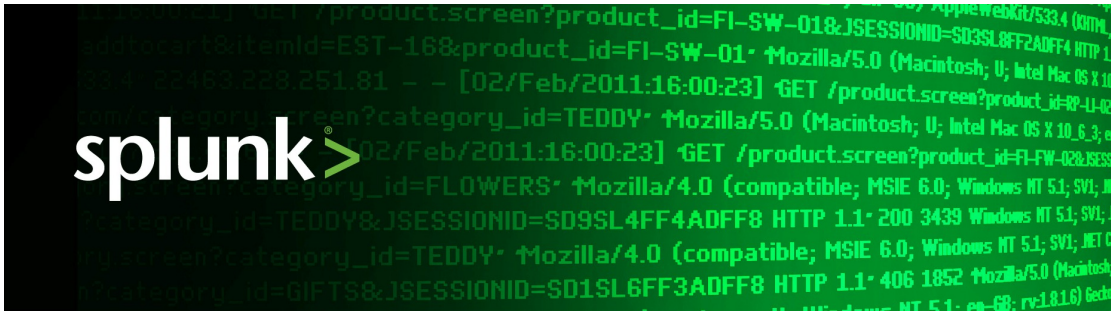

Splunk® Enterprise 6.5.0

Splunk Enterprise 概述

生成时间：2016 年 9 月 26 日，下午 10:27

Table of Contents

简介

本手册包含哪些内容

本手册有两个目的。

- 提供 Splunk Enterprise 及其用户相关的技术概述。讨论功能并描述 Splunk Enterprise 部署的构成组件。
- 提供主题，帮助您基于您希望完成的任务而导航文件。

关于 Splunk Enterprise

关于 Splunk Enterprise

Splunk Enterprise 是什么？

Splunk Enterprise 是搜索、分析和可视化从网站、应用程序、传感器、设备等处收集的、机器生成数据（构成 IT 基础架构或业务）的软件产品。

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。

您可以使用搜索处理语言或交互式数据透视表功能构建报表和可视化。

Splunk Enterprise 功能

下表强调了 Splunk Enterprise 的 7 种功能。您可以在 Splunk.com 上了解更多功能。

功能	描述
索引	Splunk Enterprise 为机器数据建立索引。这包括源于打包的自定义应用程序、应用程序服务器、Web 服务器、数据库、网络、虚拟机、电信设备、操作系统、传感器等的数据流（构成您的 IT 基础架构）。最大索引量取决于 Splunk Enterprise 授权。
数据模型	数据模型是有关一个或多个数据集语义知识的分层结构搜索时间映射。它将编码构建这些数据集的各种专门搜索所需的域知识。这些专门搜索被 Splunk Enterprise 用于为数据透视表用户生成报表。数据模型对象表示 Splunk Enterprise 索引的较大数据组内不同的数据集。
数据透视表	数据透视表指您使用数据透视表编辑器创建的表格、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或图表数据可视化，而不需要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。
搜索	搜索是用户导航 Splunk Enterprise 中数据的主要方式。您可以编写搜索，从索引中检索事件；使用统计命令计算指标并生成报告；在滚动时间窗内搜索特定条件；确定数据中的模式、预测未来趋势等。搜索可以保存为报表并为仪表板面板提供依据。
告警	历史搜索和实时搜索结果满足条件时就会触发告警。可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 源并运行自定义脚本，如将告警事件发布至 syslog 的脚本。
报表	报表为保存的搜索和数据透视表。您可以临时运行报表，计划使其以固定间隔运行，在运行结果满足特殊条件时设置计划报表以生成告警。报表可添加至仪表板作为仪表板面板。
仪表板	仪表板由包含搜索框、字段、图表、表格和表单等模块的面板组成。仪表板面板通常关联到保存的搜索或数据透视表。它们能够显示已完成搜索的结果以及后台运行的来自实时搜索的数据。

下载 Splunk Enterprise 快速参考指南

Splunk Enterprise 快速参考指南（更新至 6.3.0 版本）只能以 PDF 文件格式查阅。它是一个 6 页的参考卡，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创建、标准化和使用情况。 • 将数据导入 Splunk Enterprise，或与管理员一起操作。 • 创建并共享数据模型。
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 基础架构健康状况、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	• 基于知识管理器创建的数据模型，使用数据透视表构建报表。 • 创建报表和仪表板，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

