Integration von Splunk in Umbrella Log Management mit S3 und lokaler Synchronisierung

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Splunk für die Analyse von DNS-Datenverkehrsprotokollen aus einem von Cisco verwalteten S3-Bucket konfiguriert wird.

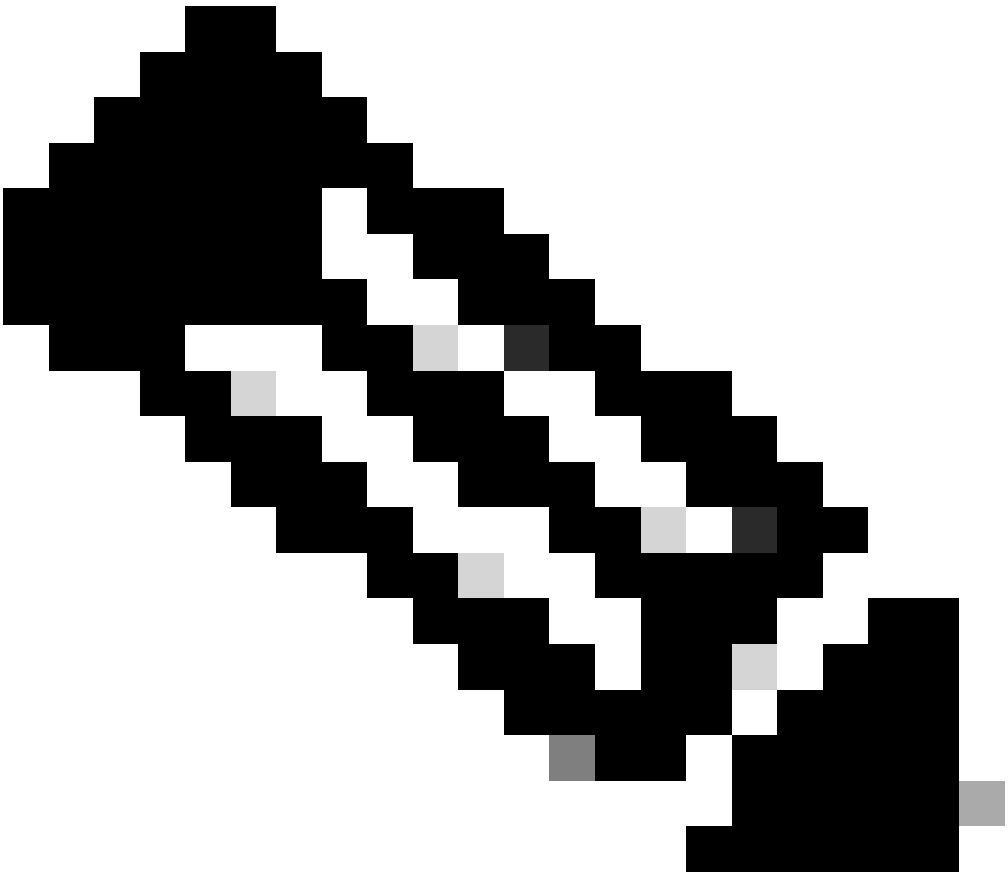
Überblick

Splunk ist ein Tool zur Protokollanalyse. Es bietet eine leistungsstarke Schnittstelle zum Analysieren großer Datenmengen, wie z. B. die von Cisco Umbrella für Ihren DNS-Datenverkehr bereitgestellten Protokolle. In diesem Artikel wird Folgendes beschrieben:

- Richten Sie Ihre von Cisco verwaltete S3-Bucket in Ihrem Dashboard ein.
- Stellen Sie sicher, dass die AWS-Befehlszeilenschnittstelle (AWS CLI) die Voraussetzungen erfüllt.
- Erstellen Sie einen Cron-Job, um Dateien aus dem Bucket abzurufen und lokal auf dem Server zu speichern.
- Konfigurieren von Splunk zum Lesen aus einem lokalen Verzeichnis

Voraussetzungen

- Laden Sie die AWS-Befehlszeilenschnittstelle (AWS CLI) herunter, und installieren Sie sie.
- Erstellen Sie Ihren von Cisco verwalteten S3-Bucket.



Anmerkung: Bestehende Umbrella Insights- und Umbrella Platform-Kunden können über das Dashboard auf Log Management mit Amazon S3 zugreifen. Die Protokollverwaltung ist nicht in allen Paketen verfügbar. Wenden Sie sich an Ihren Account Manager, wenn Sie an dieser Funktion interessiert sind.

Erstellen eines Cron-Auftrags auf dem Splunk-Server

1. Erstellen Sie ein Shell-Skript mit **pull-umbrella-logs.sh** dem angegebenen Inhalt, das auf einem geplanten Cron-Job ausgeführt wird:

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

Ersetzen Sie die Platzhalter durch Ihre tatsächlichen Werte:

-

: Verzeichnis auf der Festplatte, in dem die heruntergeladenen Protokolldateien gespeichert werden.

