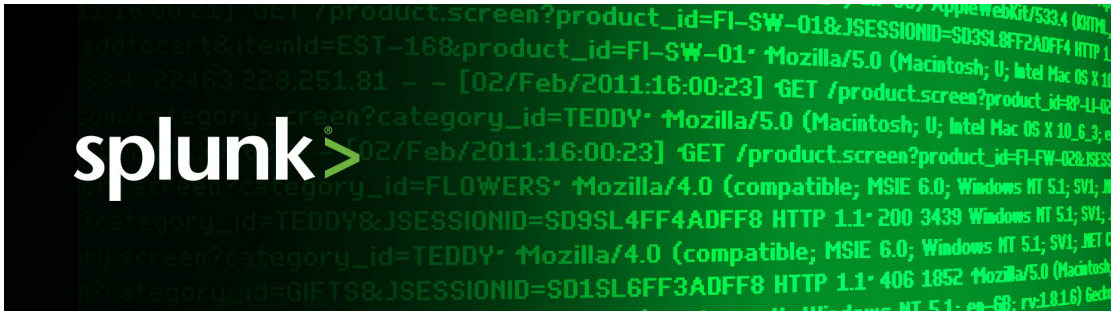

Splunk® Enterprise 7.2.0

添加 McAfee 数据：单实例

生成时间：2018 年 10 月 17 日，上午 11:19

Table of Contents

安装和配置

McAfee 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。
- 托管重型转发器的 Linux 框。

要部署 Splunk DB Connect，请确认您具有以下应用：

- Splunk Enterprise 6.4.0。
- 已启用的 Java 平台和 Java 平台上的 Java 运行时间环境 (JRE) 8，标准版。
- 在网络本地或其他位置运行的受支持的数据库。

启用 Splunk Enterprise 实例作为接收器

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。

安装重型转发器

要使用 Linux 安装重型转发器并将其连接到 Splunk 平台部署，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。

安装 Splunk Enterprise 时，请注意以下内容。

- `tar` 的一些非 GNU 版本可能没有 `-C` 参数。在这种情况下，要安装到 `/opt/splunk`，可在运行 `tar` 命令之前将目录更改为 `/opt` 或将 tar 文件放入 `/opt`。这种方法适用于您的主机文件系统上的任何可访问目录。
- Splunk Enterprise 不会新建 Splunk 用户。要以特定用户身份运行 Splunk Enterprise，您必须在安装之前手动新建用户。
- 确保磁盘分区拥有足够空间可容纳您计划保留索引的未压缩数据量。

