
方框空白表示软件在此平台上不受支持。

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 许可证	免费许可证	试用许可证	通用转发器包
Windows Server 2016 和 Server 2019（所有安装选项）	x86（64 位）	**X**	**X**	**X**	**X**

Windows 10	x86（64 位）		X	X	X
	x86（32 位）				X
Windows Server 2012 和 Server 2012 R2	x86（64 位）				X

X：Splunk 件可用于该平台。
方框空白表示软件在此平台上不受支持。

容器化的计算平台

官方存储库包含构建 Splunk Enterprise 和通用转发器映像的 Dockerfiles。该存储库可以在 Splunk-Docker 的 GitHub 上找到。Splunk-Docker GitHub 上的“支持指南”中提供了 Docker 和 Splunk 软件的要求列表。

对于容器编排，GitHub 上的 Splunk Operator for Kubernetes 使您能够快速轻松地在您选择的私有或公共云提供商上部署 Splunk Enterprise。操作员通过在实施 Kubernetes 最佳实践的同时自动化工作流程，简化了 Splunk Enterprise 的扩展和管理。

Splunk Enterprise 架构支持	产品
单实例 Splunk Enterprise 部署。	GitHub 上的 Splunk-Docker
分布式或单实例 Splunk Enterprise 部署。	GitHub 上的 Splunk Operator for Kubernetes

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 Enterprise 架构和流程
- 选择 Splunk Enterprise 应以其身份运行的 Windows 用户
- “决定如何监视远程 Windows 数据的注意事项”（*数据导入*）

支持监视控制台的操作系统

Splunk Enterprise 监视控制台只能在 Linux 和 Windows 的部分版本中运行。有关支持监视控制台的平台架构的信息，请参阅*《故障排除手册》*中的“支持的平台”。要了解监视控制台的其他前提条件，请参阅*监视 Splunk Enterprise* 中的“监视控制台设置前提条件”。

已弃用操作系统和功能

随着更新 Splunk 软件，我们有时会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”。

在操作系统上新建和编辑不使用 UTF-8 字符集编码的配置文件

Splunk 软件预计配置文件使用 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新建不使用 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。

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 Enterprise”。

支持的浏览器

Splunk Enterprise 支持以下浏览器：

- Firefox（最新）

- Safari（最新）
- Chrome（最新）

Splunk Enterprise 不支持以下浏览器：

- Internet Explorer（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。请参阅*《容量规划手册》*中的“参考硬件”。

有关生产部署的硬件规划讨论，请参阅*《容量规划手册》*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计算机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。

Splunk Enterprise 和容器化基础设施

容器化部署必须提供满足或超过 Splunk Enterprise 部署推荐的硬件容量的硬件资源。请参阅“容器化的计算平台”。

推荐的硬件容量

有关生产部署的硬件要求信息，请参阅*《容量规划手册》*中的“参考硬件”。

通用转发器的硬件要求

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“通用转发器系统要求”。

支持的文件系统

如果在本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	ext3、ext4、btrfs、XFS、NFS 3/4
Solaris（仅限于通用转发器）	UFS, ZFS, VXFS, NFS 3/4
FreeBSD（仅限于通用转发器）	FFS, UFS, NFS 3/4, ZFS
Mac OS X	HFS, APFS, NFS 3/4
AIX（仅限于通用转发器）	JFS, JFS2, 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**。只有冷或冻结的数据桶支持 NFS 上的 Splunk Enterprise。
- 不要使用 NFS 共享索引器群集中的冷或冻结索引数据库，因为这样可能会新建一个单点故障。
- 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）对 Splunk Enterprise 而言较为可靠。

- 不禁用属性缓存。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、部署和搜索。ulimit 命令控制对必须调整为 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。

您的 Splunk Enterprise 实例进行的任务越多，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”。

下表显示了 Splunk Enterprise 使用的系统范围资源。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	最小建议值
打开文件	ulimit -n	64000
用户进程	ulimit -u	16000
数据段大小	ulimit -d	您希望 Splunk Enterprise 分配的最大 RAM（以千字节为单位）。例如，8GB 是 8000000。
文件大小	ulimit -f	-1 设置为 -1 会将文件大小设置为无限制。

在采用 Linux 操作系统且 Splunk Enterprise 服务由 systemd 管理的计算机上，您可以更新 /etc/systemd/system/Splunkd.service 单元文件以设置下表中列出的值。查看值并根据可用的计算机资源调整值。

系统范围资源	systemd 单元文件参数	最小建议值
打开文件	LimitNOFILE=	64000
用户进程	LimitNPROC=	16000
数据段大小	LimitDATA=	您希望 Splunk Enterprise 分配的最大 RAM（以字节为单位）。例如，8GB 是 8000000000。
文件大小	LimitFSIZE=	infinity 设置为 "infinity" 会将文件大小设置为无限制。
总线程	TasksMax=	一个服务可以创建的最大任务数。此设置符合用户进程限制 LimitNPROC，并且该值可以设置以确保匹配。例如，16000。

在运行 FreeBSD 的计算机上，您可能需要增加默认的 kernel 参数，并最大化进程堆叠大小。以下表显示必须在主机上的 /boot/loader.conf 中显示的参数。

系统范围资源	Kernel 参数	推荐的值
默认的进程数据大小（软限制）	dfldsiz	2147483648
最大的进程数据大小（硬限制）	maxdsiz	2147483648

在运行 AIX 的计算机上，您可能需要增加系统中最大文件大小（fsize）和常驻内存大小（rss）的资源限制。以下表显示必须为运行 Splunk 软件的用户在 /etc/security/limits 中显示的参数。

系统范围资源	ulimit 调用	推荐的值
数据段大小	ulimit -d	1073741824
常驻内存大小	ulimit -m	536870912
打开文件数	ulimit -n	8192
文件大小限制	ulimit -f	-1 （无限制）

本注意事项不适用于基于 Windows 的系统。

有关固态磁盘驱动器的注意事项

当与布隆过滤器组合使用时，固态驱动器（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：

- 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

如果您在一个使用透明大内存页面的 Unix 计算机上运行 Splunk Enterprise，在尝试安装 Splunk Enterprise 之前请参阅*发行说明*中的“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。

进一步阅读

请参阅“下载 Splunk Enterprise 页面”以获得最新可用版本。

如需本发行中已知和已解决问题的详细信息，请参阅发行说明。

有关更多信息，请参阅*容量规划*手册中的“Splunk Enterprise 容量规划介绍”了解评估容量信息。

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。

Splunk Enterprise 流程需要网络连接。有关显示了所用网络端口的表格和图表，请参阅*《继承 Splunk Enterprise 部署》*手册中的“组件及其与网络的关系”。

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 pythonservice.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 实例上新建特定数据导入时，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

splunk-perfmon.exe 将会运行，此时配置 Splunk Enterprise 以监视本地 Windows 计算机的性能数据。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

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

splunk-regmon

splunk-regmon.exe 将会运行，此时配置 Splunk 的注册表监视输入。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

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

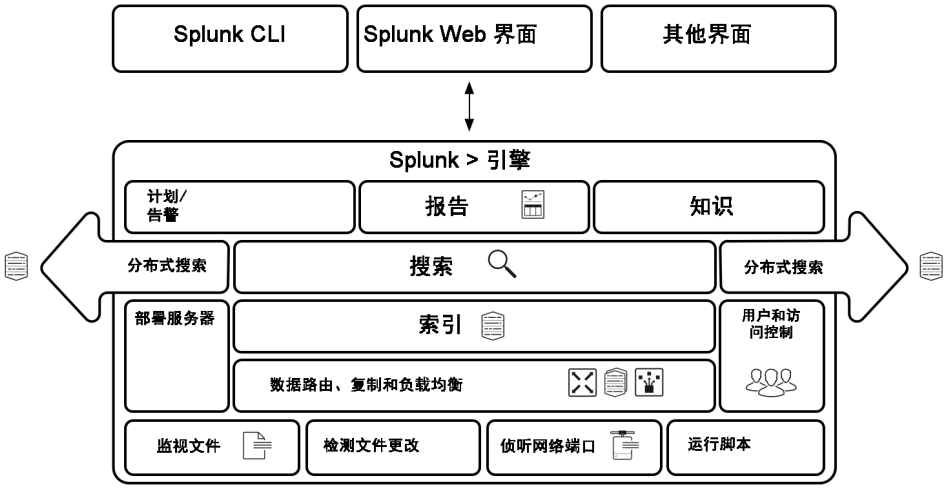
splunk-winprintmon

splunk-winprintmon 在配置 Splunk 的打印监视输入时，将会运行。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 Splunk Enterprise 附带的其他 Windows 第三方二进制文件的信息

了解 Splunk Enterprise 和 Splunk 通用转发器软件包附带的第三方 Windows 二进制文件的信息。

有关通用转发器的更多信息，请参阅*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。Splunk Enterprise 产品包括这些二进制文件，除非另行指定。

二进制文件将为 Splunk Enterprise 提供功能，如同其各个描述所述。二进制文件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。

Splunk Enterprise 未附带的二进制文件、应用和脚本未通过 Certified for Windows Server 2008 R2 (CFW2008R2) Windows 徽标合规性测试。

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。

Jsmin.exe

Jsmin.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 libxslt（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' 压缩工具的最小实施工具。

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

使用下面的链接获取在您的操作系统中安装 Splunk Enterprise 的说明：

- Windows
- Windows（来自命令行）
- Linux

要使用 Splunk Enterprise 的容器化实例，请参阅：

- 在 Docker 容器中部署和运行 Splunk Enterprise

使用 Free 或 Trial 许可证时，适用于 macOS 10.14 和 10.15 的 Splunk Enterprise 可用：

- macOS

部分操作系统的 Splunk Enterprise 可用性已移除

这些平台已移除 Splunk Enterprise 支持，但提供了通用转发器包：

- Solaris
- FreeBSD
- AIX

有关此发行版支持的操作系统和版本的列表，请参阅“受支持的操作系统”。

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指纹来验证 Splunk Enterprise 安装文件下载。使用受信任版本的 OpenSSL。

MD5 验证

此过程帮助您比较从 Splunk 网站上下载的安装文件的 MD5 哈希与文件应有的哈希。您用来比较文件的工具可能会根据您运行的操作系统有所不同。您可能需要在验证 MD5 哈希前，下载这些工具。

1. 下载平台的安装软件包和您想要的 Splunk 软件版本。
2. 在“感谢下载”页面，请单击此软件包 MD5 哈希文件的链接。
3. 打开 Shell 提示符或终端窗口。
4. 打印 MD5 哈希文件的内容。

   ```
   cat splunk-x.x.x-xxxxxxxxxxxx-Linux-x86-64.tgz.md5
   MD5 (splunk-x.x.x-xxxxxxxxxxxx-Linux-x86_64.tgz) = c63c869754d420bb62f04f4096877481
   ```
5. 针对安装程序软件包运行 `md5` 工具。

   ```
   md5 splunk-x.x.x-xxxxxxxxxxxx-Linux-x86-64.tgz
   MD5 (splunk-x.x.x-xxxxxxxxxxxx-Linux-x86_64.tgz) = c63c869754d420bb62f04f4096877481
   ```
6. 比较两种命令的输出。
7. 如果哈希匹配，那么您已确认下载的安装软件包和 splunk.com 网站上的一样。

SHA512 验证

要比较从 Splunk 网站上下载的安装文件的 SHA512 哈希与文件应有的哈希：

1. 检查您的操作系统上是否已经安装了 SHA 比较工具。
2. 下载平台的安装软件包和您想要的 Splunk 软件版本。
3. 在“感谢下载”页面中，选择所需的链接并将其复制到安装程序软件包。例如：
   https://download.splunk.com/products/splunk/releases/8.0.0/windows/splunk-8.0.0-1357bef0a7f6-x86-release.msi
4. 将 SHA512 附加到链接中文件扩展名的末尾处。例如：
   https://download.splunk.com/products/splunk/releases/8.0.0/windows/splunk-8.0.0-1357bef0a7f6-x64-release.msi.sha512
5. 将链接粘贴到网页浏览器中以下载 SHA512 哈希文件。
6. 验证 Splunk 安装软件包和哈希文件在同一位置。
7. 针对哈希文件运行 SHA 比较工具。
8. 如果该工具确认哈希值与安装软件包匹配，则表示已确认下载的安装软件包与 splunk.com 托管的软件包相同。

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。签名仅适用于 RPM 软件包。对于所有其他软件包类型，请使用校验和文件。

1. 下载 GnuPG 公共密钥文件。（此链接执行传输层安全（TLS）。）
2. 安装密钥。

   ```
   rpm --import <filename>
   ```
3. 验证软件包签名。

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

示例：

```
$ rpm -K splunk-8.0.0-1357bef0a7f6-linux-2.6-x86_64.rpm

splunk-8.0.0-1357bef0a7f6-linux-2.6-x86_64.rpm: rsa sha1 (md5) pgp md5 OK
```

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

设置用户和使用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“使用外部系统设置用户验证”。

配置好用户后，可在 Splunk Enterprise 中分配确定并控制操作和访问级别的角色。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，该软件使您可以选择 Windows 用户（将以其身份运行）。

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。默认情况下，本地系统用户可以访问本地计算机上的所有数据，但不能访问任何其他内容。本地系统之外的用户可以访问任意您想让他访问的数据。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，则该策略控制所有用户密码的有效性。如果该策略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，并重新配置每台计算机上的 Splunk Enterprise 服务以便使用更改的密码，然后重新启动每台计算机上的 Splunk Enterprise。
- 配置 Splunk Enterprise 使用的帐户，以便密码不会到期。
- 使用受管服务帐户。请参阅本主题后面介绍的“使用受管服务帐户”。

使用受管服务帐户

如果可以满足下列条件，您可以使用受管服务帐户 (MSA) 运行 Splunk Enterprise：

- 在 Active Directory 中运行 Windows Server 2008 R2 或更新版本、或 Windows 8 或更新的版本
- 在 Active Directory 中至少有一个域控制器运行 Windows Server 2008 R2 或更新版本

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 的计算机上的域帐户相同的权限。
- MSA 必须是运行 Splunk Enterprise 计算机的本地管理员。
- 您无法在不同计算机上使用同一帐户，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 的计算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”。

要使用 MSA 安装 Splunk Enterprise，请参阅“以网络或域用户身份准备用于 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，运行实例的计算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“以网络或域用户身份准备用于 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 林中的一些计算机，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。

新建并启用 GPO 后，您的林中的计算机将在下次计划 AD 复制周期（通常为每 1.5 至 2 小时）或下次启动时选取更改。或者，您可以使用希望更新组策略的计算机上的 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，这些权限将覆盖计算机上相同的本地安全策略权限。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 服务运行所需的权限。您想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 命令行工具为环境中的 GPO 应用程序进行故障排除。

以网络或域用户身份为运行 Splunk Enterprise 准备 Windows 网络

以网络或域用户而非“本地系统”用户身份，准备 Windows 网络以运行 Splunk Enterprise。

这可能和您安装软件所用的用户身份不同。无论您以哪种用户身份运行 Splunk Enterprise，您必须用具有安装计算机上本地管理员特权的帐户安装软件。

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)，或您新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。做出这些更改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计算机数量。或者，在 Windows Server 2008 R2 或更高版本上，可以设置受管用户帐户 (MSA)，进一步限制风险。

如果您无法接受和理解此程序随附的安全风险，请不要执行。

配置 Active Directory 以域用户身份运行 Splunk 软件

以下程序为您准备了 Active Directory，以便以域用户身份安装 Splunk Enterprise 或 Splunk 通用转发器。

要使用 PowerShell 配置 Active Directory 以安装 Splunk Enterprise，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。

新建用户

新建运行 Splunk Enterprise 的用户时，请遵循 Microsoft 最佳方法。请参阅 MS TechNet 中的 Microsoft 最佳做法。

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. 选择您希望准备用于 Splunk Enterprise 操作的域。
3. 单击**操作 > 新建 > 用户**
4. 输入新用户的用户名并单击**下一步**。
5. 取消勾选**用户必须在下一次登录时更改密码**。
6. 单击**下一步**。
7. 单击**完成**。
8. （可选）重复此步骤以新建其他用户。
9. （可选）退出 Active Directory 用户和计算机。

