



## Splunk® Enterprise 7.2.0

### 添加 McAfee 数据：托管式 Cloud

生成时间：2018 年 10 月 17 日，上午 11:19

# Table of Contents

<b>安装和配置</b>	<b>3</b>
McAfee Guided Data Onboarding 手册: 托管式 Splunk Cloud	3
为 Splunk Cloud 配置转发和接收	3
安装重型转发器	3
在重型转发器上安装 DB Connect	5
在重型转发器上安装适用于 McAfee 的 Splunk 加载项	5
在 Splunk Cloud 实例上安装适用于 McAfee 的 Splunk 加载项	5
为适用于 McAfee 的 Splunk 加载项配置 syslog 输入	5
为适用于 McAfee 的 Splunk 加载项配置 Splunk DB Connect v3.1	6
输入	
验证 McAfee 数据	7
<b>额外资源</b>	<b>8</b>
额外资源	8

# 安装和配置

## McAfee 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。
- 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 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。

## 为 Splunk Cloud 配置转发和接收

将 Splunk Cloud 实例用作接收器。使用这些任务配置转发器以将数据发送到 Splunk Cloud。

### 下载并安装转发器凭据将转发器连接到 Splunk Cloud 实例

要使用转发器将数据发送到 Splunk Cloud，请下载通用转发器凭据文件。此文件包含 Splunk Cloud 部署的自定义证书。从本主题介绍的以下两种安装选项中选择一种将其安装在转发器上。尽管凭据包被称为通用转发器凭据，但请将它们应用于您需要连接到 Splunk Cloud 实例的任何一类转发器。

#### 下载转发器凭据

1. 在 Splunk Cloud 部署中，导航到 Splunk Cloud 主页。
2. 单击**通用转发器**。
3. 在 splunkclouduf 主页上，单击**下载通用转发器凭据**下载 `splunkclouduf.spl` 文件。
4. 收到提示后，单击**保存文件**，然后单击**确定**。默认情况下，`splunkclouduf.spl` 文件会下载到 `downloads` 目录下。如果它下载到其他位置，请记下该位置的路径。

#### 安装选项 1：在单一转发器上安装转发器凭据

1. 将 `splunkclouduf.spl` 文件从其下载位置移动到转发器的 `$SPLUNK_HOME/etc/apps/` 目录中。
2. 打开命令提示窗口，然后运行以下 `tar xvf splunkclouduf.spl` 命令。
3. 导航到部署服务器的 `/bin` 子目录。
4. 在命令提示窗口中，运行以下命令：

```
splunk install app <full path to splunkclouduf.spl> -auth <username>:<password> 其中 <full path to splunkclouduf.spl> 是 splunkclouduf.spl 文件所处目录的路径，<username>:<password> 是转发器上现有管理员帐户的用户名和密码。
```

5. 重新启动转发器：`/splunk restart`。

#### 安装选项 2：在部署服务器上安装转发器凭据

1. 将 `splunkclouduf.spl` 文件从其下载位置移动到部署服务器的 `$SPLUNK_HOME/etc/deployment-apps/` 目录中。
2. 打开命令提示窗口，然后运行命令 `tar xvf splunkclouduf.spl`。
3. 导航到部署服务器的 `/bin` 子目录。
4. 在命令提示窗口中，运行以下命令：`splunk install app <full path to splunkclouduf.spl> -auth <username>:<password>`，其中 `<full path to splunkclouduf.spl>` 是 `splunkclouduf.spl` 文件所在目录的路径，`<username>:<password>` 是通用转发器上现有管理员帐户的用户名和密码。
5. 重新启动部署服务器：`/splunk restart`。

## 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**。
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 ePO 数据库中的数据导入 Splunk 部署，请先在重型转发器上安装最新版的 Splunk DB Connect。Splunk DB Connect 是使用 Splunk 数据库的最佳解决方案。

要部署 Splunk DB Connect，请确认您具有以下应用：

- 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。

然后，开始 DB Connect 安装流程：

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. 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 Splunk Cloud 实例上安装适用于 McAfee 的 Splunk 加载项

在托管式 Splunk Cloud 部署上安装加载项，如下所示：

1. 在 Splunk Web 主页中，单击**应用**旁边的齿轮图标。
2. 单击**安装应用**。
3. 单击**安装**来安装加载项。  
如果没有列出您想要的应用，或者加载项表示不支持自助式安装，请联系 Splunk 支持。
4. 遵照提示完成安装过程。

当您安装某个具有公认的依赖关系的应用时，Splunk Cloud 会通过 Splunkbase 自动解析依赖关系。要了解有关公认的依赖关系的更多信息，请参阅 Splunk 包装工具套件。

## 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 Splunk Enterprise 接收的且与 `props.conf` 和 `transforms.conf` 中来源类型规则匹配的数据。

### 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。

## 使用 CLI 添加网络输入

如需访问 Splunk Enterprise CLI，请导航至 `$SPLUNK_HOME/bin/` 目录，并使用 `./splunk` 命令。

如果您遇到困难，CLI 内有帮助说明。键入 `splunk help` 即可访问 CLI 主要帮助。每个命令也都设有单独的帮助页面，键入 `splunk help <command>` 即可访问。

