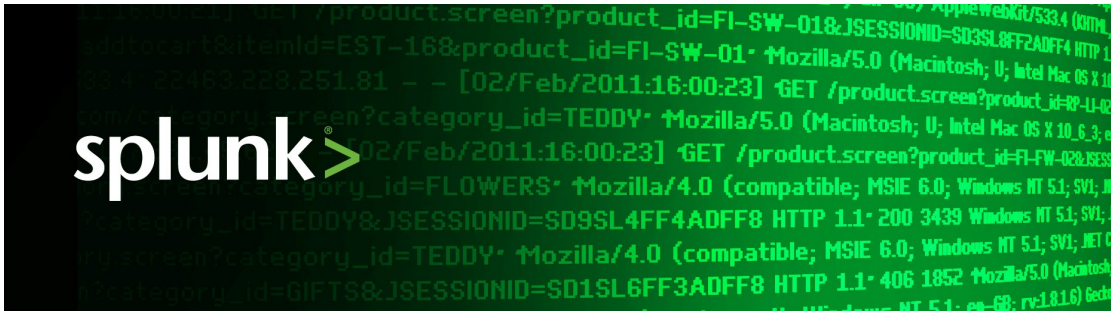

Splunk® Enterprise 7.2.0

添加 Symantec Endpoint Protection 数据：具有索引器群集化功能的分布式部署

生成时间：2018 年 10 月 17 日，上午 11:21

Table of Contents

安装和配置

Symantec Endpoint Protection Guided Data Onboarding 手册：具有索引器群集化功能的分布式部署

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。

- 具有索引器群集化功能的分布式 Splunk Enterprise 部署已启用。
- Splunk Web 的访问权限。
- 允许应用安装的用户角色。

在 Symantec Endpoint Protection 实例上安装和配置通用转发器

要将数据转发到 Splunk 部署中，请在 Symantec Endpoint Protection 主机上安装 Splunk **通用转发器**。

在 Windows 上安装通用转发器

在 Windows 上安装通用转发器，如下所示：

- 在系统驱动器（启动您 Windows 主机的驱动器）上的 `\Program Files\SplunkUniversalForwarder` 中安装通用转发器。
- 使用 TCP/8089 的默认管理端口安装通用转发器。
- 以“本地系统”用户身份配置通用转发器。
- 新建 Splunk 管理员密码。
- 启用“应用程序、系统和 Windows 安全事件日志”数据导入。

以默认选项在 Window 上安装转发器

1. 从 splunk.com 下载通用转发器。
2. 双击 MSI 文件开始安装。
3. 要查看许可协议，单击**查看许可协议**按钮。
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”按钮。或者，单击**安装**按钮进行软件的默认安装。

   以下有两个步骤，至少执行其中一个步骤。否则，通用转发器无法将数据发送到任何地方：

6. （可选）在**部署服务器**窗格中，输入通用转发器应连接的部署服务器的主机名称或 IP 地址和管理端口，并单击**下一步**。
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，并单击**下一步**。
8. 单击**安装**以继续。

   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。

用自定义选项安装

如果您在通用转发器设置对话框中选择了自定义选项，安装程序会显示以下选项：

1. （可选）单击**更改**指定其他安装目录。
2. （可选）选择 SSL 证书以验证本计算机的身份。根据证书要求不同，您可能需要指定密码和根证书颁发机构 (CA) 证书，以验证证书身份。或者，将这些字段留空。
3. 勾选**本地系统**或**域帐户**复选框，并单击**下一步**。如果指定的是本地系统，安装程序会显示**启用 Windows 输入**对话框。如果指定的是域帐户，安装程序会显示第二个对话框供您输入域和用户信息。
4. 如果勾选的是“域帐户”，安装程序会显示一个对话框让您输入用户名和密码凭据。在**用户名**和**密码**字段输入用户名和密码。仅以 `domain\username` 格式指定用户名。
5. 在**确认密码**字段再次输入密码。
6. 要将您指定的域用户添加到本地管理员组中，勾选**将用户添加为本地管理员**，并单击**下一步**。随后，安装程序会将您指定的域用户添加到本地管理员组。
7. （可选）从列表选择一个或多个 Windows 输入，并单击**下一步**。
8. 为 Splunk `admin` 用户新建密码，然后单击**下一步**。
9. （可选）输入您的部署服务器的主机名称或 IP 地址和管理端口，并单击**下一步**。
10. （可选）输入主机名称或 IP 地址和**接收端口**，并单击**下一步**。