新建组

此程序为运行 Splunk Enterprise 的计算机和用户新建组。

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. 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**新建组织单位。
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. 确认**组范围**设置为**本地域**，同时**组类型**设置为**安全**。
7. 单击**确定**新建组。
8. 新建第二个组，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. 确认**组范围**为**本地域**，同时**组类型**为**安全**。

为组分配用户和计算机

此部分程序分配您在之前部分中新建的用户和计算机。

1. 将帐户添加到 **Splunk 帐户**组。
2. 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。
3. （可选）退出 **Active Directory 用户和计算机**。

定义组策略对象 (GPO)

您在此新建的组策略对象将分布在运行 Splunk Enterprise 的所有计算机。此操作分配权限到计算机，使运行 Splunk Enterprise 更简单。

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。
8. 停留在 GPMC 中。在下一部分，您将在 GPMC 中进行其他操作。

添加权限到 GPO

1. 仍然在 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. 在打开的对话框中，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，键入您之前新建的 "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”关闭右侧属性对话框。
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**
4. 停留在组策略管理编辑器中。在下一部分，您将在 GPMC 中进行其他操作。

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。

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. 在出现的**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，键入您之前新建的 "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。
4. 停留在 GPMC 中。在下一部分，您将在 GPMC 中进行其他操作。

限制 GPO 应用程序选择计算机

此程序控制哪个计算机将接收新的 GPO，因此更改用户权限分配，以便他们能够运行 Splunk Enterprise。

1. 在 GPMC 时，如果还未选定，在 GPMC 左窗格选择您新建的 GPO 并添加权限。GPMC 在右窗格中显示有关 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"（或代表您之前新建的已启用 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（代表您之前新建的 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”。
9. 停留在 GPMC 中。在下一部分，您将在 GPMC 中进行其他操作。

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新建的 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…**。

   如果您仅希望 GPO 对您之前新建的 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，选择您新建和编辑的 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“配置 Active Directory 以域用户身份运行 Splunk 软件”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. 新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“修正 Windows 安装期间选择的用户”主题所述。

   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

您可以使用 PowerShell 为 Splunk Enterprise 服务配置 Active Directory 环境。您不想使用基于 GUI 的管理应用程序时，可以使用此选项。

新建 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. 新建新用户：

```
> 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：

- 命令新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>* 是您希望新建的用户名称。
- *<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。

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。

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>* 是您新建将运行 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计算机。
   - 如果使用本地计算机，登录并打开 PowerShell 提示符（如果未执行此操作）。
   - 如果连接到远程计算机，在远程主机上新建一个新的 `PSSession`，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-PSSession -Computername <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. 在本地计算机上新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. 使用备份新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. 为新策略信息文件新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。
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**条目。
   2. 单击**添加用户或组…**
   3. 单击**浏览…**
   4. 以您之前新建的“Splunk 计算机”组的名义输入，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**。
6. 单击**确定**。
7. 单击**确定**。

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，则可提供更多选项（如静默安装）。请参阅“在 Windows 上从命令行安装”，了解命令行安装程序。

在 64 位 Windows 计算机上，不能再安装或运行 Splunk Enterprise 的 32 位 Windows 版本。您也不能在运行不支持的 OS 的计算机上安装 Splunk Enterprise。例如：您无法在运行 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。

注意：要安装 Splunk **通用转发器**而不是安装 Splunk Enterprise，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 Splunk Enterprise 的单独可执行文件，使用不同的安装程序。

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。

考虑将 Splunk 软件安装到路径名称较短的路径下

默认情况下，Splunk MSI 文件将软件安装到系统驱动的 `\Program Files\Splunk`（启动您的 Windows 计算机的驱动）。此目录适用于许多 Splunk 软件，但对于在分布式部署中运行或使用搜索头、索引器群集等高级 Splunk 功能的安装来说，可能存在问题。

Windows API 有 `MAX_PATH` 路径限制，Microsoft 定义为包括驱动器号、冒号、反斜杠、256 个字符的路径和一个空的终止字符的 260 个字符。Windows 无法寻址长于此长度的文件路径，如果 Splunk 软件新建的文件路径长度长于 `MAX_PATH`，之后将无法检索文件。此配置无法更改。

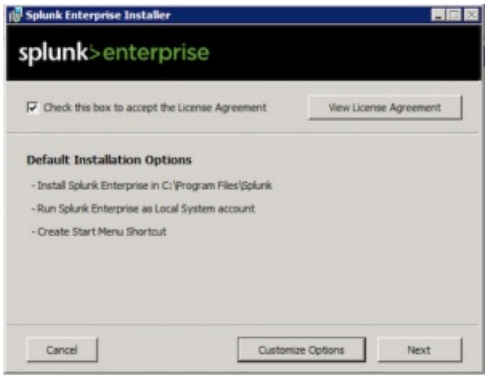
按照如下方法解决此问题，如果您知道实例将成为搜索头或索引器群集的成员，考虑将软件安装到路径较短的目录中，如 `C:\Splunk` 或 `D:\SPL`。

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. 从 Splunk 下载页面下载 Splunk 安装程序。
2. 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。



3. 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“下一个”按钮。
4. （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：

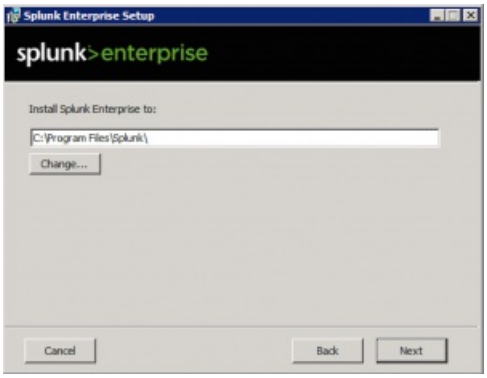
- 在启动您的 Windows 计算机的驱动器上的 \Program Files\Splunk 中安装 Splunk Enterprise。
- 使用默认管理和 Web 网络端口安装 Splunk Enterprise。
- 以“本地系统”用户身份配置 Splunk Enterprise。
- 提醒您新建 Splunk 管理员密码。您必须在安装继续之前进行此步骤。
- 为软件新建“开始菜单”快捷方式。

如果您希望更改任何默认安装设置，点击**自定义选项**并按此主题中的“自定义选项”说明继续操作。

如果无需更改，单击**下一步**。您将收到为 Splunk 管理员用户提供密码的提醒。您提供密码后，安装开始，然后您可以按照本主题中的“完成安装”说明继续。

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。

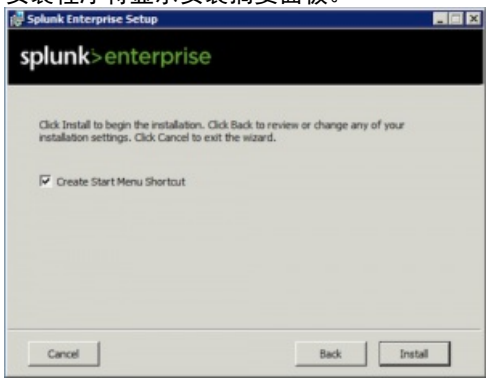
4. 输入 Splunk Enterprise 用于在计算机上的 Windows 凭据，点击**下一步**。

   这些凭据不同于您在下一步中新建的 Splunk 管理员凭据。

5. 通过输入用户名和符合如面板中显示的最小资格要求的密码为 Splunk 管理员用户新建凭据，然后点击**下一步**。

   您必须实施此操作，因为不完成此操作无法继续安装。如果您没有输入用户名，安装程序会在安装过程中新建 admin 用户。

6. 安装程序将显示安装摘要面板。



7. 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合适的用户。

1. （可选）选中**使用 Splunk 启动浏览器**和**新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。

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安装 Splunk Enterprise
- 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 某一版本的系统上安装 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。

在 Windows 上安装 Splunk Enterprise 的前提条件

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

应配置 Windows 网络以支持 Splunk Enterprise 安装。

在安装之前，请参阅“以网络或域用户身份为 Splunk Enterprise 安装准备 Windows 网络”，获得如何配置您的域以运行 Splunk Enterprise 的相关说明。

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。带设备驱动程序（作为 Splunk Enterprise 和操作系统间的媒介）的所有软件均可限制 Splunk Enterprise 的处理能力。这可能导致缓慢，甚至是系统无响应。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

准备好 Splunk 管理员用户凭据

安装 Splunk Enterprise 时，您必须为 Splunk 管理员用户新建用户名和密码。默认情况下安装程序不会为用户新建凭据。实施安装时，想一想用户名和密码组合并准备提供。如果您在静默安装期间并未提供任何密码，Splunk Enterprise 可以在没有定义任何用户（这会阻止登录）时安装。然后您必须新建一个 user-seed.conf 文件以修复问题并重新启动软件。

考虑将 Splunk 软件安装到路径名称较短的路径下

默认情况下，Splunk MSI 文件将软件安装到系统驱动的 \Program Files\Splunk（启动您的 Windows 计算机的驱动）。此目录适用于许多 Splunk 软件，但对于在分布式部署中运行或使用加速的数据模型、搜索头、索引器群集等高级 Splunk 功能的安装来说，可能存在问题。

Windows API 有 MAX_PATH 路径限制，Microsoft 定义为包括驱动器号、冒号、反斜杠、256 个字符的路径和一个空的终止字符的 260 个字符。Windows 无法寻址长于此长度的文件路径，如果 Splunk 软件新建的文件路径长度长于 MAX_PATH，之后将无法检索文件。此配置无法更改。

要解决此问题，考虑将软件安装到路径长度较短的目录中，如 C:\Splunk 或 D:\SPL。

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。请参阅“选择 Splunk Enterprise 应以何种 Windows 用户身份运行”，以了解您应该使用何种用户身份安装 Splunk 实例的相关信息。
- 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“通过命令行安装 Windows 通用转发器”。

标记	用途	默认
AGREETOLICENSE=Yes|No	使用本标记以同意 EULA。您必须将此标记设为“是”以实施静默安装。当您单击 MSI 开始安装时，此标记无效。	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 Enterprise 的安装目录被称为 $SPLUNK_HOME 或 %SPLUNK_HOME%。	C:\Program Files\Splunk
SPLUNKD_PORT=<port number>	使用这些标记指定 splunkd 和 splunkweb 要使用的替代端口。 如果指定端口，同时该端口不可用，则 Splunk Enterprise 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 splunkd 和 splunkweb 要使用的替代端口。 如果指定端口，同时该端口不可用，则 Splunk Enterprise 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 WINEVENTLOG_SET_ENABLE=1/0	使用这些标记指定 Splunk Enterprise 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 设置日志	0 （关闭）
REGISTRYCHECK_U=1/0 REGISTRYCHECK_BASELINE_U=1/0	使用这些标记指定 Splunk Enterprise 是否应 从中索引事件 捕获 Windows 注册表用户单元 （HKEY_CURRENT_USER）的基准快照。 **注意：**您可以同时设置这两个动作。	0 （关闭）
REGISTRYCHECK_LM=1/0 REGISTRYCHECK_BASELINE_LM=1/0	使用这些标记指定 Splunk Enterprise 是否应 从中索引事件 捕获 Windows 注册表用户单元 （HKEY_LOCAL_MACHINE）的基准快照。 **注意：**您可以同时设置这两个动作。	0 （关闭）
WMICHECK_CPUTIME=1/0 WMICHECK_LOCALDISK=1/0 WMICHECK_FREEDISK=1/0 WMICHECK_MEMORY=1/0	使用这些标记指定 Splunk 应索引哪个基于 WMI 的流行性能指标： CPU 使用情况 本地磁盘使用情况 可用磁盘空间 内存统计数据 **注意：**如果需要本 Splunk Enterprise 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 Enterprise 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“选择 Splunk Enterprise 应以何种 Windows 用户身份运行”。	0 （关闭）

	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”。	
LOGON_USERNAME="<domain\username>" LOGON_PASSWORD="<pass>"	为 Windows 用户使用这些标记提供 Splunk Enterprise 以其身份运行的 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：请勿使用此标记设置 Splunk 管理员密码。 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。有关要使用的凭据的其他信息，请阅读本手册的“选择 Splunk Enterprise 应以其身份运行的 Windows 用户”。	无
SPLUNK_APP="<SplunkApp>"	使用本标记指定为本次 Splunk 安装启用的附带 Splunk Enterprise 应用程序配置。目前，<SplunkApp> 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。 如果在此指定 Splunk 转发器或轻型转发器，则还必须指定 FORWARD_SERVER="<server:port>"。 要安装不带任何应用程序的 Splunk Enterprise，请忽略本标记。 **注意：**完整版本的 Splunk Enterprise 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。	无
FORWARD_SERVER="<server:port>"	仅在您使用 SPLUNK_APP 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	使用此标记指定在安装完成后 Splunk 软件是否应该启动，是否在计算机启动时自动启动。 **注意：**如果使用 SPLUNK_APP 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新建 Splunk 快捷方式。	1 （打开）
SPLUNKUSERNAME=<username>	为 Splunk 管理员用户新建用户名。如果您使用 /quiet 标记指定静默安装，不指定此设置，那么软件会使用 admin 默认的值，但是您必须通过 SPLUNKPASSWORD 或 GENRANDOMPASSWORD 标记指定安装密码以成功添加凭据。	admin
SPLUNKPASSWORD=<password>	为 Splunk 管理员用户新建密码。密码必须符合资格要求。每个操作系统都可以使用唯一的转义符语法。在为密码选择特殊字符时，请先测试转义的密码字符串，然后再将其用于生产安装。如果您指定 /quiet 安装，而且不指定此字段或 SPLUNKUSERNAME 字段，那么软件会在没有管理员用户的情况下安装，而您必须通过编辑 user-seed.conf 配置文件来新建一个管理员用户。	N/A
MINPASSWORDLEN=<positive integer>	使用 SPLUNKPASSWORD 标记设置密码时，您还可以为密码新建和修改设置密码资格要求。MINPASSWORDLEN 标记指定满足这些资格要求的最小密码长度。无法设置为 0 或负整数。您新建的任何密码和您更改的任何现有密码在您设置此标记后必须符合新的要求。	> 1
MINPASSWORDDIGITLEN=<integer>	使用 SPLUNKPASSWORD 标记设置密码时，您还可以为密码新建和修改设置密码资格要求。MINPASSWORDDIGITLEN 标记指定要符合这些资格要求，密码必须包含的数字字符（0 到 9）的最小数量。无法设置为负整数。您新建的任何密码和您更改的任何现有密码在您设置此标记后必须符合新的要求。	0
MINPASSWORDLOWERCASELEN=<integer>	使用 SPLUNKPASSWORD 标记设置密码时，您还可以为密码新建和修改设置密码资格要求。MINPASSWORDLOWERCASELEN 标记指定要符合这些资格要求，密码必须包含的小写字母字符（'a' 到 'z'）的最小数量。无法设置为负整数。您新建的任何密码和您更改的任何现有密码在您设置此标记后必须符合新的要求。	0
MINPASSWORDUPPERCASELEN=<integer>	使用 SPLUNKPASSWORD 标记设置密码时，您还可以为密码新建和修改设置密码资格要求。MINPASSWORDUPPERCASELEN 标记指定要符合这些资格要求，密码必须包含的大写字母字符（'A' 到 'Z'）的最小数量。无法设置为	0

	负整数。您新建的任何密码和您更改的任何现有密码在您设置此标记后必须符合新的要求。	
MINPASSWORDSPECIALCHARLEN=<integer>	使用 SPLUNKPASSWORD 标记设置密码时，您还可以为密码新建和修改设置密码资格要求。MINPASSWORDSPECIALCHARLEN 标记指定要符合这些资格要求，密码必须包含的特殊字符的最小数量。无法设置为负整数。':'（冒号）字符无法用作特殊字符。您新建的任何密码和您更改的任何现有密码在您设置此标记后必须符合新的要求。	0
GENRANDOMPASSWORD=1/0	为 admin 用户生成随机密码并将密码写入到安装日志文件。安装程序会将凭据写入 %TEMP%\splunk.log。在安装完成后，您可以使用 findstr 实用工具在该文件中搜索单词 "PASSWORD"。获得凭据后，删除安装日志文件，因为保留文件会构成重大的安全风险。	0

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。

静默安装 Splunk Enterprise 以作为本地系统用户运行并将 Splunk 管理员凭据设置为 "SplunkAdmin/MyNewPassword"

