



Splunk® Enterprise 7.2.0

添加 Palo Alto Networks 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 11:20

Table of Contents

添加 Palo Alto Networks 数据	3
Palo Alto Networks Guided Data Onboarding 手册：具有索引器群	3
集化功能的分布式部署	
安装 syslog 服务器	3
配置登录 Palo Alto Networks 设备的系统	3
在各 syslog-ng 服务器上安装重型转发器	3
在 Splunk Enterprise 部署上安装适用于 Palo Alto Networks 的	5
Splunk 加载项	
配置 syslog-ng 服务器将 Palo Alto Networks 数据发送到 Splunk 平	7
台部署	
验证数据	8
额外资源	9
额外资源	9

添加 Palo Alto Networks 数据

Palo Alto Networks 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。

安装 syslog 服务器

安装基于 Linux 的 syslog-ng 服务器以发送 Palo Alto Networks 部署相关的 syslog 消息。

调整评估大小

Palo Alto Networks 日志大小差别很大。每条消息大小一般为 850 字节。通常无论是否允许，用户每次连接时都会看到一条消息。分支机构每天可生成数百 MB，而数据中心群集每天可生成近 250 GB。

Palo Alto Networks 内的 `show session info` 命令显示自启动以来发生的连接次数。评估事件量的一种方法是检查随后几天同一时间的数量。然后计算你通常每天能看到的连接数量。乘以 850 字节数之后，您可获得数据大小的近似期望值。

或者，您可执行 `rsyslog config` 命令。然后，追踪磁盘上新建的文件大小来确定数量。

请参阅 Palo Alto Networks PAN-OS 8.0 CLI 配置指南了解更多。

安装 syslog-ng 服务器

1. （可选）如果部署中自带了 rsyslog，取消安装：

```
sudo rpm -e --nodeps rsyslog
```
2. 使用 yum 安装 syslog-ng：

```
sudo yum-get install syslog-ng
```
3. 配置 yum 搜索 EPEL 报告：

```
sudo yum --enablerepo=epel install syslog-ng
```
4. （可选）安装 `syslog-ng-libdbi` 模块防止每次启动 syslog-ng 时出现警告消息：

```
sudo yum install --enablerepo=epel syslog-ng-libdbi
```
5. 安装完成后，启动 syslog-ng：

```
sudo systemctl start syslog-ng.service  
sudo systemctl enable syslog-ng.service
```
6. 检查 pid 确认 syslog-ng 是否正在运行：

```
pidof syslog-ng
```

配置登录 Palo Alto Networks 设备的系统

要配置 Palo Alto Networks 设备捕获事件字段并通过 TCP 或 UDP 将安全相关日志信息发送到运行 syslog 服务器的服务器，请完成以下任务：

1. 新建 syslog 服务器资料。使用端口号将 Palo Alto Networks 部署指向侦听 syslog 服务器的端口。默认端口号是 514。
2. 将 syslog 资料应用于相关数据类型。
3. 确认 syslog 服务器能否连接到 PAN 设备。
4. 配置 PAN 设备以使用 syslog 服务器资料执行日志转发规则。
5. 使用分配的端口号确认 PAN 设备能否接到 syslog 服务器。

在各 syslog-ng 服务器上安装重型转发器

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 Splunk Enterprise 部署上安装适用于 Palo Alto Networks

的 Splunk 加载项

要在分布式 Splunk Enterprise 部署上安装适用于 Palo Alto Networks 的 Splunk 加载项，请完成以下步骤：

在 Splunkbase 上下载适用于 Palo Alto Networks 的 Splunk 加载项。

在分布式 Splunk Enterprise 部署中的搜索头上安装适用于 Palo Alto Networks 的 Splunk 加载项

完成以下步骤在搜索头上安装适用于 Palo Alto Networks 的 Splunk 加载项：

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**上传**。
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**。

在分布式 Splunk 平台部署中准备要安装的加载项安装包

在为分布式 Splunk 平台部署部署加载项之前，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。

在分布式 Splunk Enterprise 部署中的群集索引器上安装加载项

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。

准备配置软件包

`$SPLUNK_HOME/etc/master-apps` 目录中的一组子目录组成**配置软件包**。

对想要分发到对等节点的文件进行以下编辑准备配置软件包。尽量将所有更新合并单个软件包中，这样可降低对对等节点工作的影响：

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 `$SPLUNK_HOME/etc/master-apps` 目录中。

（可选）验证软件包并检查重新启动

在将文件分发到一组对等节点之前，先在独立测试索引器上验证软件包并测试文件，以确认这些文件可正常使用。

验证对确保软件包顺利应用到所有对等节点很有用。验证过程中还提供对调试无效的软件包而言有用的信息。

使用 Splunk Web 验证软件包并检查重新启动

1. 在 Splunk Web 的主节点上，单击**设置 > 索引器群集化**。
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。
如果软件包验证和检查重新启动成功，则可将该软件包分发到对等节点。有关验证软件包的信息显示在 Splunk Web 中，包括您是否必须要重新启动对等节点。

