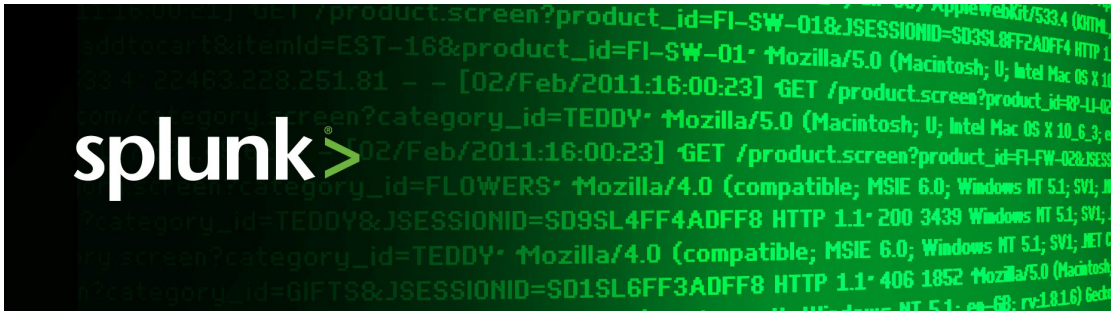

Splunk® Enterprise 7.2.0

添加 Microsoft Windows 数据：单实例

生成时间：2018 年 10 月 17 日，上午 11:20

Table of Contents

安装和配置

Microsoft Windows Guided Data Onboarding 手册：单实例

Guided Data Onboarding 文档假设您熟悉 Splunk 软件。如果您不知道如何使用 Splunk Enterprise 或不了解 Splunk Cloud，请参阅本手册中的*额外资源*主题。

以下为 Guided Data Onboarding 手册的前提条件。

- 已安装并正在运行的 Splunk Enterprise 单实例部署。
- Splunk Web 的访问权限。
- 允许应用安装的用户角色。

在 Splunk Enterprise 单实例部署上启用接收器

要将数据来源中的数据导入 Splunk Enterprise 实例，您必须同时配置**接收器**和**转发器**。接收器是一个 Splunk Enterprise 实例。您可在数据主机上安装转发器以将数据发送到接收器。

使用 Splunk Web 启用接收器

1. 以管理员身份登录接收器。
2. 单击**设置 > 转发和接收**。
3. 在**配置接收**处，单击**新增**。
4. 您可以使用 `netstat` 工具确定系统上可用的端口。确保 Splunk Web 或 Splunkd 没有使用您选择的端口。
5. 指定您想要用作**接收端口**的 TCP 端口。您可以指定任何未使用端口。
6. 单击**保存**。Splunk 软件开始在您指定的端口处接收传入的数据。
7. 重新启动 Splunk 软件。

启用 Windows 数据集合

使用适用于 Microsoft Windows 的 Splunk 加载项收集 Windows 事件日志。

配置 Windows 以启用数据集合

要使用适用于 Microsoft Windows 的 Splunk 加载项收集 Windows 事件日志，请配置 Windows 环境以收集数据：

1. 使用您希望通用转发器以其身份运行的用户新建和配置安全组。您可选择配置通用转发器帐户为托管式服务帐户。
2. 在通用转发器上，针对安全策略和用户权限分配新建和配置组政策对象 (GPO)。分配适当用户权限给 GPO。
3. 使用更新的设置部署 GPO 至适当对象。
4. Microsoft 启用用户帐户的用户权限和特权管理。如需更多信息，请参阅 Microsoft 文档的*配置用户权限*主题。

安装 Splunk 通用转发器

要将数据转发到 Splunk Enterprise 部署中，请完成以下步骤在远程 Windows 主机上安装通用转发器：

1. 下载 Splunk 通用转发器。
2. 双击 MSI 文件开始安装。
3. 单击**查看许可协议**。
4. 勾选**勾选此框以接受许可协议**复选框。
5. 要更改任何默认安装设置，单击**自定义选项**。
6. 单击**安装**按钮进行软件的默认安装。
7. （可选）在**接收索引器**窗格中，输入通用转发器应将数据发送至的接收索引器的主机名称或 IP 地址和接收端口，然后单击**下一步**。
8. 单击**安装**。安装程序将运行并显示“安装完成”对话框。通用转发器自动启动。
9. 在**控制面板**中，确认 `SplunkForwarder` 服务正在运行。

