Umbrella Log Management 및 S3와 QRadar 통합 구성

목차

소개

이 문서에서는 Umbrella 로그 관리를 위해 AWS S3 버킷에서 로그를 수집하도록 QRadar를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

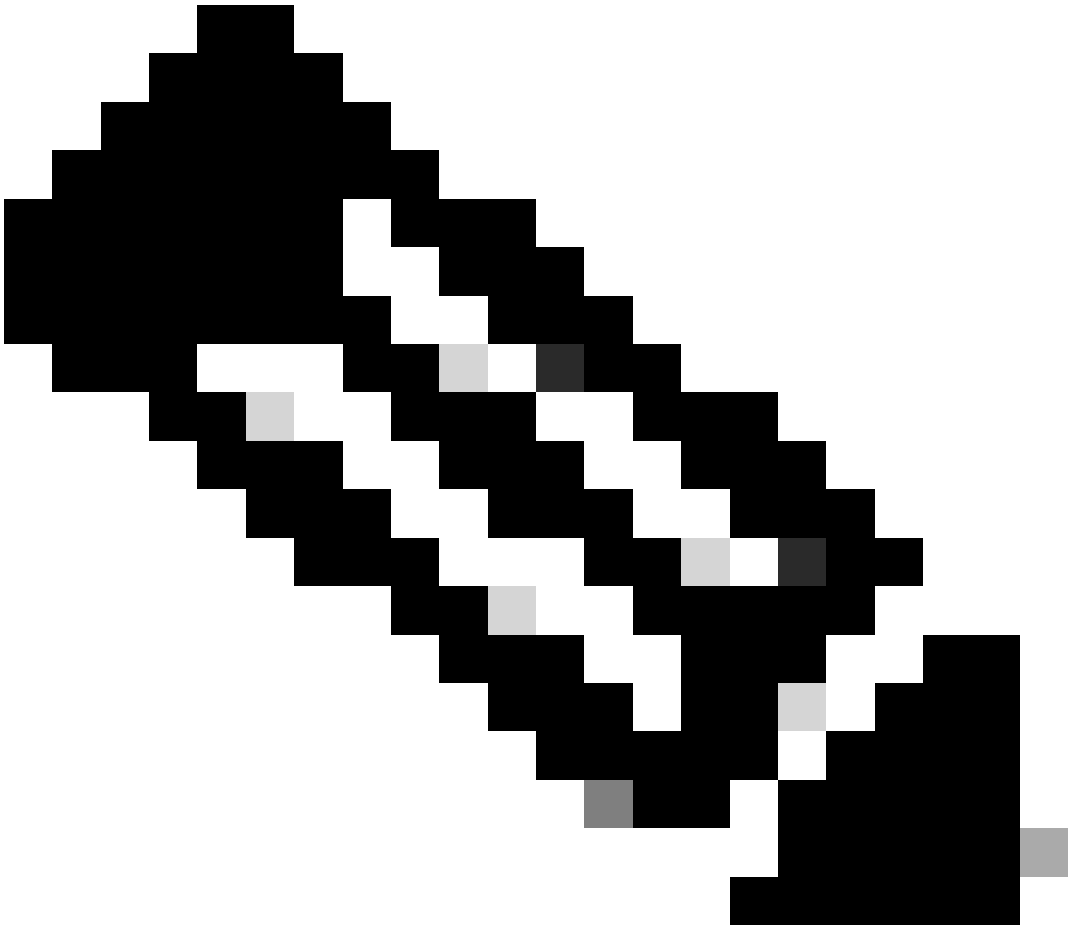
- 이 문서에서는 Amazon AWS S3 버킷이 Umbrella(Settings(설정) > Log Management(로그 관리))에서 구성되었으며 최근 로그가 업로드된 상태에서 녹색으로 표시된다고 가정합니다. 이 기능을 구성하는 방법에 대한 자세한 내용은 AWS S3의 Umbrella Log Management에서 로그 다운로드를 참조하십시오.
- QRadar 어플라이언스, Amazon S3 컨피그레이션 및 Umbrella 대시보드에 대한 관리 권한 외에, 이러한 지침에서는 QRadar 관리자가 LSX(Log source Extension) 파일을 생성하는 데 익숙하다고 가정합니다.

사용되는 구성 요소

이 문서의 정보는 Cisco Umbrella를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

개요



> 참고: Cisco Umbrella와 함께 사용하도록 QRadar를 구성하는 가장 좋은 방법은 Cisco Cloud Security App을 사용하는 것입니다. 앱을 구성할 수 없는 경우에만 이 메서드를 진행합니다.