Splunk Enterprise 和您的 IT 基础架构

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。只要生成数据的机器是您网络的一部分，那么 Splunk Enterprise 可以从任何地方的机器中收集数据，无论是本地（企业内部服务器房间）、远程（托管在数据中心），还是完全在云端或两者情况（例如本地和云端）。

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、管理并创建知识对象、运行搜索、创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。

Splunk Enterprise 支持多用户和分布式产品架构。这意味着您可以跨一个数据中心的多个 Splunk Enterprise 部署或全局式跨多个数据中心和云基础结构搜索和报告数据。

Splunk Enterprise 组件

组件	描述
应用	应用是配置、知识对象和客户设计的视图和仪表板的集合，扩展 Splunk Enterprise 环境以适应 Unix 或 Windows 系统管理员、网络安全专家、网站经理、业务分析师等组织团队的特定需求。单个 Splunk Enterprise 安装可以同时运行多个应用。
转发器	转发器是将数据转发至另一个 Splunk Enterprise 实例（索引器或另一个转发器）或至第三方系统的 Splunk Enterprise 实例。大多数转发器都是轻型实例，资源使用率最小，允许其更容易驻留在生成数据的计算机上。
索引器	索引器是用于为数据创建索引的 Splunk Enterprise 实例。它通常从一组转发器接收数据。索引器将数据转换为事件并将事件存储至索引中。索引器还搜索索引数据，以响应搜索请求。 在分布式搜索部署中，您可能有多个索引器，也称为搜索节点。

	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	在分布式搜索部署中，搜索头是处理搜索管理功能、指引搜索请求至一组索引器，然后将结果合并返回至用户的 Splunk Enterprise 实例。在单实例部署中，一个实例既用作搜索头，又用作索引器。 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。

想要了解更多有关这些组件及其在分布式部署中角色的信息，请参阅*《分布式部署手册》*中的"使用 Splunk Enterprise 组件调整您的部署规模"。

Splunk Enterprise 资源和文档

产品资源

本主题概述了文档、教育、社区资源，帮助您查找有关 Splunk Enterprise 和其他 Splunk 产品的信息。

文档

您在查找什么？	您应在哪里查找？
Splunk Enterprise	您需要了解的 Splunk Enterprise 配置和使用相关信息都在 Splunk Enterprise 文档中。以下主题将帮助您查找 Splunk Enterprise 文档中信息。 • Splunk Enterprise 管理 • 搜索和报告： • 管理知识 • 自定义并扩展 Splunk Enterprise • 故障排除
Splunk 产品	Splunk 平台产品包括 Splunk Enterprise、Splunk Cloud 和 Splunk Light。每个 Splunk 产品都有其独自的文档组，可在 Splunk.com 文档站点上查阅。
Splunkbase	每个应用应具备其独自的文档。通常，应用的文档链接自应用的下载页面，或包含在应用的下载软件包中。只有在 Splunk 支持应用的情况下，Splunk 文档站点中才会包含该应用的文档。
Splunk SDK	Splunk SDK 的文档在 Splunk for Developer 站点上。您将在该处查找到有关各个 Splunk SDK 的信息、教程和示例。可以在 Splunk SDK 文档站点中找到模型库和其他参考资料。

教育

您在查找什么？	您应在哪里查找？
Splunk Education	Splunk 课程和证书追踪
如何记录教学视频	Splunk Education 视频

社区

您在查找什么？	您应在哪里查找？
Splunk Answers	如果您在文档中不能查找到您正在寻找的内容，则搜索 Splunk Answers 查看社区内容或在该处询问您的问题。

#splunk	登录至 efnet 上的 IRC 服务器，咨询 Splunk 开发人员、Splunk 支持和其他 Splunk 社区成员。

Splunk Enterprise 管理

本主题列出了有关管理员可能希望实现的任务，并指引您查阅手册和主题了解如何实现相关任务。

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	计划您的安装
预估硬件容量需求	预估硬件需求
安装 Splunk Enterprise	在 Windows 上安装 Splunk Enterprise 在 Unix、Linux 或 MacOS 上安装 Splunk Enterprise
升级 Splunk Enterprise	从早期版本升级
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”为您提供有关 Splunk 数据导入的信息，包括如何使用来自外部来源的数据，以及如何增强您的数据值。

任务：	查看此处：
了解如何使用外部数据	如何将数据导入 Splunk Enterprise
配置文件和目录输入	获取文件和目录的数据
配置网络输入	获取网络事件
配置 Windows 输入	获取 Windows 数据
配置其他输入	其他数据导入方式
增强您的数据值	配置事件处理 配置时间戳 配置索引字段提取 配置主机值 配置来源类型 管理事件分段
查看您的数据在建立索引后的显示效果	“设置 Sourcetype”页面
过程改善	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”告诉您如何配置索引。它还介绍了如何管理维护索引的组件：索引器和索引器群集。

