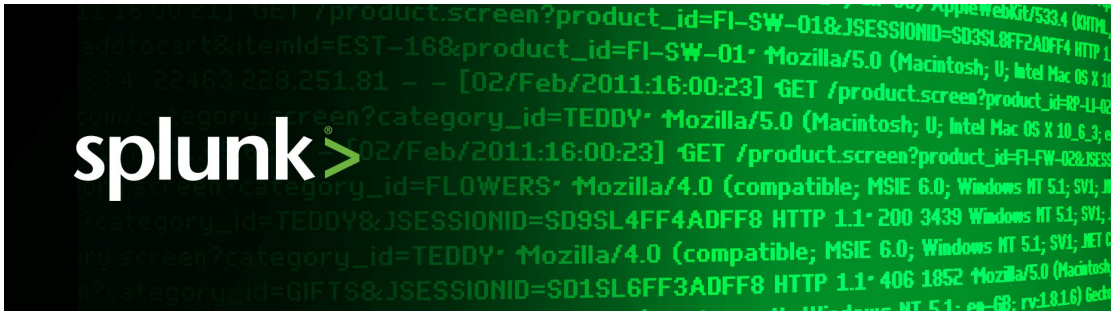


Splunk® Enterprise 7.2.0

Splunk Enterprise 概述

生成时间：2018 年 10 月 17 日，上午 8:55

Table of Contents

关于 Splunk Enterprise

关于 Splunk Enterprise

Splunk Enterprise 是一款软件产品，允许您搜索、分析和可视化从 IT 基础设施或业务组件收集的数据。Splunk Enterprise 可从网站、应用程序、传感器、设备等处获取数据。您定义完数据源后，Splunk Enterprise 对数据流建立索引并将其解析至一系列您可以查看和搜索的单独事件中。

大多数用户使用 Web 浏览器连接 Splunk Enterprise 并使用 **Splunk Web** 管理其部署、管理并新建知识对象、运行搜索、新建数据透视表和报表等。您还可以使用命令行界面管理您的 Splunk Enterprise 部署。

您可使用应用扩展 Splunk Enterprise 环境以满足组织的特定需求。**应用**是在 Splunk 平台上运行的配置、知识对象、视图和仪表板的集合。单个 Splunk Enterprise 安装可以同时运行多个应用。浏览 Splunkbase 上的可用应用或在 Splunk 开发人员站点上构建自己的应用。

Splunk Enterprise 的功能

以下部分强调了 Splunk Enterprise 的 7 种功能。您可在 Splunk.com 的 Splunk Enterprise 页面了解有关功能的更多信息。

索引

Splunk Enterprise 可索引构成 IT 基础设施的数据。您可从网站、应用程序、服务器、数据库、操作系统等处获取数据。Splunk 实例的最大索引量取决于 Splunk Enterprise 许可证。

搜索

搜索是用户导航 Splunk Enterprise 中数据的主要方式。您可将搜索另存为报表并用来驱动仪表板面板。通过搜索可深入了解数据，例如：

- 从索引中检索事件
- 计算指标
- 搜索滚动时间窗口内的特定条件
- 识别数据模式
- 预测未来趋势

告警

当历史搜索和实时搜索的搜索结果符合配置条件时告警会通知您。您可以配置告警以触发操作，如发送告警信息至指定电子邮件地址；将告警信息发布至 RSS 源及运行自定义脚本，如将告警事件发布至 syslog 的脚本。

仪表板

仪表板包含模块面板，如搜索框、字段、图表等。仪表板面板通常连接到已保存的搜索或数据透视表。它们可显示已完成搜索的结果以及后台运行的实时搜索的数据。

数据透视表

数据透视表指您使用**数据透视表编辑器**新建的表格、图表或数据可视化。数据透视表编辑器允许用户将数据模型对象定义的属性映射至表格、图表或数据可视化，而不需要在**搜索处理语言 (SPL)** 中编写搜索来生成属性。数据透视表可以保存为报表并添加至仪表板。

报表

Splunk Enterprise 允许您将搜索和数据透视表另存为报表，然后将报表添加至仪表板作为仪表板面板。临时运行报表，计划使其以固定间隔运行，在结果满足特殊条件时设置计划报表以生成告警。

数据模型

数据模型对关于一组或多组已建立索引数据的专业域知识进行编码。借助数据模型，“数据透视表编辑器”用户可新建报表和仪表板，而无需对生成它们的搜索进行设计。

下载 Splunk Enterprise 快速参考指南

Splunk Enterprise 快速参考指南是一个 6 页的 PDF 参考指南，提供有关 Splunk Enterprise 功能、概念、搜索命令和搜索示例的信息。

