使用S3和本地同步将Splunk与Umbrella日志管理集成

目录

简介

本文档介绍如何配置Splunk以分析来自思科管理的S3存储桶的DNS流量日志。

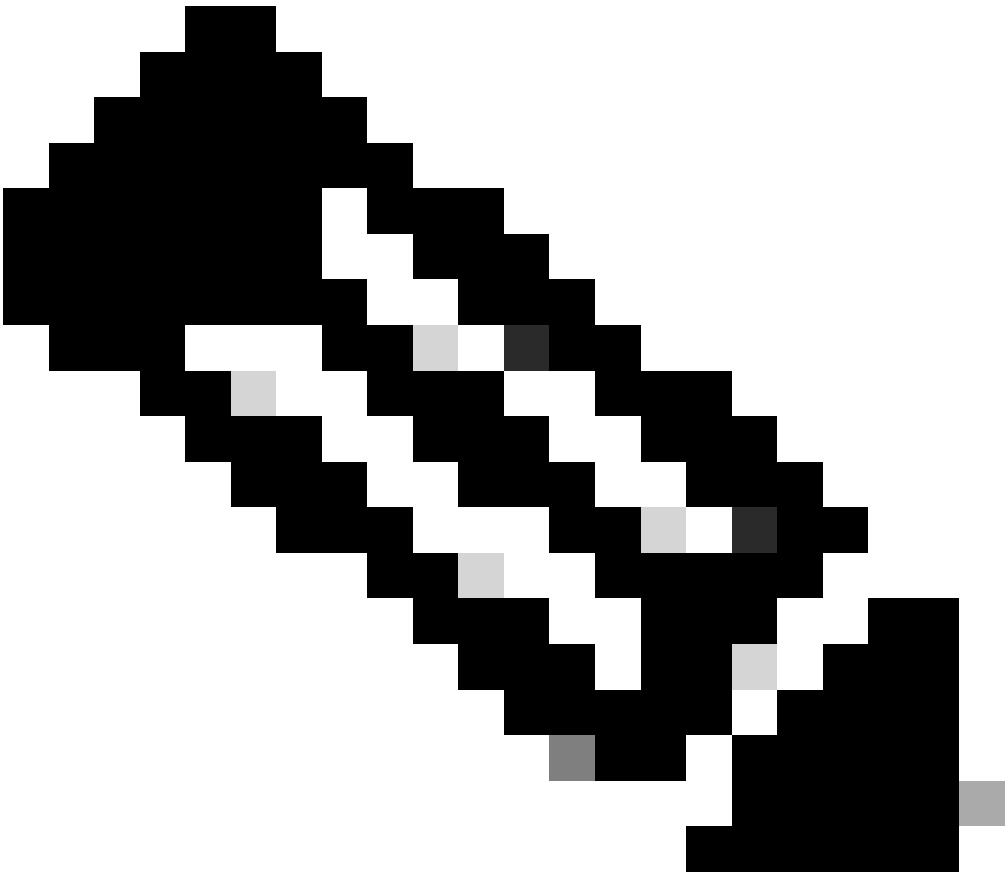
概述

Splunk是一种日志分析工具。它提供强大的接口来分析大数据块，例如Cisco Umbrella为DNS流量提供的日志。本文描述如何：

- 在您的控制面板中设置思科管理的S3存储桶。
- 确保满足AWS命令行界面(AWS CLI)必备条件。
- 创建cron作业以从存储桶中检索文件，并将这些文件本地存储在服务器上。
- 将Splunk配置为从本地目录读取。

先决条件

- 下载并安装AWS命令行界面(AWS CLI)。
- 创建思科管理的S3存储桶。



注意：现有的Umbrella Insights和Umbrella Platform客户可以通过控制面板访问Amazon S3的日志管理。并非所有包都提供“日志管理”。如果您对此功能感兴趣，请与您的客户经理联系。

在Splunk服务器上创建Cron作业

1. 使用提供的内容创**pull-umbrella-logs.sh**建名为shell脚本，该脚本在计划的cron作业上运行：

```
#!/bin/sh
cd <local data dir>
AWS_ACCESS_KEY_ID=<accesskey> AWS_SECRET_ACCESS_KEY=<secretkey> aws s3 sync <data path> .
```

