使用S3和本地同步將Splunk與Umbrella日誌管理整合

目錄

簡介

本文檔介紹如何配置Splunk以分析來自Cisco管理的S3儲存桶的DNS流量日誌。

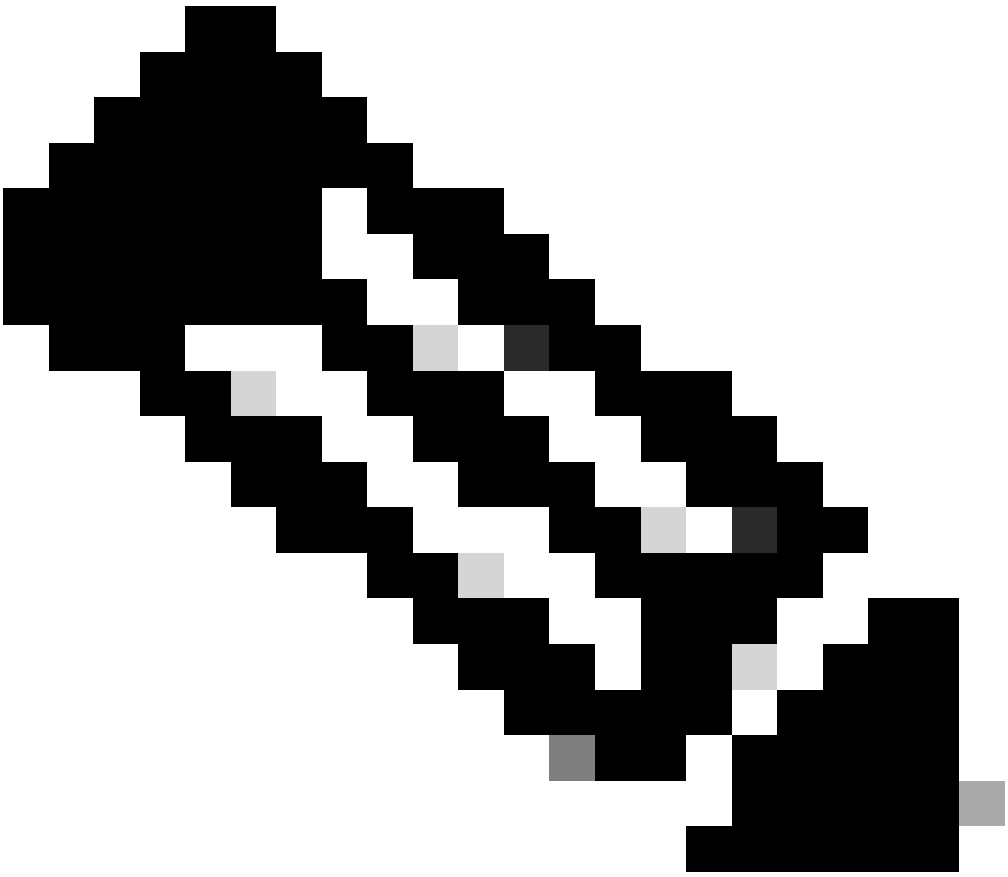
概觀

Splunk是日誌分析的工具。它提供強大的介面來分析大資料塊，例如Cisco Umbrella為DNS流量提供的日誌。本文描述如何：

- 在您的控制面板中設定思科管理的S3儲存桶。
- 確保滿足AWS命令列介面(AWS CLI)前提條件。
- 建立cron作業以從儲存桶中檢索檔案並將其儲存在本地伺服器上。
- 將Splunk配置為從本地目錄讀取。

必要條件

- 下載並安裝AWS命令列介面(AWS CLI)。
- 建立思科管理的S3儲存桶。



附註：現有的Umbrella Insights和Umbrella Platform客戶可以通過控制面板訪問Amazon S3的日誌管理。日誌管理並非在所有包中均可用。如果您對此功能感興趣，請聯絡您的客戶經理。