在通用转发器上安装适用于 Windows 的 Splunk 加载项

1. 从 Splunkbase 下载适用于 Windows 的 Splunk 加载项。
2. 解压缩 .tgz 软件包。
3. 将产生的 `Splunk_TA_<add-on_name>` 文件夹放入转发器上的 `$SPLUNK_HOME/etc/apps` 目录中。
4. 重新启动通用转发器。

安装适用于 Windows 的 Splunk 加载项

您可从 Splunkbase 下载适用于 Windows 的 Splunk 加载项。

1. 下载加载项。
2. 在 Splunk Web 主屏幕中，单击**应用**旁边的齿轮图标。
3. 单击**通过文件安装应用**。
4. 查找已下载的文件并单击**上载**。
5. 如收到重启提示，则重新启动 Splunk Enterprise。

要验证安装是否成功，请检查适用于 Microsoft Windows 的 Splunk 加载项是否在目录中显示：`$SPLUNK_HOME/etc/apps/Splunk_TA_windows`。

配置适用于 Windows 的 Splunk 加载项收集数据

1. 使用文本编辑器，打开本地目录 `%SPLUNK_HOME%\etc\apps\Splunk_TA_Windows\local\inputs.conf` 中的 `inputs.conf`。如果 `inputs.conf` 文件不存在，则在本地目录中新建该文件。
2. 启用加载项应通过将这些属性段落的禁用属性设为 0 收集数据的输入。
3. 保存文件并将其关闭。
4. 将 `%SPLUNK_HOME%\etc\apps` 中的 `Splunk_TA_windows` 目录的内容复制到任何其他转发器。

配置 Splunk 实例以接收数据

通过配置 `$SPLUNK_HOME/etc/system/local` 中的 `inputs.conf` 启用接收。如果此文件不存在，请新建文件。

1.在每个索引器上，打开 `$SPLUNK_HOME/etc/system/local` 中的 `inputs.conf`。

2.添加指定接收端口的 [splunktcp] 段落。在本例中，接收端口如下所示：

```
9997: [splunktcp://9997]
disabled = 0
```

3.重新启动 Splunk 软件使更改生效。

验证数据

运行 Splunk 软件的 `search` 字段中的以下搜索 `sourcetype="WinEventLog*"` 验证 Microsoft Windows 数据是否在部署中显示。

额外资源

额外资源

以下部分提供了额外信息和链接。

关于 Guided Data Onboarding

同时使用 Splunk Web 和 Splunk 文档，Guided Data Onboarding (GDO) 提供端对端指导，以便将特定数据来源导入特定的 Splunk 平台部署。如果您已启动 Splunk 部署并正在运行，并且您具有可以安装加载项的管理员角色或同等角色，您可使用这些指南将热门数据来源导入 Splunk。

查找 Guided Data Onboarding 的位置

从 Splunk Web 主页面中，可通过单击**添加数据**查找数据导入指南。然后，您可以搜索数据来源或浏览不同的数据来源类别。目前，分类有**网络**、**操作系统**和**安全**。

选择数据来源后，您必须选择部署方案。这样您可查看方案和高级步骤来设置和配置数据来源。

Splunk Web 链接到更详细说明如何设置和配置数据来源的文档。您可单击 Splunk Enterprise 文档站点上的**添加数据**选项卡查找所有 Guided Data Onboarding 手册。

支持的部署方案

对于每个数据来源，目前有三种 Splunk 部署方案支持 Guided Data Onboarding。请参阅下表查看每种方案的说明：

部署方案	描述
单实例 部署	Splunk Enterprise 单实例可处理**索引**和**搜索管理**。在此部署方案中，您通常还可以在生成数据的主机上安装**转发器**以向单实例提供主机数据。
分布式部署 索引器群集化	在分布式部署中，多个 Splunk Enterprise **实例**协同工作，以支持数据来自多台计算机的环境，或很多用户需要搜索数据的环境。索引器群集化是一种 Splunk Enterprise 功能，通过此功能**索引器群集**可复制数据以实现若干目标。包括数据可用性、数据保真度、灾难容错和改进的搜索性能。
Splunk Cloud	Splunk Cloud 作为基于云的托管式服务提供 Splunk Enterprise 优势。