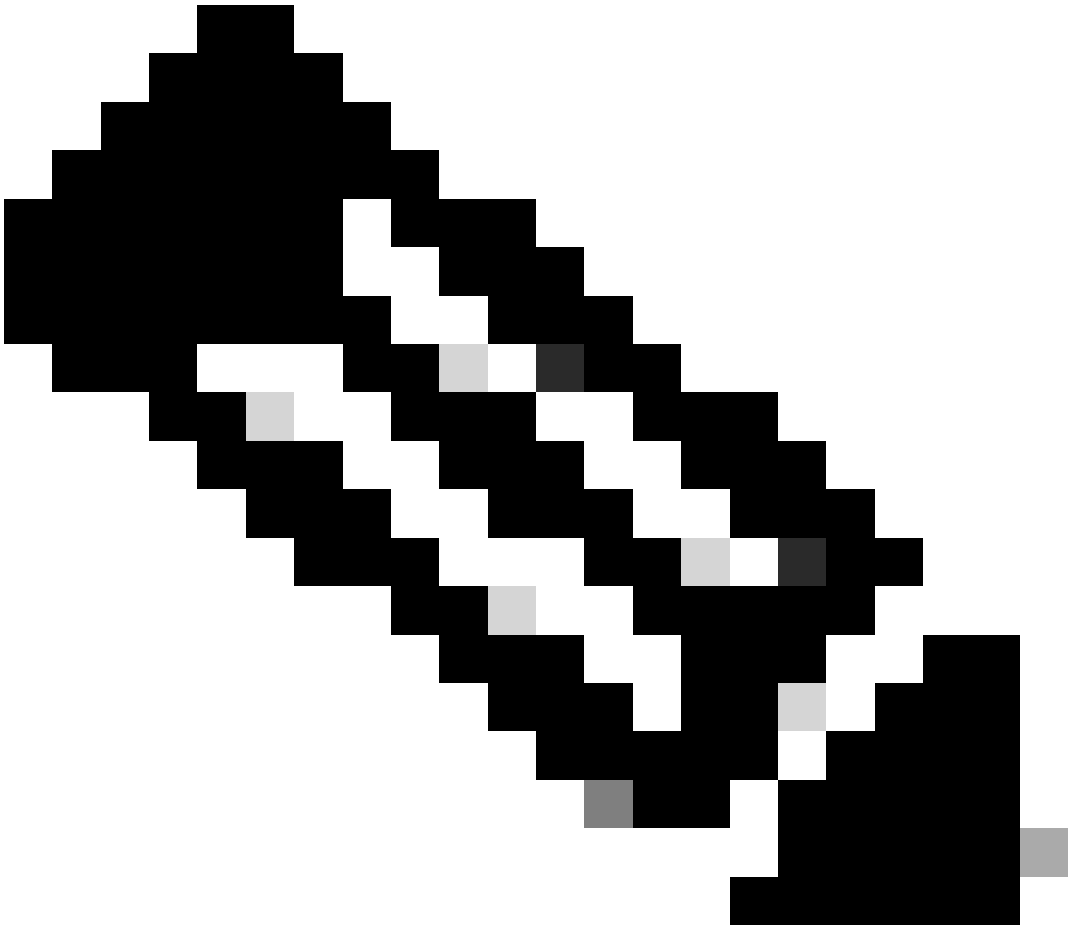
IBM의 QRadar는 로그 분석을 위해 널리 사용되는 SIEM입니다. Cisco Umbrella는 조직의 DNS 트래픽을 위해 Cisco Umbrella에서 제공하는 로그와 같은 대량의 데이터를 분석할 수 있는 강력한 인

터페이스를 제공합니다.

이 문서에서는 S3 버킷에서 로그를 가져와 사용할 수 있도록 QRadar를 설정하고 실행하는 방법에 대해 간략하게 설명합니다. 두 가지 주요 단계가 있습니다.

- QRadar에서 로그에 액세스할 수 있도록 AWS S3 보안 자격 증명을 구성합니다.
- 버킷을 가리키도록 QRadar 자체를 구성합니다.