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 CLI 验证软件包并检查重新启动

运行 `splunk validate cluster-bundle: <code>splunk validate cluster-bundle`。该命令将返回一条确认软件包验证已启动的消息。在某些验证失败的情况下，消息中还会说明失败的原因。

要验证软件包并检查是否需要重新启动，请包含 `--check-restart` 参数：

`splunk validate cluster-bundle --check-restart` 此版本的命令首先会验证软件包。如果验证成功，则命令会检查是否需要重新启动对等节点。

要查看软件包验证状态，请运行 `splunk show cluster-bundle-status` 命令。此命令会提示您验证成功。如果验证失败，命令也会深入了解失败原因并说明是否需要重新启动对等节点。

以下示例为验证成功后 `splunk show cluster-bundle-status` 命令输出的内容：

```
master
  cluster_status=None
  active_bundle
    checksum=576F6BBB187EA6BC99CE0615B1DC151F
    timestamp=1495569737 (in localtime=Tue May 23 13:02:17 2017)
  latest_bundle
    checksum=576F6BBB187EA6BC99CE0615B1DC151F
    timestamp=1495569737 (in localtime=Tue May 23 13:02:17 2017)
  last_validated_bundle
    checksum=1E0C4F0A7363611774E1E65C8B3932CF
    last_validation_succeeded=1
    timestamp=1495574646 (in localtime=Tue May 23 14:24:06 2017)
  last_check_restart_bundle
    checksum=1E0C4F0A7363611774E1E65C8B3932CF
    last_check_restart_result=restart required
    timestamp=1495574646 (in localtime=Tue May 23 14:24:06 2017)

Peer 1      1D00A8C2-026B-4CAF-90D6-5D5D39445569      default
  active_bundle=576F6BBB187EA6BC99CE0615B1DC151F
  latest_bundle=576F6BBB187EA6BC99CE0615B1DC151F
  last_validated_bundle=1E0C4F0A7363611774E1E65C8B3932CF
  last_bundle_validation_status=success
  last_bundle_checked_for_restart=1E0C4F0A7363611774E1E65C8B3932CF
  last_check_restart_result=restart required
  restart_required_apply_bundle=0
  status=Up
...

```

设置为：

通知字段名称	描述
last_validated_bundle	识别新验证的软件包。此字段与 <code>active_bundle</code> 不同，后者将识别最近刚应用到节点上而且目前在各对等节点中启用的软件包。
last_validation_succeeded=1	表明验证成功。
last_check_restart_result=restart required	在主节点上， <code>last_check_restart_result=restart required</code> 表示至少需要重新启动一个群集对等节点。
last_check_restart_result=restart required	在对等节点上， <code>last_check_restart_result=restart required</code> 表示需要重新启动个别对等节点。

将软件包应用到对等节点

要应用配置软件包到对等节点，您可以使用 Splunk Web 或 CLI。如果软件包推送当前正在进行中，那么您无法启动配置软件包推送。

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**。
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**。
弹出窗口将警告您分发可能会重新启动所有对等节点。
4. 单击 **推送更改**。
此屏幕提供有关分发进度和分发是否成功完成的信息。
 - 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。
 - 如果分发失败，主节点会说明哪些节点无法接收分发，这样您就可以解决这些节点问题。如果所有节点都无法接受分发，那么这些节点将无法应用软件包。

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。将文件保留在此位置。

使用 CLI 将软件包应用到对等节点。

1. 要将配置软件包应用到对等节点，请在主节点上运行以下 CLI 命令：

```
splunk apply cluster-bundle
```

警告消息显示：

Caution: Under some circumstances, this command will initiate a rolling restart of all peers. This depends on the contents of the configuration bundle. For details, refer to the documentation. Do you wish to continue? [y/n]:

2. 要继续，请键入 `y`。
 - 主节点会将新的配置软件包分发到各个对等节点，这些对等节点随后会分别验证软件包。在所有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。对等节点将使用一组新的配置，这些配置位于其本地 `$SPLUNK_HOME/etc/slave-apps` 中。将文件保留在此位置。
 - 如果任何对等节点无法验证配置软件包，它会向主节点发送消息，主节点会在 Splunk Web 的相应仪表板中显示这一错误。您必须修复主节点提示的所有问题并重新运行 `splunk apply cluster-bundle`。

查看软件包推送的状态

您可以使用 Splunk Web 或 CLI 查看软件包推送的状态。

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。仅在 Splunk 支持的指示下并确信软件包有效后方可使用此标记。请勿使用此标记避开验证流程。

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。

使用 CLI 查看软件包推送的状态

要查看群集软件包推送的进展情况，请从主节点运行以下命令：

```
splunk show cluster-bundle-status
```

此命令会告诉您软件包验证是否成功。它还指示每个对等节点的重新启动状态。

使用部署服务器将加载项安装到转发器上

使用部署服务器将内容和配置（统称为部署应用）分发到分组为不同服务器类的部署客户端上。部署应用既可以是完整的应用（例如 Splunkbase 中提供的应用），也可以只是一些简单的配置组。

