



Splunk® Enterprise 7.2.0

添加 Palo Alto Networks 数据：单实例

生成时间：2018 年 10 月 17 日，上午 11:20

Table of Contents

安装和配置	3
Palo Alto Networks Guided Data Onboarding 手册：单实例	3
安装 syslog 服务器	3
配置登录 Palo Alto Networks 设备的系统	3
在 Splunk Enterprise 实例上启用接收器	3
在 syslog-ng 服务器上安装通用转发器	4
在 Splunk Enterprise 部署上安装适用于 Palo Alto Networks 的 Splunk 加载项	5
配置 syslog-ng 服务器将 Palo Alto Networks 数据发送到 Splunk Enterprise 部署	5
验证数据	6
额外资源	7
额外资源	7

安装和配置

Palo Alto Networks 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。

安装 syslog 服务器

要将数据的导入 Splunk Enterprise 单实例部署，请配置基于 Linux 的 syslog 服务器以发送 Palo Alto Networks (PAN) 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

完成以下步骤以安装 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 Palo Alto Networks 设备。
4. 配置 Palo Alto Networks 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 Palo Alto Networks 设备能否接到 syslog 服务器。

在 Splunk Enterprise 实例上启用接收器

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。

在 syslog-ng 服务器上安装通用转发器

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

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

安装

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。

您可通过在 `$SPLUNK_HOME/etc/apps/Splunk_TA_paloalto` 中查找适用于 Palo Alto Networks 的 Splunk 加载项来确认安装是否成功。

配置 syslog-ng 服务器将 Palo Alto Networks 数据发送到 Splunk Enterprise 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。