关于 Splunk Enterprise 用户

Splunk Enterprise 服务于不同类型的用户。使用 Splunk Enterprise 的人员主要有 5 种角色：

角色	行业角色	活动
管理员	网络工程师、系统管理员	配置、管理、优化并确保 Splunk Enterprise 部署安全 设置用户帐户和权限 将数据导入 Splunk Enterprise
知识管理器	数据分析师、系统管理员	监视各团队、部门和部署之间知识对象的新建、标准化和使用情况 将数据导入 Splunk Enterprise，或与管理员一起操作 新建并共享数据模型
搜索用户	数据分析师、IT 专业人员、网络工程师、安全分析师、系统管理员	使用搜索调查服务器问题、了解配置、监视用户活动并排除上报的问题 构建报表和仪表板，以监视其 IT 基础设施健康状况、性能、活动及其能力 确定代表常见问题的类型和趋势
数据透视表用户	业务专业人员、数据分析师、执行人员、IT 专业人员、经理、系统管理员	基于知识管理器新建的数据模型，使用数据透视表构建报表 新建报表和仪表板，以监视其业务 确定其业务健康状况和性能趋势
开发人员	系统集成人员、专业开发人员	利用 Splunk Enterprise 集成数据和应用的功能 利用自定义仪表板和数据可视化构建 Splunk 应用和加载项

关于 Splunk Enterprise 部署

来自服务器、应用程序、数据库、网络设备、虚拟机的数据构成了 IT 基础架构，Splunk Enterprise 对这些数据建立索引。只要生成数据的计算机是网络中的一部分，Splunk Enterprise 可从任何位置，无论是本地、远程或在云中收集数据。

Splunk Enterprise 会在处理数据时执行三项主要功能：

1. 从文件、网络或其他来源获取数据。
2. 分析并索引数据。
3. 对索引的数据运行搜索。

部署类型

您可根据自身需要将 Splunk Enterprise 部署为单一实例，或者您可跨多个实例新建部署，几百甚至上千个实例均可。

单实例部署

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

分布式部署

要支持大型环境，其中数据由很多计算机产生，您需要处理大量数据或者很多用户需要搜索数据，您可通过跨多个计算机分布 Splunk Enterprise 实例来调整部署规模。这称为“分布式部署”。

在典型的分布式部署中，每个 Splunk Enterprise 实例可执行专门的任务并驻留在主要处理功能对应的三个处理层其中一个：

- 数据导入层
- 索引层
- 搜索管理层

例如，您可新建部署，其中大部分实例驻留在数据导入层并仅引入数据，若干其他实例驻留在索引层并索引数据，一个实例驻留在搜索管理层并管理搜索。这些专门的实例称为“组件”。