在Splunk伺服器上建立Cron作業

1. 使用提供的內容創**pull-umbrella-logs.sh**建名為shell指令碼，該指令碼在計畫的cron作業上運行：

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

用實際值替換佔位符：

- :用於儲存已下載日誌檔案的磁碟上的目錄。
-

:從Umbrella控制面板訪問金鑰。

- :來自Umbrella控制面板的金鑰。
- :來自日誌管理UI的資料路徑(例如s3://cisco-managed-

/1_2xxxxxxxxxxxxxxxxa120c73a7c51fa6c61a4b6/dnslogs/

)。

2. 儲存shell指令碼並設定運行許可權。指令碼必須由root使用者擁有。

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

3. 手動運pull-umbrella-logs.sh行指令碼，以確認同步進程是否正常工作。不需要完全完成；此步驟確認憑據和指令碼邏輯正確。

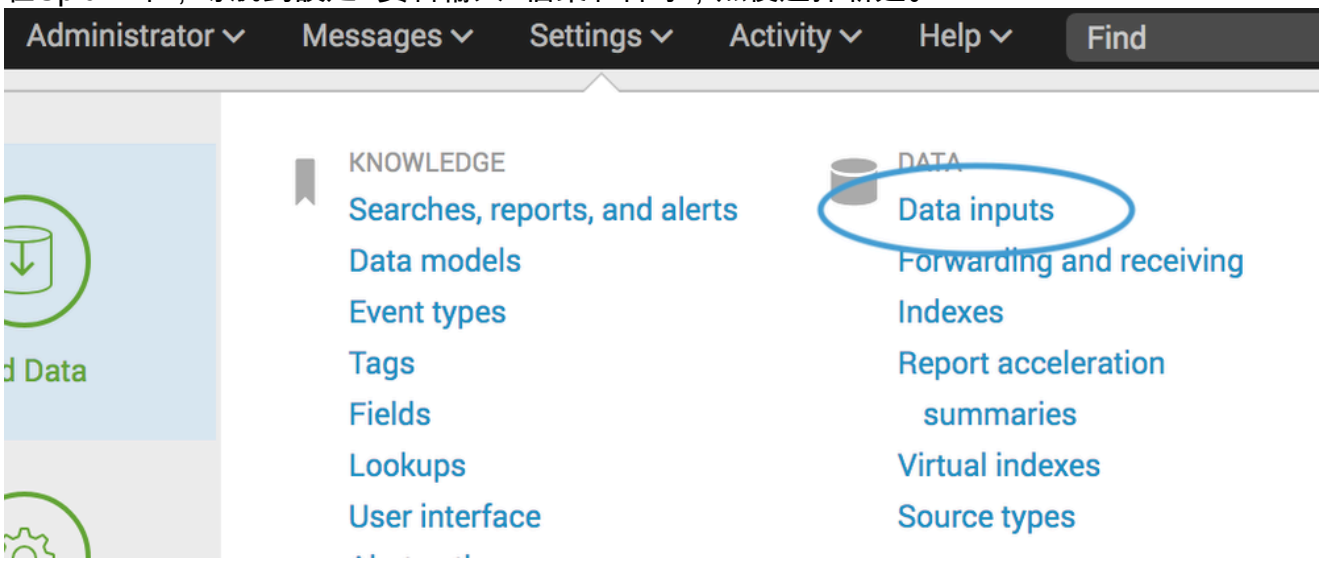
4. 將此行新增到Splunk伺服器crontab:

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

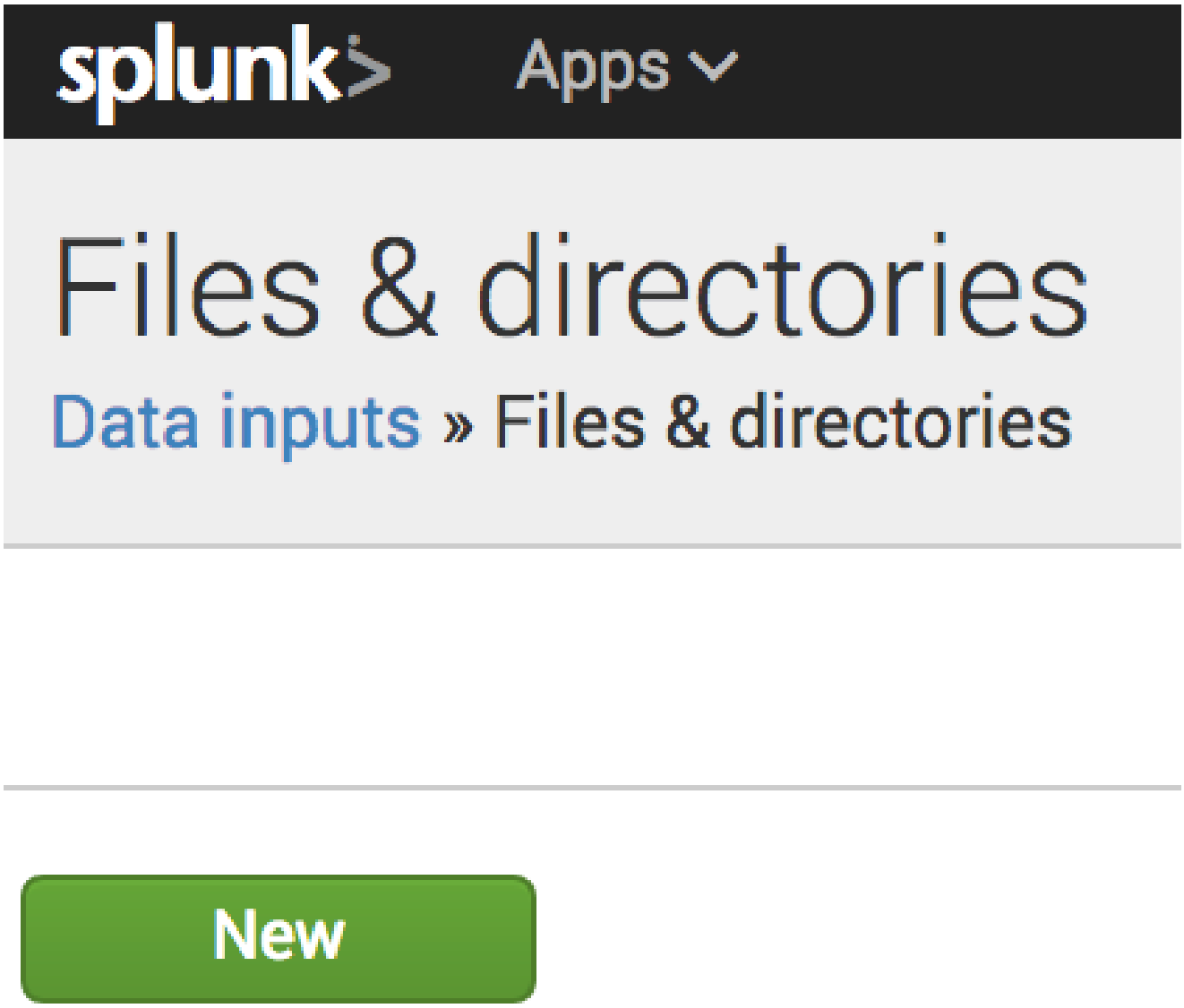
請務必編輯該行，以使用正確的指令碼路徑。每5分鐘運行一次同步。S3儲存目錄每10分鐘更新一次，資料在S3儲存上保留30天。這使得兩者保持同步。