```
msiexec.exe /I Splunk.msi SPLUNKUSERNAME=SplunkAdmin SPLUNKPASSWORD=MyNewPassword /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" SPLUNKPASSWORD=MyNewPassword FORWARD_SERVER="<server:port>"
LOGON_USERNAME="AD\splunk" LOGON_PASSWORD="splunk123"
```

启用 Splunk 重型转发器，为默认的 Splunk 管理员用户生成一个随机密码，启用 Windows 系统事件日志的索引并在静默模式下运行安装程序

```
msiexec.exe /i Splunk.msi SPLUNK_APP="SplunkForwarder" GENRANDOMPASSWORD=1 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。

使用 C:\TEMP\SplunkInstall.log 的详细记录安装 Splunk Enterprise

```
msiexec.exe /I Splunk.msi /l*v C:\TEMP\SplunkInstall.log
```

请参阅 Windows 开发中心的命令行选项以了解 msiexec.exe 的附加记录和命令行选项。

后续步骤

当前您已安装 Splunk Enterprise，**了解接下来会发生什么。**

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。

您更改所选的用户必须是具有您安装软件的本地计算机上的管理权限的用户。请参阅“选择 Splunk Enterprise 应以其身份运行的 Windows 用户”查看有关为 Splunk Enterprise 操作选择正确的 Windows 用户的更多信息。

在下列几种方案中，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
- 如果您需要以受管系统帐户 (MSA) 身份安装 Splunk Enterprise 实例
- 如果通过 ZIP 文件安装软件，并希望将 Splunk Enterprise 服务的默认系统用户更改为 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. 运行服务工具。在**开始**菜单中，单击**控制面板 > 管理工具 > 服务**。
2. 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。
3. 右键单击某个服务，并选择**属性**。
4. 单击**登录**选项卡。
5. 单击**此帐户**按钮。
6. 填写正确的 domain\user 名称和密码。
7. 单击**应用**。
8. 单击**确定**。
9. （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。
10. 从服务管理器或命令行界面启动 Splunk Enterprise 服务。

在 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，有不同的安装包和独立的安装程序。

升级 Splunk Enterprise

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

Tar 文件安装

使用 tar 文件安装之前需要了解什么

了解以下项目有助于确保使用 tar 文件成功安装：

- 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 不会新建 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新建用户。
- 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。

安装过程

1. 用 tar 命令将 tar 文件解压缩到相应的目录：

   ```
   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。

使用rpm 更新时，该软件包装不提供任何保护。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。

安装后，软件包验证命令（如 rpm -Vp <rpm_file> 可能因为中间文件在安装过程中被删除而失败。要验证您的 Splunk 安装包，请改用 splunk validate files CLI 命令。

1. 确保您想要的 RPM 软件包可在目标主机本地使用。
2. 验证将运行 Splunk 服务的 Splunk Enterprise 用户帐户是否可以读取和访问文件。
3. 如果需要，可更改文件权限。
   ```
   chmod 644 splunk_package_name.rpm
   ```
4. 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
   ```
5. （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
   ```

使用 RPM 软件包替换现有的 Splunk Enterprise 安装

- 使用 --prefix 标记运行 rpm 并引用现有的 Splunk Enterprise 目录。

  ```
  rpm -i --replacepkgs --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
```

`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，而不能是符号链接。
- 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。
- 软件包不会新建环境变量来访问 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。

安装过程

- 运行将 Splunk Enterprise Debian 软件包名称用作参数的 `dpkg` 安装程序。

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

显示安装状态的 Debian 命令

Splunk 软件包状态：

```
dpkg --status splunk
```

列出所有软件包：

```
dpkg --list
```

预期默认 Shell 的信息和 Debian Shell 的注意事项

Splunk Enterprise 希望您从 `bash` Shell 运行命令。预期 `bash` 从 `/bin/sh` 获得。

Debian Linux 的更新版本（比如 Debian Squeeze）中，默认 Shell 为 `dash` Shell。

使用 `dash` Shell 可能导致僵尸进程 - 已执行完但是仍然留在进程表中无法终止或移除的进程。

如果运行 Debian Linux，考虑更改您的默认 Shell 为 `bash`。

后续步骤

安装 Splunk Enterprise 后，

- 将其启动，并新建管理员凭证。请参阅“首次启动 Splunk Enterprise”。
- 配置转发器在开机时启动。请参阅“配置 Splunk 软件在开机时启动”。
- 了解后续内容。请参阅“接下来呢？”

卸载 Splunk Enterprise

有关如何卸载 Splunk Enterprise 的信息，请参阅“卸载 Splunk Enterprise”。

在 MacOS 上安装

您可以使用 DMG 软件包或 .tgz 文件在 macOS 10.15 和 10.14 上安装 Splunk Enterprise。

macOS 11 不支持 Splunk Enterprise。提供转发器安装软件包。

安装选项

macOS 安装包有两种格式：DMG 软件包和 .tgz 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 .tgz 文件。DMG 只能将 Splunk Enterprise 安装到 /Applications/Splunk 路径中。

图形安装

1. 导航到安装程序所在的文件夹或目录。
2. 双击 DMG 文件。
   将打开包含 splunk.pkg 的 Finder 窗口。
3. 双击 Install Splunk 图标以启动安装程序。
4. **简介**面板将列出版本和版权信息。单击**继续**。
5. **许可证**面板列表显示软件许可协议。单击**继续**。
6. 您需要同意软件许可协议的条款。单击**同意**。
7. 在**安装类型**面板中，单击**安装**。这将在默认目录 /Applications/Splunk 中安装 Splunk Enterprise。
8. 系统将提醒您键入用于登录到计算机的密码。
9. 当安装完成时，弹出的信息会通知您必须实施初始化。单击**确定**。
10. 终端窗口显示，提醒您指定用户 ID 和密码以使用 Splunk Enterprise。

    密码长度必须至少为 8 个字符。键入时光标不会移动。
    记下用户 ID 和密码。您将使用这些凭据登录 Splunk Enterprise。

11. 弹出一个询问您想要做什么的窗口。单击**启动并显示 Splunk**。Splunk Enterprise 的登录页面在您的浏览器窗口中打开。
12. 关闭**安装 Splunk** 窗口。

    安装程序在桌面上生成一个快捷方式，以便您可以随时从桌面启动 Splunk Enterprise。

tar 文件安装

使用 .tgz 文件执行 Splunk Enterprise 的手动安装。使用 .tgz 文件安装 Splunk Enterprise 时：

- 未创建服务帐户。如果想以特定用户身份运行 Splunk Enterprise 服务，则必须在启动服务之前先创建该用户。
- 解压缩 .tgz 文件时，默认安装目录是当前的工作目录。tar 解压缩会将所有文件放在 <working_directory>/Splunk 文件夹中。

要在 macOS 上安装 Splunk Enterprise，请执行以下操作：

1. 将 <splunk_package_name.tgz> 文件放入一个文件夹中。
2. 在终端上，使用 tar 命令将 tar 文件解压缩到本地目录：

   ```
   tar xvzf splunk_package_name.tgz
   ```
3. 将目录更改为 Splunk/bin，然后启动服务。

后续步骤

安装 Splunk Enterprise 后，

- 要启动 Splunk Enterprise 服务，请参阅“第一次启动 Splunk Enterprise”。
- 要将 Splunk Enterprise 服务配置为在开机时启动，请参阅**《管理员手册》**中的“配置 Splunk 软件在开机时启动”。
- 有关相关操作的更多指导，请参阅“接下来呢？”。

您是否正在寻找通用转发器安装软件包？

通用转发器是单独的安装软件包，有自己的安装流程。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”。

升级？

如果要升级 Splunk Enterprise 实例，请参阅“如何升级 Splunk Enterprise”。

卸载 Splunk Enterprise

如果想移除 Splunk Enterprise，请参阅“卸载 Splunk Enterprise”。

以其他或非 root 用户身份运行 Splunk Enterprise

在基于 *nix 的系统中，您可以用户身份而非根身份运行 Splunk Enterprise。这是 Splunk 最佳做法，您应该尽可能配置系统作为非根用户运行软件。

如果您以非根用户身份运行 Splunk 软件，请确认软件可以执行以下功能：

- 读取您配置它去监视的文件和目录。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。请参阅*告警手册*中的“为告警操作配置脚本”或*数据导入*中的“通过脚本式输入获取 API 中的数据和其他远程数据界面”。
- 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。

由于小于 1024 的网络端口仅预留用于 root 访问，因此如果以 root 用户身份运行，Splunk 软件仅能侦听端口 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）以将 syslog 数据写入到文件，并让 Splunk 监视该文件。

设置 Splunk 软件以非根用户身份运行

1. 如果您有根访问权限，以根用户身份安装 Splunk 软件。否则，将软件安装到特定目录，即您希望 Splunk 软件以其身份运行的用户对其有写入权限的目录中。
2. 将 $SPLUNK_HOME 目录的所有权更改为希望 Splunk 软件以其身份运行的用户。
3. 开启 Splunk 软件。

这是以非根用户安装 Splunk 软件的示例说明

在此示例中，$SPLUNK_HOME 代表 Splunk Enterprise 安装目录的路径。

1. 登录到您想要以根身份安装 Splunk 软件的计算机。
2. 新建 splunk 用户和组。
   在 Linux 上：
   ```
   useradd splunk
   groupadd splunk
   ```
   在 Mac OS X 上：您可以使用**系统首选项 > 帐户**系统首选项面板添加用户和组。
3. 如平台安装说明所述安装 Splunk 软件。请参阅“安装说明”。

   不要启动 Splunk Enterprise。
4. 运行 chown 命令以将 splunk 目录及其下内容的所有权更改为您希望以其身份运行软件的用户所有。

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

   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，请参阅系统中 man 主页。
5. 成为非根用户。

   ```
   su - <user>
   ```

   您还可以登出根帐户并以该用户身份登录。
6. 开启 Splunk 软件。

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

以其他用户身份使用 sudo 开启或停用 Splunk 软件

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

此样本命令假定：

- Splunk Enterprise 已安装于默认安装目录中。如果在其他位置安装 Splunk Enterprise，则相应更新命令中的路径。
- 您的系统中有可用的 sudo 命令。如果不是这样，请使用 su 或获取并安装 sudo。
- 您已新建要运行 Splunk 软件的用户。
- splunk 用户有 /dev/urandom 设备的访问权限以生成产品证书。

进一步阅读

- 要以非根用户对 Splunk 软件进行开机运行配置，请参见*管理员手册*中的“以非根用户身份启用开机启动”。
- 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“选择 Splunk Enterprise 应以何种用户身份运行 Splunk Enterprise”。
- 要了解如何更改 Splunk Enterprise 服务使用的 Windows 用户，请参阅“更改 Windows 安装期间选择的用户”。

在虚拟和容器化环境中安装 Splunk Enterprise

在 Docker 容器中部署和运行 Splunk Enterprise

在 Docker 容器中运行 Splunk Enterprise 以快速部署 Splunk 软件并获得实践经验。官方存储库包含构建 Splunk Enterprise 和通用转发器映像的 Dockerfiles。该存储库可以在 Splunk-Docker 的 GitHub 上找到。

此映像当前不支持 Splunk Enterprise Security (ES) 和 Splunk IT Service Intelligence (ITSI) 的安装。有关在容器中将这些应用程序与 Splunk Enterprise 一起使用的更多信息，请联系 Splunk 服务人员。

Splunk Enterprise 的容器编排

对于容器编排，GitHub 上的 Splunk Operator for Kubernetes 使您能够快速轻松地在您选择的私有或公共云提供商上部署 Splunk Enterprise。操作员通过在实施 Kubernetes 最佳实践的同时自动化工作流程，简化了 Splunk Enterprise 的扩展和管理。

容器化 Splunk 软件的前提条件

Splunk-Docker GitHub 上的“支持指南”中提供了 Docker 和 Splunk 软件的要求列表。要求包括操作系统架构、Docker 版本和支持的 Splunk 架构。

部署 Splunk Enterprise Docker 容器

您可以通过在 Docker 中下载并启动所需的 Splunk Enterprise 图像，在 Docker 容器中部署 Splunk Enterprise。此图像是一个可执行的软件包，包括您运行 Splunk Enterprise 所需的一切。有关通用转发器的说明，请参阅*《转发器手册》*中的“在 Docker 容器中部署和运行通用转发器”。

1. 在 shell 提示符中，运行以下命令将所需的 Splunk Enterprise 图像下载到本地 Docoker 图像库中。

   ```
   docker pull splunk/splunk:latest
   ```
2. 运行下载的 Docker 图像。

   ```
   docker run -d -p 8000:8000 -e SPLUNK_START_ARGS='--accept-license' -e SPLUNK_PASSWORD='<password>' splunk/splunk:latest
   ```
   - `SPLUNK_PASSWORD='<password>'` 参数设置管理员用户的登录密码。设置密码时有最低要求，这些要求会随着 Splunk Enterprise 的不同版本而变化。要查看最低密码要求，请参阅*《确保 Splunk 平台安全》*手册中的“在 Authentication.conf 中配置 Splunk 密码策略”。
   - 端口定义 `-p <host_port>:<container_port>` 将容器化应用程序使用的端口映射到本地主机上的端口，从而将其暴露给外部网络。在上面的示例中，SplunkWeb 端口 8000 映射到主机端口 8000。如果主机端口已被另一个服务占用，则可以使用 `-p` 参数将端口重新映射到主机上的另一个可用端口，例如：`-p 9000:8000`. 您可以稍后通过运行以下命令来验证正在使用的端口 `docker port <container_id>`
3. `docker run` 命令的输出是哈希数字和字母，表示新的 Splunk Enterprise 实例的容器 ID。运行以下包含容器 ID 的命令显示容器状态。

   ```
   docker ps -a -f id=<container_id>
   ```

- 要验证容器 ID，请运行 `docker ps` 以查看所有正在运行的容器的容器 ID、状态和端口映射。

- 打开主机上的网页浏览器，并使用以下地址访问容器内的 SplunkWeb：

```
localhost:8000
```
- 使用您运行 Docker 图像时设置的用户名 `admin` 和密码登录到容器内部的 Splunk Enterprise。

管理 Splunk Enterprise Docker 容器

您可以使用以下 Docker 命令管理容器。

- 要查看用于在容器中运行 Splunk Enterprise 的示例命令和环境变量的列表，请运行：

  ```
  docker run -it splunk/splunk help
  ```
- 要查看正在运行的容器的列表，请运行：
  ```
  docker ps
  ```
- 要停止您的 Splunk Enterprise 容器，请运行：

  ```
  docker container stop <container_id>
  ```

- 要重新启动已停止的容器，请运行：

  ```
  docker container start <container_id>
  ```
- 要访问正在运行的 Splunk Enterprise 容器并执行管理任务，如修改配置文件，请运行：

  ```
  docker exec -it <container_id> bash
  ```

要了解有关 Splunk Enterprise 和 Docker 命令的更多信息，请参阅 GitHub 上有关 Splunk-Docker 的文档。

使用 Splunk Enterprise 启动

首次启动 Splunk Enterprise

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和您的数据是安全的。

作为初次启动程序的一部分，Splunk Enterprise 会提示您为管理员用户新建凭据。您可以选择一个用户名或使用默认的 admin。您还可以输入一个密码。要正常启动和操作 Splunk Enterprise，您必须完成这两步。

请参阅*确保 Splunk 安全*手册中的以下主题了解更多信息：

- 强化标准
- 新建安全管理员凭据

如果您第一次使用 --no-prompt CLI 参数启动 Splunk Enterprise，那么软件不会提示您新建管理员凭据。如果您没有新建凭据，之后登录时 Splunk Enterprise 会显示没有用户的消息。您必须在登录之前手动新建凭据并重新启动 Splunk Enterprise。请参阅本主题后面介绍的“手动新建管理员凭据”了解有关新建凭据的说明。

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。

从命令提示符或 PowerShell 窗口，运行以下命令：