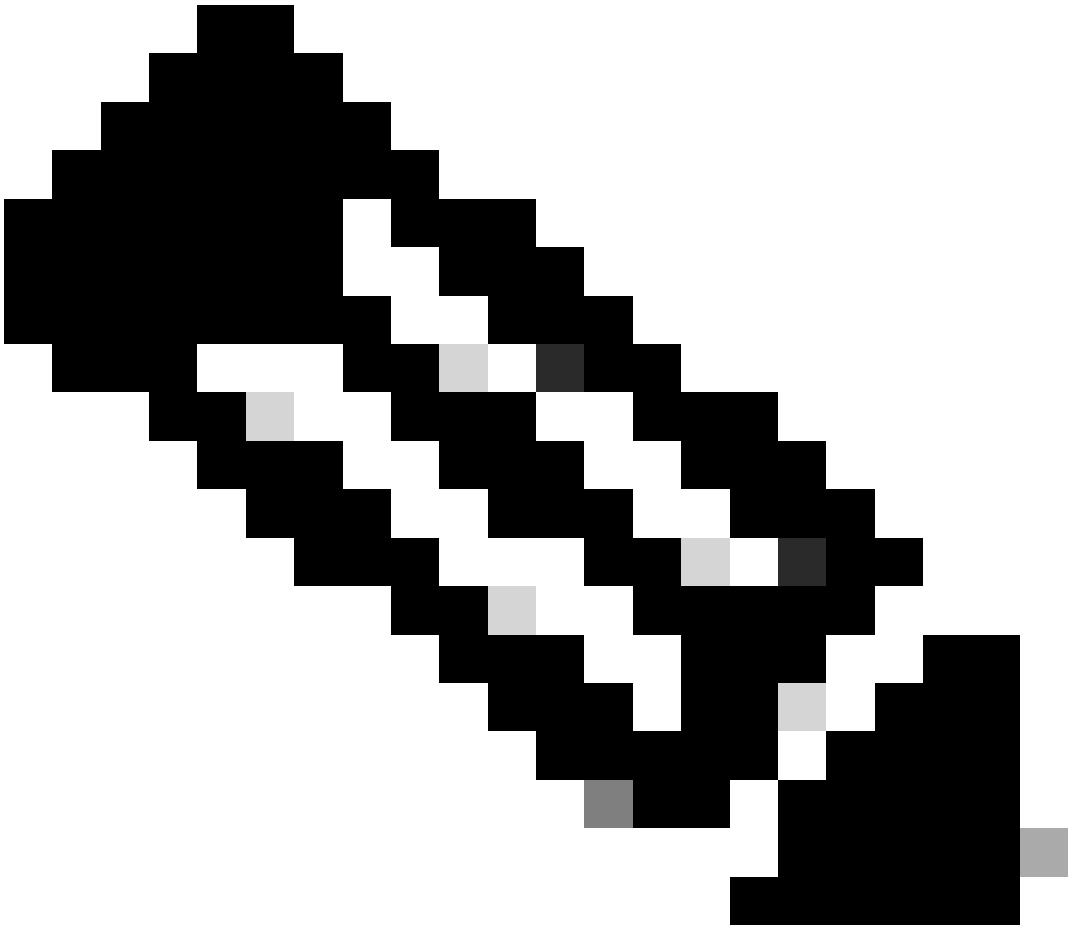
Cisco에서 관리하는 S3 버킷을 사용하는 경우 AWS CLI를 사용하여 Umbrella Log Management에서 로그 다운로드 문서의 지침을 사용하십시오.



참고: 이 통합은 고객 관리 S3 버킷 및 Cisco 관리 S3 버킷 모두에서 테스트되었습니다. 이 문서에서 논의된 정보는 이 문서(2019년 10월)를 기준으로 최신 정보입니다. QRadar와 AWS 서비스 인터페이스의 방식에 따라 변경될 수 있습니다. 이 문서는 실제 문서입니다. 피드백을 받았거나 다른 고객에게 도움이 될 수 있는 유용한 정보나 힌트를 찾은 경우 Cisco Umbrella Support에 문의하십시오.

QRadar에 대한 지원은 IBM에서 제공되어야 합니다. Cisco에서는 타사 하드웨어 또는 소프트웨어를 직접 지원할 수 없기 때문입니다. Umbrella 대시보드를 S3 버킷에 연결하는 데 문제가 있을 경우 Cisco Umbrella에서 지원을 제공할 수 있습니다. 이 기사에서 발견된 많은 정보는 IBM 웹사이트에서도 찾을 수 있다.

1단계: AWS에서 보안 자격 증명 구성



> 참고: 이러한 단계는 버킷에서 로그를 다운로드하기 위해 툴을 구성하는 방법(AWS S3의 Umbrella Log Management에서 로그 다운로드)에 대해 설명하는 문서와 동일합니다. 이러한 단계를 이미 수행한 경우, IAM 사용자의 보안 자격 증명이 있어야 버킷에 QRadar를 인증할 수 있지만 2단계로 건너뛸 수 있습니다.