要安装 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.
   ```

如果您已在命令行中使用 `--no prompt` 参数启动 Splunk Enterprise，则不会提醒您新建首次登录 Splunk Enterprise 时需要的管理员凭据。

启用 Splunk Enterprise 实例作为重型转发器

您可以使用 Splunk Web 或 CLI 来启用 Splunk 实例的转发。

使用 Splunk Web 设置重型转发器

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**转发默认值**。
4. 选择**是**存储并保留已索引数据的本地副本到转发器。

使用 CLI 设置重型转发

在命令行，在 Splunk Enterprise 实例上启用转发，然后配置转发到指定的接收器。

1. 从命令或 shell 提示符，转到 `$SPLUNK_HOME/bin/`。
2. 键入以下命令以启用转发：
   ```
   splunk enable app SplunkForwarder -auth <username>:<password>
   ```
3. 重新启动 Splunk Enterprise。

使用 CLI 启动转发

将数据发送到您指定的接收索引器。

1. 从 shell 或命令提示符转到 `$SPLUNK_HOME/bin` 目录。
2. 使用 `splunk add forward-server` 命令指定接收器。
   ```
   splunk add forward-server <host>:<port> -auth <username>:<password>
   ```
3. 重新启动转发器。

在重型转发器上安装 DB Connect

要将 McAfee ePolicy Orchestrator (ePO) 数据库中的数据导入 Splunk Enterprise 部署，请在重型转发器上安装最新版的 Splunk DB Connect。

前提条件

- Splunk Enterprise 6.4.0 或更高版本。
- 已启用的 Java 平台和 Java 平台上的 Java 运行时间环境 (JRE) 8，标准版。
- 在网络本地或其他位置运行的受支持的数据库。

安装 DB Connect

1. 下载 Splunk DB Connect。
2. 在 Splunk Web 主页中，单击左侧边栏中**应用**旁边的齿轮图标。
   1. 单击**通过文件安装应用**。
   2. 导航到您下载 `splunk_app_db_connect.tgz.` 的安装包
   3. 单击**上载**。
   4. 重新启动 Splunk 软件。
3. 启动 Splunk DB Connect。

在重型转发器上安装适用于 McAfee 的 Splunk 加载项

1. 从 Splunkbase 下载加载项。

2. 在重型转发器的 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. 如果转发器提示您重新启动，请重新启动。

通过在 `$SPLUNK_HOME/etc/apps/Splunk_TA_mcafee` 中查找适用于 McAfee 的 Splunk 加载项来验证安装

在 Splunk Enterprise 实例上安装适用于 McAfee 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。

为适用于 McAfee 的 Splunk 加载项配置 Splunk DB Connect v3.1 输入

适用于 McAfee 的 Splunk 加载项可通过 Splunk DB Connect 收集 ePO 中的数据。遵照您安装的 DB Connect 版本说明。

设置数据库连接

执行以下任务设置数据库连接：

1. 如果尚未安装适用于 SQL Server 的 Microsoft JDBC 驱动程序，请先安装。
2. 在 Splunk 平台中新建一个身份以连接数据库。
3. 使用 Splunk DB Connect GUI 或 `db_connections.conf` 文件新建 SQL Server 数据库连接。

下载并安装适用于 SQL Server 的 Microsoft JDBC 驱动程序

要启用 Microsoft SQL Server 连接，请下载并安装适用于 SQL Server 的 Microsoft JDBC 驱动程序。

1. 使用 SQL Server 用户名和密码（附加非域名）登录 SQL Server 数据库。
2. 下载合适的适用于 SQL Server 的 JDBC 驱动程序。
    1. 要下载适用于 SQL Server 的 Microsoft JDBC 驱动程序，即“MS Generic 驱动程序”。
        1. 请前往“适用于 SQL Server 的 Microsoft JDBC 驱动程序”下载页面，单击**下载**。
        2. 在“选择您想要下载的驱动程序”页面，勾选相应的下载程序旁边的复选框：对于 Linux，请选择 `sqljdbc_4.2.8112.100_enu.tar.gz`；对于 Windows，请选择 `sqljdbc_4.2.8112.100_enu.exe`。确保下载 4.2 版的驱动程序，然后单击**下一步**。
        3. 解压缩下载的文件。
    2. 对于开源 jTDS 驱动程序，请从 jTDS 项目下载驱动程序。
3. 将驱动程序文件移动到当前位置：
    1. 对于 MS Generic 驱动程序，请通过 `sqljdbc_4.2` 目录执行以下步骤。
        1. 将 `sqljdbc42.jar` 文件复制或移动到 `$SPLUNK_HOME/etc/apps/splunk_app_db_connect/drivers` 目录。
        2. 在 Windows 主机上，目录为 `%SPLUNK_HOME%\etc\apps\splunk_app_db_connect\drivers`。
    2. 如果您需要利用 Generic 驱动程序在 Windows 上使用数据库服务帐户，您还需要安装 JDBC 验证库：
        1. 在适用于 SQL Server 的 Microsoft JDBC 驱动程序 4.2 的下载页，查找 `sqljdbc_auth.dll` 文件。此文件位于以下路径，其中 *<region_code>* 是由三个字母组成的区域代码。例如，在英语中，代码是 "enu"。*<architecture>* 是处理器类型。选项有 "x86" 和 "x64"：`Microsoft JDBC Driver 4.2 for SQL Server\sqljdbc_4.2\<region_code>\auth\<architecture>\sqljdbc_auth.dll`。
