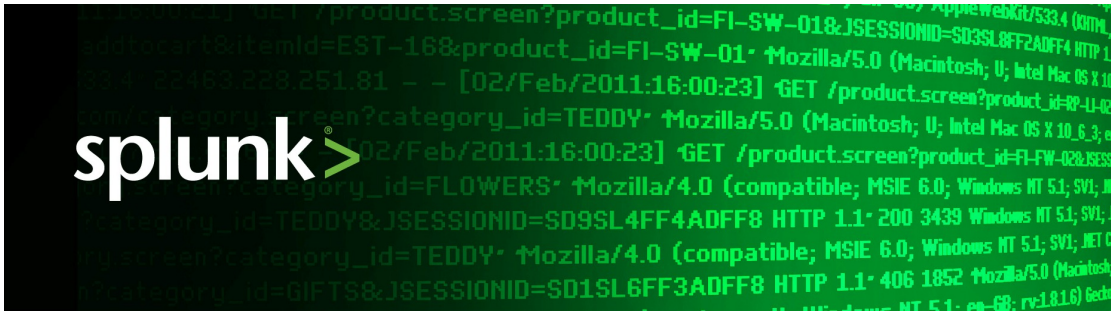

Splunk® Enterprise 7.2.0

添加 Symantec Endpoint Protection 数据：托管式 Cloud

生成时间：2018 年 10 月 17 日，上午 11:21

Table of Contents

添加 Symantec Endpoint Protection 数据

Symantec Endpoint Protection Guided Data Onboarding 手册：托管式 Splunk Cloud

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托管式 Splunk Cloud 部署。
- Splunk Web 的访问权限。
- 允许应用安装的用户角色。

在 Symantec Endpoint Protection 实例上安装重型转发器

要将数据转发到托管式 Splunk Cloud 实例中，请在 Symantec Endpoint Protection 主机上安装 Splunk 重型转发器。

要使用 Linux 安装重型转发器并将其连接到 Splunk Cloud 部署，请执行以下步骤：

1. 下载并安装完整 Splunk Enterprise 实例。
2. 启用 Splunk Enterprise 实例作为重型转发器。

为 Linux 安装并配置重型转发器

下载 Linux 版的 Splunk Enterprise。

要在重型转发器上安装 Splunk Enterprise，请遵循以下步骤：

1. 将 Splunk Enterprise 文件解压到正确的目录：
   ```
   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
   ```
2. 命令行窗口提醒您新建管理员密码。收到提示后，键入密码。首次登录 Splunk Enterprise 需要此密码。
   ```
   This appears to be your first time running this version of Splunk.

   An Admin password must be set before installation proceeds.
   ```

设置重型转发

根据前面的步骤，您应该已在即将转发数据的实例中以 `admin` 的身份登录 Splunk Web。

1. 必要时，以 `admin` 身份登录会转发数据的 Splunk Web 实例。
2. 单击**设置** > **转发和接收**。
3. 在**配置转发**处，单击**新增**。
4. 输入 Splunk 接收实例的主机名称或 IP 地址，以及配置接收器时指定的**接收端口**。例如，您可以输入 `receivingserver.com:9997`。
5. 单击**保存**。
6. 重新启动 Splunk Web。

配置重型转发器以索引和转发数据

使用重型转发器本地索引数据然后将数据转发到另一个实例。

1. 以 `admin` 身份登录会转发数据的 Splunk Web 实例。
2. 单击**设置** > **转发和接收**。
3. 选择**转发默认。**
4. 选择**是**存储并保留已索引数据的本地副本到转发器。