任务：	查看此处：
了解索引	索引概述
管理索引	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	关于群集和索引复制
部署群集	部署群集
配置群集	配置群集

管理群集	管理群集
了解群集架构	群集如何工作

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。关联手册详细介绍分布式组件：

- 《转发数据手册》介绍转发器。
- 《分布式搜索手册》介绍搜索头。
- 《更新 Splunk 组件手册》阐述如何使用部署服务器和转发器管理来管理您的部署。

任务：	查看此处：
了解分布式 Splunk Enterprise	分布式 Splunk Enterprise 概述
针对 Splunk 部署执行容量规划	预估硬件需求
了解如何转发数据	转发数据
跨多个索引器进行分布式搜索	跨多个索引器搜索
更新部署	在您的环境中部署配置更新

确保 Splunk Enterprise 安全

“确保 Splunk 安全”介绍了如何确保您的 Splunk Enterprise 部署的安全。

任务：	查看此处：
验证用户和编辑角色	用户和基于角色的访问控制
使用 SSL 确保 Splunk 数据安全	安全验证和加密
审计 Splunk Enterprise	使用 Splunk Enterprise 审计您的系统活动
将单一登录 (SSO) 与 Splunk Enterprise 配合使用	配置单点登录
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、创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、配置告警并创建仪表板。

搜索：

*《搜索手册》*介绍了如何搜索和使用**搜索处理语言 (SPL)**。参阅*搜索参考*了解带有语法、描述和各命令示例的搜索命令目录。

任务：	查看此处：
您之前未使用过 Splunk Enterprise，希望了解如何搜索和使用搜索处理语言	以搜索教程开始
了解更多有关搜索处理语言	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 搜索命令分类 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

创建数据透视表

*《知识管理器手册》*包含介绍如何使用数据模型编辑器设计和构建数据模型的章节。*《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：
您之前未使用过 Splunk Enterprise，希望了解数据模型和数据透视表	数据透视表教程
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*

报告

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
了解不同类型的可视化（表格、图表、事件列表等）	仪表板和可视化 可视化的数据结构要求
保存搜索或报表为报表	创建和编辑报表
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》*了解如何创建和分发告警。

任务：	查看此处：
了解告警	关于告警
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	使用告警管理器查看触发的告警
使用配置文件设置告警	在 savedsearches.conf 中配置告警

创建仪表板和可视化

任务：	查看此处：
了解如何创建和编辑仪表板	仪表板概览
了解不同类型的可视化（表格、图表、事件列表等）	可视化参考
了解默认活动和摘要仪表板	Splunk 默认仪表板
了解 Splunk Web 框架	Splunk Web 框架概述

管理知识

这些表格指引您查看相关主题，了解并管理事件、字段、查找和数据模型等知识对象。

Splunk Enterprise 知识

任务：	查看此处：
了解 Splunk Enterprise 知识	Splunk Enterprise 知识是什么？ 了解和使用通用信息模型
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

任务：	查看此处：
配置事件处理	配置事件处理
管理事件分段	管理事件分段
了解事件和事件类型	关于事件类型 在 Splunk Web 中定义和维护事件类型

字段和字段提取

任务：	查看此处：
了解字段	关于字段 使用默认字段 配置多值字段 关于已计算字段
了解并管理字段提取	关于字段 当 Splunk Enterprise 提取字段时 关于 Splunk Enterprise 正则表达式

构建数据模型

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	设计数据模型数据集

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

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	Splunk Web 框架代码示例
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
了解如何改进您的日志，以使用 Splunk	登录概述 登录最佳实践
参阅 REST API 参考	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 参考

扩展 Splunk Enterprise 功能

开发人员可以扩展搜索语言，以进行自定义处理或计算以及以编程方式自定义数据输入。

任务：	查看此处：
扩展搜索语言	编写自定义搜索命令 在设置中定义搜索宏 配置脚本式告警
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。您也可以查阅其他手册了解特定信息。例如，您可以在《搜索手册》中查找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	本版本的新功能 本版本已知问题
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 在 Splunk 应用中使用 Splunk
使用平台信息框架	有关平台工具框架
了解 Splunk Enterprise 日志文件	Splunk Enterprise 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