11. 单击**安装**。

在安装程序中启用数据导入的注意事项

如果在安装通用转发器时启用了**启用输入**对话框中的数据导入，安装程序也会安装适用于 Windows 的 Splunk 加载项。安装程序会将启用这些输入的配置保存到加载项中。此配置包括索引定义。

这表示此转发器发送数据至其中的接收索引器必须具有以下定义的索引：

- `perfmon` ，用于“性能监视”输入。
- `windows` ，用于一般的 Windows 输入。
- `wineventlog` ，用于“Windows 事件日志”输入。

默认情况下，索引器未定义这些索引。在安装通用转发器之前定义索引，或在索引器上安装适用于 Windows 的 Splunk 加载项。

有关通用转发器附带的 Windows 第三方二进制文件的相关信息

有关 Windows 版通用转发器提供的 Windows 第三方二进制文件的信息，请参阅 Splunk Enterprise *安装手册*中的*有关随 Splunk Enterprise 分布的 Windows 第三方二进制文件的信息*主题。

使用 Linux 安装通用转发器

要使用 Linux 安装**通用转发器**并将其连接到 Splunk 平台部署，请执行以下步骤：

1. 下载适用于 Linux 的 Splunk 通用转发器。
2. 安装通用转发器。
3. 启动通用转发器。
4. 配置通用转发器。
5. 在 Splunk Web 中启用转发器管理。

下载通用转发器

1. 下载 Splunk 通用转发器。
2. 选择适用于操作系统的平台安装包。
3. 单击**立即下载**。
4. 阅读并同意 **Splunk 软件许可协议**。
5. 单击**立即开始下载**。
6. 将下载包移动到您想要安装通用转发器的目录中。

安装通用转发器

在包含或可访问您想要收集并转发到 Splunk Enterprise 实例的数据的计算机上安装通用转发器。要在其他计算机上安装通用转发器，在执行此任务之前将通用转发器安装包文件复制到该计算机上。通用转发器默认安装到 `splunkforwarder` 目录。

要安装到特定目录，请将目录更改为您想要安装转发器的目录，或在运行 `tar` 命令前将 tar 文件放到该目录。

- 用 `tar` 命令将 tar 文件解压缩到相应的目录。默认安装位置是当前工作目录中的 `splunk`：

```
tar xvzf splunkforwarder-<…>-Linux-x86_64.tgz
```

- 要安装到 `/opt/splunkforwarder`，请运行以下命令：

```
tar xvzf splunkforwarder-<…>-Linux-x86_64.tgz -C /opt
```

启动通用转发器

启动通用转发器，这样可获取配置并转发数据。

1. 启动通用转发器：

   ```
   cd $SPLUNK_HOME/bin ./splunk start
   ```

   第一次启动转发器时，会提示您新建管理员密码：

   ```
   This appears to be your first time running this version of Splunk.

   An Admin password must be set before installation proceeds.
   Password must contain at least:
   * 8 total printable ASCII character(s).
   Please enter a new password:
   ```

2. 转发器会显示许可协议。要想不查看许可协议就接受许可协议，请运行以下命令：
   ```
   cd $SPLUNK_HOME/bin ./splunk start --accept-license
   ```
3. 要确认转发器是否正在运行，请运行 `status` 命令：
   ```
   $SPLUNK_HOME/bin ./splunk status
   ```
4. 重新启动通用转发器：
   ```
   cd $SPLUNK_HOME/bin ./splunk restart
   ```

配置通用转发器使其连接到接收端口

在转发器上，从 shell 或命令提示符运行以下命令：

```
./splunk add forward-server <host name or ip address>:<listening port>
```

例如，要连接到主机名为 `idx.mycompany.com` 的接收器且该主机侦听转发器的 9997 端口，则键入此命令：

```
./splunk add forward-server idx1.mycompany.com:9997
```

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

您可从 Splunkbase 下载适用于 Symantec Endpoint Protection 的 Splunk 加载项。

要在分布式 Splunk Enterprise 部署中安装适用于通用转发器的加载项，请完成以下步骤：

1. 解压加载项。
2. 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。
3. 重新启动通用转发器：
   - Linux：`./splunk restart`
   - Windows ：`.\splunk restart`