为 Microsoft Windows 安装并配置重型转发器

要使用 Microsoft Windows 安装重型转发器并将其连接到 Splunk 部署，请执行以下步骤：

1. 启用接收器。
2. 在数据来源主机上下载并安装 Splunk Enterprise 实例。

3. 在 Splunk Enterprise 实例上启用转发。

使用 Splunk Web 启用接收器

1. 以管理员用户或等同的管理身份登录您想要用作接收器的实例。
2. 在系统栏中，单击**设置 > 转发和接收**。
3. 在**配置接收**处，单击**新增**。
4. 指定您想要接收器侦听的 TCP 网络端口。这是**侦听端口**，也就是**接收端口**。
5. 单击**保存**。
6. 重新启动 Splunk 软件使更改生效。

使用配置文件设置接收

通过配置 `inputs.conf` 配置文件在 Splunk Enterprise 实例上启用接收。`inputs.conf` 必须驻留在 `%SPLUNK_HOME%/etc/system/local` 目录中。如果文件不存在，则需要新建。

1. 使用文本编辑器，打开 `inputs.conf`（位于 `%SPLUNK_HOME%\etc\system\local`）。
2. 要启用接收，添加指定接收端口的 `[splunktcp]` 段落。在本例中，接收端口是 9997：

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

3. 重新启动 Splunk 软件使更改生效。

表单 `[splunktcp://9997]` 和 `[splunktcp://:9997]`（有一个或两个冒号）等效。

在重型转发器上下载并安装 Splunk Enterprise 实例。

1. 下载 Windows 版的 Splunk Enterprise。
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. 勾选**勾选此框以接受许可协议**。这样就能激活**自定义安装**和**安装**按钮。
4. 选择安装选项。以默认设置选择 nstall：
   - 在系统驱动器（启动 Windows 系统的驱动器）上的 `\Program Files\Splunk` 中安装 Splunk Enterprise。
   - 安装 Splunk Enterprise 到默认管理和 Web 端口上。
   - 以“本地系统”用户身份配置 Splunk Enterprise。
   - 为软件新建“开始菜单”快捷方式。
5. 单击**安装**继续。

通过命令行界面 (CLI) 在 Windows 上安装

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

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
- 要启用的 Splunk 附带的应用程序配置
- Splunk Enterprise 是否应在安装完成后自动启动

使用 Splunk Web 启用 Splunk Enterprise 实例作为重型转发器

1. 以管理员身份登录要转发数据的 Splunk Web 实例。
2. 在系统栏中，单击**设置 > 转发和接收**。
3. 在**配置转发**处，单击**新增**。
4. 输入 Splunk 接收实例的主机名或 IP 地址，以及配置接收器时指定的**接收端口**。
5. 单击**保存**。
6. 重新启动。

配置重型转发器以索引和转发数据

- 以管理员身份登录 Splunk Web，在此实例中将转发数据。

- 单击**设置 > 转发和接收**。
- 选择**转发默认。**
- 选择**是**存储并保留已索引数据的本地副本到转发器。
必须在 `outputs.conf.` 中完成所有其他配置

使用 CLI 设置重型转发

使用 CLI 按如下步骤在 Splunk Enterprise 实例上启用转发，然后配置转发到指定的接收器。

1. 在您想要转发数据的计算机上，打开命令提示符或 PowerShell 窗口。
2. 从命令提示符或 PowerShell 窗口导航到 `%SPLUNK_HOME%\bin`。
3. 键入以下内容以启用转发：`msiexec.exe /i Splunk.msi SPLUNK_APP="SplunkForwarder" FORWARD_SERVER="<server:port>"`
4. 重新启动 Splunk Enterprise。