1단계

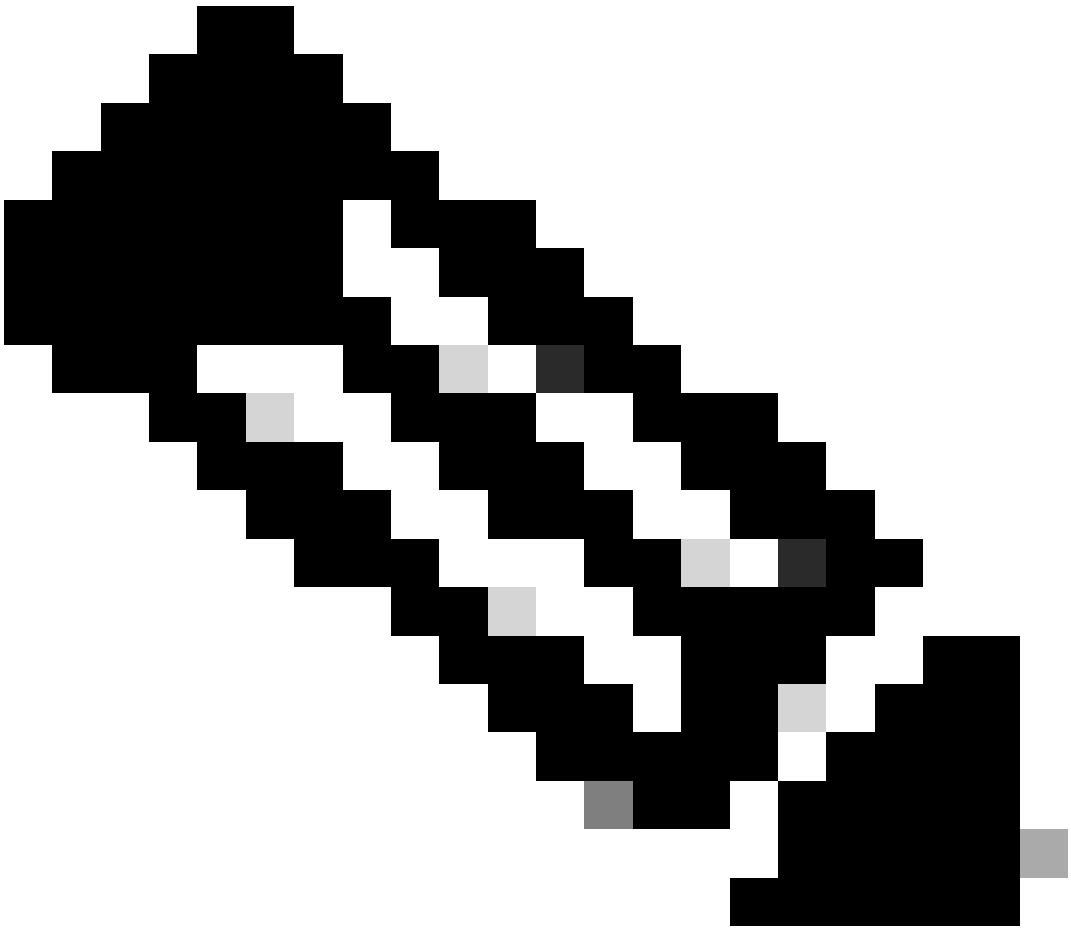
1. Amazon Web Services 계정에 액세스 키를 추가하여 로컬 툴에 대한 원격 액세스를 허용하고 S3에서 파일을 업로드, 다운로드 및 수정할 수 있는 기능을 제공합니다.

1. AWS에 로그인합니다.
2. 오른쪽 상단 모서리에서 계정 이름을 선택합니다.
3. 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 마스터 계정(예: 사용자 계정)이 아님을 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 AWS 설명서를 참조하십시오.

2단계

1. Get Started with IAM Users(IAM 사용자로 시작하기)를 선택하여 S3 버킷에 액세스할 수 있는 IAM 사용자를 생성합니다. 그러면 IAM 사용자를 생성할 수 있는 화면으로 이동합니다.
2. 신규 사용자를 선택한 후 필드를 완료합니다.



참고: 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 제공됩니다. Umbrella는 오른쪽 아래 버튼을 사용하여 이러한 정보를 다운로드하고 백업할 것을 적극 권장합니다. 이 액세스 키는 설치 시 이 단계 이후에는 사용할 수 없습니다. 액세스 키 ID와 비밀 액세스 키는 이후 단계에서 필요하므로 기록해 두십시오.

3단계

다음으로, IAM 사용자가 S3 버킷에 액세스할 수 있도록 IAM 사용자에 대한 정책을 추가합니다.

1. 방금 생성한 사용자를 선택한 다음, [정책 첨부] 버튼이 표시될 때까지 사용자의 등록 정보를 아래로 스크롤합니다.