Splunk Enterprise 组件和处理层

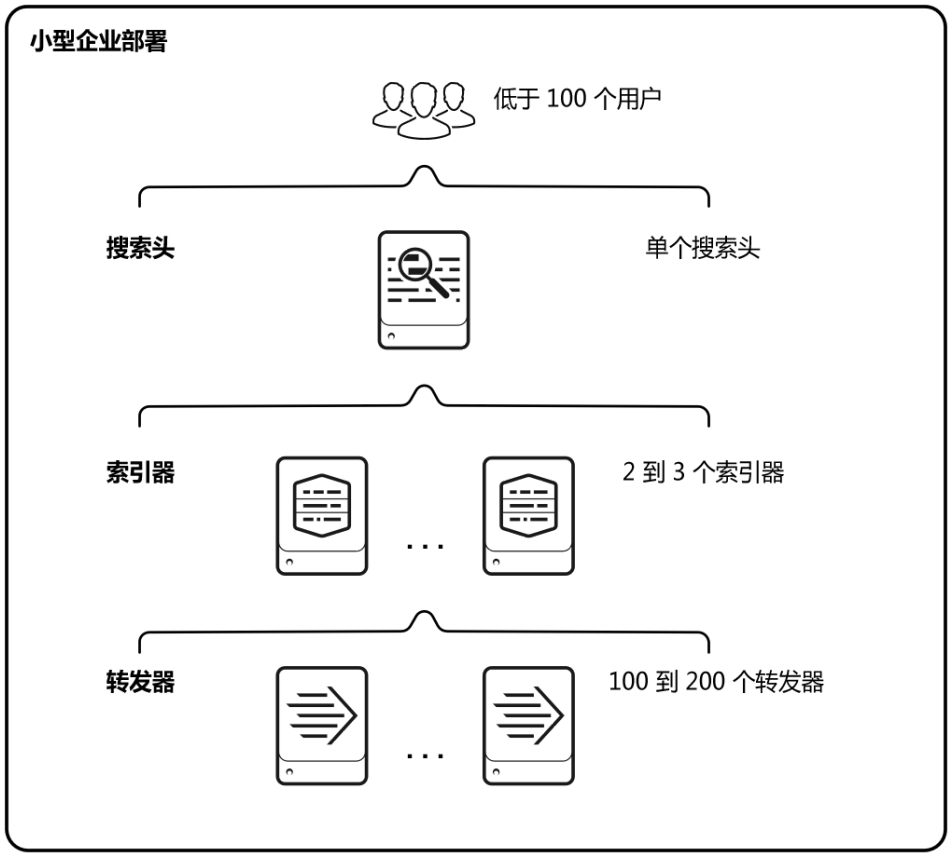
此表列出了处理组件及其占用的层。还介绍了各组件可执行的功能。

组件	层	描述
转发器	数据导入	转发器可获取数据，然后通常会将数据继续转发至索引器。转发器通常需要很少资源，允许其更容易驻留在生成数据的计算机上。
索引器	索引	索引器会索引传入数据，通常会从转发器组接收数据。索引器将数据转换为事件并将事件存储至索引中。索引器还会搜索索引数据，以响应搜索头的搜索请求。 如要确保数据高可用性并防止数据丢失，或只为简化管理多个索引器，则可以在索引器群集中部署多个索引器。
搜索头	搜索管理	搜索头与用户交互，将搜索请求指向一组索引器，并合并结果返回给用户。 要确保高可用性并简化横向扩展，您可以在搜索头群集中部署多个搜索头。

必要时您可为各层添加组件，支持该层上的更大需求。例如，如果您有大量用户，您可另行添加搜索头以更好地服务用户。

分布式部署示例

此图说明了可以支持小型企业需求的部署类型。



关于组件以及如何部署组件以调整 Splunk Enterprise 规模的更多信息，请参阅*分布式部署手册*。

Splunk Enterprise 资源和文档

Splunk Enterprise 支持和资源

本主题概述了支持、文档和其他可用资源，帮助您查找有关 Splunk Enterprise 和其他 Splunk 产品的信息。

支持

获取 Splunk Enterprise 支持：

- 提出问题并通过 Splunk Answers 社区支持获取答案。
- 如果您有支持合同，请使用 Splunk 支持门户记录相应情况。
- 如果您有支持合同，请联系客户支持。

文档

本部分将向您介绍如何查找特定产品或任务相关文档。

Splunk Enterprise

使用以下主题在 Splunk Enterprise 文档内查找您所需的信息：

- Splunk Enterprise 管理
- 搜索和报告
- 管理 Splunk Enterprise 知识
- 自定义并扩展 Splunk Enterprise
- 故障排除

应用和加载项

通常，应用的文档链接自应用的下载页面，或包含在 Splunkbase 中应用的下载软件包中。只有 Splunk 支持产品时，Splunk 才会提供应用或加载项。

Splunk SDK

Splunk for Developer 站点提供 Splunk SDK 信息、教程和示例。请参阅 Splunk SDK 文档站点查看模块库和其他参考资料。

资源

访问 Splunk Enterprise 的其他资源：

- 阅读 Splunk Enterprise 快速参考指南了解 Splunk Enterprise 功能、概念、搜索命令和搜索示例相关信息。
- 加入 Splunk 用户组 Slack 通道
- 开始 Splunk Education 训练或证书追踪。
- 在 Splunk 社区页面上访问更多社区资源。

Splunk Enterprise 管理

本主题列出了常见管理员任务并介绍相关手册内的相关主题。

安装和升级 Splunk Enterprise

*安装手册*介绍如何安装和升级 Splunk Enterprise。

任务：	查看此处：
了解安装要求	安装概述
预估硬件容量需求	Splunk Enterprise 容量规划简介
安装 Splunk Enterprise	选择 Splunk Enterprise 应以其身份运行的 Windows 用户 在 Linux 上安装 在 Mac OS X 上安装