将加载项部署到部署客户端

1. 在部署服务器上，导航到 `$SPLUNK_HOME/etc/deployment-apps/`
2. 将加载项添加到 `/deployment-apps/` 目录中。
3. 提取加载项。
4. 导航到 `$SPLUNK_HOME/etc/deployment-apps/<APP NAME>/default/inputs.conf`
5. 为要收集的数据添加输入。
6. 保存更改。
7. 重新启动部署服务器：`/splunk restart`

查看应用部署状态

转到“应用”选项卡。选项卡会提供每个应用所部署到的客户端数量的相关信息。单击应用转到该应用的详细页面。**应用数据大小**字段指定了应用软件包的大小。该软件包为包含应用在内的压缩文件。客户端收到软件包后，将解压缩软件包并在适当的位置安装应用。

配置 syslog-ng 服务器将 Palo Alto Networks 数据发送到 Splunk 平台部署

1. 导航到 `/etc/syslog-ng/syslog-ng.conf` 并在进行其他配置之前保存 `syslog-ng.conf` 的副本作为备份。
2. 导航到 `/etc/syslog-ng/conf.d/` 并新建名为 `pan.conf` 的文件。
3. 打开 `pan.conf` 并粘贴以下信息，以配置服务器侦听 UDP 端口 514：

```
# syslog-ng config to receive syslog messages from Palo Alto Networks devices

options{
    create-dirs(yes);
};

#Listen on UDP port 514
```

```

source s_net{
    udp(port("514"));
};

#Destinations where syslog-ng should write to
destination d_threat      { file("/var/log/syslog/pan/$HOST/threat/$YEAR-$MONTH-$DAY-threat.log"); };
destination d_traffic    { file("/var/log/syslog/pan/$HOST/traffic/$YEAR-$MONTH-$DAY-traffic.log"); };
destination d_system     { file("/var/log/syslog/pan/$HOST/system/$YEAR-$MONTH-$DAY-system.log"); };
destination d_config     { file("/var/log/syslog/pan/$HOST/config/$YEAR-$MONTH-$DAY-config.log"); };
destination d_hipmatch   { file("/var/log/syslog/pan/$HOST/hipmatch/$YEAR-$MONTH-$DAY-hipmatch.log"); };
};
destination d_endpoint   { file("/var/log/syslog/pan/$HOST/endpoint/$YEAR-$MONTH-$DAY-endpoint.log"); };
};
destination d_wildfire   { file("/var/log/syslog/pan/$HOST/wildfire/$YEAR-$MONTH-$DAY-wildfire.log"); };
};
destination d_correlation { file("/var/log/syslog/pan/$HOST/correlation/$YEAR-$MONTH-$DAY-
correlation.log"); };
destination d_aperture   { file("/var/log/syslog/pan/$HOST/aperture/$YEAR-$MONTH-$DAY-aperture.log"); };
};

#Filters to route sourcetypes to sepearate files
filter f_threat          { message("THREAT"); };
filter f_traffic         { message("TRAFFIC"); };
filter f_system          { message("SYSTEM"); };
filter f_config          { message("CONFIG"); };
filter f_hipmatch        { message("HIPMATCH"); };
filter f_endpoint        { message("ENDPOINT"); };
filter f_wildfire        { message("WILDFIRE"); };
filter f_correlation     { message("CORRELATION"); };
filter f_aperture        { message("APERTURE"); };

#Log definitions
log { source(s_net); destination(d_threat); filter(f_threat); };
log { source(s_net); destination(d_traffic); filter(f_traffic); };
log { source(s_net); destination(d_system); filter(f_system); };
log { source(s_net); destination(d_config); filter(f_config); };
log { source(s_net); destination(d_hipmatch); filter(f_hipmatch); };
log { source(s_net); destination(d_endpoint); filter(f_endpoint); };
log { source(s_net); destination(d_wildfire); filter(f_wildfire); };
log { source(s_net); destination(d_correlation); filter(f_correlation); };
log { source(s_net); destination(d_aperture); filter(f_aperture); };

```

4. 保存更改。要选择更改端口，请输入想要的端口号替换 `source s_net{ udp(port("514"));`
5. 重新启动 syslog-ng 应用更新。

```
sudo service syslog-ng restart
```

验证数据

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

```
index=* sourcetype=pan*
```


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： <ul style="list-style-type: none">• 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： <ul style="list-style-type: none">• 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	<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"> • 单实例 • 具有索引器群集化功能的分布式部署 • Splunk Cloud <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"> • 单实例 • 具有索引器群集化功能的分布式部署 • Splunk Cloud <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"> • 单实例 • 具有索引器群集化功能的分布式部署 • Splunk Cloud <p>您还可访问 splunk.paloaltonetworks.com 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"> • 单实例 • 具有索引器群集化功能的分布式部署 • Splunk Cloud <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。