S3 및 로컬 동기화를 사용하여 Splunk를 Umbrella 로그 관리와 통합

목차

소개

이 문서에서는 Cisco 관리 S3 버킷의 DNS 트래픽 로그를 분석하도록 Splunk를 구성하는 방법에 대해 설명합니다.

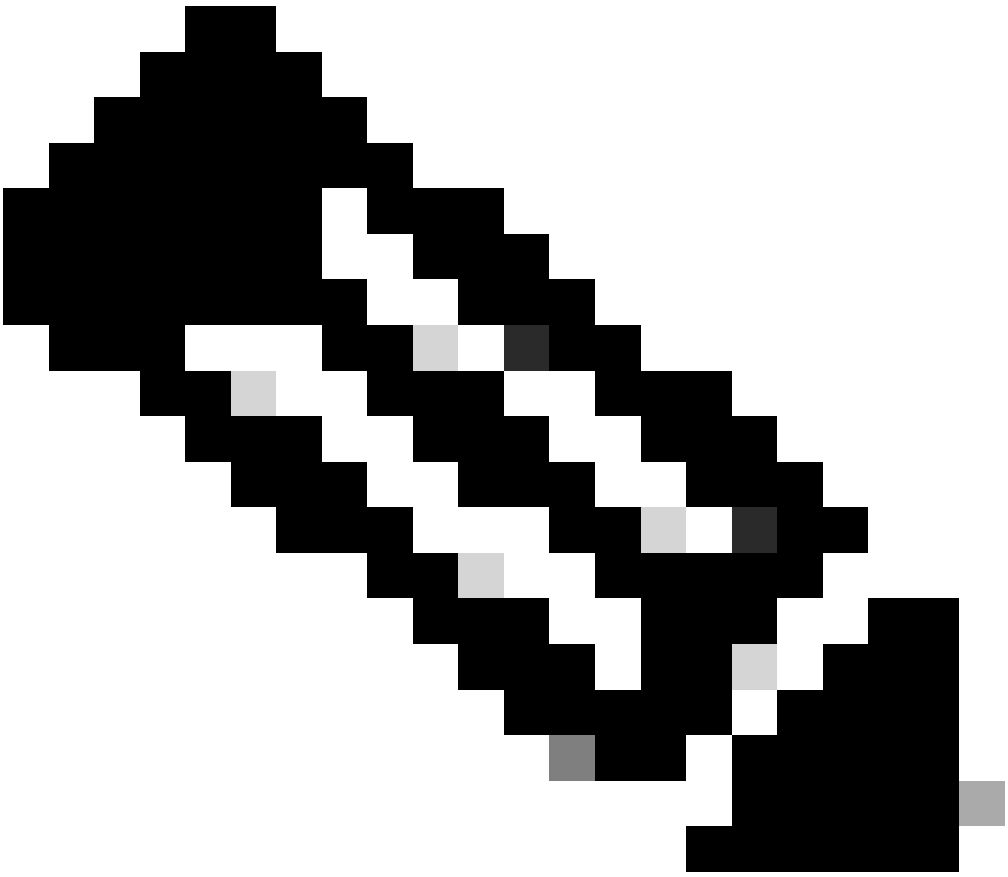
개요

Splunk는 로그 분석을 위한 툴입니다. DNS 트래픽을 위해 Cisco Umbrella에서 제공하는 로그와 같은 대용량 데이터를 분석할 수 있는 강력한 인터페이스를 제공합니다. 이 문서에서는 다음 작업을 수행하는 방법을 설명합니다.

- 대시보드에서 Cisco 매니지드 S3 버킷을 설정합니다.
- AWS 명령줄 인터페이스(AWS CLI) 사전 요구 사항이 충족되었는지 확인합니다.
- 버킷에서 파일을 검색하고 서버에 로컬로 저장하는 cron 작업을 만듭니다.
- 로컬 디렉터리에서 읽도록 Splunk를 구성합니다.

사전 요구 사항

- AWS 명령줄 인터페이스(AWS CLI)를 다운로드하고 설치합니다.
- Cisco 매니지드 S3 버킷을 생성합니다.



참고: 기존 Umbrella Insights 및 Umbrella Platform 고객은 대시보드를 통해 Amazon S3로 로그 관리에 액세스할 수 있습니다. 로그 관리는 일부 패키지에서 사용할 수 없습니다. 이 기능에 관심이 있는 경우 어카운트 매니저에게 문의하십시오.

Splunk 서버에서 Cron 작업 생성

1. 예약된 cron 작업에서 실행되**pull-umbrella-logs.sh**는 제공된 내용으로 명명된 셸 스크립트를 만듭니다.

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

자리 표시자를 실제 값으로 바꿉니다.