升级 Splunk Enterprise	如何升级 Splunk Enterprise
执行备份	备份配置信息 备份索引数据 设置退休和归档策略

将数据导入 Splunk Enterprise

*数据导入*介绍 Splunk 数据导入类型以及如何将数据导入 Splunk 部署。

任务：	查看此处：
了解如何使用外部数据	什么数据可以建立索引？
配置文件和目录输入	监视文件和目录
配置网络输入	从 TCP 和 UDP 端口获取数据
配置 Windows 输入	有关确定如何监视远程 Windows 数据的注意事项
配置其他输入	监视先进先出 (FIFO) 队列 监视对文件系统的更改 通过脚本式输入从 API 及其他远程数据接口获取数据
增强您的数据值	事件处理概述 时间戳分配如何工作 关于索引字段提取 关于主机 来源类型为何重要 关于事件分段
查看您的数据在建立索引后的显示效果	“设置 Sourcetype”页面
改善数据导入过程	使用测试索引测试输入
了解数据管道	数据如何通过 Splunk Enterprise：数据管道

管理索引和索引器

*管理索引器和群集*介绍如何配置索引和管理索引器以及维护索引的组件。

任务：	查看此处：
了解索引	索引、索引器和索引器群集
管理索引	关于管理索引
管理索引存储	索引器如何存储索引
备份索引	备份索引数据
归档索引	设置退休和归档策略
了解群集和索引复制	关于索引器群集和索引复制
部署群集	索引器群集部署概述
配置群集	主节点配置概述
管理群集	查看主节点仪表板
了解群集架构	高级用户的基本索引器群集概念

调整 Splunk Enterprise 规模

*分布式部署手册*介绍如何跨多个组件（例如，转发器、索引器和搜索头）来分布 Splunk Enterprise 功能。

任务：	查看此处：
了解 Splunk Enterprise 分布式部署	使用 Splunk Enterprise 组件调整您的部署规模
针对 Splunk 部署执行容量规划	Splunk Enterprise 容量规划简介
了解如何转发数据	关于转发和接收
跨多个索引器进行分布式搜索	关于分布式搜索
在您的环境中部署配置更新	关于部署服务器和转发器管理

关联手册详细介绍分布式组件：

- 有关转发器的信息，请参阅*转发数据*手册。
- 有关搜索头的信息，请参阅*分布式搜索*手册。
- 要使用部署服务器和转发器管理管理部署，请参阅*更新 Splunk Enterprise 实例*手册。

确保 Splunk Enterprise 安全

*确保 Splunk 安全*介绍如何确保您的 Splunk Enterprise 部署的安全。

任务：	查看此处：
验证用户和编辑角色	关于用户验证
使用 SSL 确保 Splunk 数据安全	关于确保 Splunk Web 安全
审计 Splunk Enterprise	使用 Splunk Enterprise 审计您的系统活动 审计 Splunk 活动 使用审计事件确保 Splunk Enterprise 安全 管理数据完整性
将单一登录 (SSO) 与 Splunk Enterprise 配合使用	关于使用反向代理进行单点登录
将 Splunk Enterprise 与 LDAP 配合使用	设置使用 LDAP 进行的用户验证

搜索和报告

搜索和报告应用允许您搜索数据、新建数据模型和数据透视表、将您的搜索和数据透视表保存为报告、配置告警并新建仪表板。默认提供此应用。

搜索

*搜索手册*介绍了如何搜索和使用**搜索处理语言 (SPL)**。请参阅*搜索引用*查看各搜索命令的语法、说明和示例。

任务：	查看此处：
了解如何搜索和使用搜索处理语言	关于本搜索教程
了解有关搜索处理语言的更多信息	搜索入门 关于搜索语言 了解 SPL 语法 有关转换命令和搜索 关于实时搜索和报表
查找特定搜索命令或功能	命令快速参考 命令分类 评估函数 统计和图表函数

管理搜索任务	关于任务和任务管理 查看搜索任务属性

新建数据透视表

*知识管理器手册*介绍如何使用数据模型编辑器设计和构建数据模型。*数据透视表手册*介绍如何构建数据透视表表格和图表。

任务：	查看此处：
了解数据模型及其构建方法	关于数据模型
了解更多有关数据透视表和如何使用数据透视表编辑器设计表格和图表	*数据透视表手册*

报表

在*《报告手册》*中查看更多关于报告的信息和报告管理。

任务：	查看此处：
使用搜索命令生成报表	有关转换命令和搜索
了解可视化类型	可视化参考 可视化的数据结构要求
保存搜索或报表为报表	新建和编辑报表
加速报表 了解报表加速要求	加速报表
计划报表	计划报表
将您的报表生成 PDF 格式	生成报表和仪表板的 PDF

告警

参阅*《告警手册》*了解如何新建和分发告警。

任务：	查看此处：
了解告警	告警入门
设置电子邮件通知、RSS 通知或告警脚本	设置告警操作
参阅告警示例	告警示例
参阅最新触发的告警	触发的告警
使用配置文件设置告警	在 savedsearches.conf 中配置告警

