S3とローカル同期を使用したSplunkとUmbrella口グ管理の統合

内容

はじめに

このドキュメントでは、シスコが管理するS3バケットからのDNSトラフィック口グを分析するようにSplunkを設定する方法について説明します。

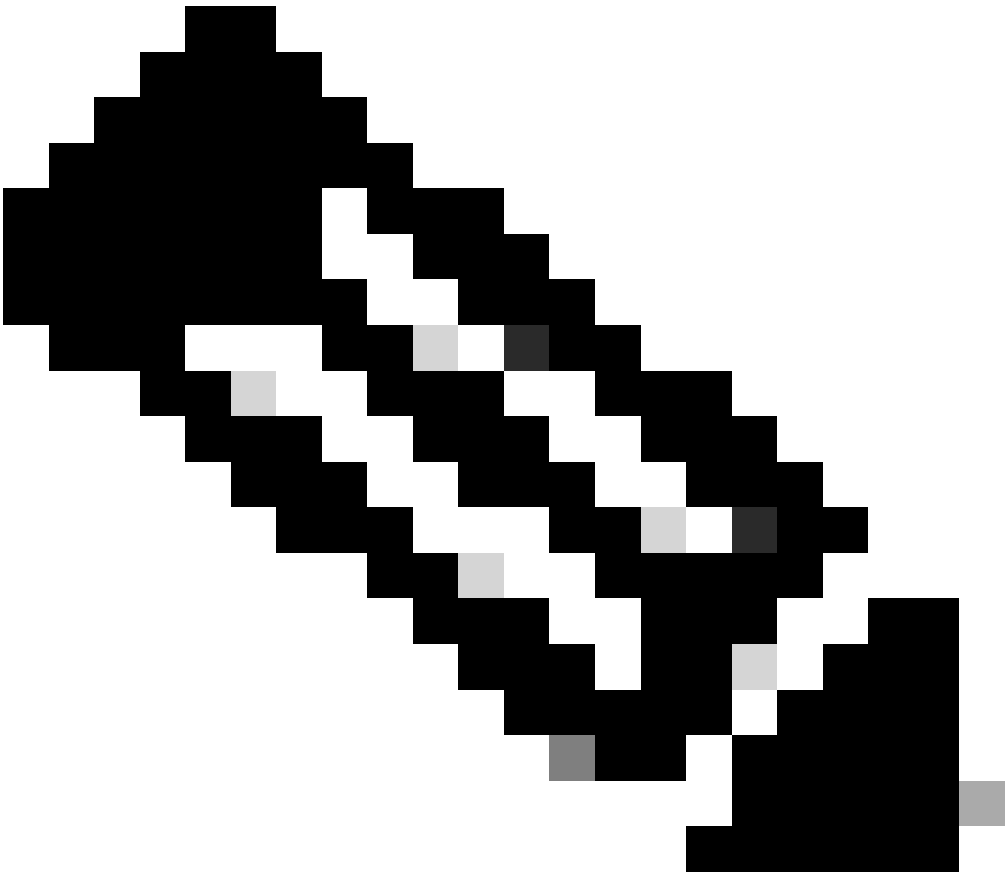
概要

Splunkは、口グ分析のためのツールです。DNSトラフィック用にCisco Umbrellaから提供される口グなど、大量のデータを分析するための強力なインターフェイスを提供します。この記事では、次の方法について説明します。

- ダッシュボードでシスコ管理のS3バケットを設定します。
- AWSコマンドラインインターフェイス(AWS CLI)の前提条件が満たされていることを確認します。
- cronジョブを作成して、バケットからファイルを取得し、サーバにローカルに保存します。
- ローカルディレクトリから読み取るようにSplunkを設定します。

前提条件

- AWSコマンドラインインターフェイス(AWS CLI)をダウンロードしてインストールします。
- シスコが管理するS3バケットを作成します。



注：既存のUmbrella InsightsおよびUmbrella Platformのお客様は、ダッシュボードを通じてAmazon S3のLog Managementにアクセスできます。ログ管理は、一部のパッケージでは使用できません。この機能に興味がある場合は、アカウントマネージャにお問い合わせください。

SplunkサーバでのCronジョブの作成

1. 指定された内容で**pull-umbrella-logs.sh**という名前のシェルスクリプトを作成します。このスクリプトは、スケジュールされたcronジョブで実行されます。

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

プレースホルダを実際の値に置き換えます。

- <local data

dir>：ダウンロードしたログファイルを保存するディスク上のディレクトリ。
- <accesskey>:Umbrellaダッシュボードからのアクセスキー。
- **<secretkey>**:Umbrellaダッシュボードの秘密キー。
- **<data path>**：ログ管理UIからのデータパス(例：s3://cisco-managed-<region>/1_2xxxxxxxxxxxxa120c73a7c51fa6c61a4b6/dnslogs/)。