        2. 将 `sqljdbc_auth.dll` 文件复制到 Splunk Enterprise 服务器上的 `C:\Windows\System32` 中。
        3. 从 Windows 控制面板中，前往 **Splunk 服务**中的**服务** > **获取属性**。
        4. 单击“登录”选项卡，然后将“本地系统”帐户中的“登录身份”设置更改以域用户身份登录。域用户必须有足够的权限访问 SQL Server 实例。
        5. 针对 jTDS 驱动程序，将您下载的 .jar 文件复制到 `$SPLUNK_HOME/etc/apps/splunk_app_db_connect/drivers` 目录中。在 Windows 主机上，目录为 `%SPLUNK_HOME%\etc\apps\splunk_app_db_connect\drivers`。
4. 保存更改，然后重新启动 Splunk Enterprise 服务器使更改生效。

在 Splunk Enterprise 中新建身份

新建一个身份以连接数据库。确保此身份的用户具有系统角色。

您可使用用户名和密码进行验证，或使用 Windows 验证。但是，使用带有 Windows 验证的 DB Connect 3.1 和适用于 SQL Server 的 JDBC 驱动程序需要其他步骤。请参阅 Splunk DB Connect 手册了解更多信息。

然后，您需要使用 Splunk DB Connect GUI 或 `db_connections.conf` 文件新建 SQL Server 数据库连接。

使用 Splunk DB Connect GUI 配置数据库输入

如果你想要新建 McAfee 数据库输入，请在 Splunk DB Connect 中的**模板**下选择为适用于 McAfee 的 Splunk 加载项新建的模板。

为适用于 McAfee 的 Splunk 加载项配置 syslog 输入

某些 McAfee 产品日志不是从 McAfee ePO 数据库中收集的。

配置 McAfee 网络安全平台（也称为 IntruShield）将 syslog 发送到 Splunk Enterprise 网络接收端口，或发送到写入 Splunk Enterprise 监视的目录中的 syslog 服务器。

配置 Splunk Enterprise 以将来源类型设置为 `mcafee:ids`。将自动识别发送到 Splunk Enterprise 的数据，该数据和 `props.conf` 以及 `transforms.conf` 中来源类型规则匹配。

从 TCP 和 UDP 端口获取数据

您可以配置 Splunk Enterprise 以接受任何 TCP 或 UDP 端口上的输入。Splunk Enterprise 将获取抵达这些端口的任何数据。使用此方法从网络服务（如 syslog）捕获数据。

TCP 是以 Splunk Enterprise 数据分发方案为基础的网络协议。使用该协议从任意远程主机发送数据到您的 Splunk Enterprise 服务器。Splunk Enterprise 可以为来自 `syslog-ng` 或任何其他通过 TCP 传输的应用程序的远程数据建立索引。

尽量改用 TCP 发送网络数据。UDP 无法确保网络封包的交付。

当您监视 TCP 网络端口时，Splunk Enterprise 以该身份运行的用户必须获得授权访问您想要监视的端口。默认情况下，在很多 Unix 操作系统上，您必须以根用户的身份运行 Splunk Enterprise 才能直接侦听 1024 以下的端口。

如您必须使用 UDP 发送网络数据，请参阅 Splunk 社区 Wiki 上的“使用 UDP 连接”以获取相关建议。

请在您使用网络监视输入前确定您的网络设备如何处理外部监视

在您开始使用 Splunk Enterprise 网络监视器监视网络设备的输出前，请先确认该网络设备与外部网络监视器的交互方式。

如果您在一些网络设备（如 Cisco 自适应安全设备 (ASA)）上配置 TCP 日志，且该网络设备无法连接至监视器，则可能会导致性能减弱或停止日志。默认情况下，Cisco ASA 将在遭遇网络拥挤或网络连接问题时停止接受传入的网络连接。

使用 Splunk Web 添加网络输入

1. 单击 Splunk 主页中的**添加数据**链接。
2. 请单击**监视**以监视本地计算机上的网络端口或**转发**以从另一个计算机上接收网络数据。
3. 如果您选择了**转发**，则选择或新建要此输入应用的转发器组。
4. 单击**下一步**。

指定网络输入

1. 在左窗格中，请单击 **TCP / UDP** 以添加输入。
2. 单击 **TCP** 或 **UDP** 按钮即可在 TCP 或 UDP 输入之间进行选择。
3. 在**端口**字段中，输入端口号。
4. 更改 `Source name override` 值前请先咨询 Splunk 支持。
5. 对于 TCP 输入，请指定此端口是应接受所有主机的连接还是只接受 `Only accept connections from` 字段中的一个主机的连接。如果您要输入接受来自一个主机的连接，则输入主机名或 IP 地址。可以使用通配符指定主机。
6. 单击**下一步**。

指定输入设置

“输入设置”页面允许您指定来源类型、应用程序上下文、默认主机值和索引。所有这些参数均为可选参数。

1. 设置**来源类型**。这是 Splunk Enterprise 添加到事件中并用来确定处理特性（如时间戳和事件界限）的默认字段。
2. 设置主机名称值。主机只是设置生成事件中的**主机**字段。而不是引导 Splunk Enterprise 查找网络中的特定主机。您有几个选择：
    1. **IP** 将输入处理器设置为使用远程服务器的 IP 地址重写主机。
    2. **DNS** 将主机设置为远程服务器的 DNS 项。
    3. **自定义**将主机设置为用户定义的标签。
3. 为此输入设置 Splunk Enterprise 将数据发送到其中的**索引**。如果未定义多个索引来处理不同类型的事件，请保留默认值。除了用户数据的索引之外，Splunk Enterprise 还有很多实用工具索引，这些索引也会显示在

此下拉框中。
4. 请单击**查看**。

查看您的选择

在您指定输入设置后，可查看您的选择。Splunk Enterprise 会列出您勾选的选项，包括监视器的类型、数据来源、来源类型、应用程序上下文和索引。

1. 查看该设置。
2. 如果这些设置不符合您的需要，单击 **<** 即可返回到向导中的上一个步骤。否则，请单击**提交**。

然后，Splunk Enterprise 会加载确认页面并开始索引指定的网络输入。

验证 McAfee 数据

运行 Splunk 软件的 `search` 函数中的以下搜索验证 McAfee 数据是否在 Splunk 平台部署中显示：

```
sourcetype=mcafee*
```

。

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。