新建仪表板和可视化

请参阅**仪表板和可视化**手册了解有关仪表板和可视化工作流和使用 **Splunk Web 框架**的更多信息。

任务：	查看此处：
了解如何新建和编辑仪表板	仪表板概览
了解可视化类型	可视化参考
了解默认活动和摘要仪表板	Splunk Enterprise 摘要仪表板
了解 Splunk Web 框架	Splunk Web 框架概述

管理 Splunk Enterprise 知识

本主题列出了 Splunk 软件知识管理中的常见任务，向您介绍了解和管理知识对象，如事件、字段、查找和数据模型的相关主题。

Splunk Enterprise 知识

请参阅*知识管理器手册*了解有关使用和维护知识对象的更多信息。

任务：	查看此处：
了解 Splunk Enterprise 知识对象	Splunk 知识是什么？ 了解和使用通用信息模型加载项
管理知识对象	监视和组织知识对象 禁用或删除知识对象

事件和事件处理

请参阅*知识管理器手册*了解有关事件的更多信息。有关配置事件处理的更多信息，请参阅*数据导入*手册。

任务：	查看此处：
了解事件和事件类型	关于事件类型 在 Splunk Web 中定义事件类型
配置事件处理	事件处理概述
管理事件分段	关于事件分段

字段和字段提取

请参阅*知识管理器手册*了解有关字段和字段提取的更多信息。

任务：	查看此处：
了解字段	关于字段 使用默认字段 通过 fields.conf 配置多值字段提取 关于已计算字段
了解并管理字段提取	关于字段 当 Splunk 软件提取的字段时 关于 Splunk 正则表达式

构建数据模型

请参阅*知识管理器手册*了解有关数据模型和使用数据模型编辑器的更多信息。

任务：	查看此处：
了解数据模型和数据集	关于数据模型
管理数据模型和数据集	管理数据模型
使用数据模型编辑器	设计数据模型

自定义并扩展 Splunk Enterprise

开发人员可以利用其他工具和应用程序构建 Splunk 应用并集成 Splunk Enterprise。按这些链接操作可帮助您开始。

开发 Splunk 应用

有关 **Splunk Web 框架**的更多信息、代码示例和教程，请参阅 Splunk for Developer 站点。

任务：	查看此处：
使用 Splunk Web 框架	Splunk Web 框架概述
参阅 Splunk Web 框架示例	使用 Splunk Web 框架的代码示例
参阅 Splunk Web 框架组件	Splunk Web 框架组件参考

使用 Splunk REST API

开发人员可以使用 Splunk REST API，以编程方式从任意应用程序中索引、搜索和可视化 Splunk Enterprise 中的数据。

任务：	查看此处：
从 Splunk REST API 开始	Splunk REST API 概述
了解如何使用 Splunk REST API	Rest API 教程
改进日志以使用 Splunk	登录概述 登录最佳实践
参阅 REST API 参考	使用 REST API 参考

下载和安装 Splunk SDK

可在 Splunk for Developer 站点和 Splunk SDK 文档站点中找到有关 Splunk SDK 相关信息。

任务：	查看此处：
了解有关 Splunk SDK 的更多信息	Splunk SDK 概述
参阅 Splunk SDK 代码库和示例。	Splunk SDK

扩展 Splunk Enterprise 功能

扩展搜索语言，以进行自定义处理或计算以及自定义数据导入。

任务：	查看此处：
扩展搜索语言	如何使用适用于 Python 的 Splunk SDK 新建自定义搜索命令 在“设置”中定义搜索宏 配置告警操作的脚本
管理自定义数据输入	脚本式输入概述 模块化输入概述

故障排除

*故障排除手册*介绍了如何利用 Splunk Enterprise 分析活动并诊断问题。特定故障排除相关信息，请参阅该主题相关手册。例如，您可以在*搜索手册*中找到有关如何提高搜索性能的主题。

任务：	查看此处：

了解有关新功能、已知问题和已修复问题的信息	欢迎使用 Splunk Enterprise 已知问题 已修复的问题
了解 Splunk Enterprise 故障排除工具	Splunk Enterprise 故障排除简介 使用 btool 排除配置故障 关于监视控制台
使用平台检测框架	关于 Splunk Enterprise 平台检测
了解 Splunk Enterprise 日志文件	Splunk 软件记录有关自身的哪些内容 有关 metrics.log
排除搜索性能故障	编写更好的搜索 查看搜索任务属性
故障排除许可证违规问题	关于许可证违规 使用“许可证使用情况报表视图”