將Splunk配置為從本地目錄讀取

1. 在Splunk中，導航到設定>資料輸入>檔案和目錄，然後選擇新建。

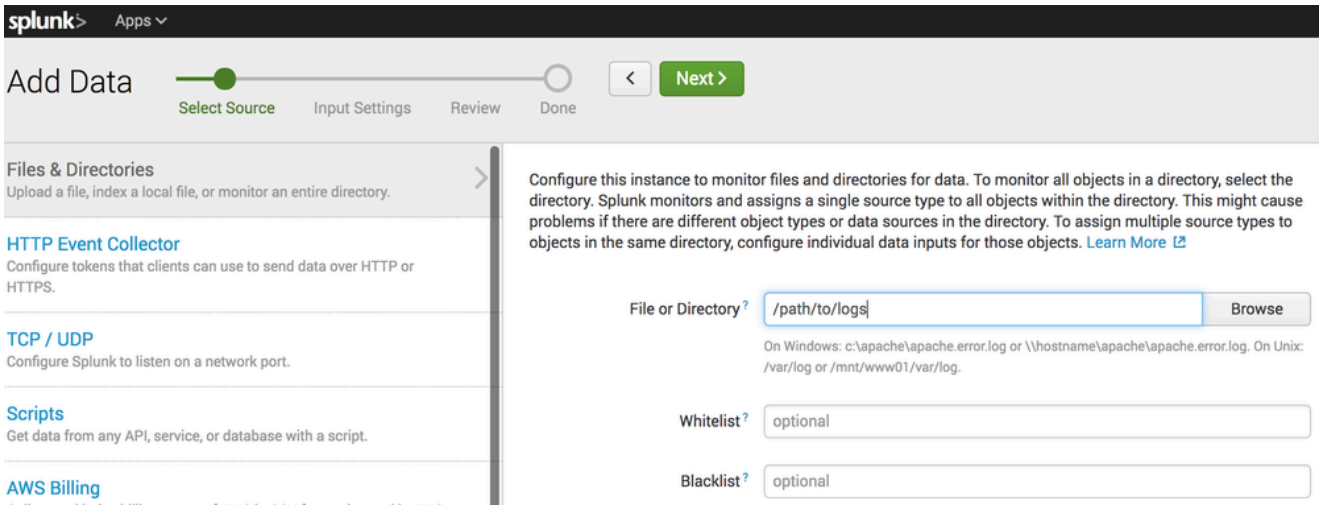


360002731126



360002731146

2. 在File or Directory欄位中，指定S3同步放置檔案的本地目錄。



360002731106

3. 按一下Next並使用預設設定完成嚮導。

一旦本地目錄中存在資料並且配置了Splunk，就可以在Splunk中對這些資料進行查詢和報告。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。