셀프 관리 S3 버킷으로 Splunk 구성

목차

소개

이 문서에서는 셀프 관리 S3 버킷으로 Splunk를 구성하는 방법에 대해 설명합니다.

개요

Splunk는 로그 분석을 위한 일반적인 툴입니다. Cisco Umbrella는 조직의 DNS 트래픽을 위해 Cisco Umbrella에서 제공하는 로그와 같은 대량의 데이터를 분석할 수 있는 강력한 인터페이스를 제공합니다.

이 문서에서는 Splunk가 S3 버킷에서 로그를 가져와 사용할 수 있도록 Splunk를 설치하고 실행하는 기본 사항에 대해 간략하게 설명합니다. 두 가지 주요 단계가 있습니다. 하나는 Splunk가 로그에 액세스할 수 있도록 AWS S3 보안 자격 증명을 구성하는 것이고, 두 번째는 버킷을 가리키도록 Splunk 자체를 구성하는 것입니다.

AWS S3용 Splunk 추가 기능에 대한 설명서가 여기에 있으며, 이 중 일부는 이 문서에 축어적으로 복사되었습니다. Splunk 설정에 대한 구체적인 질문은 http://docs.splunk.com/Documentation/AddOns/latest/AWS/Description을 참조하십시오.

이 문서에는 다음 섹션이 있습니다.

- 사전 요구 사항
- 1단계: AWS에서 보안 자격 증명 구성(자체 관리 버킷 전용)
- 2단계: S3 버킷에서 DNS 로그 데이터를 가져오도록 Splunk 설정
    - 1단계: 자체 관리 S3 버킷에서 DNS 로그 데이터를 가져오도록 Splunk 설정
- 3단계: Splunk에 대한 데이터 입력 구성

사전 요구 사항

Amazon Web Services용 Splunk 추가 기능은 이러한 플랫폼을 지원합니다.

