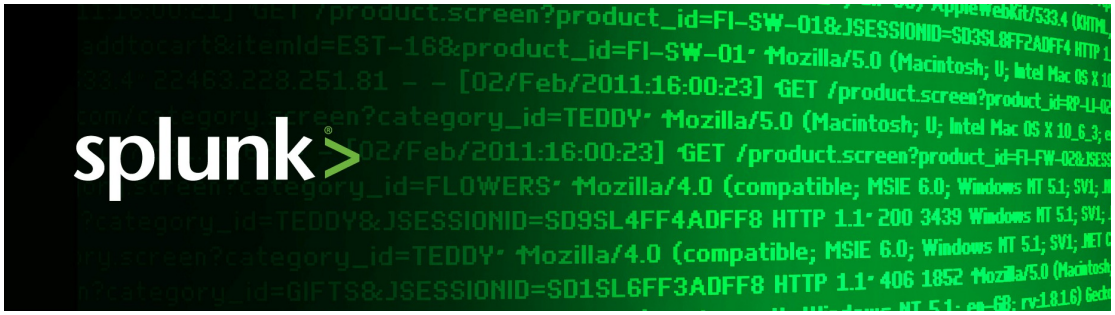

Splunk® Enterprise 7.2.0

添加 Cisco ASA 数据：单实例

生成时间：2018 年 10 月 17 日，上午 11:18

Table of Contents

安装和配置

Cisco 自适应安全设备 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。

安装和配置 syslog-ng 服务器

要将数据导入 Splunk Enterprise 单实例部署，请配置基于 Linux 的 syslog 服务器以发送 Cisco 自适应安全设备 (ASA) 部署相关的 syslog 消息。

确定 Cisco ASA 日志大小

每个防火墙消息约 230 字节，通常用户每次连接可查看一条消息。最佳做法是使用登录允许的连接和已拒绝的连接。日志量取决于 ASA 设备的大小。

仅使用 Cisco 内置工具，使用 `show ip inspect statistics` 命令查看上次重置之后连接了多少次。

下表显示每种服务日志的近似大小：

服务	日志的近似大小
边缘防火墙	忽略不计
区域防火墙	每个事件 230 字节
VPN 服务	每个会话 10 Kb + 防火墙活动
可操作	每个 ASA 每天约小于 200 MB

安装 syslog-ng 服务器

要安装 syslog-ng 服务器，请完成以下步骤：

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 syslog-ng 服务器

1. 编辑 `syslog-ng.conf` 之前请先保存一份副本。
2. 打开 `syslog-ng.conf`，然后编辑以更改配置。以下 `syslog-ng.conf` 文件显示如何使用 regex 过滤器将传入事件分隔的示例。每个唯一的数据来源类型都在 `/home/syslog/logs` 下新建了目录。如果目录不存在，将 `create_dirs` 属性设为 `yes` 以新建必要的目录。

   ```
   # syslog-ng configuration file.
   #
   #
   options {
   chain_hostnames(no);
   create_dirs (yes);
   ```

```
dir_perm(0755);
dns_cache(yes);
keep_hostname(yes);
log_fifo_size(2048);
log_msg_size(8192);
perm(0644);
time_reopen (10);
use_dns(yes);
use_fqdn(yes);
};
source s_network {
udp(port(514));
};
#Destinations
destination d_cisco_asa { file("/home/syslog/logs/cisco/asa/$HOST/$YEAR-$MONTH-$DAY-cisco-asa.log"
create_dirs(yes)); };

# Filters
filter f_cisco_asa { match("%ASA" value("PROGRAM")) or match("%ASA" value("MESSAGE")); };
filter f_all { not (
filter(f_cisco_asa)
);
};
# Log
log { source(s_network); filter(f_cisco_asa); destination(d_cisco_asa); };
log { source(s_network); filter(f_all); destination(d_all); };
```