```
cd <Splunk Enterprise installation directory>\bin
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

1. 使用 Splunk Enterprise 命令行界面 (CLI)：

   ```
   cd <Splunk Enterprise installation directory>/bin
   ./splunk start
   ```
2. 新建 Splunk Enterprise 管理员用户名。这是您登录 Splunk Enterprise 时使用的用户，而不是您登录计算机或 splunk.com 时使用的用户。您可以按 Enter 键使用默认的用户名 admin。
   ```
   This appears to be your first time running this version of Splunk.

   Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
   Create credentials for the administrator account.
   Characters do not appear on the screen when you type in credentials.

   Please enter an administrator username:
   ```
3. 为您刚刚新建的用户新建密码。您可以使用这些凭据登录 Splunk Enterprise。
   ```
   Password must contain at least:
   * 8 total printable ASCII character(s).
   Please enter a new password:
   ```
4. 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。
5. 您还可以设置 SPLUNK_HOME 环境变量到 Splunk Enterprise 安装目录。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：

   ```
   export SPLUNK_HOME=<Splunk Enterprise installation directory>
   cd $SPLUNK_HOME/bin
   ./splunk start
   ```
6. 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。

在 Mac OS X 上

从 Finder 启动 Splunk Enterprise

1. 双击桌面上的 **Splunk** 图标启动名为 "Splunk's Little Helper" 的 Splunk 帮助应用程序。
2. 单击**确定**，允许 Splunk 初始化并设置 Trial 许可证。

3. （可选）单击**开启并显示 Splunk** 以开启 Splunk Enterprise 并用 Web 浏览器打开 Splunk Web 的页面。
4. （可选）单击**只开启 Splunk** 以启动 Splunk Enterprise，但不在浏览器中打开 Splunk Web。
5. （可选）单击**取消**退出帮助应用程序。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

1. 在 macOS 上，默认 Splunk Enterprise 安装目录为 /Applications/splunk。

   ```
   cd <Splunk Enterprise installation directory>/bin
   ./splunk start
   ```
2. 新建 Splunk Enterprise 管理员用户名。这是您登录 Splunk Enterprise 时使用的用户，而不是您登录计算机或 splunk.com 时使用的用户。您可以按 Enter 键使用默认的用户名 admin。
   ```
   This appears to be your first time running this version of Splunk.

   Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
   Create credentials for the administrator account.
   Characters do not appear on the screen when you type in credentials.

   Please enter an administrator username:
   ```
3. 为您刚刚新建的用户新建密码。您可以使用这些凭据登录 Splunk Enterprise。
   ```
   Password must contain at least:
   * 8 total printable ASCII character(s).
   Please enter a new password:
   ```

其他启动选项

首次启动时自动接受 Splunk 许可证

1. 将 --accept-license 选项添加到 start 命令：
   ```
   $SPLUNK_HOME/bin/splunk start --accept-license
   ```
2. 新建 Splunk Enterprise 管理员用户名。这是您登录 Splunk Enterprise 时使用的用户，而不是您登录计算机或 splunk.com 时使用的用户。您可以按 Enter 键使用默认的用户名 admin。
   ```
   This appears to be your first time running this version of Splunk.

   Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
   Create credentials for the administrator account.
   Characters do not appear on the screen when you type in credentials.

   Please enter an administrator username:
   ```
3. 为您刚刚新建的用户新建密码。您可以使用这些凭据登录 Splunk Enterprise。
   ```
   Password must contain at least:
   * 8 total printable ASCII character(s).
   Please enter a new password:
   ```
4. 将显示启动序列：
   ```
   Splunk>

   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
```

在不作任何提示，或回答任何提示“是”的情况下启动 Splunk Enterprise

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，直到必须问一个问题。然后，它将显示问题和退出原因并退出。在这种情境下，不会提示您输入管理员凭据。您必须在登录之前手动新建凭据并重新启动。请参阅本主题后面介绍的“手动新建管理员凭据”了解程序。
- 如果运行 `SPLUNK_HOME/bin/splunk start --answer-yes`，Splunk Enterprise 将继续启动并对在启动期间遇到的所有是/否问题自动回答“是”。显示每个问题并回答后继续。

如果您在一行中使用所有三个选项运行启动 Splunk Enterprise，将出现以下情况：

- 软件会自动接受许可证，不会要求您接受。
- 软件将对所有“是/否”问题回答“是”。
- 如果软件遇到无法用“是”或者“否”来回答的问题，软件会退出。

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”。

手动新建管理员凭证

如果您首次启动 Splunk Enterprise 并使用 `--no-prompt` CLI 参数，Splunk Enterprise 会在没有管理员用户的情况下开始运行，这样将导致无法登录。要解决该问题，您必须新建凭证，然后重新启动 Splunk Enterprise。

1. 停止 Splunk Enterprise：
   ```
   ./splunk stop
   ```
2. 使用文本编辑器新建 `$SPLUNK_HOME/etc/system/local/user-seed.conf`，在您安装软件的地方替换 `$SPLUNK_HOME`。
3. 在文件中添加以下行，用 `your new password` 替换密码：
   ```
   [user_info]
   USERNAME = admin
   PASSWORD = <your new password>
   ```
4. 保存文件并将其关闭。
5. 根据先前在本主题中阐述的说明重新启动 Splunk Enterprise。

有关管理员凭证新建（包括自动安装的密码管理）的更多信息，请参阅*保证 Splunk Enterprise 安全性*中的“新建安全的管理员密码”。

非首次启动的 Splunk Enterprise 故障排除

如果您遇到 Splunk Enterprise 不启动的情形，尤其是升级之后，请确认您没有将任何非法参数作为启动进程的一部分传递到 Splunk CLI。如果您传递了非法参数，在没有参数的情况下重新运行 `splunk start` 命令。

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。

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。请参阅*《数据导入》*中的“Splunk 软件可以监视的内容”。
- 了解如何添加 Splunk 用户和角色。请参阅*《确保 Splunk Enterprise 安全》*中的“关于用户和角色”。
- 了解如何预估数据的存储要求。请参阅*《容量规划》*中的“预估存储要求”。
- 了解如何计划您的 Splunk Enterprise 部署，从每天数 GB 到数 TB。请参阅《容量规划手册》。
- 了解如何搜索、监视、报告等等。请参阅搜索教程。
- 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**。请参阅“Splunk 知识是什么？”。

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。此处理称之为**建立索引**。有关建立索引过程的信息，请参阅*数据导入*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，请参阅以下内容：

- *《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，您将获得有效期为 60 天的 Enterprise Trial 许可证。要在试用后继续使用产品的所有功能，您需要安装 Splunk Enterprise 许可证，或更改为 Free 许可证。请参阅*《管理员手册》*中的“从 Enterprise Trial 许可证切换到 Free”。

添加新许可证

1. 登录 Splunk Web。
2. 导航到**设置 > 许可证**。
3. 单击**添加许可证**。
4. 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。
5. 单击**安装**。Splunk Enterprise 安装您的许可证。
6. 如果这是您安装的第一份 Enterprise 许可证，系统会提示您重新启动 Splunk Enterprise 服务。

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

使用命令行来管理许可证

有关使用命令行管理 Splunk Enterprise 许可授权的示例，请参阅*《管理员手册》*中的“使用 CLI 管理许可证”。

了解有关许可授权的更多信息

您可以通过以下方式了解有关许可授权的信息：

- 有关 Splunk 许可授权的简介，请参阅*《管理员手册》*中的“Splunk 许可授权如何工作”。
- 有关在 Splunk Enterprise 实例之间分配许可量的信息，请参阅*《管理员手册》*中的“分配许可量”。
- 要比较许可证类型并了解哪些许可证可以合并，请参阅*《管理员手册》*中的“Splunk 软件许可证类型”。
- 要了解许可证警告和违规，请参阅*《管理员手册》*中的“关于许可证违规”。

升级或迁移 Splunk Enterprise

如何升级 Splunk Enterprise

升级单个 Splunk Enterprise 实例的过程非常简单。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。

升级分布式或群集 Splunk Enterprise 部署的过程会因部署类型以及实例是否托管了各种 Splunk 应用程序和加载项等因素而有所差异。

如果要升级的 Splunk Enterprise 实例或部署安装了一个或多个高级 Splunk 应用程序（如 Splunk IT 服务情报、Enterprise Security 或用户行为分析），则需要规划升级顺序和目标版本级别，以保持版本与高级应用程序的兼容性。Splunk 产品版本兼容性矩阵说明了 Splunk Enterprise 的哪些特定版本兼容和支持高级 Splunk 应用程序。

无论是哪一种部署类型，您都必须使用具有足够权限的操作系统帐户升级 Splunk Enterprise，以满足以下要求：

- 该帐户在执行升级的计算机上具有管理权限
- 该帐户可以写入实例目录及其所有子目录。

本主题提供有关从早期版本升级到 8.2 版本的具体信息。如果您不想升级到 8.2 版本，请在**版本**下拉列表中选择所需的发行版本。

务必使用适用于目标升级版本的升级说明。适用于较低或较高版本的升级说明所提供的信息可能会与目标版本中的信息相冲突。

版本 8.2 的升级信息

请继续阅读，了解升级 Splunk Enterprise 部署所需的信息，包括可用的升级路径，升级时可能会影响您的信息，以及指向功能和发行说明等信息的链接。

升级到版本 8.2 的路径

下表介绍了从 Splunk Enterprise 的早期版本升级的可用升级路径。

先在第一列中找到您当前运行的版本，然后阅读相关内容并确定该版本的升级路径。如果第一列中没有列出您所使用的版本，则表示该版本没有升级到最新版本的可用升级路径。此时，您需要先将版本升级到此列表中列出的某个版本。

您当前的版本	先升级到	再升级到	README 链接	Rel. 注释链接
6.6.x	7.2.x	请参阅此表中的 7.2.x 条目	7.2 README	7.2 Rel. 注释
7.0.x	8.0.X 或 8.1.x	8.2.x	8.0 README、 8.1 README	8.0 发行说明 8.1 Rel. 注释
7.1.x	8.0.X 或 8.1.x	8.2.x	8.0 README、 8.1 README	8.0 发行说明 8.1 Rel. 注释
7.2.x	8.0.X 或 8.1.x	8.2.x	8.0 README、 8.1 README	8.0 发行说明 8.1 Rel. 注释
7.3.x	8.0.X 或 8.1.x	8.2.x	8.0 README、 8.1 README	8.0 发行说明 8.1 Rel. 注释
8.0.x	8.2.x	N/A	8.2 README	8.2 发行注释
8.1.x	8.2.x	N/A	8.2 README	8.2 发行注释

Splunk Enterprise 升级过程

Splunk Enterprise 的升级过程包括三个阶段：

- 阶段 1：识别、备份和验证组件是否按预期正常工作
- 阶段 2：安装更新后的 Splunk Enterprise 组件
- 阶段 3：确认升级后一切正常

此过程适用于所有 Splunk Enterprise 部署的升级。根据您所采用的部署的类型，有些步骤可能与此页面显示的有所不同。

阶段 1：识别、备份和验证组件是否按预期正常工作

使用以下步骤为 Splunk Enterprise 升级做好准备。因为部署的大小和类型以及您的部署是否运行了高级 Splunk 应用程序等因素，具体步骤可能会有所不同。

1. 识别部署中的所有组件。这决定了您在升级阶段必须遵循的升级过程：
    - 识别所有单实例组件。
    - 识别不在群集中的所有分布式组件。
    - 识别所有群集组件。
2. 备份现有部署，包括配置和数据。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*《管理索引器和索引器群集》*手册中的“备份索引数据”。
3. 验证您的备份并确认这些备份可以还原。
4. 在适用的情况下，使用监视控制台对现有 Splunk Enterprise 部署的运行状况拍摄快照。
5. 如果您运行的是群集 Splunk Enterprise 环境，请使用监视控制台确认群集的运行状况良好。
6. 如果您运行的是 Splunk Enterprise 许可证主服务器，请确认服务器的运行状况良好，所有索引器都成功连接到服务器，并且所有许可证密钥都可用于输入或已经存在于备份介质上。
7. 如果您在搜索头群集上运行 Deployer，请确认它的运行状况良好，并且可以将配置软件包毫无问题地推送到所有 SHC 对等节点。
8. 如果您运行的是部署服务器计算机，请确认它的运行状况良好，配置已成功地重新加载，并且所有转发器都可以连接到该计算机。
9. 在*《通用转发器》*手册的“转发器与索引器兼容性”章节中查看转发器-索引器之间的兼容性矩阵，以确认部署中的所有转发器都兼容您计划升级到的索引器版本。由于各种安全密码的更改，旧版本的转发器可能不兼容。
10. 对于任何类型的分布式部署，请确认索引层中的所有计算机都满足以下条件：
    - 有足够的磁盘空间可用于安装更新软件
    - 可以毫无问题地运行基本搜索
    - 没有运行自己保存的搜索
11. 对于任何类型的分布式部署，请确认搜索层中的所有计算机都满足以下条件：
    - 要升级的 Splunk Enterprise 版本可以运行您的应用程序、加载项和仪表板
    - 您拥有所有安全密钥、配置和凭据，可以随时重新输入
    - 验证凭据不正确不会导致搜索失败

阶段 2：安装更新后的 Splunk Enterprise 组件

完成阶段 1 中的升级前步骤后，您可以开始升级各个 Splunk Enterprise 组件。根据您的部署类型，您可能需要执行额外步骤。

1. 在开始升级之前，请详细阅读“关于升级到 8.2：首先阅读”。
2. 如果您运行了高级 Splunk 应用程序，请参阅 Splunk 产品版本兼容性矩阵，以确定您的应用程序支持的版本。
3. 根据您在阶段 1 中确定的部署架构，升级部署中的 Splunk Enterprise 组件：
    - 对于没有群集的分布式环境，请按照“如何升级分布式 Splunk Enterprise 环境”中的说明操作。
    - 对于群集环境，请参阅以下主题之一：
        - 要升级索引器群集，请参阅*《管理索引器和索引器群集》*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”。
    - 对于单实例部署，请按照适用于您的操作系统类型的升级说明进行操作：
        - 在 *nix 上升级到 8.2
        - 在 Windows 上升级到 8.2
4. 在升级期间，您可能需要执行验证步骤以确保升级成功，具体取决于您升级的组件。
    - 在群集主节点上，您可能需要运行验证搜索或使用操作系统工具来确定群集主节点的运行状况和准备情况，然后才能进入下一个升级阶段。
    - 在转发器上，您可以使用监视控制台来确定，在转发器重新联机后，数据提取级别是否保持在升级前的速率。
    - 在独立索引器上，您可以运行搜索来确定数据提取和搜索参与都很正常。
    - 在群集索引器上，您可以使用监视控制台来确定索引器已重新联机并且在“群集状态”页面中显示为正常。

阶段 3：验证升级后一切正常

完成 Splunk Enterprise 组件的升级后，请按照以下高级步骤确认升级已经成功。与其他阶段一样，具体步骤可能会因您在部署中使用的 Splunk Enterprise 组件的数量和种类的不同而有所不同。

1. 确认您的 Splunk 应用程序和加载项的工作方式与升级前相同。
2. 如果您使用的是分布式部署，请使用监视控制台验证所有 Splunk Enterprise 组件。
    - 查看所有组件的资源利用率，并与升级前的基准值进行比较。
    - 确认所有组件均可用。
3. 如果您使用的是分布式部署，请确认许可证主服务器工作正常，并且所有索引器都已连接到服务器，就像升级之前一样。
4. 如果您使用的是群集部署，请确认群集主服务器正常运行，并且群集对等节点正确连接。
5. 如果您使用的是分布式部署，请确认搜索层正常运行，并且搜索和索引器的通信没有问题
6. 如果您使用的搜索头群集，请使用监视控制台验证搜索头群集的状态和各个群集对等节点。
7. 如果您使用的索引器群集，请确认所有索引器群集节点都重新与群集主服务器建立了通信。