用实际值替换占位符：

- :用于存储已下载日志文件的磁盘上的目录。
-

:从Umbrella控制面板访问密钥。

- :来自Umbrella控制面板的密钥。
- :来自日志管理UI的数据路径(例如s3://cisco-managed-

/1_2xxxxxxxxxxxxxxxxxa120c73a7c51fa6c61a4b6/dnslogs/

)。

2. 保存shell脚本并设置运行权限。脚本必须由root用户拥有。

```
$ chmod u+x pull-umbrella-logs.sh
```

3. 手动运pull-umbrella-logs.sh行脚本，确认同步进程运行正常。不需要完全完成；此步骤确认凭证和脚本逻辑正确。

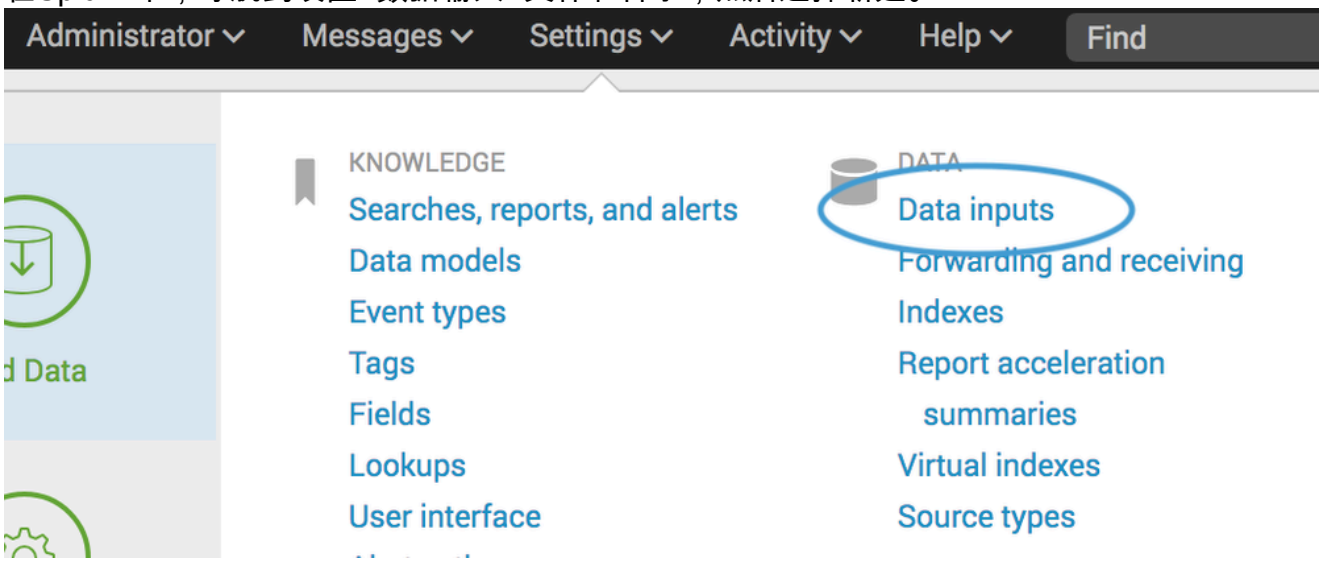
4. 将此行添加到Splunk服务器crontab:

```
*/5 * * * * root root /path/to/pull-umbrella-logs.sh &2>1 >/var/log/pull-umbrella-logs.txt
```