- : Zugriffsschlüssel über das Umbrella Dashboard.
- : Geheimer Schlüssel aus dem Umbrella Dashboard.
- : Datenpfad von der Benutzeroberfläche für die Protokollverwaltung (z. B. s3://cisco-managed-

/1_2xxxxxxxxxxxxxxxxxa120c73a7c51fa6c61a4b6/dnslogs/

).

2. Speichern Sie das Shell-Skript, und legen Sie die Ausführungsberechtigung fest. Das Skript muss im Besitz von root sein.

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

3. Führen Sie das **pull-umbrella-logs.sh** Skript manuell aus, um sicherzustellen, dass der Synchronisierungsprozess funktioniert. Eine vollständige Durchführung ist nicht erforderlich. Mit diesem Schritt wird bestätigt, dass die Anmeldeinformationen und die Skriptlogik korrekt sind.

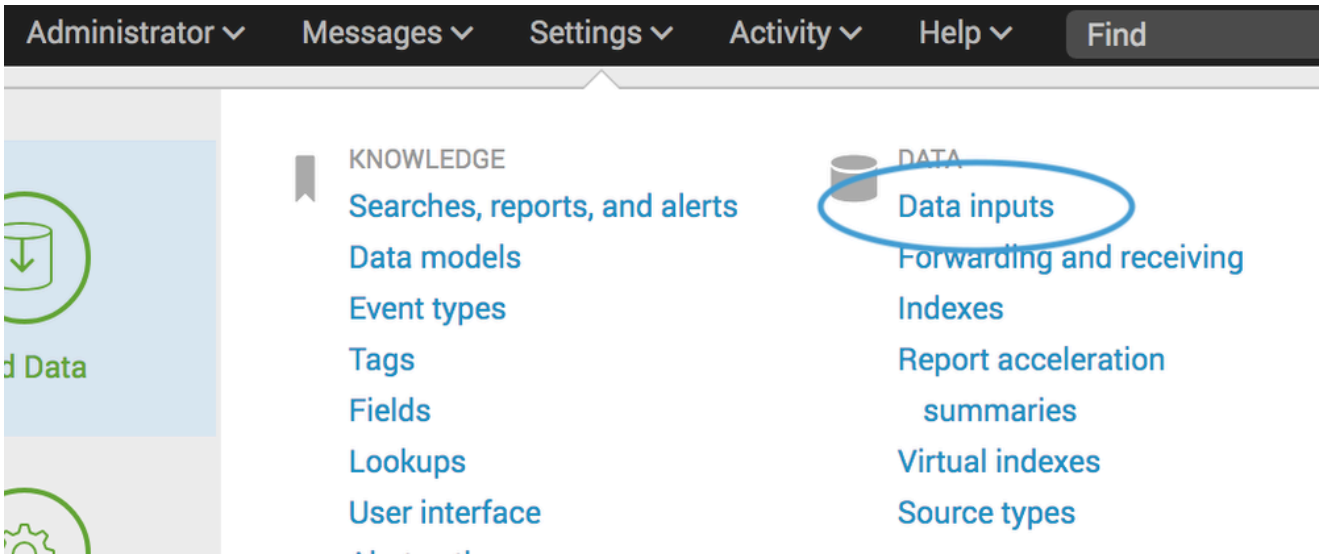
4. Fügen Sie diese Zeile zur crontab Ihres Splunk-Servers hinzu:

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

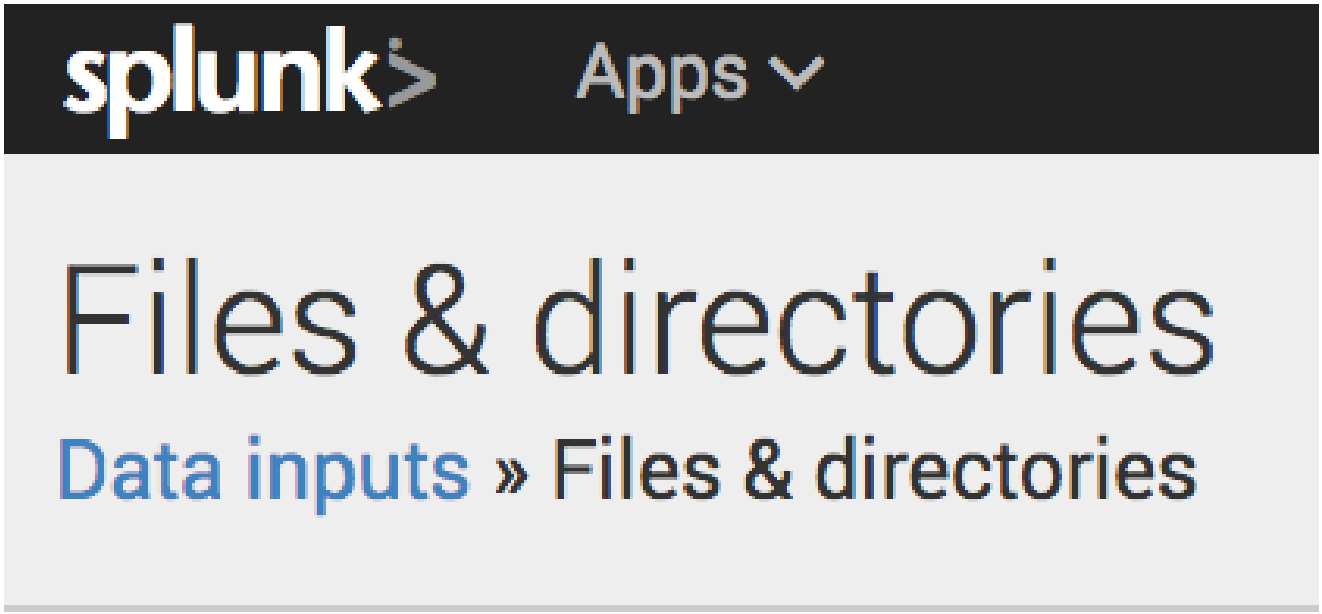
Stellen Sie sicher, dass Sie die Zeile bearbeiten, um den richtigen Pfad zum Skript zu verwenden. Das führt alle fünf Minuten eine Synchronisierung durch. Das S3-Speicherverzeichnis wird alle 10 Minuten aktualisiert, und die Daten verbleiben 30 Tage im S3-Speicher. Dadurch bleiben die beiden synchronisiert.

Konfigurieren von Splunk zum Lesen aus einem lokalen Verzeichnis

1. Navigieren Sie in Splunk zu Einstellungen > Dateneingaben > Dateien & Verzeichnisse, und wählen Sie Neu aus.

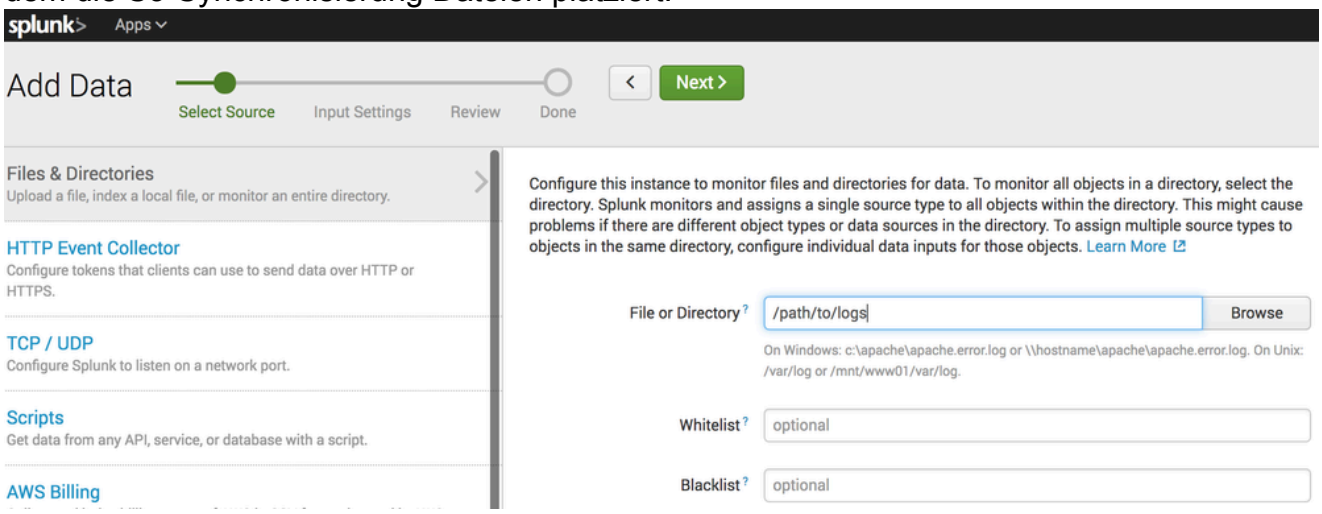


360002731126



360002731146

2. Geben Sie im Feld File (Datei) oder Directory (Verzeichnis) das lokale Verzeichnis an, in dem die S3-Synchronisierung Dateien platziert.



360002731106

3. Klicken Sie auf Weiter, und schließen Sie den Assistenten mit den Standardeinstellungen ab.

Sobald sich Daten im lokalen Verzeichnis befinden und Splunk konfiguriert ist, können die Daten in Splunk abgefragt und gemeldet werden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.