可选的升级活动

下面的部分介绍了升级后可以执行的可选步骤。

查看并配置 tsidxWritingLevel

Splunk Enterprise 7.2 引入了一种新的文件格式，并针对 tsidx 文件进行了优化，从而通过减少 I/O、降低存储使用量以及提高 SmartStore 缓存使用率提高了搜索性能。这些优化封装在各个级别中，更高版本的 Splunk Enterprise 中添加了新的级别。更改默认的 tsidxWritingLevel 会更改索引 tsidx 文件和数据模型加速所使用的优化。

要确定自上次升级以来可用的 tsidx 级别是否已更改，以及要将 tsidxWritingLevel 设置为什么值，请参阅*《管理索引器和索引器群集》*手册中的“tsidx 写入级别”。

替换丢失的安装包清单文件

Splunk Enterprise 安装包中含有 Splunk Enterprise 需要运行的清单文件。清单文件在 Splunk Enterprise 安装的根中，以 -manifest 结尾。如果文件不存在，那么 Splunk Enterprise 就无法运行，因为无法验证是否为有效安装。

如果在升级过程中，或出于任何原因删除这些文件，您可以根据以下步骤恢复它们：

1. 下载与您之前下载的版本相同的 Splunk Enterprise 安装程序副本。此副本的版本和架构必须相同，因为每个版本的清单文件不同。
2. 将文件提取到不是现有 Splunk Enterprise 安装的目录。
3. 将此目录文件复制到 Splunk Enterprise 安装的根目录。
4. 启动 Splunk Enterprise 并确认启动正常。

关于升级到 8.2 首先阅读此主题

以下列出了在升级到 8.2 版本时，需要注意的 Splunk Enterprise 和 Splunk 通用转发器在行为上的一些改变。

首先选择要将 Splunk Enterprise 升级到的版本，然后查看此页面。本主题较低或较高版本的内容所提供的信息可能会与目标版本中的信息相冲突。

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 8.2 版兼容。

- 若想了解哪些版本的 Splunk IT Service Intelligence 和 Splunk Enterprise Security 与该版本的 Splunk Enterprise 兼容，请参阅“Splunk 产品版本兼容性矩阵”。
- 您可以访问 Splunkbase 以确认您的应用程序和加载项是否与此版本兼容。

如果您的应用程序或加载项与 8.2 版本不兼容，请考虑延迟升级，直到有兼容的版本可用。

升级到 8.2 版本的要点

以下列出了升级 Splunk Enterprise 及其组件之前必须考虑的重要因素。以下章节提供了支撑这些要点的具体细节。在开始升级活动之前，请仔细阅读本主题中的所有章节。

- 将您的 KV 存储存储引擎从内存映射 (MMAP) 存储引擎迁移到 WiredTiger 存储引擎，以显著减少所需的存储量并提高性能。要规划迁移，请参阅*《管理员手册》*中的“迁移 KV 存储的存储引擎”。
- Splunk® Enterprise 8.0 和更高版本中的 Splunk 数据收集做法已更改。为更好地为您提供支持，Splunk 现在自动选择退出您在升级后共享遥测数据。您仍然可以选择退出，请参阅本主题稍后介绍的“Splunk 数据收集做法已更改”了解如何退出。
- 升级之前，调整脚本和模板以使用 Python 3 兼容的语法。请参阅“选择适合 Python 3 迁移的 Splunk Enterprise 升级路径”了解更多信息。
- 使用 Splunk 产品版本兼容性矩阵来确保您运行的所有高级 Splunk 应用程序和加载项都与 8.2 版本兼容。如果不兼容，则在有兼容的版本可用之前不要升级。
- 仅支持从 Splunk Enterprise 或通用转发器版本 8.0.x 和 8.1.x 直接升级到版本 8.2。任何版本 7.x.x 上的 Splunk Enterprise 或通用转发器必须先升级到版本 8.0 或 8.1，然后再升级到 8.2.0。
- 要升级搜索头或索引器群集，请参阅本主题稍后介绍的“按特定说明升级群集”。
- 在开始升级之前先备份应用键值存储（KV 存储）数据库。如果运行的 Splunk Enterprise 版本为 7.1 或更低，则必须先停止 Splunk Enterprise 实例。
- 如果您运行的是使用第二次扩展 (ext2) 文件系统的 Linux 计算机，请在开始升级之前将该文件系统升级到第三次扩展 (ext3)。

可能会破坏 Splunk Enterprise 安装的更改

目前没有方式可以将安装回滚到之前的版本。请遵循适用于这些关键项目的指导，以避免在升级期间破坏现有安装。

计划您的升级以进行 Python 3 迁移

适用组件： Splunk Enterprise
适用操作系统： 全部
引入的版本： 8.0、8.1

从版本 8.1 开始，Splunk Enterprise 默认情况下会全局使用 Python 3 解释器。您可以选择全局恢复为 Python 2，但 Splunk Web 仅支持 Python 3.7。升级之前，依赖于 Splunk Web 的脚本和模板必须经过调整，以便可以使用 Python 3 兼容的语法。不依赖于 Splunk Web 的 Python 脚本既不需要进行调整以使用 Python 3 兼容的语法，也不需要恢复为 Python 2。**Splunk® Enterprise 的未来版本中将删除 Python 2。恢复为 Python 2 只是一个临时解决方法。**请参阅“选择适合 Python 3 迁移的 Splunk Enterprise 升级路径”了解更多信息。

请注意以下重要事项：

- 在版本 8.1 中，直接调用 `splunk cmd python`（和 `$SPLUNK_HOME/bin/python`）始终由 Python 3 解释器完成。即使您配置了 Splunk Enterprise 实例以使默认值为 Python 2，也是如此。
- 如果搜索由使用 Python 3 的 Splunk® Enterprise 执行，而且其结果包含多字节字符，那么在使用 Splunk Enterprise SDK for Python（介于版本 1.6.5 和 1.6.13 之间）实施自定义搜索命令的应用中，这些搜索会失败。有关更多信息和解决方法，请参阅*发行说明*的“已知问题”主题中的问题 SPL-194426。

Splunk Enterprise 和通用转发器必须是 7.x 或更高版本才能升级到 8.2 版本

适用组件： Splunk Enterprise 和 Splunk 通用转发器
适用操作系统： 全部
引入的版本： 7.3

如果想升级到 Splunk Enterprise 和通用转发器 8.2 版本，则目前安装的版本必须为 7.x 版本。如果目前安装的版本为 6.6.x 或更低，则必须先升级到版本 7.2.x，再升级到目标版本。有关更多信息，请参阅“升级到版本 8.2 的路径”。

如果您需要首先升级到 7.2.x，请阅读版本 7.2 的“首先阅读”主题，以了解有关该版本可能发生的重大更改的重要信息。

按照特定说明升级群集

适用组件： Splunk Enterprise
适用操作系统： 全部
引入的版本： 7.3

要升级索引器或搜索头群集，请按照您的部署类型适用的升级过程进行操作。

- 如果您的部署有索引器群集，请按照索引群集升级说明进行操作。
- 如果您的部署有搜索头群集，请按照搜索头群集升级说明进行操作。

在 Splunk Enterprise 索引器群集管理器节点上，在升级前启用维护模式

适用组件： Splunk Enterprise 和 Splunk 通用转发器
适用操作系统： 全部
引入的版本： 8.1

因为随着最新版本的 Metrics Store 的发布而对数据桶数据进行了更改，所以运行低于 8.1 的 Splunk Enterprise 版本的索引器无法处理来自运行 8.1 或更高版本的数据桶复制。在您升级群集管理器节点之前，先确保此节点处于维护模式。这是索引器群集更新过程的标准环节。

请参阅*《管理索引器和索引器群集》*中的“使用维护模式”。

在开始升级之前先备份应用键值存储

适用组件： Splunk Enterprise
适用操作系统： 全部
引入的版本： 7.3

在任何维护操作（如升级）之前，先备份应用键值存储（KV 存储）。

如果要从版本 7.1 或更低的版本升级，则必须先停止 Splunk Enterprise，然后才能备份 KV 存储数据库。确认您已在升级计划中考虑了这部分的停机时间。有关详细信息，请参阅“备份和恢复 KV 存储”。

已移除 Linux 中对第二次扩展（ext2）文件系统的支持

适用组件：Splunk Enterprise 和 Splunk 通用转发器
适用操作系统：Linux
引入的版本：7.1

已移除 Linux 操作系统中对 ext2 文件系统的支持。如果您仍在运行 Splunk Enterprise 的 Linux 计算机上运行 ext2 文件系统，在您升级 Splunk Enterprise 之前，必须至少将该文件系统升级到 ext3。

Splunk Enterprise 凭据新建方案可能影响脚本化升级

适用组件：Splunk Enterprise 和 Splunk 通用转发器
适用操作系统：全部
引入的版本：7.2

Splunk Enterprise 7.1 为用户引入了更新的验证方案，要求您为管理员帐户创建密码。在版本 7.2 中已对方案进行扩展，允许您自定义用于 Splunk Enterprise 实例的管理员凭据新建。

此方案包括其他设置和配置选项，这会影响在使用脚本自动化升级进程时您的升级方式。您可能需要在实施脚本化升级之前更改您的升级脚本。尤其是确认您没有在升级期间为了启动或重启 Splunk Enterprise 而向 Splunk CLI 传递任何非法参数，因为这会导致在升级完成后 Splunk Enterprise 不启动的情况。

搜索头池已删除

适用组件：Splunk Enterprise
适用操作系统：全部
引入的版本：8.0

搜索头池已从 Splunk Enterprise 中删除。此功能被搜索头群集替换，已弃用很多年了。如果您仍然使用搜索头池，那么请勿升级到版本 8.0。尽量考虑尽快切换到搜索头群集。

一些看似是问题但其实不是的情况

在升级期间或升级后，您可能会立即发现一些情况，似乎表明升级无效。在几乎所有情况下，这里会发生的情况都是可以预期的。

如果在升级过程中发生以下情况，请继续升级，不要中断升级。如果这些情况在升级之后立即出现，请对部署执行基准测试，并将测试结果与您在升级的第一阶段中设置的基准进行比较。只有当这些基准值差异很大时，才需考虑联系 Splunk 支持。

- 在索引器上，由于以下原因，内存和 CPU 使用率增加：
  - 新的数据提取管道
- Splunk Enterprise introspection 目录的权限可能会更改。确认运行 Splunk Enterprise 的用户拥有 `$SPLUNK_HOME/var/log/introspection` 目录的写入权限。
- 由于应用程序包的哈希重新计算，部署服务器可能会将更新推送到所有部署客户端。

索引器上的 CPU 和内存使用率增加

适用组件：Splunk Enterprise
适用操作系统：全部
引入的版本：7.3

默认情况下，新数据提取管道在启用后会消耗更多资源。

introspection 目录的权限可能会更改

适用组件：Splunk Enterprise 和 Splunk 通用转发器
适用操作系统：全部
引入的版本：7.3

确认运行 Splunk Enterprise 的用户拥有 `$SPLUNK_HOME/var/log/introspection` 目录的写入权限。

由于应用程序包的哈希重新计算，部署服务器可能会将更新推送到所有部署客户端。

适用组件：Splunk Enterprise 和 Splunk 通用转发器
适用操作系统：全部
引入的版本：7.3

计划视图获取进程可能会增加启动时磁盘 I/O 和 CPU 的使用量

适用组件： Splunk Enterprise
适用操作系统： 全部
引入的版本： 7.1

当升级到 Splunk Enterprise 7.1 或更高版本时，检查并删除孤立计划视图的新进程将会运行，例如按计划生成 PDF 的已保存搜索或报告。这会在 Splunk Enterprise 启动时发生，可能会导致启动时磁盘 I/O 和 CPU 使用量的增加。

更改或删除功能的注意事项

此版本已更改或删除了以下主要功能。如果您使用的功能已删除，而且您尚未迁移这些功能，请考虑延迟升级，直到您完成迁移。

使用 SSL 压缩替换为 HTTP 压缩，转发时除外

适用组件： Splunk Enterprise
适用操作系统： 全部
引入的版本： 8.2

为了提高可扩展性和效率，Splunk Enterprise 实例之间的 SSL 通信默认不再启用使用 SSL 压缩。默认情况下，SSL 压缩替换为 HTTP 压缩，但通过 SSL 转发数据时除外。在与早期 Splunk Enterprise 实例通过 SSL 协商通信时，此更改不会阻止使用 SSL 压缩。例如，与 8.2 实例协商的早期客户端仍将使用 SSL 压缩，而与早期服务器协商的 8.2 客户端将使用 HTTP 压缩。

此更改会影响现有设置：

设置	8.2 的新默认值	之前的默认值
server.conf useHTTPClientCompression	true	false
server.conf useClientSSLCompression	false	true
outputs.conf useClientSSLCompression	true	引用了 server.conf useClientSSLCompression 设置（默认值：true）

如果您过去修改过 useHTTPClientCompression 或 useClientSSLCompression 设置，请检查您的环境以确定升级后新的默认值是否会影响您的压缩设置。使用 btool 验证如何根据上述设置在您的环境中设置压缩，以及进行这些更改的位置。

如果您已明确启用 server.conf 设置useClientSSLCompression如果使用自定义应用或本地 .conf 文件，升级后将同时启用 SSL 和 HTTP 压缩。升级完成后，验证useClientSSLCompression设置，并确保禁用 SSL 压缩。

用于简单 XML 仪表板版本控制的新设置

适用组件： Splunk Enterprise
适用操作系统： 全部
引入的版本： 8.2

包括用于简单 XML 仪表板版本控制的新设置，以支持更新简单 XML 使用的库。不要更改或设置 web.conf 设置 simplexml_dashboard_create_version。唯一支持的值是默认的 simplexml_dashboard_create_version = 1.0。没有定义值的仪表板将默认为 1.0。

索引的默认 tsidxWritingLevel 已更改

适用组件： Splunk Enterprise
适用操作系统： 全部
引入的版本： 8.2

从此版本开始，indexes.conf 中的默认 tsidxWritingLevel 已从 1 更改为 2。

Splunk Enterprise 7.2 引入了一种新的文件格式，并针对 tsidx 文件进行了优化，从而通过减少 I/O、降低存储使用量以及

提高 SmartStore 缓存使用率提高了搜索性能。这些优化封装在各个级别中，更高版本的 Splunk Enterprise 中添加了新的级别。更改默认的 tsidxWritingLevel 会更改索引 tsidx 文件和数据模型加速所使用的优化。请参阅*《管理索引器和索引器群集》*手册中的“tsidx 写入级别”。

splunkd.log 事件现在包括线程名称

适用组件： Splunk Enterprise
适用操作系统： 全部
引入的版本： 8.2

splunkd.log 事件的默认日志记录级别现在包括线程名称以改进故障排除。

为多站点群集执行可搜索的滚动重新启动时，有一个附加选项可用

适用组件： Splunk Enterprise
适用操作系统： 全部
引入的版本： 8.2

当满足先决条件时，新的 server.conf 设置 searchable_rolling_site_down_policy 提高了可搜索滚动重新启动的性能。

请参阅*《管理索引器和索引器群集》*手册中的“管理器节点如何确定每轮中要重新启动的多站点对等节点的数量”。

Splunk Enterprise 或通用转发器安装将不再使用主机名创建 input.conf

适用组件： Splunk Enterprise
适用操作系统： 全部
引入的版本： 8.1

Splunk Enterprise 和通用转发器实例的默认安装行为发生了变化。安装早期版本时，安装过程将确定主机名并将其设置在新创建的 $SPLUNK_HOME/etc/system/local/inputs.conf 文件中。在 8.1 及更高版本中，splunkd 在安装期间不再创建 input.conf 文件。该服务在服务启动时检查并将主机名设置为 inputs.conf 设置 host = $decideOnStartup 的一部分。

验证系统的某些日志记录类别已更改

适用组件： Splunk Enterprise
适用操作系统： 全部
引入的版本： 8.1

为支持安全断言标记语言 (SAML) 验证方案我们所做的其中一个整体改进措施是，更改了 Splunk 平台验证系统的各种日志记录通道。日志记录类别名称以前以 AuthenticationManager 开头，但现在以 AuthenticationProvider 开头。升级后，请查看 $SPLUNK_HOME/etc/ 中的 log.cfg，确认名称已成功更改。