在托管式 Splunk Cloud 部署上安装适用于 Symantec Endpoint Protection 的 Splunk 加载项

要在托管式 Splunk Cloud 部署上安装适用于 Symantec Endpoint Protection 的 Splunk 加载项，请完成以下步骤：

使用“支持”在托管式 Splunk Cloud 部署中的搜索头和索引器上安装加载项

使用自助式应用安装流程在托管式 Splunk Cloud 部署中的搜索头和索引器上安装加载项：

1. 从 Splunk Web 主页，单击“应用”齿轮图标。
2. 单击**安装应用**。

如果没有列出您想要的加载项，或者加载项表示不支持自助式安装，请直接联系 Splunk 支持或在 Splunk 支持门户上提交案例。

在转发器上安装适用于 Symantec Endpoint Protection 的 Splunk 加载项

在 Splunk Cloud 部署的转发器上安装适用于 Symantec Endpoint Protection 的 Splunk 加载项。

在分布式 Splunk 平台部署中准备要安装的加载项安装包

在部署加载项之前，请对加载项安装包做出如下更改：

- 移除 `eventgen.conf` 文件。
- 移除 `samples` 文件夹中的所有文件。
- 移除 `inputs.conf` 文件。
- 移除 `inputs.conf.spec` 文件。

1. 从 Splunkbase 下载加载项。
2. 解压加载项。
3. 将产生的 `Splunk_TA_<add-on_name>` 文件夹放入重型转发器上的 `$SPLUNK_HOME/etc/apps` 目录中。
4. 重新启动重型转发器 `splunk restart`。

在重型转发器主机上安装 Splunk Enterprise

1. 下载 Windows（如支持）或 Linux 版的 Splunk Enterprise。
2. 要启动安装程序，请双击软件包文件。安装程序运行并显示 **Splunk Enterprise 安装程序**面板。
3. 勾选“勾选此框以接受许可协议”复选框。这样就能激活**自定义安装**和**安装**按钮。
4. 如果您希望查看许可证协议，单击**查看许可证协议**。
5. 以默认安装设置进行安装，然后单击**安装**进行安装。

启用 Splunk Enterprise 实例作为重型转发器

1. 以 `admin` 身份登录 Splunk Web 重型转发器。
2. 在系统栏中，单击**设置 > 转发和接收**。
3. 单击**新增**配置转发。
4. 输入 Splunk 接收实例的主机名或 IP 地址，以及配置接收器时指定的**接收端口**。
5. 单击**保存**。
6. 重新启动 Splunk Enterprise 实例。
7. 在会转发数据的实例上以管理员身份登录 Splunk Web。
8. 单击**设置 > 转发和接收**。
9. 选择**转发默认。**
10. 选择**是**存储并保留已索引数据的本地副本到转发器。

配置 Symantec Endpoint Protection Manager 导出日志数据

访问 Symantec Endpoint Protection Manager 控制台并按照 Symantec 文档说明将日志数据导出到 dump 文件中。

为适用于 Symantec Endpoint Protection 的 Splunk 加载项配置监视器输入

适用于 Symantec Endpoint Protection 的 Splunk 加载项会监视 Symantec Endpoint Manager 产生的本地 dump 文件。使用部署服务器配置部署转发器上的输入。

要配置此输入，请在运行 Symantec Endpoint Manager 的计算机上安装通用转发器。您还必须知道 Symantec Endpoint Manager dump 文件的路径。