-

: 다운로드한 로그 파일을 저장할 디스크의 디렉토리

- : Umbrella 대시보드에서 키에 액세스합니다.
- : Umbrella 대시보드의 비밀 키입니다.
- : 로그 관리 UI의 데이터 경로(예:)s3://cisco-managed-

/1_2xxxxxxxxxxxxxxxxxa120c73a7c51fa6c61a4b6/dnslogs/

.

2. 셸 스크립트를 저장하고 실행 권한을 설정합니다. 스크립트는 root가 소유해야 합니다.

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

3. 스크립트를 **pull-umbrella-logs.sh** 수동으로 실행하여 동기화 프로세스가 작동하는지 확인합니다. 완전한 완성은 필요하지 않습니다. 이 단계에서는 자격 증명 및 스크립트 로직이 올바른지 확인합니다.

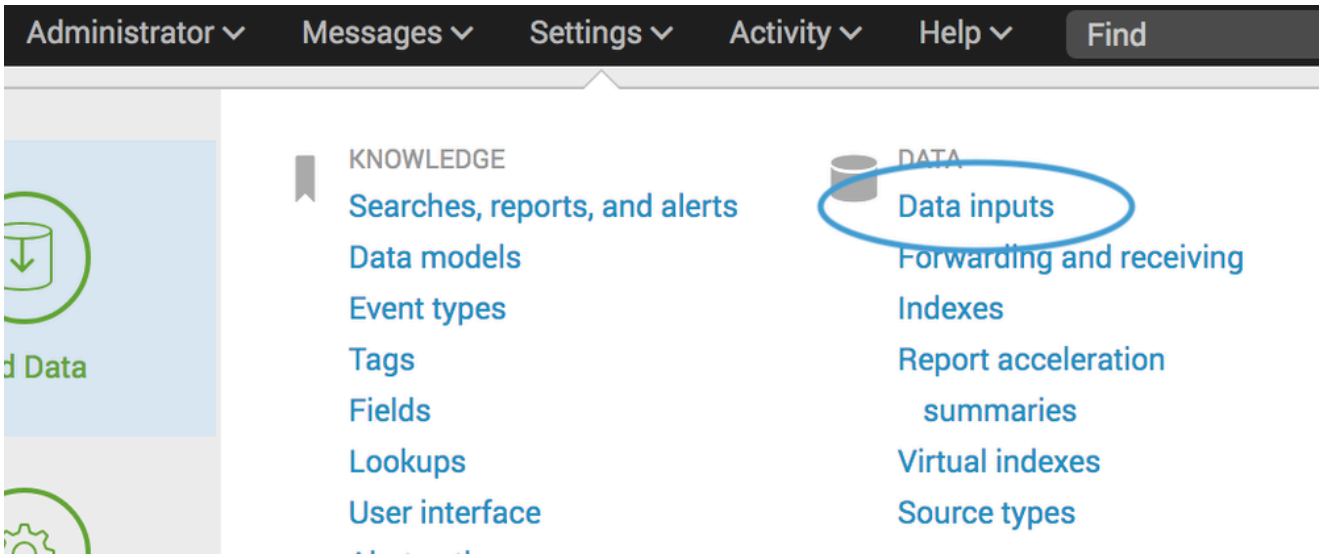
4. Splunk server crontab에 이 행을 추가합니다.