2. シェルスクリプトを保存し、実行権限を設定します。スクリプトはrootが所有している必要があります。

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

3. **pull-umbrella-logs.sh**スクリプトを手動で実行して、同期プロセスが機能していることを確認します。このステップでは、クレデンシャルとスクリプトロジックが正しいことを確認するため、完全な完了は必要ありません。

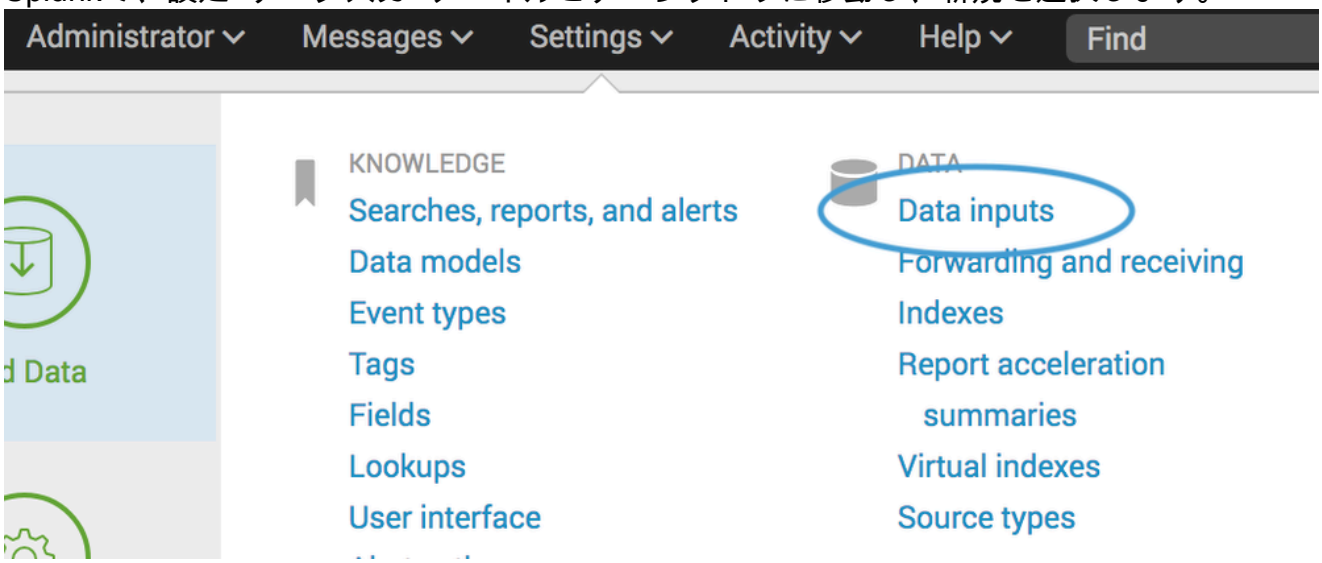
4. Splunkサーバのcrontabに次の行を追加します。

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

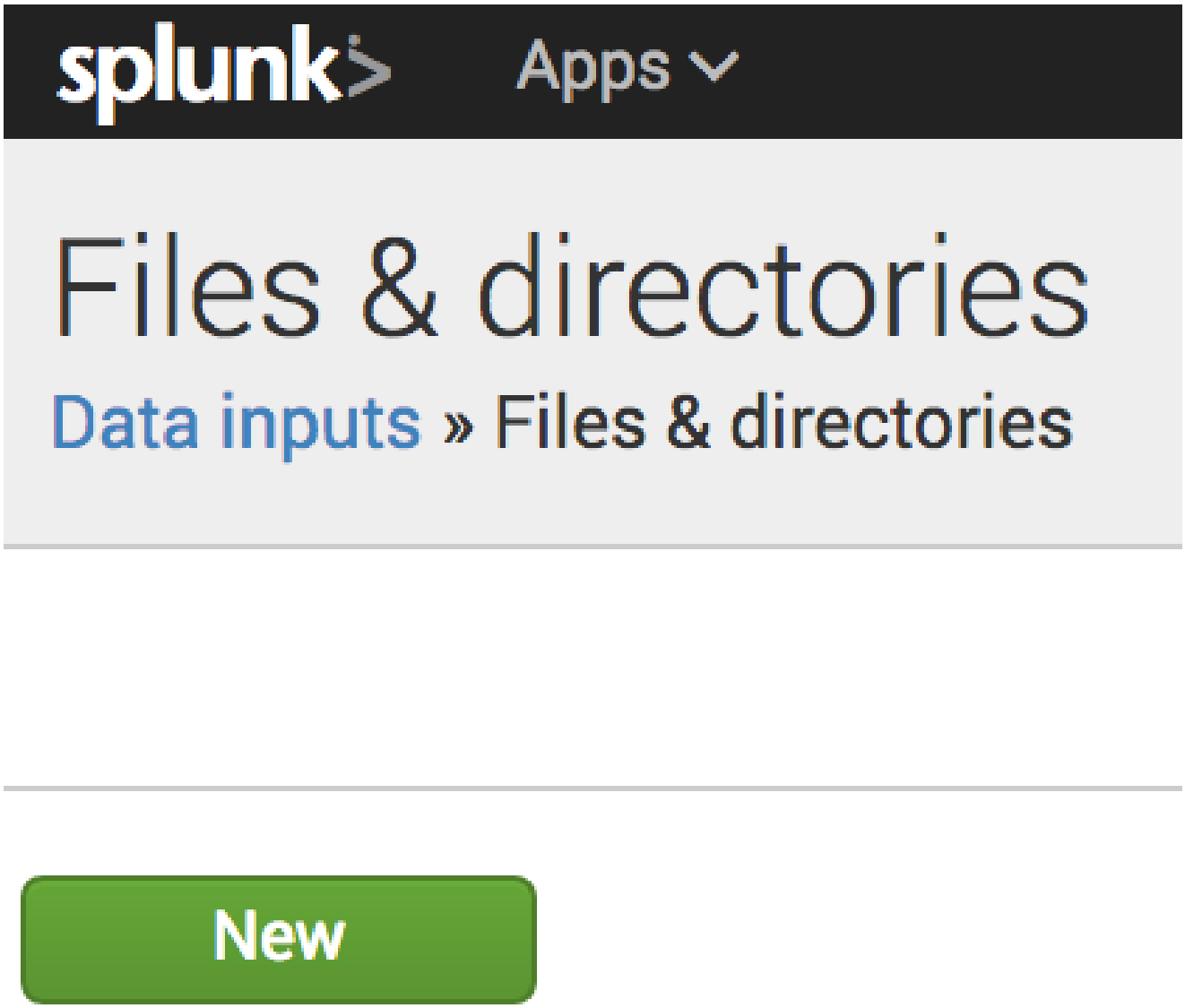
