

AWS S3의 Umbrella Log Management에서 로그 다운로드

목차

[소개](#)

[개요](#)

[1단계: AWS에서 보안 자격 증명 구성](#)

[1단계](#)

[2단계](#)

[3단계](#)

[2단계: 버킷에서 DNS 로그를 다운로드하도록 도구 구성](#)

[MacOS 및 Linux용 s3cmd](#)

[Windows 명령줄 실행 파일\(s3.exe\)](#)

[3단계: 버킷에서 파일 다운로드 테스트](#)

[1단계: 다운로드 테스트](#)

[OS/X 및 Linux용 s3cmd](#)

[Windows 명령줄 실행 파일\(s3.exe\)](#)

[2단계: 다운로드 자동화](#)

소개

이 문서에서는 AWS S3의 Umbrella Log Management에서 로그를 다운로드하는 방법에 대해 설명합니다.

개요

Amazon S3의 로그 관리가 올바르게 작동하는지 설정하고 테스트한 후에는 보존 또는 사용(또는 둘 모두)을 위해 네트워크 인프라 내에서 로그를 자동으로 다운로드하고 저장하는 것이 좋습니다.

이를 위해 <http://s3tools.org>에서 s3tools를 사용한 접근 방식을 [간략하게 살펴보았습니다](#). s3tools는 Linux 또는 OS/X용 s3cmd 명령줄 유틸리티를 사용합니다. Windows 사용자를 위해 유사한 기능을 수행할 수 있는 다른 툴이 있습니다.

- 명령줄 도구의 경우 [여기서](#) 작은 명령줄 실행 파일을 다운로드할 수 있습니다.
- 그래픽 인터페이스를 선호한다면 S3 브라우저(<https://s3browser.com/>)를 체크 아웃하십시오. 그러나 그래픽 인터페이스는 프로세스 자동화를 위해 스크립팅할 수 없기 때문에 사용 방법은 다루지 않습니다. 이 문서에서는 두 명령줄 도구를 모두 설정하는 단계를 제공합니다. 원한다면 1단계의 정보를 사용하여 s3browser 애플리케이션을 구성할 수 있습니다.

사용하려는 운영 체제에 대한 도구를 다운로드하는 것부터 시작합니다. 지금은 OS/X 및 Linux용 s3cmd에 대해서만 다루지만 버킷에 액세스하고 데이터를 다운로드하는 단계는 Windows에서는 사실상 동일합니다.

[여기](#) s3tools에서 설치 프로그램을 [가져옵니다](#).

설치 프로그램에서는 명령줄을 실행하기 위해 프로그램을 설치할 필요가 없으므로 다운로드한 패키지를 추출하기만 하면 됩니다.