如果您确定部署时需要帮助，请参阅*继承 Splunk Enterprise 部署*手册。

支持的数据来源

目前以下几种数据来源支持 Guided Data Onboarding：

数据来源	描述
Cisco ASA	允许管理员将 Cisco ASA 设备、Cisco PIX 和 Cisco FWSM 事件映射到 Splunk **CIM**。 我们可为以下部署方案提供 Guided Data Onboarding： • 单实例 • 具有索引器群集化功能的分布式部署 • 托管式 Cloud 您还可参阅*适用于 Cisco ASA 的 Splunk 加载项*手册了解更多。
McAfee ePO	允许管理员收集防病毒信息和漏洞扫描报告。 我们可为以下部署方案提供 Guided Data Onboarding： • 单实例 • 具有索引器群集化功能的分布式部署 • Splunk Cloud 您还可参阅*适用于 McAfee 的 Splunk 加载项*手册了解更多。

Microsoft Active Directory	允许管理员从 Windows 主机收集 Active Directory 和域名服务器调试日志，这些主机用作受支持的 Windows 服务器版本的域控制器。 我们可为以下部署方案提供 Guided Data Onboarding： • 单实例 • 具有索引器群集化功能的分布式部署 • Splunk Cloud 您还可参阅*适用于 Microsoft Active Directory 的 Splunk 加载项*手册了解更多。
Microsoft Windows	允许管理员通过数据导入收集 CPU、磁盘、I/O、内存、日志、配置和用户数据。 我们可为以下部署方案提供 Guided Data Onboarding： • 单实例 • 具有索引器群集化功能的分布式部署 • Splunk Cloud 您还可参阅*适用于 Windows 的 Splunk 加载项*手册了解更多。
Palo Alto Networks	允许管理员收集 Palo Alto Networks Next-generation Security Platform 中每个产品的数据。 我们可为以下部署方案提供 Guided Data Onboarding： • 单实例 • 具有索引器群集化功能的分布式部署 • Splunk Cloud 您还可访问 splunk.paloaltonetworks.com 了解更多。
Symantec Endpoint Protection	允许管理员通过 dump 文件收集 Symantec Endpoint Protection Manager 中的日志。 我们可为以下部署方案提供 Guided Data Onboarding： • 单实例 • 具有索引器群集化功能的分布式部署 • Splunk Cloud 您还可参阅*适用于 Symantec Endpoint Protection 的 Splunk 加载项*手册了解更多。

关闭 Guided Data Onboarding

如果您不想要在 Splunk Web 中显示 Guided Data Onboarding 功能，请前往 `$SPLUNK_HOME/etc/apps/splunk_gdi/default/gdi_settings.conf` 文件将 `allowWebService` 变量设为 false。

Splunk 文档

Splunk 文档类型多样，包括教程、使用案例、管理员、开发人员和用户手册。

- 要获取 Splunk Enterprise 软件的深入介绍，请参阅 *Splunk Enterprise 概览*手册。
- 更多有关 Splunk Cloud 的更多信息，请参阅 *Splunk Enterprise 用户*手册。
- 如果您是一名继承了 Splunk Enterprise 部署的系统管理员，或者您不确定您拥有哪种类型的部署方案，请参阅*继承 Splunk Enterprise 部署*手册。
- 有关将数据的导入 Splunk 软件的更多信息，请参阅*数据导入*手册。
- 有关安装加载项的更多信息，请参阅 *Splunk 加载项*手册。

您可以在 Splunk 文档站点中找到其他信息。

Splunk 社区

通过 Splunk Answers、Slack、用户组和日志，您可以找到要聊天的其他用户。在社区门户上查找您和 Splunk 社区联系所需的所有内容。

Splunk Education

要了解更多 Splunk 功能和使用方法，请参阅 Splunk Education 视频和课程系列。