Splunk Enterprise 许可证强制实施更改

适用组件： Splunk Enterprise
适用操作系统： 全部
引入的版本： 8.1

对于每天许可量少于 100GB 的许可证堆栈，如果出现违反许可证限制的情况，而且在 60 天的滚动窗口内发出了 45 次警告，则 Splunk Enterprise 将禁用搜索。有关更多信息，请参阅 splunk.com 上的“许可证强制实施常见问题”。

审计日志的默认日志记录级别已更改

适用组件： Splunk Enterprise 和 Splunk 通用转发器
适用操作系统： 全部
引入的版本： 8.1

某些管理事件（进入 _audit 索引的信息）的审计日志的默认日志记录级别已从 INFO 级别降低到 DEBUG 级别。此外，您现在可以控制审计事件所在的日志记录级别。

尽管由于日志记录的默认详细程度较低，这对大多数客户来说是绝对的好消息，但这也意味着由于日志级别较低，默认情况下不会再记录某些审计事件（例如功能检查）。要恢复旧的行为，您可以配置 Splunk 平台日志记录实用程序，具体方式为：编辑 $SPLUNK_HOME/etc/log-local.cfg 文件，并将 category.AuditLogger 条目从 DEBUG 提升回 INFO。

Splunk 数据收集实践已更改

适用组件： Splunk Enterprise 和 Splunk 通用转发器
适用操作系统： 全部
引入的版本： 8.0

为了更好地为可提供支持并改进产品和服务，Splunk 已更改其数据收集实践。升级后，Splunk 会自动让您退出共享遥测数据。要了解 Splunk 收集哪些数据，请参阅*《管理员手册》*中的“Splunk 收集哪些数据”。

升级后，当您与管理员用户首次登录实例时会发生更改。您会收到指示策略更改的弹出消息，并且在您确认弹出消息之后，实例会覆盖任何现有的数据共享配置。

您仍可以随时选择退出共享遥测数据。要了解如何退出，请参阅*《管理员手册》*中的“在 Splunk Enterprise 中共享数据”主题中的“如何退出”。

“访问控制”Splunk Web 菜单选项已更改

适用组件： Splunk Enterprise
适用操作系统： 全部
引入的版本： 8.0

Splunk Web 中设置菜单下“用户和验证”标题下的“访问控制”菜单项目已替换为指向用户、角色、密码和验证计划管理的单个链接。

工作负荷类别的默认内存资源分配已更改

适用组件： Splunk Enterprise
适用操作系统： Linux
引入的版本： 8.0

升级到版本 8.x 之后，引入工作负荷类别的默认内存资源分配从 20% 更改为 100%。这可能会导致升级后引入类别中内存使用情况的增加。搜索和 misc. 类别的默认内存资源分配保持不变，分别是 70% 和 10%。

关于工作负荷类别的更多信息，请参阅*《工作负荷管理》*手册中的“配置工作负荷类别”。

Splunk Web 错误消息 "failure to localize search" 被替换为 "partial results" 消息

适用组件： Splunk Enterprise
适用操作系统： 全部
引入的版本： 8.0

当您升级到版本 8.x 并运行遇到本地化错误的搜索时，Splunk Web 中显示的消息已更改。Splunk Web 会通知用户搜索进程可能会返回部分结果，而不是显示 "failure to localize" 消息。

具有 "install_apps" 功能的角色还需要 "list_settings" 功能才能访问特定 REST 端点

适用组件： Splunk Enterprise
适用操作系统： 全部
引入的版本： 8.0

在您升级到 Splunk Enterprise 版本 8.x 之后，任何具有 install_apps 功能的角色必须也具有角色用户能够通过 REST（例如，使用 manager/appinstall/<app> 端点）管理应用安装的 list_settings 功能。

8.x 版的 Splunk Enterprise 转发器无法将指标数据转发到运行版本低于 8.x 的索引器上

适用组件： Splunk Enterprise 和 Splunk 通用转发器
适用操作系统： 全部
引入的版本： 8.0

不支持将指标数据从运行版本 8.x 的转发器转发到运行版本 7.3 或更低版本的索引器。如果您需要将转发版本 8.x 转发器中的指标数据，确认接收此类数据的所有索引器也运行版本 8.x。

已升级的搜索头节点会发现低版本的索引器节点中丢失指标索引

适用组件： Splunk Enterprise 和 Splunk 通用转发器
适用操作系统： 全部
引入的版本： 8.0

如果您将分布式搜索环境升级为 Splunk Enterprise 版本 8.x，但是索引器节点还是低于版本 8.0，那么您的搜索节点会生成告警，提示他们尝试将 metrics.log 事件发送到索引器时丢失 _metrics 索引。您无法通过将 _metrics 索引添加到索引器群集来解决这个问题，因为指标数据的格式与运行较低版本的索引器上的数据不同。尽量将所有 Splunk Enterprise 组件升级为最新版本。

升级后，在处理指标数据的所有搜索头群集节点上配置 limits.conf 设置

适用组件： Splunk Enterprise 和 Splunk 通用转发器
适用操作系统： 全部
引入的版本： 8.0

将搜索头和索引器群集升级为 Splunk Enterprise 8.x 之后，编辑各搜索头群集上的 limits.conf 并将 [mcollect] 段落下的 always_use_single_value_output 设置设为 false。这样设置允许这些节点在您使用 mcollect 命令或使用指标汇总将日志转换为指标时，使用“每个指标数据点有多个度量”方案。新的方案可增加您的数据存储容量并提高指标搜索性能。

仅在指标索引中，默认情况下，当数据桶从热滚动到温时，Splunk 软件会删除这些数据桶中的原始数据日志文件

适用组件： Splunk Enterprise 和 Splunk 通用转发器
适用操作系统： 全部
引入的版本： 8.1

指标搜索不使用原始数据日志文件。但是，在 8.0 中引入优化之后，原始数据日志文件会占用大量指标索引数据桶。在版本 8.1 及更高版本中，默认情况下，当指标索引数据桶从热滚动到温时，Splunk 软件会删除指标索引数据桶中的这些文件。该软件会从数据桶的 /rawdata 目录中删除该文件，并用一个虚拟日志文件替代，该虚拟文件除了日志标题外没有其他可用数据。这减少了指标索引所占的磁盘空间量。

这不适用于为索引器群集启用了复制功能（在 limits.conf 中，repFactor = auto）的指标索引。有关更多信息，或要了解如何禁用特定索引的原始数据日志删除，请参阅 limits.conf.spec 中有关 metric.stubOutRawdataJournal 设置的说明。

无法针对指标名称为空白或全部是空格的指标数据点建立索引或进行搜索

适用组件： Splunk Enterprise 和 Splunk 通用转发器
适用操作系统： 全部
引入的版本： 8.1

在版本 8.1 及更高版本中，Splunk Enterprise 无法针对指标名称为空白或全部是空格的指标数据点建立索引。引入的指标数据以及通过日志到指标源类型或其他方法转换为指标数据的事件数据，都可能会发生这种情况。

在升级之后，如果指标数据点是由旧版本的 Splunk 建立索引，而且这些数据点包含空白或全部是空格的指标名称，则 Splunk Enterprise 搜索将无法返回这些指标数据点。

现在，默认情况下，StatsD 指标数据输入会生成单测量值指标数据点

适用组件： Splunk Enterprise 和 Splunk 通用转发器
适用操作系统： 全部
引入的版本： 8.0.3

为了易于使用，Splunk Enterprise 版本 8.0.3 和更高版本默认会将 StatsD 指标数据转换为单测量值指标数据点，这些数据点针对指标名称有一个键值对，针对指标值也有一个键值对。如果在早于 8.0.3 的版本中，您使用了 StatsD 输入将其数据转换为可以带多个测量值的指标数据点，则需要在 props.conf 中的针对该指标源类型的段落中添加 STATSD_EMIT_SINGLE_MEASUREMENT_FORMAT=false。

流指标告警不可用于运行版本 7.2 或更低版本的索引器群集。

适用组件： Splunk Enterprise 和 Splunk 通用转发器
适用操作系统： 全部
引入的版本： 8.0

Splunk Enterprise 版本 8.0 引入了流指标告警，此告警是连续评估的并且可以通过启用类似告警共享相同的搜索过程来减少系统的负荷。运行版本 7.2 或更低版本的索引器群集上不支持流指标告警。如果您有索引器群集和搜索头群集，且您将搜索头群集升级到版本 8.x，您会使用触发该搜索头群集流指标告警的功能。如果您需要保留此功能，先将索引器群集升级到版本 8.x。

在使用 mstats 命令的实时搜索中，您不能再使用通配符

适用组件： Splunk Enterprise
适用操作系统： 全部
引入的版本： 8.0

从 Splunk Enterprise 版本 8.0 开始，您不能再在包含 `mstats` 命令的实时搜索中使用通配符。如果您有这些搜索类型，进行更改这样他们升级前不会再使用任何类型的通配符，无论是在聚合字段还是指标名称中。

指标索引和搜索现在是区分大小写的

适用组件： Splunk Enterprise 和 Splunk 通用转发器
适用操作系统： 全部
引入的版本： 8.0

从 Splunk Enterprise 8.0 开始，指标数据的索引和搜索方案是区分大小写的。版本低于 8.0 的 Splunk Enterprise 的实例在搜索运行版本 8.0 或更高版本的实例时可能在检索结果时会遇到问题。

知识软件包复制的旧的已弃用配置文件设置已被删除

适用组件： Splunk Enterprise
适用操作系统： 全部
引入的版本： 8.0

`distsearch.conf` 中 `[replicationSettings]` 段落下的很多旧的之前已弃用的设置已被删除。如果您的配置使用这些设置，考虑在开始升级前更改这些设置。

用于指定知识软件包复制的已安装软件包选项的配置文件设置已更改

适用组件： Splunk Enterprise
适用操作系统： 全部
引入的版本： 8.0

用于指定知识软件包复制的已安装软件包选项的 distsearch.conf 设置已更改。之前的设置是 `shareBundles=false`。新的设置是 `replicationPolicy=mounted`。如果升级过程在您的配置文件中发现旧设置，升级过程中会自动将该设置转换为新设置，这样就不需要您手动转换。

工作负荷管理会为其他过程类型添加单独的工作负荷类别

适用组件： Splunk Enterprise
适用操作系统： Linux
引入的版本： 7.3

从 7.2 升级到 7.3 或从 7.2 升级到 8.0 之后，工作负荷管理会自动创建工作负荷类别（该类别会根据过程类型（搜索、引入和 misc.）分配资源）并替换合适的工作负荷类别中的工作负荷池，如下所示：

- 搜索：将所有现有的搜索池置于搜索类别之下。现有的 default_pool 会变成搜索类别中的 default_category_pool。
- 引入：现有的 ingest_pool 会变成引入类别中的 default_category_pool。
- misc.：Misc 类别新建时没有定义的池。

关于升级工作负荷管理的更多信息，请参阅*《工作负荷管理》*手册中的“升级工作负荷管理”。

Splunk 凭据方案可能影响新的脚本化安装

适用组件： Splunk Enterprise 和 Splunk 通用转发器
适用操作系统： 全部
引入的版本： 7.2

在升级期间软件保留现有凭据，如果您实施脚本化安装，那些可能明显受新的凭据方案影响。在使用软件 7.2 及更高版本实施脚本化安装之前，您可能需要修改您的脚本。仔细阅读以下主题以了解已升级的安装进程：

- 请参阅*安装手册*中的“在 Linux 上安装”
- 使用*安装手册*中的命令行在 Windows 上安装。

要了解已升级密码策略相关的更多信息，请参阅管理员的密码最佳做法。

另外，您的 Splunk 管理员可能会引入密码资格要求，这一要求会影响在升级后更改密码。请参阅*确保 Splunk Enterprise* 中的“配置 Splunk 密码策略”了解更多信息。

Django 框架已移除

适用组件： Splunk Enterprise
适用操作系统： 全部
引入的版本： 7.3

Django 框架及其所有相关组件已从 Splunk 平台中移除。使用此框架的应用程序和仪表板将无法正常工作。在升级之前，请确认您经常使用的应用程序和仪表板不再使用 Django，否则升级会使它们无法运行。

更新的字段别名行为可能会导致空值

适用组件： Splunk Enterprise
适用操作系统： 全部
引入的版本： 7.2

升级到版本 7.2 或更高版本的 Splunk Enterprise 时，某些**字段别名**配置的行为会有所改变。此行为会影响在字段别名处理发生之前已拥有别名字段的事件。

- 如果事件中既有源字段又有别名字段，则搜索头会覆盖别名字段的值以匹配源字段的值。
- 如果事件中有别名字段但没有源字段或源字段为空值，则搜索头会从事件中删除别名字段。

这就是在以上情况中字段别名的处理方式。但是，您的部分搜索可能依赖于旧的字段别名行为。新增了一个新的 `ASNEW` 语法，让您能够为字段别名配置提供 7.2 版本之前的行为。

7.2 版本之前的字段别名行为使用户能够创建一组字段别名配置，这些配置以一个别名字段与多个源字段相匹配。您可以使用 `ASNEW` 语法继续采用这种方式。更好的做法是，使用**计算字段**。该字段使用 `coalesce` 函数新建一个字段，该字段获取一个或多个现有字段的值。此方法让您可以明确输入字段值在空值字段中的排序。例如：`EVAL-ip = coalesce(clientip,ipaddress)`。

有关更多详细信息，请参阅*发行说明*中的“字段别名行为更改”。

Splunk Enterprise 会计量数据量小于 150 字节的指标数据点，其大小与用于事件数据的范围类似。

适用组件： Splunk Enterprise 和 Splunk 通用转发器
适用操作系统： 全部
引入的版本： 7.3

Splunk Enterprise 在 7.3 版本中计量指标数据的方式发生了变化。在此版本之前，所有标准数据点都根据许可证计算，就好像它们都是 150 字节一样。从 7.3 版本开始，Splunk Enterprise 会计量每个标准数据点，其量度为小于 150 字节的数据量，其大小与用于事件数据的范围类似。此范围不得超过 150 字节。数据量超过 150 字节的指标事件以其只有 150 字节计量。因此，此类事件的许可证使用率可能低于之前的版本。

有关许可的其他信息，请参阅*《管理员手册》*中的“Splunk Enterprise 许可授权如何工作”。

Tstats 命令现在报告索引数据桶中匹配事件的实际数量，作为这些事件的扫描计数

适用组件： Splunk Enterprise
适用操作系统： 全部
引入的版本： 7.3

`tstats` 命令对 `tsidx` 文件中的索引字段执行统计查询，已更新在数据桶中找到的事件数量的行为。

之前，命令已报告数据桶中扫描的事件计数。升级之后，命令立即报告数据桶中匹配事件的实际数量，作为扫描计数。如果您将 `tstats` 用于搜索，您可能会看到扫描计数明显下降。这并不表示结果不正确。

数据模型搜索现在只使用数据模型内定义的字段。

适用组件： Splunk Enterprise
适用操作系统： 全部
引入的版本： 7.1

当您升级到 Splunk Enterprise 7.2 或更高版本时，数据模型搜索只能使用数据模型中定义的字段名称。Splunk Enterprise 不再自动提取字段名称。依赖于此类字段的知识对象将要求数据模型明确添加此类字段，以便继续按预期工作。

另外，如果您有引用包含空格的自动提取字段名称的数据模型搜索，您需要知道数据模型不允许包含空格的字段名称。

分级统计地图的默认颜色方案已更改

适用组件： Splunk Enterprise

适用操作系统：全部
引入的版本：7.1

Splunk Enterprise 7.2 中的分级统计图的颜色方案和单值可视化已更改。现有的可视化将通过升级保留，但升级后您新建的任何新的可视化将使用新的颜色方案。