3. 重新启动 `syslog-ng` 以应用更新。

```
sudo systemctl restart syslog-ng.service
```

更多信息，请访问 OneIdentity.com 中的 `syslog-ng` 安装手册。

通用转发器所安装的主机与 syslog-ng 服务器相同

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 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 Splunk Enterprise 部署上安装适用于 Cisco ASA 的 Splunk 加载项

Splunk Enterprise 单实例部署既可用作**索引器**，也可用作**搜索头**。在单实例部署中，您还可在生成 Cisco ASA 数据的主机上安装**转发器**。转发器会为索引器提供主机中的数据，其中索引器也可用作**接收器**。

前提条件

- Cisco ASA 可将 TCP 用作 syslog 传输，并可使用 syslog-ng 服务器维护开放的 TCP 端口。
- 不要在 ASA 和 syslog 服务器之间放置负载均衡器。
- 实现以下 DNS 配置：
  - 对于为 ASA 管理分配的各 IP 地址，确保地址 (A) 记录和记录路由 (R) 记录存在并匹配。
  - 对于分配给设备的每个出口 NAT 地址，请确保 A 和 R 记录存在并匹配。
  - 对于分配给设备的每个入口 NAT 地址，确保 R 记录和内部目标 A 匹配。不需要此 IP 的 A 记录。
- 在 Splunkbase 上下载适用于 Cisco ASA 的 Splunk 加载项。

安装步骤

要安装适用于 Cisco ASA 的 Splunk 加载项，请完成以下步骤：

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_cisco-asa` 中查找适用于 Cisco ASA 的 Splunk 加载项来确认安装是否成功。

在 Splunk Enterprise 部署上配置适用于 Cisco ASA 的 Splunk 加载项

要在 Splunk Enterprise 单实例部署上配置适用于 Cisco ASA 的 Splunk 加载项，请使用 Splunk Web 添加网络端口的输入内容：

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. 如果是 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，则输入该主机的主机名或 IP 地址。可以使用通配符指定主机。
6. 单击**下一步**以继续到**输入设置**页面。

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 `Source type`。来源类型是 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 `Host` 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 `Index`，Splunk Enterprise 会将数据发送到此索引中。如果未定义多个索引来处理不同类型的事件，请保留 `default` 值。除了用户数据的索引之外，Splunk Enterprise 还有许多实用工具索引，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

在您指定所有输入设置后，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“成功”页面并开始索引指定的网络输入。

请参阅 Cisco 文档查看有关如何记录 Cisco ASA 部署中特定事件的信息。

配置在 Cisco ASA 设备上的系统登录

配置 Cisco ASA 设备以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 的服务器。

前提条件

- 确定要记录哪些 syslog 消息。使用 Cisco ASA 系列一般操作 CLI 配置指南筛选生成的 syslog 消息，这样只会将特定的 syslog 消息发送给特定的输出目标。
- 使用 Cisco ASA 系列一般操作 CLI 配置指南指定 syslog 消息严重性级别。
- 配置 ASA 和自适应服务设备服务模块 (ASASM)，这样可根据以下条件将 syslog 消息引导到输出目标：
    - Syslog 消息 ID 编号
    - Syslog 消息严重性级别

- Syslog 消息等级（相当于 ASA 和 ASASM 的功能区域）

通过新建您可以指定何时设置输出目标的消息列表来自定义这些条件。或者，您可以配置 ASA 或 ASASM 将特定的消息类别发送到独立于消息列表的各类输出目标。

配置 Cisco ASA 设备以通过 TCP 或 UDP 将日志信息发送到 Splunk Enterprise 平台

要配置 ASA、专用网络交换 (PIX) 或防火墙服务模块 (FWSM) 将系统日志消息发送到 syslog 服务器，请执行以下命令：

```
hostname(config)# logging host interface_name ip_address [tcp[/port] | udp[/port]] [format emblem]
```

有关 syslog 配置的更多信息，请参阅 Cisco ASA 系列一般操作 CLI 配置指南。

验证数据

运行 Splunk 软件的 `search` 字段中的以下搜索验证 Cisco ASA 数据是否在 Splunk 平台部署中显示。

```
sourcetype=cisco:asa
```

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。