- AWS 리눅스
- 레드햇
- Windows 2008R2, 2012R2

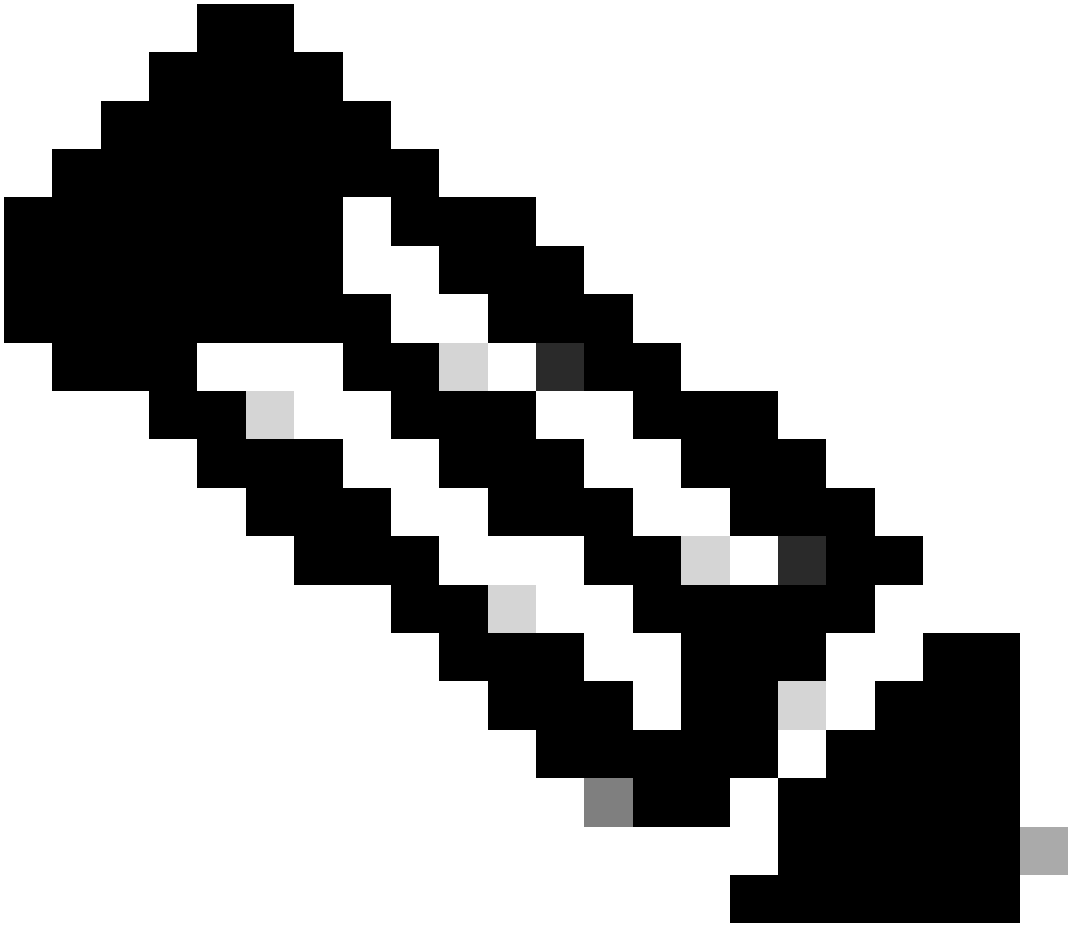
Splunk Enterprise 시스템 요구 사항

이 애드온은 Splunk Enterprise에서 실행되므로 Splunk Enterprise 시스템의 모든 요구 사항이 적용됩니다. Splunk Enterprise 설명서의 "시스템 요구 사항" 설치 설명서를 참조하십시오. 이 지침은 Splunk Enterprise 버전 6.2.1을 위한 것입니다.

Umbrella 요건

이 문서에서는 Amazon AWS S3 버킷이 Umbrella 대시보드(Admin> Log Management)에 구성되었으며 최근 로그가 업로드된 상태에서 녹색으로 표시된다고 가정합니다. 로그 관리에 대한 자세한 내용은 Amazon S3의 Cisco Umbrella Log Management를 참조하십시오.

1단계: AWS에서 보안 자격 증명 구성



참고: 이러한 단계는 버킷에서 로그를 다운로드하기 위해 도구를 구성하는 방법을 설명하는 문서에 설명된 단계와 동일합니다(방법: AWS S3의 Cisco Umbrella Log Management에서 로그 다운로드). 이러한 단계를 이미 수행한 경우 2단계로 건너뛸 수 있습니다. 단, IAM 사용자의 보안 자격 증명이 있어야 버킷에 대한 Splunk 플러그인을 인증할 수 있습니다.

1단계

1. Amazon Web Services 계정에 액세스 키를 추가하여 로컬 툴에 대한 원격 액세스를 허용하고 S3에서 파일을 업로드, 다운로드 및 수정할 수 있는 기능을 제공합니다. AWS에 로그인하고 오른쪽 상단에 있는 계정 이름을 클릭합니다. 드롭다운에서 Security Credentials를 선택합니다.
2. Amazon 모범 사례를 사용하고 AWS Identity and Access Management(IAM) 사용자를 생성하라는 메시지가 표시됩니다. 기본적으로 IAM 사용자는 s3cmd가 버킷에 액세스하는 데 사용하는 계정이 전체 S3 컨피그레이션의 기본 계정(예: 계정)이 아닌지 확인합니다. 계정에 액세스하는 사용자를 위해 개별 IAM 사용자를 생성하면 각 IAM 사용자에게 고유한 보안 자격 증명 집합을 제공할 수 있습니다. 각 IAM 사용자에게 서로 다른 권한을 부여할 수도 있습니다. 필요한 경우 언제든지 IAM 사용자의 권한을 변경하거나 취소할 수 있습니다.

IAM 사용자 및 AWS 모범 사례에 대한 자세한 내용은 다음을 참조하십시오.
https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

2단계

1. Get Started with IAM Users를 클릭하여 S3 버킷에 액세스할 IAM 사용자를 만듭니다. IAM 사용자를 생성할 수 있는 화면으로 이동합니다.
2. Create New Users(새 사용자 생성)를 클릭한 다음 필드를 입력합니다. 사용자 계정에는 공백을 포함할 수 없습니다.
3. 사용자 계정을 생성한 후에는 Amazon User Security 자격 증명이 포함된 두 가지 중요한 정보를 얻을 수 있는 기회가 한 번만 주어집니다. 오른쪽 아래 버튼을 사용하여 이러한 정보를 다운로드하고 백업하는 것이 좋습니다. 이 단계는 설치 시 이후로는 사용할 수 없습니다. 나중에 Splunk를 설정할 때 필요한 액세스 키 ID와 비밀 액세스 키를 모두 기록해 두십시오.