默认 Splunk 应用中已修改的导航菜单将在升级后删除

适用组件：Splunk Enterprise
适用操作系统：全部
引入的版本：7.1

升级到 Splunk Enterprise 7.2 或更高版本后，您在默认 Splunk 应用程序中对导航菜单所做的所有修改都会移除。

在此提醒您，不应该对默认应用或配置进行编辑，因为升级后，所有编辑基本都会被移除。编辑本地配置而不是对 Splunk 默认配置和应用作出修改。

统计百分位结果可能按百分之几转移

适用组件：Splunk Enterprise
适用操作系统：全部
引入的版本：7.0

Splunk 软件使用近似值算法在统计和相关命令（tstats, streamstats, eventstats, chart, timechart, sistats, sichart, sitimechart）中计算百分位和中值，除非您使用 exactperc 聚合函数。在低于 Splunk Enterprise 7 的版本中。，这些命令使用名为 rdigest 的近似值算法。升级后，默认摘要行为将更改为 tdigest，在某些情况下，它显示出比 rdigest 更强的性能，尤其是在指标数据方面。

使用百分位和中值的报表可能在升级到 Splunk Enterprise 7.x 后输出略微不同的结果。差异通常很小（小于 1%），但对于高度扭曲的数据集来说可能就显得较大。初步转移后，stats 继续使用新的摘要方式，且不会产生再一次转移，除非转移回到使用 rdigest 方式。

如有需要，您可以在 limits.conf 中全局还原摘要行为。stats、tstats、streamstats、eventstats、chart 和 timechart 的行为由 stats 段落中的设置控制。sistats、sichart 和 sitimechart 的行为由 sistats 段落中的设置控制。

请参阅*《管理员手册》*中的 limits.conf.spec。

无法再在搜索或其他查找中使用禁用查找

适用组件：Splunk Enterprise
适用操作系统：全部
引入的版本：7.0

您不再可以将禁用查找用作搜索的一部分或其他查找。升级以后，当您尝试使用禁用查找时，您将收到错误消息 The lookup table '<lookup name>' is disabled。

新功能的注意事项

Splunk 在此版本的 Splunk Enterprise 中引入了以下新功能。您可能需要在升级后执行某些配置以启用并使用这些功能。

用于导入结构化数据文件的新配置设置

适用组件：Splunk Enterprise 和 Splunk 通用转发器
适用操作系统：全部
引入的版本：8.0

Splunk Enterprise 8.0.0 和更高版本已添加一些新的配置结构化数据索引的设置。之前，结构化数据处理器是将其在标题字段名称中遇到的既不是字母数字也不是空格的字符转换为下划线。利用 props.conf 中的新的 HEADER_FIELD_ACCEPTABLE_SPECIAL_CHARACTERS 设置，您可以控制处理器接受哪些字符作为标题字段名称中的有效字符。某些字符可能会导致处理器故障，因此，如果您导入很多结构化数据并想要使用此功能，使用测试索引确认处理器以您想要的方式导入数据。

Systemd 支持开机时启动

适用组件：Splunk Enterprise 和 Splunk 通用转发器
适用操作系统：Linux
引入的版本：7.2.2

Splunk Enterprise 7.2.2 及更高版本通过更新的 enable boot-start 命令为 Linux 上的 systemd 添加了广泛支持，让您可以自动配置 systemd 以将 splunkd 作为服务进行管理。使用 systemd 会更改用于管理 Splunk 进程的命令，并要求非根用户具有某些 sudo 操作。这些差异可能需要更改所有脚本、自动化或支持文档。

有关说明，请参阅“将 Splunk Enterprise 作为 systemd 服务运行”。

Splunk Enterprise 会将新的密码套件和消息验证码用于 Splunk 间通信

适用组件： Splunk Enterprise 和 Splunk 通用转发器
适用操作系统： 全部
引入的版本： 7.2

Splunk Enterprise 7.2 引入了新的密码套件和消息验证码 (MAC)，以此替换用于安全处理 Splunk 间通信的现有密码套件。

新套件和 MAC 与旧套件不兼容。已默认配置运行 7.2 或更高版本 Splunk 软件的 Splunk 实例，允许使用新旧套件进行 Splunk 间通信。但是，如果您之后配置 7.2 或更高版本实例以只运行新套件和 MAC，那么只运行旧套件的版本之间无法实现 Splunk 间通信。您不能配置更早版本的 Splunk 软件使用新套件。

有关更改的更多信息，请参阅*确保 Splunk Enterprise 安全*中的“使用更新的密码套件和消息验证码配置安全的 Splunk 间通信”。

HTTP 事件收集器当前默认清理闲置的索引器 ACK 通道

适用组件： Splunk Enterprise 和 Splunk 通用转发器
适用操作系统： 全部
引入的版本： 7.1

升级到 Splunk Enterprise 7.2 版本后，HTTP 事件收集器立即按照 inputs.conf 配置文件中设置中的定义，默认清理发现的所有闲置时间超过 maxIdleTime 秒的索引器 ACK 通道。这会改善 HEC 性能，在清理过程中，网络和 CPU 活动可能会少量增加。

自定义已检索的报表数功能可能会降低浏览器性能

适用组件： Splunk Enterprise
适用操作系统： 全部
引入的版本： 7.0

现在，您可以通过修改 web.conf 中的条目，增加或减少 Splunk Web 一次可以检索的报表数。如果您增加可以在升级后检索的报表数，可能因为可用的报表数过多而导致浏览器性能问题。

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，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。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。搜索头池已从 Splunk Enterprise 版本 8.0 中删除，因此，没有该类型的分布式部署的升级说明。

- 要升级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。

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。

如果应用向您预期的那样有效，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`。

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”中所述。
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。

升级转发器

在完成分布式环境升级后，请检查环境中使用的转发器版本，并检查功能兼容性和支持。请参阅*《转发器手册》*中的“转发器和 Splunk Enterprise 索引器之间的兼容性”。

要升级通用转发器，请参阅*《转发器手册》*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

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 7.3.x 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便用于新版本。

更改

- Django Web Framework 已从 Splunk Enterprise 7.3.0 的产品中删除。Django Web Framework 最先是从 Splunk Enterprise 6.3.0 中弃用。使用 Django Web Framework 构建的应用和页面在 Splunk Enterprise 7.3.0 及更高版本中无法使用，会返回 404 错误。客户应将基于 Django 的应用和页面迁移到 Simple XML 或 HTML 仪表板框架。
- 要了解有关 Splunk 应用开发的更多内容或其他更改，请访问 Splunk 开发门户。

访问 Splunk 开发门户

要了解 Splunk 应用开发的更多内容，请访问 Splunk 开发门户。

在 UNIX 上升级到版本 8.2

在升级之前

在升级之前，请参阅“关于升级到 8.2 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. 转到要升级的 Splunk Enterprise 实例所在的计算机，然后打开 shell 提示符。
2. 验证安装 Splunk Enterprise 的文件夹，然后切换到 `$SPLUNK_HOME/bin` 目录。
3. 停止 Splunk Enterprise 服务，方法是运行 `systemctl stop Splunkd.service` 或 `$SPLUNK_HOME/bin/splunk stop`
4. 确认没有其他进程会自动启动 Splunk Enterprise，例如配置管理或服务管理工具。
5. 要升级和迁移现有配置，请直接在现有部署上安装最新的 Splunk Enterprise 软件包。
   - 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。这将覆盖并替换默认文件，但不会删除唯一的文件或文件路径。示例： `tar xzf splunk-8.2.0-12345678-Linux-x86_64.tgz -C /opt`
   - 如果您使用的是软件包管理器（如 RPM），请键入 `rpm -U splunk_package_name.rpm`
   - 如果您在 MacOS 上使用 `.dmg` 文件，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. 启动 Splunk Enterprise 服务，方法是运行 `systemctl start Splunkd.service` 或 `$SPLUNK_HOME/bin/splunk start`
   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. （可选）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，还是继续迁移并立即升级。如果选择查看预期的更改，脚本会提供一个列表，但不会启动任何服务。
   在查看完迁移更改并准备继续迁移和升级之后，再次启动 Splunk Enterprise 服务。

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。

- 要在继续升级之前接受许可证并查看预期的更改，请使用以下命令：

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

- 要接受许可证并开始升级而不查看更改，使用以下命令：

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

在 Windows 上升级到版本 8.2

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 8.2 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。

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 中新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. 转到 Splunk.com 的“免费试用版和下载”页面（需要登录）。
2. 在“Splunk 核心产品”下方，选择“Splunk Enterprise”。
3. 选择“立即下载”以获取最新版本，或单击“旧版本”链接以找到特定版本。
4. 将 MSI 文件下载到主机。
5. 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。当它找到旧的安装文件时，会显示一个窗格，请您接受许可协议。
6. 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。安装程序在升级完成时重新启动 Splunk Enterprise 服务，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. 转到 Splunk.com 的“免费试用版和下载”页面（需要登录）。
2. 在“Splunk 核心产品”下方，选择“Splunk Enterprise”。
3. 选择“立即下载”以获取最新版本，或单击“旧版本”链接以找到特定版本。
4. 将 MSI 文件下载到主机。
5. 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 LOGON_USERNAME 和 LOGON_PASSWORD 标记在命令行说明中指定该用户的凭据。
   - 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）。
6. 根据规格不同，Splunk Enterprise 可能在您完成安装后自动启动。

将 Splunk Enterprise 实例从一个物理计算机迁移到另一个

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。

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。

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 实例新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 Enterprise 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。分布式环境必须在同一操作系统上运行，并且还有其他要求。请参阅*《管理索引器和索引器群集》*手册中的“关键要求摘要”。

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 服务。
2. 复制旧主机中 $SPLUNK_HOME 目录的完整内容到新主机。复制此目录也会复制 mongo 子目录。
3. 将 Splunk Enterprise 安装到新主机上。
4. 验证索引配置（indexes.conf）文件的卷、大小和路径设置在新主机上仍然有效。
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：

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，新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。

计划您的 Splunk Enterprise 升级以进行 Python 3 迁移

选择适合 Python 3 迁移的 Splunk Enterprise 升级路径

Splunk Enterprise 管理员必须规划升级到 Splunk Enterprise 版本 8.1，以考虑 Python 2.7 生命周期结束需要考虑的其他步骤。

此页面仅适用于 Splunk Enterprise。如果您是 Splunk Cloud 管理员，使用 Splunk 支持规划您的升级。

在 Splunk Enterprise 版本 8.1 中，Splunk Enterprise 默认情况下会全局使用 Python 3 解释器。您可以选择恢复为 Python 2，但 Splunk Web 仅支持 Python 3.7。根据 Splunk Web 确定的脚本和模板在升级之前，必须调整为使用 Python 3 可兼容的语法，但是您有多个选项可以选择如何以及何时调整不依赖于 Splunk Web 的 Python 脚本。

对于那些不依赖于 Splunk Web 的文件，Splunk Enterprise 8.1 在配置文件中按文件提供了 Python 版本切换开关。此外，全局切换让您可以修改默认的 Python 版本。

根据您的组织需求，您可以选择升级到 Python 3，尽量和升级到 Splunk Enterprise 版本 8.1 一样全面，可使用双兼容的 Python 代码或重新写入 Python 脚本使其只与 Python 3 兼容。或者，您可以选择升级到 8.1 版，而不立即执行完整的 Python 3 迁移，具体方式为：将默认的 Python 版本更改为 Python 2 并且仅修改依赖于 Splunk Web 的脚本和模板。

使用下表选择最适合您的升级路径。如果您使用的是专用的家用应用，关于升级的时间和方法，您有更多的选择。如果您使用 Splunkbase 应用，在 Python 2 和 Python 3 的兼容性方面，您受应用开发者的选择限制。

如果在升级到 Spunk Enterprise 8.0 时选择迁移到 Python 3，则无需完成有关 Python 迁移的任何其他任务即可升级到 Splunk Enterprise 8.1。

最能描述您的语句	整体工作	说明
我想使用默认的 Python 3 运行时。	**建议使用。**最低的整体工作。	使用 Python 3 运行时间和自定义脚本中的双重兼容 Python 语法升级
我想以最小的工作量进行升级，无论 Python 是什么版本。	短期内的较少工作， 长期内的较多工作。	使用 Python 2 运行时间进行升级，对 Python 代码做最小的更改

如果您不确定哪个语句最适合您，最好的做法是使用 Python 3 运行时间和自定义脚本中的双重兼容 Python 语法升级。

使用 Python 3 运行时间和自定义脚本中的双重兼容 Python 语法升级

按照此升级路径过渡到使用 Python 3 运行时。要确定是否需要进行任何更改，请参阅“为 Python 3 迁移规划 Splunk Enterprise 升级路径”。

Splunk Enterprise 版本 7.x 和更低版本不支持 Python 3。若要选择编写仅兼容 Python 3 的私有应用程序，那么如果在升级到 Splunk Enterprise 版本 8.0 或更高版本之前安装了应用，或者如果应用之前的版本在 Splunk Web 相关的脚本和模板中有 Python 2 语法，则可能会遇到更改中断的问题。

此升级路径由三部分组成：

1. 预升级步骤
2. 升级 Splunkbase 应用并验证
3. 升级 Splunk Enterprise

预升级步骤

在升级到 Splunk Enterprise 版本 8.1 过程中，在迁移到 Python 3 之前，请采取以下步骤。使用测试环境是可选的。如果您不使用测试环境，此过程可能会影响性能。更多信息，请参阅*《Splunk Platform Upgrade Readiness 应用》*手册中的“性能注意事项”。

使用 Splunk Platform Readiness 应用准备升级

1. 可选：在测试环境中，安装所有生产应用并在应用上下文之外复制您包含在生产环境中的任何自定义脚本。
2. 安装 Splunk 平台升级准备应用并运行，最好是在测试实例上。更多信息，请参阅*《Splunk Platform Upgrade Readiness 应用》*手册中的“关于 Splunk Platform Upgrade Readiness 应用”。
3. 查看您专用应用的测试结果，按照升级准备程序中的说明解决任何问题。重写 Python 脚本使其和 Python 2 和 Python

3 兼容。有关更多信息，请参阅*《Python 3 迁移》*手册中的“编写和 Python 2 和 Python 3 兼容的 Python 脚本”。
4. 检查从 Splunkbase 下载的应用程序的测试结果，并检查包含自定义或扩展内容的文件路径。按照升级准备应用中的说明解决问题。

手动准备升级

如果您选择不使用升级准备应用，手动检查 Splunk Enterprise 部署是否存在问题。继续之前，确认您的专用应用和扩展满足这些升级准备要求：

1. 可选：在测试环境中，安装所有生产应用并在应用上下文之外复制您包含在生产环境中的任何自定义脚本。
2. 删除所有高级 XML。
3. 如果您正在运行 SplunkWeb 传统模式，通过编辑 `%SPLUNK_HOME%\etc\system\local\web.conf` 删除 `appServerPorts` 和 `httpport` 属性禁用该模式。
4. 将名为 `test.py` 的所有文件重命名为非保留的名称。
5. 将自定义 Mako 模板调整为 Python 2 和 Python 3 可兼容的。
6. 将应用中的自定义 CherryPy 端点调整为 Python 2 和 Python 3 可兼容的。
7. 使用 Python SDK 或利用六个或未来的库重写所有剩余的 Python 代码使其与 Python 2 和 3 双重兼容。保留您重写的文件列表，这样您升级时可以测试这些文件。
   有关这些升级要求的更多信息，请参阅*《Python 3 迁移》*手册中的“通过 Splunk 平台迁移 Python 3”。

升级 Splunkbase 应用并验证

仅当您完成所有准备步骤之后，按照三个阶段的 Splunk Enterprise 升级流程，在测试环境中升级到 Splunk Enterprise 8.1。有关更多信息，请参阅“Splunk Enterprise 升级流程”。