2. Attach Policy를 선택한 다음 정책 유형 필터에 "s3"을 입력합니다. 이는 다음 두 가지 결과를 보여줍니다.

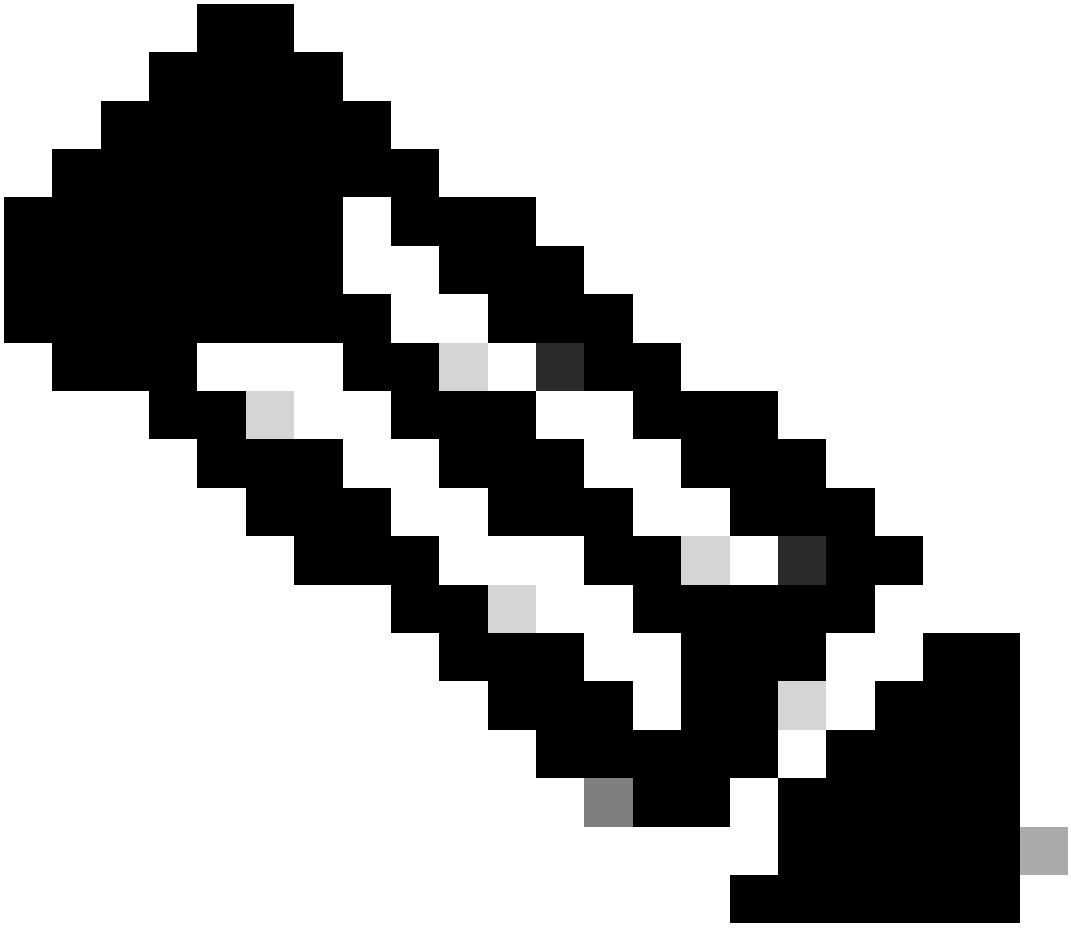
- AmazonS3FullAccess
- AmazonS3ReadOnly액세스

3. AmazonS3FullAccess를 선택한 다음 오른쪽 하단의 Attach Policy(정책 추가)를 선택합니다.

2단계: S3 버킷에서 DNS 로그 데이터를 가져오도록 QRadar 설정

QRadar는 계정에 대한 AWS API 호출을 기록하고 로그 파일을 전달하는 웹 서비스인 AWS CloudTrail 서비스를 사용합니다.

QRadar가 Amazon S3에 액세스하기 전에 IBM에서 이 절차를 완료하여 Amazon 서버 인증서를 가져옵니다. 이 부분은 어렵기 때문에 반드시 지시사항을 정확히 작성해 주시기 바랍니다.



참고: 테스트에서는 Firefox 브라우저를 사용하여 예상대로 작동해야 합니다.

Amazon 서버 인증서를 가져오려면 DER 형식의 인증서를 적절한 QRadar 어플라이언스로 이동해야 합니다. 인증서가 필요한 QRadar 어플라이언스는 Amazon AWS CloudTrail 로그 소스의 Target Event Collector 필드에 할당된 어플라이언스입니다.

시작하기 전에

- 인증서는 .DER 형식이어야 합니다.
- 확장명 .DER는 대/소문자를 구분하며 대문자여야 합니다.
- 인증서를 소문자로 내보낼 경우 로그 소스에 이벤트 수집 문제가 발생할 수 있습니다.