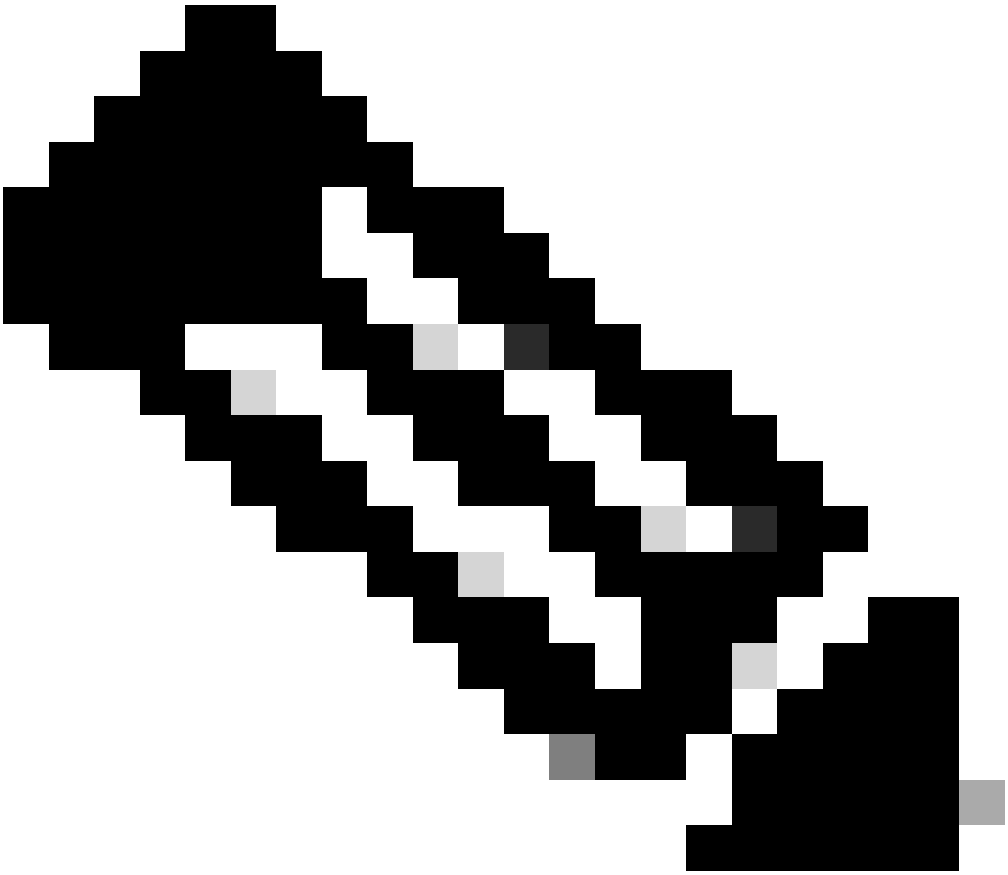
3단계

1. 그런 다음 IAM 사용자가 S3 버킷에 액세스할 수 있도록 정책을 추가합니다. 방금 생성한 사용자를 클릭한 다음 Attach Policy(정책 첨부) 버튼이 표시될 때까지 사용자의 등록 정보를 아래로 스크롤합니다.
2. Attach Policy(정책 연결)를 클릭한 다음 정책 유형 필터에 's3'을 입력합니다. 이는 다음 두 가지 결과를 보여 줍니다. "AmazonS3FullAccess" 및 "AmazonS3ReadOnlyAccess".
3. AmazonS3FullAccess를 선택하고 Attach Policy를 클릭합니다.

2단계: S3 버킷에서 DNS 로그 데이터를 가져오도록 Splunk 설정

1단계: 셀프 관리 S3 버킷에서 DNS 로그 데이터를 가져오도록 Splunk 설정

1. 먼저 Splunk 인스턴스에 "Amazon Web Services용 Splunk 추가 기능"을 설치합니다. Splunk 대시보드를 열고 Apps를 클릭하거나, 대시보드에 Splunk Apps가 나타나면 Splunk Apps를 클릭합니다. Apps(앱) 섹션에 검색 창에 "s3"를 입력하여 "Amazon Web Services용 Splunk 추가 기능"을 찾은 다음 앱을 설치합니다.