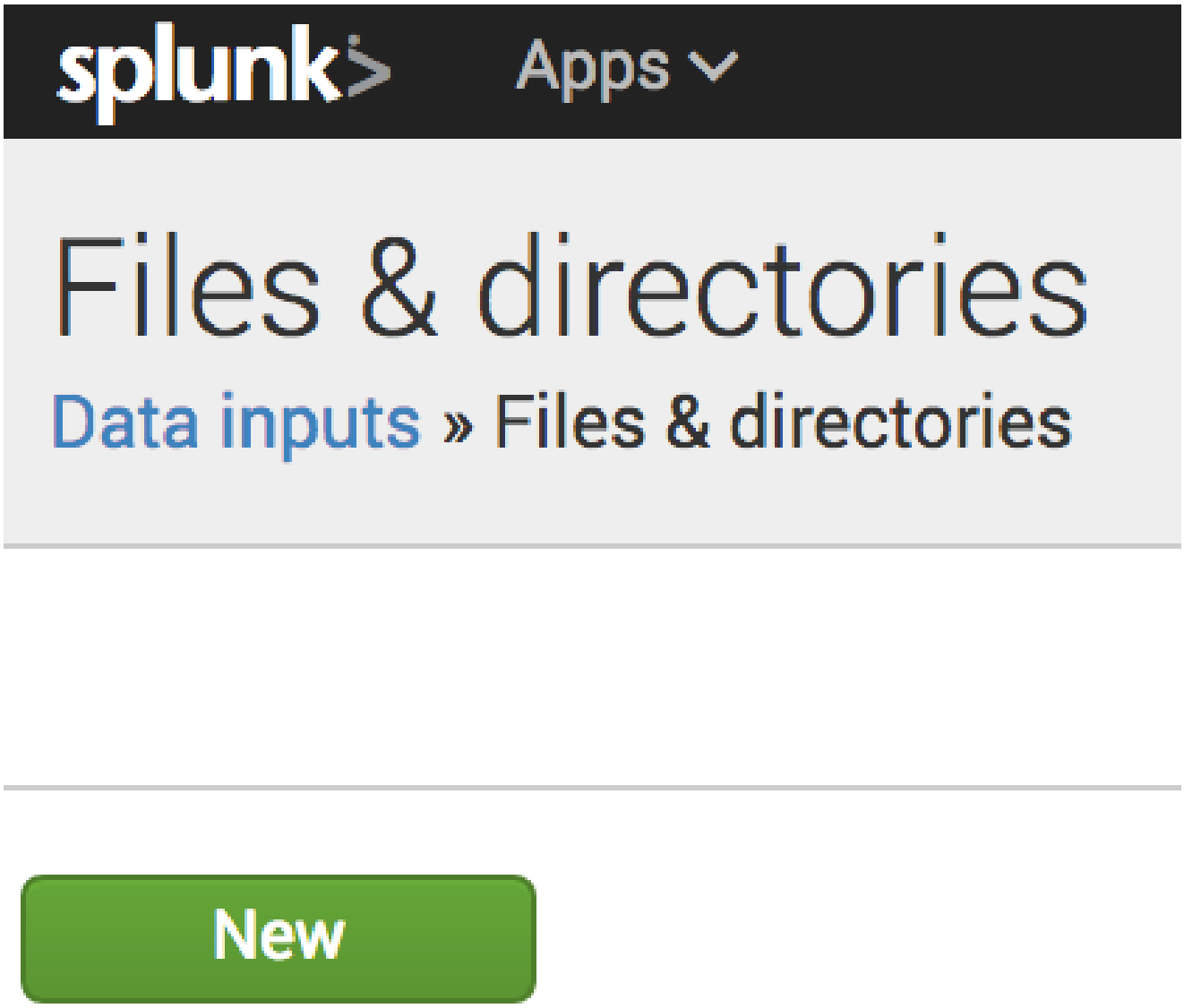
确保编辑该行以使用正确的脚本路径。每5分钟运行一次同步。S3存储目录每10分钟更新一次，数据在S3存储上保留30天。这样可使两者保持同步。

将Splunk配置为从本地目录读取

1. 在Splunk中，导航到设置>数据输入>文件和目录，然后选择新建。

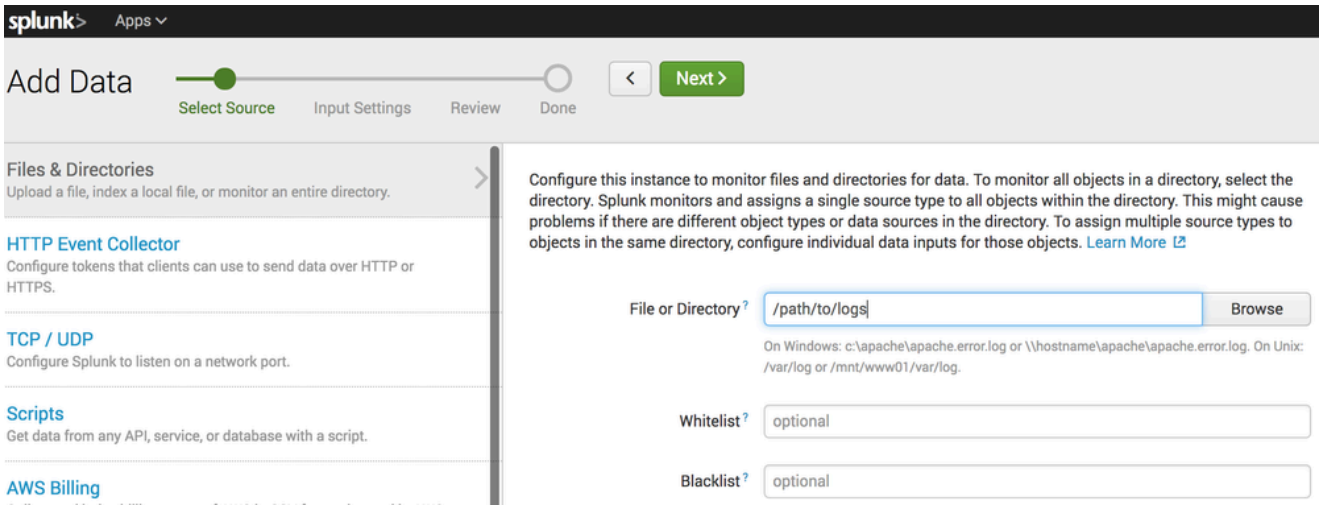


360002731126



360002731146

2. 在File or Directory字段中，指定S3同步放置文件的本地目录。



360002731106

3. 单击下一步，并使用默认设置完成向导。

一旦本地目录中有数据，并且配置了Splunk，数据就可以在Splunk中用于查询和报告。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。