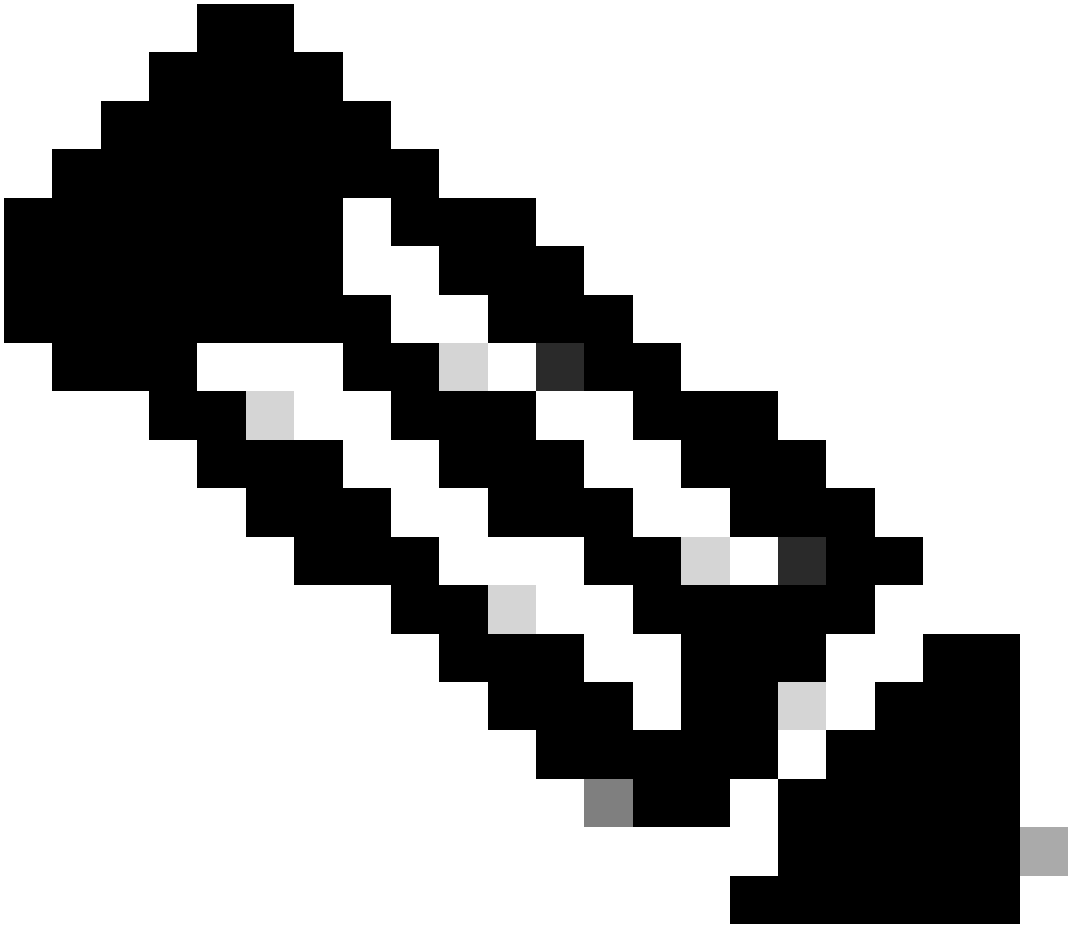
초기 단계

1. AWS CloudTrail S3 버킷 액세스: `https://<bucketname>.s3.amazonaws.com`

2. Firefox를 사용하여 AWS의 SSL 인증서를 (.DER) 인증서로 내보냅니다. Firefox는 .DER 확장자

로 필요한 인증서를 생성할 수 있습니다.