要降低性能影响，先在测试环境中升级到 Splunk Enterprise 8.1 以测试是否有更改中断的情况。请勿直接在生产环境中升级。

按照以下步骤验证测试环境中的升级：

1. 将您已安装的 Splunkbase 应用升级为可与 Splunk Enterprise 7.x 和 8.x 双重兼容的版本，因为这些版本应该和 Python 2 和 Python 3 都兼容。测试是否有更改中断的情况。如果开发人员未提供可与 Splunk Enterprise 版本 8.1 兼容的应用版本，您可以自行升级或删除应用。如果开发人员提供了 Splunk Enterprise 7.x 和 8.x 的单独版本，按照开发人员提供的升级说明操作。如果都没有提供，假设应用是仅为 Python 3 写的，选择以下其中一个选项：
   - 将实例升级到 Splunk Enterprise 8.x 之后将应用升级为仅与 Splunk Enterprise 8.1 兼容的版本，注意 Splunk Web 中可能会出现更改中断的情况。
   - 如果有很多 Splunkbase 应用只与 Python 3 兼容并可能造成意外的停机时间，升级 Splunk Enterprise 期间使您的部署离线进行维护。在此期间，删除应用、使部署离线、将应用升级到与 Splunk Enterprise 8.x 兼容的版本，然后使部署重新上线。
2. 通过访问所有依赖于自定义 CherryPy 端点或 Mako 模板的视图，测试依赖于 Splunk web 的 Python 脚本。确保它们按预期运行。
3. 测试您的双重兼容的 Python 脚本的功能。如果您愿意，可以使用 Python 3 运行每个双重兼容的脚本。查阅重写的文件列表，一次一个地转到调用每个脚本的配置文件，将 `python.version=python3` 添加到调用脚本的段落。使用下表测试错误：

脚本类型	文件	是否需要重新启动？	如何测试
自定义搜索命令	commands.conf	是	运行命令并检查是否像预期那样有效。
模块化输入	inputs.conf	是	启用输入并检查数据是否如期到达。
脚本式输入	inputs.conf	是	启用输入并检查数据是否如期到达。
自定义告警操作	alert_actions.conf	否	运行自定义告警操作然后验证是否像预期那样有效。
脚本式查找	transforms.conf	是	验证查找是否像预期那样有效。
自定义 REST 端点	restmap.conf	否	访问端点并检查是否像预期那样反应。
脚本式验证	authentication.conf	否。转到**设置** > **访问控制** > **验证方法**，然后单击**重新加载验证配置**。	

4. 如果您使用脚本式验证，检查 `scriptPath` 设置中指定的 Python 翻译器路径是否是规范的路径 `$SPLUNK_HOME/bin/python`。如果您将自定义路径输入其他解释器，脚本式验证将使用您指定的解释器而不是您在 `python.version` 设置中选择的解释器。
5. 如果您遇到任何错误，调整 Python 文件然后重新测试。
6. 在您认为所有的脚本像预期那样有效之后，在您的测试环境中指定全局 Python 3 运行时间。

1. 前往 $SPLUNK_HOME/etc/system/local/server.conf 并设置 python.version=python3。
2. 重新启动 Splunk Enterprise。
3. 测试重要路径（如脚本式验证）上的任何 Python 脚本，以确保这些脚本继续工作。

升级 Splunk Enterprise

在您的搜索头、索引器和转发器上将您的生产环境升级到版本 8.1，按照三个阶段的 Splunk Enterprise 升级流程。有关更多信息，请参阅“Splunk Enterprise 升级流程”。升级部署组件时，按照以下操作顺序操作：

1. 升级为 Splunk Enterprise 8.1。
2. 注意任何潜在的更改中断，如升级时尚与 Splunk Enterprise 版本 8.1 不兼容的应用。
3. 安装任何只与 Python 3 和 Splunk Enterprise 8.x 兼容的应用。
4. 一段时间过后，将脚本设置为只运行 Python 3。转到相应的脚本 .conf 文件，并设置 python.version=python3（如验证应用时提到的）。
5. （可选）在生产环境中指定全局 Python 3 运行时。前往 $SPLUNK_HOME/etc/system/local/server.conf 并设置 python.version=python3。
6. 启动 Splunk Enterprise。

使用 Python 2 运行时间进行升级，对 Python 代码做最小的更改

如果您想要继续尽量使用 Python 2，使用此升级路径。要查看其他升级路径选项并选择最适合您的升级路径，请参阅“选择适合 Python 3 迁移的 Splunk Enterprise 升级路径”。

此升级路径由三部分组成：

1. 解决升级阻块
2. 升级 Splunkbase 应用并验证
3. 升级 Splunk Enterprise

解决升级阻块

在准备在升级到版本 8.0 或更高版本的过程中迁移到 Python 3 时，采取以下步骤。使用测试环境是可选的。如果您不使用测试环境，此过程可能会影响性能。更多信息，请参阅*《Splunk Platform Upgrade Readiness 应用》*手册中的“性能注意事项”。

使用 Splunk Platform Readiness 应用准备升级

1. （可选）在测试环境中，安装所有生产应用并在应用上下文之外复制您包含在生产环境中的任何自定义脚本。
2. 安装 Splunk 平台升级准备应用并运行，最好是在测试实例上。更多信息，请参阅*《Splunk Platform Upgrade Readiness 应用》*手册中的“关于 Splunk Platform Upgrade Readiness 应用”。
3. 查看您专用应用的测试结果，按照升级准备程序中的说明查看任何标记为 BLOCKER 的项目来解决问题。
4. 检查从 Splunkbase 下载的应用程序的测试结果，并检查包含自定义或扩展内容的文件路径。继续之前解决问题。

手动准备升级

如果您选择不使用升级准备应用，手动检查 Splunk Enterprise 部署是否存在问题。继续之前，确认您的专用应用和扩展满足这些升级准备要求：

1. 删除所有高级 XML。
2. 如果您正在运行 SplunkWeb 传统模式，通过编辑 %SPLUNK_HOME%\etc\system\local\web.conf 删除 appServerPorts 和 httpport 属性禁用该模式。
3. 调整自定义 Mako 模板使其与 Python 2 和 Python 3 兼容。
4. 调整应用中的自定义 CherryPy 端点使其与 Python 2 和 Python 3 兼容。
   有关这些升级要求的更多信息，请参阅*《Python 3 迁移》*手册中的“通过 Splunk 平台迁移 Python 3”。
5. 在 server.conf 文件的 python.version 设置中，确保版本为 python2。

升级 Splunkbase 应用并验证

仅当您完成所有准备步骤之后，按照三个阶段的 Splunk Enterprise 升级流程，在测试环境中升级到 Splunk Enterprise 8.0 或更高版本。有关更多信息，请参阅“Splunk Enterprise 升级流程”。

要降低性能影响，先在测试环境中升级到 Splunk Enterprise 8.0 或更高版本以测试是否有更改中断的情况。请勿直接在生产环境中升级。

按照以下步骤验证测试环境中的升级：

1. 通过访问所有依赖于自定义 CherryPy 端点或 Mako 模板的视图，并确保它们按预期运行来测试依赖于 Splunk web 的

Python。
2. 将已安装的 Splunkbase 应用升级到支持 Splunk Enterprise 8.0 或更高版本的版本并测试是否有更改中断的情况。如果开发人员未提供可与 Splunk Enterprise 版本 8.0 或更高版本兼容的应用版本，您可以自行升级以满足相关要求或删除应用。

升级 Splunk Enterprise

在您的搜索头、索引器和转发器上将您的生产环境升级到版本 8.0 或更高版本，按照三个阶段的 Splunk Enterprise 升级流程。有关更多信息，请参阅“Splunk Enterprise 升级流程”。升级部署组件时，按照以下操作顺序操作：

1. 在 server.conf 文件的 [python.version] 段落中，确保版本为 python2。
2. 升级为 Splunk Enterprise 8.0 或更高版本。
3. 注意任何潜在的更改中断，如升级时尚与 Splunk Enterprise 版本 8.0 或更高版本不兼容的应用。
4. 安装任何只与 Python 3 和 Splunk Enterprise 8.0 或更高版本兼容的应用。
5. 启动 Splunk Enterprise。

完成此过程并不意味着升级到 Python 3 的操作已完成。计划将来完成升级到 Python 3 的操作。

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。

   ```
   ./splunk disable boot-start
   ```
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

如果您用的是本地软件包管理工具安装 Splunk Enterprise，使用相同的工具卸载 Splunk Enterprise。在大部分情况下，之前未被软件包安装的文件将保留。这些文件包括 Splunk Enterprise 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
```

可能希望删除的其他内容

- 如果新建了任何索引，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 新建了用户或组，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 8.1 和 10，Windows Server 2012 R2、2016 及 2019 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
  ```

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。
   用于 Linux

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

用于 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`。

   用于 Linux

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

   用于 Mac OS

   ```
   rm -rf /Applications/splunk
   ```

   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）。

   用于 Linux

   ```
   userdel splunk
   groupdel splunk
   ```

   用于 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 /x`。如果您没有此软件包，请从下载页面获取正确版本。

引用

PGP 公共密钥

您可从此页面为 Splunk 软件复制 Pretty Good Privacy（PGP）公共密钥或使用 HTTPS 下载文件。

- 此 PGP 公共密钥用于签署在 2018 年 8 月 15 日或之后发布的 Splunk 软件的软件包。
- 签名仅适用于 RPM 软件包。对于所有其他软件包类型，请使用校验和文件。请参阅“安全安装 Splunk Enterprise”。

PGP 公共密钥块

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBFtbebEBEADjLzD+QXyTqLwT2UW1Dle5MpBj+C5cbaCIpFEhl+KemcnUKHls
TlCxEpzJczZPiYtcp+wtKCaNG/zoEvYCQ0jKk6Wgoa2cLkDeHtNiuBCHrztgeDTe
FpPT+xmtLoJvu1T0JV/iPG7p5FBGYKOKApnd/awRRC47plCGfVA3VVdQP8jhpMZV
T9C86hWbNo/NRjNH69x1xAe/9POc8KmVxZQb+KGG5tulGIWa7jlTMw850HZwFcft
F13DiAVgCj516K8oZBb5bjgu2ZvpCtMRbCmrzx26ilcB7VJRsTaB6G8MqRzVgLuj
11dTG2XMuBw+3UcjAlZ/y6Cut0Gc5FHIKqwMVXf29y9uXddvIqQnkE0AkOj6flm6
OElvmq7v+NVYLRb9XTy0oWTwOtyGTTso2xwZ8itDT4rIWeta0FxtQPt8Kq369ZGy
CbKl1PU9IrKAeST0AkXyfQXqPc0IzHxz3AhOLzvwm/9/0OWs0ONbxdyTCxQjrhe6
1YBoVv2T5K27fTp7rMFEstyU0NFI3J5P/oxg5ts6y2lCMUB7Q71yAOWVZPgucOAH
7iiNmvrytuGT0c8TfJku1cneajW9jmNvKVD/r3qj6YTAL3mqC0yYx3PiLyUVm8OZ
q90hpFHAI7zV1u6zMqV4EkWg5tEknMWcjQnyIfn0Jx8LedDjbTM8Dt9VKQARAQAB
tCFTcGx1bmssIEluYy4gPHJlbGVhc2VAc3BsdW5rLmNvbT6JAk4EEwEIADgWIQRY
wzMQt6NUwSedtmle+gHts81EIAUCW1t5sQIbAwULCQgHAgYVCAkKCwIEFgIDAQIe
AQIXgAAKCRBe+gHts81EIEsUD/9urCsBW40ahPr1gBsu6TlFbVWFN6TK7NpByecr
KzhDlOGJbh7g1u1qRO88ncUb/iPFfBjpJJ0RbskrZQKVVbmnhLeNPw4oqHq4kNmN
Kc8iV9tynw55Ww5Y0cJoeWrx9Ireub3+1GhKzUomIK0TuQtMULmW7Tdwm46iEDgC
qox2hOutlMFjrT9XOFnluCeyi8HL9m6xUlvvsxYxqWIzWUvoWH3AwpGSPMwg/nzH
Vl1Wz9IJOLqjQFBiA1Vmb/UEkP60JAtXWtNKJ7OqTLag29XBSaJO1NiQFZYb8uCU
GSqNOKYUwiO3ZivmVYlXBT7fC2uHpU45g/d2PrRKgVvIOC9xKiG8+jh/WuWlTl4i
vVjAIEnIFwO8Nig7uoR9xi+0ZxzkP00tGO2Cgv0cFf3TYQrSgrD7QDRBN2az4HtF
WvxJuOYjNLl7mp+Lx0Aj9wtb1WkYNBV0NMXThhnZsDU6Uo6ijJa2uBwkT8MljCHX
n7DjVFZYoZ6m2cwUdR5XSwfpSq0lA7LcSbef4CIC1H0mVxVzeB2B6xGxpVIMNGs4
B1RXW1amVeKmv9ZbTAQpGNVMyGJ8oOhksBFL2Ng0Z5kA9aCuwr1OjyrxBdglfGd/
wmEGIX2cLNNvS+Elh4JzFuKsURWbJ8qFl7cQvKQkS+UTwu7e3CCp8VztfRqPvgQi
A+2oI7kCDQRbW3mxARAAtoBTC9nNiY3301QKzTyPvudD3XI03RZTXVsSHVP4yV0x
fobD2aRhMjxwRjrajZnMCEFKB7yYtsbyiRfznLoycFBse6p4y9gguWEIgaW6TTQP
zQTEgi6AKt38nqDN42L/WurNhAKq9R5X/85vr2t6b18Yp2kw62okbuTtVLjuNwzh
tnZE/HziWVbtBy0KfZ0c6QMUHn7j0U67+QJeIzLcQuBn4qnb177TRtnqNZ9aFTXX
mnUA7qTOAvL+wsoyOcuOboj4N45H5s/izPSiXkoUM1ITuuUI3QHi46zw5cEvSLg+
WImwwZCN4tC275abjxW7XbirglV1EOlCWoALIOAh1BwXDA/JJGwbGOp+ueE7askJ
TiAtP9EM1mJSWnbE9uKDUvEMIaavwtt0kWmQOrB4HFY0AsTOnCxWQYCOb0CDImyq
ScblC3tqvoZzbjPBHQFvxClzxfGdmvQwoxr2WRfsspLPuG1FzgmmX29/WaOV747W
TwJP9xw1OtJmAkq/+CH6J12PmXHy9sJRdk6d1PPEuHjJ588U3Kwc7B5uAtgnwQO8
aS4zPM45y6+J1D2SdM0ydwuqQ9z9wwa022EGTa89k5Vfigx+C/VaDMa1Bu/NSkZ8
7S0NpQGbRwDp76gSKvV1T/15hYVg2nOsI1hTVmM8hVZQO3kO4zFjl0rNNjwWor0A
EQEAAYkCNgQYAQgAIBYhBFjDMxC3o1TBJ522aV76Ae2zzUQgBQJbW3mxAhsMAAoJ
EF76Ae2zzUQg26YP/0dj63ldEluB8L7+dFm9stebcmpgxAugmntdlprDkGi6Rhfd
ks7ufF+mny731GZPcJWIYKi797qerG5O1AI4siaK9FRKzw4PLIGvhOoNg2wrSP/+
7qTFf+ZbT7H5VpIqwcnnnRT05pi1KiMIXW82h47daFYVNhQPbV4+USHwFG7r3Lku
XdiS4hrcoe+Y/a9zGVAdU9QwrT8CuNAw8SYNYx1rJECHiMxmMaEw42a5NARoFdbh
swnR6Mwy5sPhzOHjSI/ZPyM/W9TKAoXfmDQSGDrvnU6NAdpIbP1Ab1FtMjuARfRg
8ndqfm/n8MIvAxjzoBBZkdV5HLOndX3fLVNewnvSWQx9OlV4a7+dKXeQ8TueOMq+
XMA4RKsh3gEMJWbVRZwZnxy+3UKGJD3el0+C7m483ptR8Tj8qBq5KELO0vkcq8+a
eHIbzmQSsj9iAdNfGVLYhimzpZy5NCTl2sgmy4g33pd1jMtUzdFZhvelVzMNlkLZ
AmAJX7yZLQwLsXDEpffgp2S/U8vYAZNTdeZqKvmvCCO+fweRRC7NnnPJQ7nVhL7r
VDxHuk8oMqBQIUdE7Z+WDfyagMMhJWbeMNnnhTZdoPmpXEGkjUKwPDYl+GmF50c1
6vjXtbrcP42pu2IQxiqiaTSLei8LRwPck1eE+78sSUxjVuWRuThoYRhGYoXt
=ivRW
-----END PGP PUBLIC KEY BLOCK-----
```

GPG 密钥 ID

GPG 公共密钥 ID 是 `key ID b3cd4420`。

安装 PGP 公共密钥

请参阅“验证签名”。