참고: 설치하는 동안 Splunk를 다시 시작해야 합니다.
설치가 완료되면 Apps 아래에 폴더 이름 'Splunk_TA_aws'가 표시된 Splunk Add-on for AWS가 표시됩니다.

2. 설정을 클릭하여 앱을 구성합니다. 이 설명서에서 1단계의 보안 자격 증명이 필요한 지점입니다.
설치하려면 다음 필드를 입력해야 합니다.

- 친숙한 이름 - 이 통합을 참조하는 데 사용하는 이름
- AWS 계정 키 ID(1단계 이후)
- 비밀번호(AWS 계정 비밀 키, 1단계)

또한 Splunk에서 AWS에 연결하는 데 필요한 로컬 프록시 정보를 설정하고 로깅을 조정할 수 있습니다. 설정 화면은 다음과 같습니다.
3. 관련 정보를 추가했으면 저장을 클릭합니다. 그러면 Amazon Web Services용 Splunk 추가 기능이 완전히 구성됩니다.

3단계: Splunk에 대한 데이터 입력 구성

1. 다음으로, Amazon Web Services S3에 대한 데이터 입력을 구성하려고 합니다. 설정 > 데이터 > 데이터 입력으로 이동하고 로컬 입력 아래에 S3를 포함한 다양한 Amazon 입력의 목록이 목록 맨 아래에 표시됩니다.
2. 입력을 구성하려면 AWS S3를 클릭합니다.
3. 새로 만들기를 클릭합니다.
4. 다음 정보를 제공해야 합니다.

    - S3 통합의 이름을 입력합니다.
    - 선택: 드롭다운 메뉴에서 AWS 계정을 선택합니다. 1단계에서 제공한 친숙한 이름입니다.
    - 드롭다운에서 S3 버킷을 선택합니다. Umbrella 대시보드(Settings(설정) > Log Management(로그 관리))에 지정된 버킷 이름입니다.
    - 드롭다운에서 S3 키 이름을 선택합니다. 버킷의 모든 항목이 나열됩니다. 그 아래에 모든 파일과 디렉토리가 포함된 최상위 디렉토리 \dns-logs\를 선택하는 것이 좋습니다.
    - "메시지 시스템 컨피그레이션"에는 몇 가지 옵션이 있습니다. 이러한 옵션은 기본 설정인 그대로 두는 것이 좋습니다.
    - "More settings(추가 설정)" 아래에 추가 옵션이 있습니다. 기본적으로 aws:s3인 "Source type"이 있습니다. 이를 그대로 두는 것이 좋지만, 이를 변경하는 경우 검색의 로그 필터가 이 지침의 3단계에 설명된 것과 다르게 변경됩니다.

    세부 정보를 채우면 데이터 입력이 다음과 비슷하게 표시됩니다.

4. 다음을 눌러 상세내역을 완료합니다.
   입력이 성공적으로 생성되었음을 보여주는 화면이 나타납니다

3단계

빠른 검색을 수행하여 데이터를 제대로 가져오고 있는지 확인합니다. 오른쪽 위의 Search 창에 sourcetype="aws:s3"을 붙여넣고 검색에서 "Open sourcetype="aws:s3"을 선택합니다.

이렇게 하면 조직의 DNS 로그에서 이벤트가 표시되는 화면과 유사한 화면이 표시됩니다. 여기서 Cisco Umbrella 모바일 서비스는 iPhone에서 소셜 미디어를 차단하고 있습니다. 파일 이름의 소스를 사용하여 특정 로그 배치에 대해 필터링할 수도 있습니다.

이 시점 이후에는 백그라운드의 cron 작업이 계속 실행되면서 버킷의 로그 정보에서 최신 세트를 가져옵니다.

Splunk는 이 문서에서 설명한 것 외에도 많은 작업을 수행할 수 있습니다. 보안 대응 절차에서 이 데이터를 사용해 볼 수 있는 기회가 있다면 여러분의 의견을 듣고 싶습니다. 피드백, 질문 또는 우려 사항은 umbrella-support@cisco.com으로 보내고 이 문서를 참조하시기 바랍니다.

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.