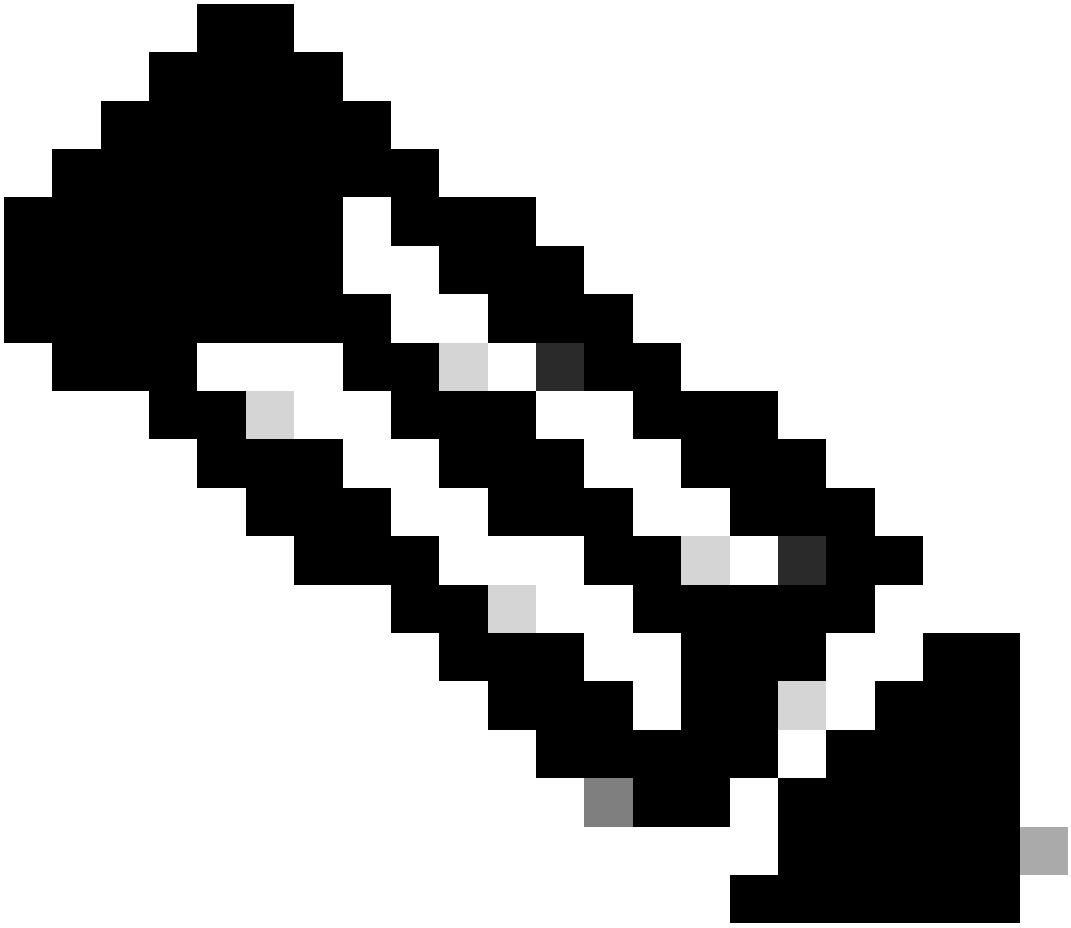
1. 사이트 ID 아이콘(주소 표시줄의 잠금 아이콘)을 선택합니다.
2. More Information(추가 정보) > View Certificate(인증서 보기)를 선택하고 Details(세부사항) 탭을 선택합니다.
3. 인증서 .DER 형식으로 내보내려면 Export(내보내기)를 선택합니다.



참고: .DER 확장명은 대/소문자를 구분하며 대문자여야 합니다.

---

3. .DER 인증서를 Amazon AWS CloudTrail 로그 소스를 관리하는 QRadar 어플라이언스의 /opt/QRadar/conf/trusted_certificates 디렉토리에 복사합니다. WinSCP를 사용하여 복사할 수 있습니다.



참고: 로그 소스를 관리하는 QRadar 어플라이언스는 Amazon AWS CloudTrail 로그 소스의 Target Event Collect 필드에 의해 식별됩니다. Amazon AWS CloudTrail 로그 소스를 관리하는 QRadar 어플라이언스에는 .DER 인증서의 사본이 /opt/QRadar/conf/trusted_certificates에 있어야 합니다.

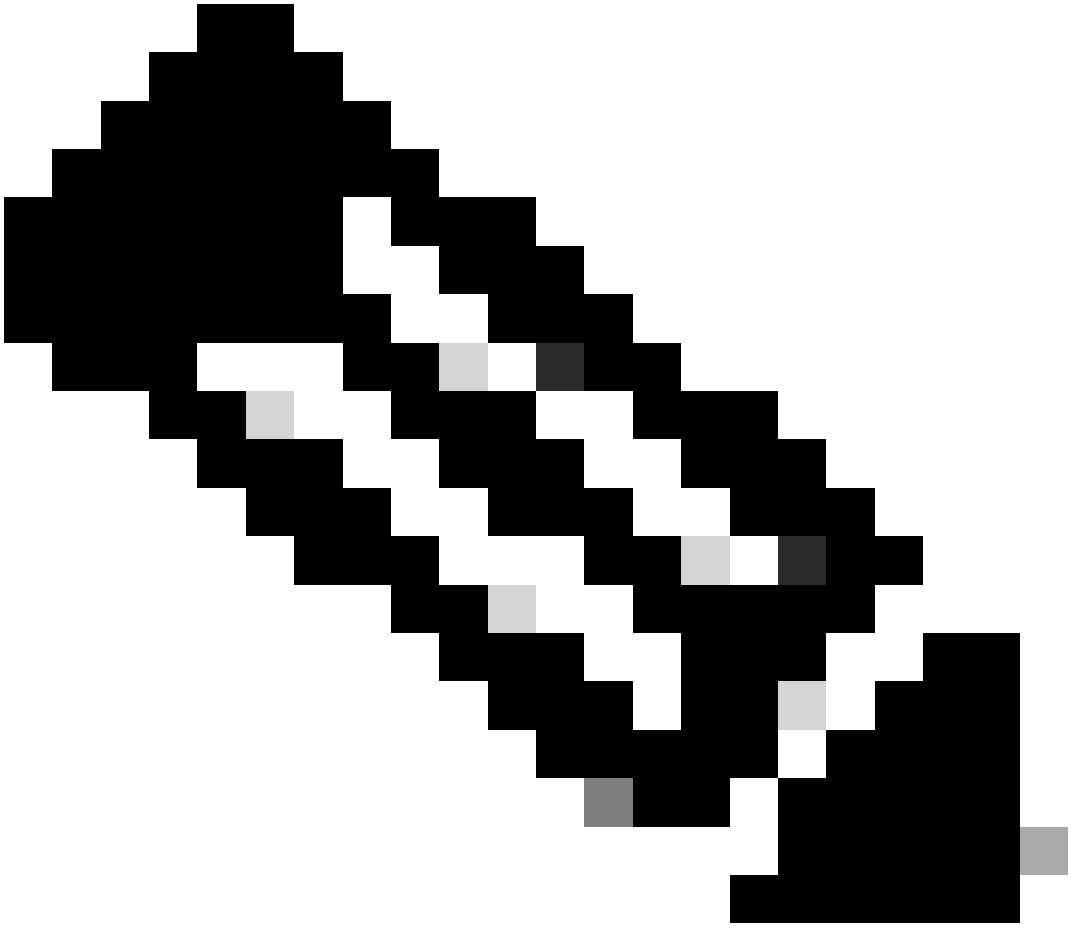
4. QRadar 사용자 인터페이스에 관리자 사용자로 로그인합니다.