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

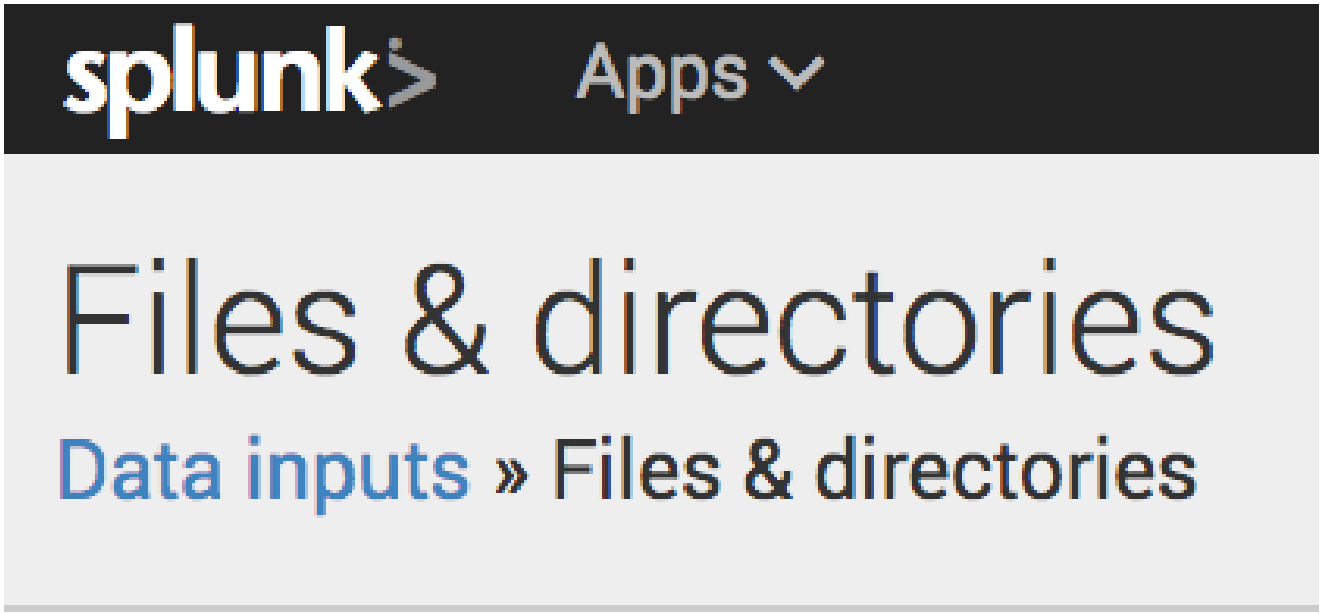
스크립트에 대한 올바른 경로를 사용하도록 줄을 편집해야 합니다. 이렇게 하면 5분마다 동기화가 실행됩니다. S3 스토리지 디렉토리는 10분마다 업데이트되며 데이터는 30일 동안 S3 스토리지에 유지됩니다. 이렇게 하면 두 항목이 동기화됩니다.

로컬 디렉터리에서 읽을 Splunk 구성

1. Splunk에서 Settings(설정) > Data Inputs(데이터 입력) > Files & Directories(파일 및 디렉토리)로 이동하고 New(새로 만들기)를 선택합니다.

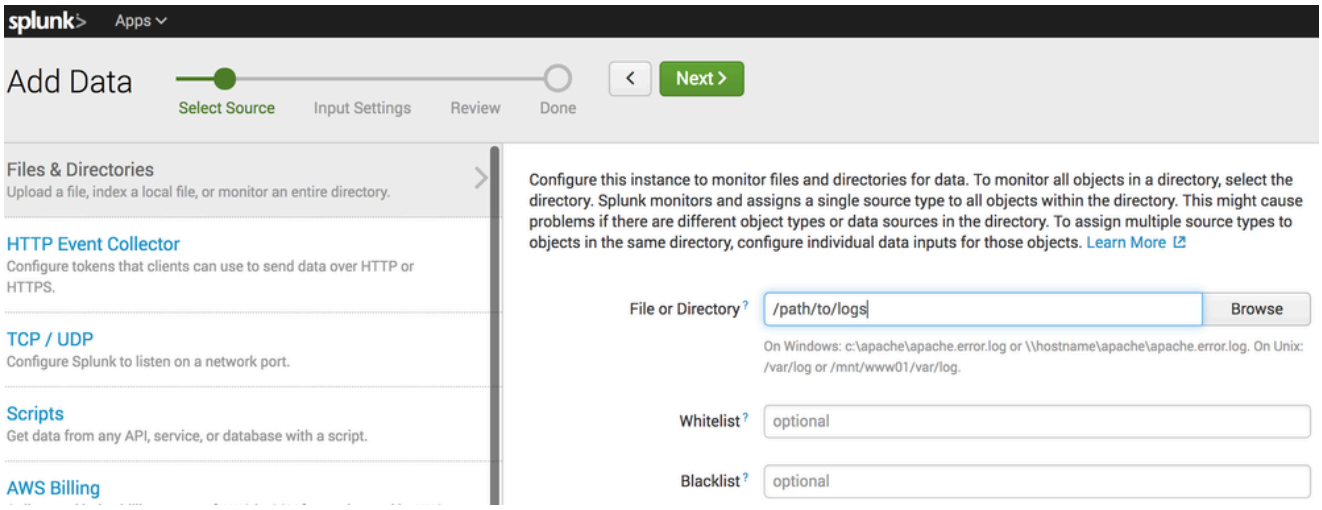


360002731126



360002731146

2. File or Directory(파일 또는 디렉토리) 필드에서 S3 동기화가 파일을 배치하는 로컬 디렉토리를 지정합니다.



360002731106

3. Next(다음)를 클릭하고 기본 설정을 사용하여 마법사를 완료합니다.

로컬 디렉토리에 데이터가 있고 Splunk가 구성되면 Splunk에서 데이터를 쿼리하고 보고하는 데 사용할 수 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.