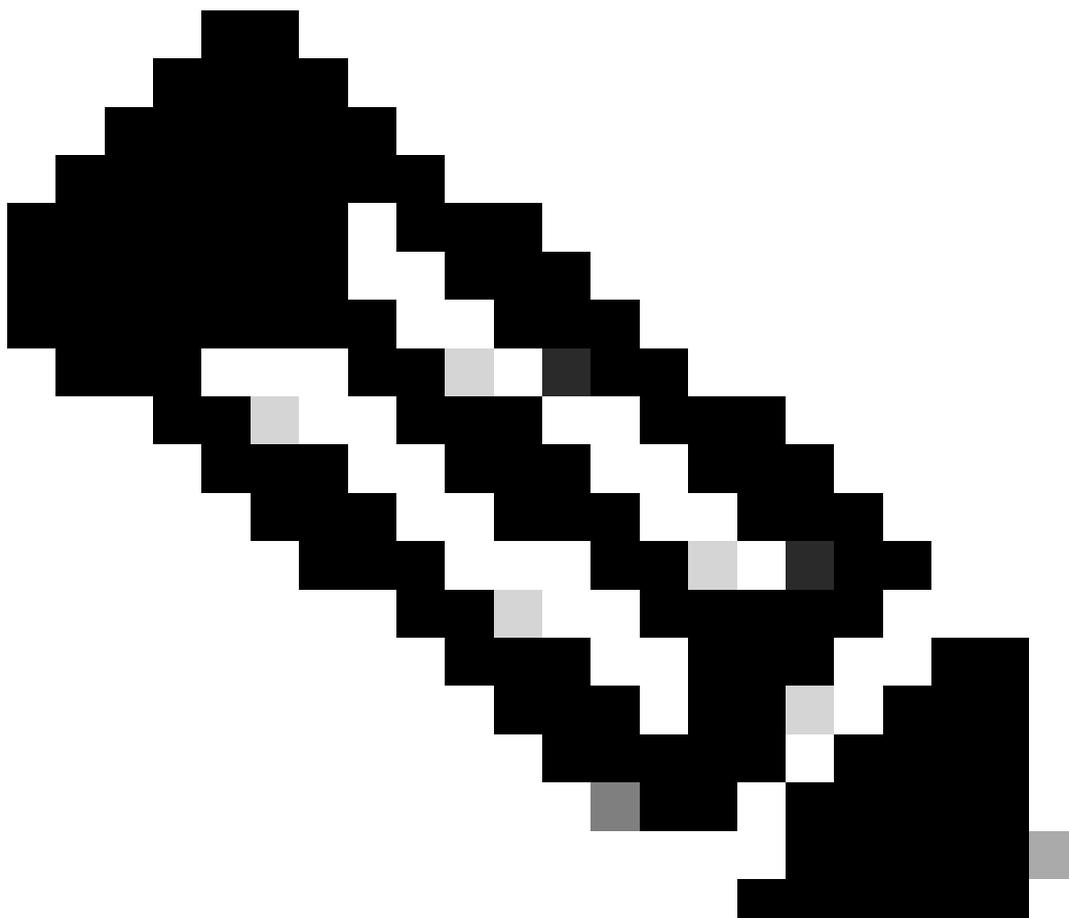
1단계: AWS에서 보안 자격 증명 구성

1단계

1. Amazon Web Services 계정에 액세스 키를 추가하여 로컬 툴에 대한 원격 액세스와 S3에서 파일을 업로드, 다운로드 및 수정하는 기능을 사용할 수 있습니다. AWS에 로그인하고 오른쪽 상단에 있는 계정 이름을 클릭합니다. 드롭다운에서 Security Credentials(보안 자격 증명)를 선택합니다.
2. 프롬프트는 Amazon 모범 사례를 사용하고 AWS Identity and Access Management(IAM) 사용자를 생성하도록 안내합니다. 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 [여기](#)를 [참조하십시오](#).

2단계

1. Get Started with IAM Users(IAM 사용자로 시작)를 클릭하여 S3 버킷에 액세스할 수 있는 IAM 사용자를 생성합니다. IAM 사용자를 생성할 수 있는 화면으로 이동합니다.
2. Create New Users(새 사용자 생성)를 클릭하고 필드를 입력합니다.
3. 사용자 계정을 생성한 후에는 Amazon User Security 자격 증명이 포함된 두 가지 중요한 정보를 확보할 수 있는 기회가 한 번뿐입니다. 오른쪽 하단에 있는 버튼을 사용하여 이러한 파일을 다운로드하는 것이 좋습니다. 이 액세스 키는 설치 시 이 단계 이후에는 사용할 수 없습니다. 액세스 키 ID와 비밀 액세스 키를 모두 기록해 두십시오. 나중에 필요한 액세스 키 ID와 비밀 액세스 키를 기록해 두십시오.



참고: 사용자 계정에는 공백을 포함할 수 없습니다.

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. 여기에는 "AmazonS3FullAccess"와 "AmazonS3ReadOnlyAccess"의 두 가지 결과가 표시됩니다.
3. AmazonS3FullAccess를 선택하고 Attach Policy를 클릭합니다.

2단계: 버킷에서 DNS 로그를 다운로드하도록 도구 구성

MacOS 및 Linux용 s3cmd

1. 이전 단계에서 s3cmd를 추출한 경로로 이동하여 터미널에서 다음을 입력합니다.

```
./s3cmd --configure
```

그러면 보안 자격 증명을 입력하라는 프롬프트가 표시됩니다.

새 값을 입력하거나 대괄호 안에 기본값을 수락하고 Enter 키를 누릅니다.

모든 옵션에 대한 자세한 설명은 사용자 설명서를 참조하십시오.

액세스 키와 비밀 키는 Amazon S3의 식별자입니다. 환경 변수를 사용하려면 비워 두십시오.

액세스 키 [귀하의 액세스 키]:

비밀 키 [YOUR SECRET KEY]:

2. 다음으로, 버킷에 대한 액세스를 구성하는 방법에 대한 일련의 질문을 받습니다. 이 경우 GPG(암호화 비밀번호)를 설정하지 않으며 HTTPS 또는 프록시 서버를 사용하지 않습니다. 네트워크 또는 환경 설정이 다른 경우 필수 필드를 입력합니다.

기본 지역 [US]:

암호화 암호는 S3로 전송하는 동안 권한이 없는 사람이 파일을 읽지 못하도록 보호하는 데 사용됩니다.