在搜索头上安装适用于 Symantec Endpoint Protection 的 Splunk 加载项

按照以下步骤在搜索头上安装适用于 Symantec Endpoint Protection 的 Splunk 加载项。

准备搜索头

要使用 Symantec 的最新威胁列表自动更新恶意软件类别查找文件，您必须准备搜索头。在搜索头群集成员上执行以下步骤：

1. 移除 `eventgen.conf` 文件和“样本”文件夹中的所有文件。
2. 移除 `inputs.conf` 文件。

在搜索头上安装应用

要安装适用于 SEP 的 Splunk 加载项，请从 Splunkbase 下载加载项。

然后，完成以下步骤：

1. 在 Splunk Web 主屏幕中，单击**应用**旁边的齿轮图标。
2. 单击**通过文件安装应用**。
3. 查找已下载的文件并单击**上载**。
4. 如果 Splunk Enterprise 提示您重新启动，请重新启动。
5. 在 Splunk Web 主屏幕中，单击**应用**旁边的齿轮图标。
6. 查找加载项并单击**编辑属性**。
7. 将**是否可见**更改为**否**。

要验证安装是否成功，请检查该加载项是否位于 `$SPLUNK_HOME/etc/apps/<Splunk_TA_name_of_add-on>`。

在索引器群集上安装适用于 SEP 的 Splunk 加载项

按照这些说明在分布式 Splunk Enterprise 部署中的群集索引器上安装加载项：

您必须使用主节点将加载项部署到对等节点上。不要使用部署服务器或任何第三方部署工具。

修改配置文件

对想要分发到对等节点的文件进行以下编辑：

1. 检查 `indexes.conf` 文件的加载项。对于在加载项特定的 `indexes.conf` 文件中定义的每个索引，设置 `repFactor=auto`，以便能够在所有对等节点之间复制索引。
2. 将加载项放在主节点上的 `master-apps` 目录中。

使用 Splunk Web 验证软件包并检查重新启动

要使用 Splunk Web 验证软件包并检查重新启动，请完成以下步骤：

1. 在 Splunk Web 的主节点上，单击**设置 > 索引器群集化**。
   “主节点”仪表板打开。
2. 单击**编辑 > 配置软件包操作**。
3. 单击**验证并检查重新启动 > 验证并检查重新启动**。
   显示一条表示软件包验证和检查重启是否成功的消息。您可以使用 Splunk Web 或 CLI 将软件包从主节点分发到对等节点。<
   如果验证和检查重新启动失败，则不可将该软件包分发到对等节点。在此情况下，查看软件包详细信息可能有助于您解决问题。请确保配置软件包结构适合分发到对等节点。

使用 Splunk Web 将软件包应用到对等节点。

要将配置软件包应用到对等节点，请完成以下步骤：

1. 在 Splunk Web 的主节点上，单击**设置 > 索引器群集化**。
   显示“主节点”仪表板。
2. 单击**编辑 > 配置软件包操作**。
   配置软件包操作仪表板打开，显示最近成功的软件包推送信息。
3. 单击**推送**。
   在某些情况下，弹出窗口将警告您分发可能启动所有对等节点的重新启动。
4. 单击**推送更改**。
   屏幕将提供有关分发进度的信息。一旦分发完成或终止，屏幕将显示结果。
   - 如果分发成功，在每个对等节点成功验证软件包后，主节点将在必要时协调所有对等节点的滚动重新启动。
   - 如果终止分发，它将显示哪些对等节点无法接收分发。每个对等节点必须成功收到并应用分发。任何不成功的对等节点都无法应用软件包。

   推送成功后，对等节点将使用一组新的配置，这些配置现位于其本地 `$SPLUNK_HOME/etc/slave-apps` 中。

   将这些文件保留在 `$SPLUNK_HOME/etc/slave-apps` 中。

使用 Splunk Web 查看软件包推送的状态

将应用分发到一组对等节点之后，您可使用 Splunk Web 启动和管理每个对等节点。

`apply cluster-bundle` 命令将使用可选标记 `--skip-validation`，以在验证流程出现问题的情况下使用。您应仅在 Splunk 支持的指示并确信软件包有效后使用本标记。不要使用本标记以包围验证流程，除非您知道正在做什么。

您可以在不应用软件包的情况下对其进行验证。如果需要调试一些验证问题，此操作很有用。

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。

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。

使用配置文件配置监视器输入

1. 在 Windows 主机上，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. 重新启动转发器服务。
6. 在 Splunk Web 中，运行以下搜索确保 Splunk 正在引入数据：

```
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. 从搜索头的 Splunk Web 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. 单击“启用 Splunk Enterprise 以使用 Symantec 的最新威胁和风险列表自动更新恶意软件类别查找表”旁边的复选框。
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 Symantec Endpoint Protection 数据

要检查您是否正在引入您想要的数据，请运行以下搜索：

```
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。