以下 CLI 命令可用于网络输入配置：

命令	命令语法	操作
<b>add</b>	<code>add tcp udp &lt;port&gt; [-parameter value] ...</code>	从 <port> 添加输入。
<b>edit</b>	<code>edit tcp udp &lt;port&gt; [-parameter value] ...</code>	编辑之前为 <port> 添加的输入。
<b>remove</b>	<code>remove tcp udp &lt;port&gt;</code>	移除之前添加的数据导入。
<b>list</b>	<code>list tcp udp [&lt;port&gt;]</code>	列出当前配置的监视器。

<port> 是用于侦听数据的端口号。您运行 Splunk 所用的用户身份必须有权访问此端口。

设置以下任何其他参数，即可修改每个输入的配置：

参数	是否必需？	描述
<code>sourcetype</code>	否	为来自输入来源的事件指定 Sourcetype 字段值。
<code>index</code>	否	为来自输入来源的事件指定目标索引。
<code>hostname</code>	否	为来自输入来源的事件指定要设置为主机字段值的主机名。
<code>remotehost</code>	否	指定只接受来自其数据的 IP 地址。
<code>resolvehost</code>	否	设置为 true 或 false (T   F)。默认为 False。设置为 true 以使用 DNS 为来自输入来源的事件设置主机字段值。
<code>restrictToHost</code>	否	指定此输入只应该接受其连接的主机名或 IP 地址。

### 示例

- 将 UDP 输入配置为监视端口 514 并将来源类型设置为 "syslog"：

```
./splunk add udp 514 -sourcetype syslog
```

- 通过 DNS 设置 UDP 输入的主机值。输入用户名和密码以使用 `auth`：

```
./splunk edit udp 514 -resolvehost true -auth admin:changeme
```

有关 UDP 最佳使用方法的信息，请参阅社区 Wiki 里“配置 Syslog 输入的最佳方法”。

## 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：

- 如果尚未安装适用于 SQL Server 的 Microsoft JDBC 驱动程序，请先安装。
- 在 Splunk 平台中新建一个身份以连接数据库。
- 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。

## 验证 McAfee 数据

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

```
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 and 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 <b>索引和搜索管理</b> 。在此部署方案中，您通常还可以在生成数据的主机上安装 <b>转发器</b> 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 <b>实例</b> 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 <b>索引器群集</b> 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 <b>CIM</b> 。 我们可为以下部署方案提供 Guided Data Onboarding： <ul style="list-style-type: none"><li>单实例</li><li>具有索引器群集化功能的分布式部署</li><li>托管式 Cloud</li></ul> 您还可参阅 <b>适用于 Cisco ASA 的 Splunk 加载项手册</b> 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： <ul style="list-style-type: none"><li>单实例</li><li>具有索引器群集化功能的分布式部署</li><li>Splunk Cloud</li></ul> 您还可参阅 <b>适用于 McAfee 的 Splunk 加载项手册</b> 了解更多。



Microsoft Active Directory	<p>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。</p> <p>我们可为以下部署方案提供 Guided Data Onboarding：</p> <ul style="list-style-type: none"> <li>• 单实例</li> <li>• 具有索引器群集化功能的分布式部署</li> <li>• Splunk Cloud</li> </ul> <p>您还可参阅<i>适用于 Microsoft Active Directory 的 Splunk 加载项手册</i>了解更多。</p>
Microsoft Windows	<p>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。</p> <p>我们可为以下部署方案提供 Guided Data Onboarding：</p> <ul style="list-style-type: none"> <li>• 单实例</li> <li>• 具有索引器群集化功能的分布式部署</li> <li>• Splunk Cloud</li> </ul> <p>您还可参阅<i>适用于 Windows 的 Splunk 加载项手册</i>了解更多。</p>
Palo Alto Networks	<p>允许管理员收集 Palo Alto Networks Next-generation Security Platform 中每个产品的数据。</p> <p>我们可为以下部署方案提供 Guided Data Onboarding：</p> <ul style="list-style-type: none"> <li>• 单实例</li> <li>• 具有索引器群集化功能的分布式部署</li> <li>• Splunk Cloud</li> </ul> <p>您还可访问 <a href="https://splunk.paloaltonetworks.com">splunk.paloaltonetworks.com</a> 了解更多。</p>
Symantec Endpoint Protection	<p>允许管理员通过 dump 文件收集 Symantec Endpoint Protection Manager 中的日志。</p> <p>我们可为以下部署方案提供 Guided Data Onboarding：</p> <ul style="list-style-type: none"> <li>• 单实例</li> <li>• 具有索引器群集化功能的分布式部署</li> <li>• Splunk Cloud</li> </ul> <p>您还可参阅<i>适用于 Symantec Endpoint Protection 的 Splunk 加载项手册</i>了解更多。</p>

### 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。