암호화 암호:

GPG 프로그램 경로 [없음]:

보안 HTTPS 프로토콜을 사용하는 경우 Amazon S3 서버와의 모든 통신은 서드파티 도청으로부터 보호됩니다. 이 방법은

일반 HTTP보다 느리고 Python 2.7 이상에서만 프록시될 수 있습니다.

HTTPS 프로토콜 사용[아니요]:

일부 네트워크에서는 모든 인터넷 액세스가 HTTP 프록시를 거쳐야 합니다.

S3에 직접 연결할 수 없는 경우 여기에 설정해 보세요

HTTP 프록시 서버 이름:

네트워크별 설정 또는 암호화를 입력하면 다음을 검토할 수 있습니다.

새 설정:

액세스 키: 키

비밀 키: 비밀 키

기본 지역: 미국

암호화 암호:

GPG 프로그램 경로: 없음

HTTPS 프로토콜 사용: 거짓

HTTP 프록시 서버 이름:

HTTP 프록시 서버 포트: 0

마지막으로, 테스트를 수행하고 성공할 경우 설정을 저장하라는 메시지가 표시됩니다.

제공된 자격 증명으로 액세스를 테스트하시겠습니까? [Y/n] y

모든 버킷을 나열하는 동안 기다려 주십시오.

성공. 액세스 키와 비밀 키가 제대로 작동했습니다◆◆

이제 암호화가 작동하는지 확인하는 중...

구성되지 않았습니다. 신경 쓰지 마

설정을 저장하시겠습니까? [y/N]

Windows 명령줄 실행 파일(s3.exe)

도구(<https://s3.codeplex.com/releases/view/47595>)를 다운로드한 후 .exe를 원하는 작업 폴더에 복사하고 명령 프롬프트에서 다음과 같이 입력하여 액세스 키와 암호를 대체합니다.

```
<#root>
```

```
s3 auth [
```

인증 구문에 대한 자세한 내용은 [여기를 참조하십시오.](#)

3단계: 버킷에서 파일 다운로드 테스트

1단계: 다운로드 테스트

OS/X 및 Linux용 s3cmd

터미널에서 이 명령을 실행합니다. 여기서 "my-organization-name-log-bucket"은 Umbrella 대시보드의 Log Management 부분에 이미 구성된 버킷의 이름입니다. 이 예에서는 s3cmd 실행 파일이 포함된 폴더에서 실행되며 파일이 동일한 경로로 전달되지만 다음과 같이 변경할 수 있습니다.

<#root>

```
./s3cmd sync s3://my-organization-name-log-bucket ./
```

버킷의 파일과 디스크의 대상 경로에 있는 파일 간에 차이가 있는 경우, 동기화에서 누락되거나 업데이트된 파일을 다운로드해야 합니다. 가장 먼저 검색된 파일은 일반적으로 업로드되는 README 파일이어야 합니다.

```
./s3cmd 동기화 s3://my-organization-name-log-bucket ./
```

```
s3://my-organization-name-log-bucket/README_FROM_UMBRELLA.txt -> <fdopen> [1/1]
```

```
1800/1800 0s 100% in 0s 15.00 kB/s 완료
```

```
완료. 1800바이트(1.0초) 다운로드, 1800.00B/s
```

존재하는 모든 로그 파일도 다운로드됩니다. 정기적으로 이 기능을 예약하기 위해 cron 작업을 설정하려는 경우 사용자의 책임이지만, 이제 버킷의 새 로그 파일 또는 변경된 로그 파일을 장기 보존을 위해 로컬 경로로 자동으로 다운로드할 수 있습니다.

Windows 명령줄 실행 파일(s3.exe)

명령 프롬프트에서 'my-organization-name-log-bucket'이 Umbrella 대시보드의 Log Management 부분에 이미 구성된 버킷의 이름인 경우 이 명령을 실행합니다. 이 예에서는 버킷의 모든 파일(별표 와일드카드로 정의됨)이 \dnslogbackups\ 폴더에 다운로드됩니다.

<#root>

```
s3 get my-organization-name-log-bucket/* c:\dnslogbackups\
```

이 명령의 구문에 대한 자세한 내용은 [여기를 참조하십시오.](#)

2단계: 다운로드 자동화

구문이 테스트되고 예상대로 작동되면 지침을 cron 작업(OS X/Linux) 또는 예약된 작업 (Windows)을 설정하는 스크립트에 복사하거나 다른 작업 자동화 도구를 사용할 수 있습니다. S3 인스턴스의 공간을 확보하기 위해 파일을 다운로드한 후 버킷에서 파일을 제거하는 도구를 사용할 수도 있습니다. 데이터 보존 정책에 가장 적합한 방법을 확인하려면 사용 중인 도구의 설명서를 살펴보는 것이 좋습니다.

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.