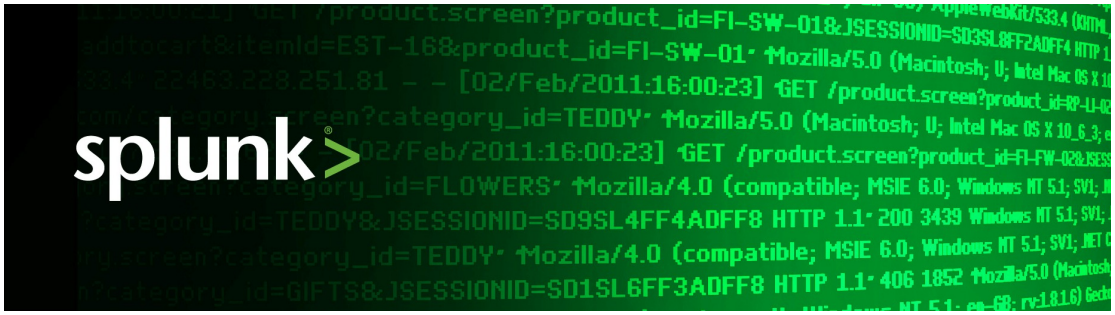

Splunk® Enterprise 7.2.0

添加 Cisco ASA 数据：托管式 Cloud

生成时间：2018 年 10 月 17 日，上午 11:19

Table of Contents

添加 Cisco ASA 数据

Cisco 自适应安全设备 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。

安装和配置 syslog-ng 服务器

完成以下步骤配置基于 Linux 的 syslog 服务器以发送 Cisco 活动安全设备 (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

要配置 syslog-ng 服务器，请完成以下步骤：

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

在 syslog-ng 服务器上安装基于 Linux 的通用转发器，以转发 Cisco ASA 部署相关的 syslog 消息：

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
```

将转发器连接到托管式 Splunk Cloud 部署

使用部署服务器将转发器连接到托管式 Splunk Cloud 部署。

下载并安装转发器凭据将转发器连接到 Splunk Cloud 实例

要启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，但请将这些凭据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`。

在托管式 Splunk Cloud 部署上安装适用于 Cisco ASA 的 Splunk 加载项

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。

使用自助式服务在托管式 Splunk Cloud 部署上安装加载项

使用自助式应用安装流程在托管式 Splunk Cloud 部署中的搜索头和索引器上安装加载项。

在托管式 Splunk Cloud 部署中，必须在您的控制下在转发器上配置输入。

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加载项，或者加载项表示不支持自助式安装，请联系 Splunk 支持。
4. 完成安装。当您安装具有公认的依赖关系的加载项时，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

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。

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。

在托管式 Splunk Cloud 平台部署上配置适用于 Cisco ASA 的 Splunk 加载项

要将网络端口输入添加到托管式 Splunk Cloud 部署，请导航到部署的通用转发器并完成以下步骤：

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
add	`add tcp|udp <port> [-parameter value] ...`	从 `<port>` 添加输入。
edit	`edit tcp|udp <port> [-parameter value] ...`	编辑之前为 `<port>` 添加的输入。
remove	`remove tcp|udp <port>`	移除之前添加的数据导入。
list	`list tcp|udp [<port>]`	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
`sourcetype`	否	为来自输入来源的事件指定 Sourcetype 字段值。
`index`	否	为来自输入来源的事件指定目标索引。
`hostname`	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。
`remotehost`	否	指定只接受来自其数据的 IP 地址。
`resolvehost`	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。
`restrictToHost`	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”。

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。