您可使用配置文件或 Splunk Web 配置监视器输入。

使用配置文件配置监视器输入

1. 在数据集合节点上，打开或新建 `%SPLUNK_HOME%\etc\apps\Splunk_TA_symantec-ep\local\inputs.conf` 文件。
2. 不需要删除文件中的任何内容，将以下段落粘贴到文件底部：

```
[monitor://<<path_to_temp_dump_file_directory>>\scm_admin.tmp]
sourcetype = symantec:ep:admin:file
disabled = false

[monitor://<<path_to_temp_dump_file_directory>>\agt_behavior.tmp]
sourcetype = symantec:ep:behavior:file
disabled = false

[monitor://<<path_to_temp_dump_file_directory>>\scm_agent_act.tmp]
sourcetype = symantec:ep:agent:file
disabled = false

[monitor://<<path_to_temp_dump_file_directory>>\scm_policy.tmp]
sourcetype = symantec:ep:policy:file
disabled = false

[monitor://<<path_to_temp_dump_file_directory>>\scm_system.tmp]
sourcetype = symantec:ep:scm_system:file
disabled = false

[monitor://<<path_to_temp_dump_file_directory>>\agt_packet.tmp]
sourcetype = symantec:ep:packet:file
disabled = false

[monitor://<<path_to_temp_dump_file_directory>>\agt_proactive.tmp]
sourcetype = symantec:ep:proactive:file
disabled = false

[monitor://<<path_to_temp_dump_file_directory>>\agt_risk.tmp]
sourcetype = symantec:ep:risk:file
disabled = false

[monitor://<<path_to_temp_dump_file_directory>>\agt_scan.tmp]
sourcetype = symantec:ep:scan:file
disabled = false

[monitor://<<path_to_temp_dump_file_directory>>\agt_security.tmp]
sourcetype = symantec:ep:security:file
disabled = false

[monitor://<<path_to_temp_dump_file_directory>>\agt_system.tmp]
sourcetype = symantec:ep:agt_system:file
disabled = false

[monitor://<<path_to_temp_dump_file_directory>>\agt_traffic.tmp]
sourcetype = symantec:ep:traffic:file
disabled = false
```

3. 在每个段落中，用 *.tmp dump 文件的路径替换 `<<path_to_temp_dump_file_directory>>`。默认目录是 `%SEPM_HOME%\data\dump`，但是路径可能不同。

4. 保存文件。
5. 重新启动数据集合节点。
6. 运行以下搜索检查您是否正在引入期望的数据：

```
sourcetype = symantec:ep
```

使用 Splunk Web 配置监视输入

1. 在数据集合节点上，前往**设置 > 数据输入 > 文件和目录**。
2. 单击**新建**。
3. 单击**浏览**并导航到您想要监视的第一个日志文件。请参阅“适用于 Symantec Endpoint Protection 的 Splunk 加载项的来源类型”查看完整的日志文件列表。
4. 单击**下一步**。
5. 在“输入设置”页面，单击“来源类型”旁边的**选择**。
6. 在“选择来源类型”下拉菜单中，选择**网络和安全**类别，然后针对此日志文件选择对应的来源类型。
7. 单击**查看**查看输入配置。
8. 单击**提交**。
9. 为您想要监视的每个其他 dump 文件重复以上步骤。
10. 运行以下搜索检查您是否正在引入期望的数据：

```
sourcetype = symantec:ep
```

为适用于 Symantec Endpoint Protection 的 Splunk 加载项查找文件启用自动更新

Symantec 在其网站上保留了最新的安全威胁列表。适用于 Symantec Endpoint Protection 的 Splunk 加载项会定期轮询此网站，用最新的列表来更新恶意软件类别。要为恶意软件类别查找文件 `symantec_ep_malware_categories.csv` 启用自动更新，请按以下步骤安装并配置加载项：

1. 在 Splunk Cloud 主屏幕中，单击**应用**旁边的齿轮符号。
2. 在适用于 Symantec Endpoint Protection 的 Splunk 加载项一行中，单击**设置**。
3. 选择启用 Splunk 软件，这样软件可用 Symantec 提供的常见威胁和风险列表自动更新恶意软件类型查找。
4. 必要时调整轮询间隔（以秒为单位）。
5. 如果您正在使用代理，勾选**启用代理**，然后填写字段。当您保存此页面时，Splunk 平台会对代理用户名和密码进行加密。
6. 如果您已勾选**启用代理**，当您想要通过代理执行 DNS 解析时，请勾选**使用代理进行 DNS 解析**框。
7. 如果您已勾选**启用代理**，在**代理类型**字段中选择要使用的代理类型。
8. 单击**保存**以保存配置。

验证数据

运行 Splunk 软件的 `search` 字段中的以下搜索验证 Symantec Endpoint Protection 数据是否在 Splunk Enterprise 部署中显示：

```
sourcetype = symantec:ep
```

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。