スクリプトへの正しいパスを使用するように行を編集してください。5分ごとに同期が実行されます。S3ストレージディレクトリは10分ごとに更新され、データはS3ストレージに30日間保持されます。これにより、2つのAPの同期が維持されます。

ローカルディレクトリから読み取るようにSplunkを設定する

1. Splunkで、設定>データ入力>ファイルとディレクトリに移動し、新規を選択します。

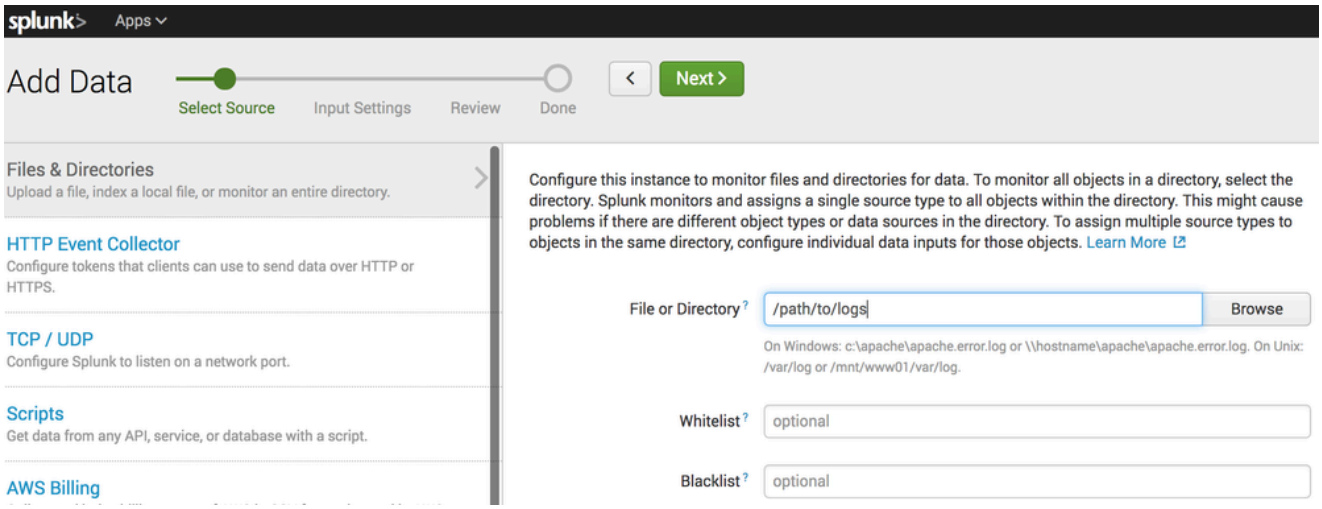


360002731126



360002731146

2. File or Directoryフィールドで、S3同期がファイルを配置するローカルディレクトリを指定します。



360002731106

3. Nextをクリックし、デフォルト設定でウィザードを完了します。

ローカルディレクトリにデータが存在し、Splunkが設定されると、そのデータをSplunkでクエリおよびレポートに使用できるようになります。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。