5. 관리 탭을 선택합니다.

6. 로그 출처 아이콘을 선택합니다.

7. Amazon AWS CloudTrail 로그 소스를 선택합니다.

8. 탐색 메뉴에서 Enable/Disable을 선택하여 Amazon AWS CloudTrail 로그 소스를 비활성화한 다음 다시 활성화합니다.



참고: 관리자가 로그 소스를 비활성화에서 활성화로 강제하면 프로토콜이 로그 소스에 정의된 대로 Amazon AWS 버킷에 연결할 수 있습니다. 그런 다음 첫 번째 통신의 일부로 인증서 확인이 수행됩니다.

9. 문제가 계속되면 로그 소스 식별자 필드에 올바른 Amazon AWS 버킷 이름이 포함되어 있는지, 로그 소스 컨피그레이션에서 원격 디렉토리 경로가 올바른지 확인하십시오.

QRadar 컨피그레이션 마무리

1. QRadar에서 모든 프로토콜, DSM 및 기타 정보가 최신 상태인지 확인합니다. 이러한 컨피그레이션(빈도, 시작 시간, 되풀이 및 기타 정보는 다를 수 있음)을 사용하여 LogFileProtocol을 선택합니다.

2. 로그 소스 탭에서 로그 소스명 및 로그 소스 설명을 입력합니다. 이건 당신이 좋아하는 것이 될 수 있어요.

3. S3 버킷 이름, AWS 액세스 키, AWS 비밀 키 및 원격 디렉토리(dnslog일 수 있으나 설정에 따라

다름)를 입력합니다. 연도와 같은 로그 소스 식별자를 추가하면 "2019"가 포함된 로그만 가져오도록 필터링하는 데 도움이 됩니다.

4. Cisco Umbrella 이벤트를 구문 분석할 수 있는 LSX(Log Source eXtension)를 생성합니다. (QRadar로 가져온 후의 모습입니다.) LSX를 생성하는 방법에 대한 자세한 내용은 IBM 웹 사이트에서 확인할 수 있습니다. 이것은 단지 하나의 예입니다. 로그에서 가져오려는 데이터는 활용 사례에 따라 달라집니다.

5. AWS 액세스 키와 AWS 비밀 키가 성공적으로 복사되어 로그 소스 구성에 붙여넣어졌는지 다시 확인합니다.

6. GZIP 프로세서 및 RegEx 기반 다중라인의 이벤트 생성기를 선택합니다. 라인당 하나의 이벤트를 가져오는 가장 쉬운 방법은 다음과 같은 시작 패턴 RegEx를 사용하는 것입니다.

```
("\d{4}-\d{2}-\d{2}\s\d{2}:\d{2}:\d{2}","")
```

로그 소스 확장 및 사용 조건을 선택한 다음 로그 소스를 저장해야 합니다.

7. QRadar에서 전체 배포를 수행합니다.

그런 다음 로그 소스에서 RestAPI를 사용하여 제공한 자격 증명과 키를 사용하여 버킷에 연결하고 이벤트 가져오기를 시작합니다.

추가 정보

버킷 로깅 사용

버킷 로깅을 사용하려면 AWS 설명서를 읽고 설명된 절차를 완료하십시오. 기본적으로 로깅은 비활성화되어 있습니다. 활성화되면 /logs라는 새 폴더가 버킷 루트에 상주하여 GETS, PUTS 및 DELETES의 정보를 표시합니다.

로그 주기 관리

S3를 사용하는 경우 버킷 내에서 데이터의 라이프사이클을 관리하여 로그를 보존할 기간을 연장할 수 있습니다. 외부 로그 관리를 사용하는 목적에 따라 기간이 매우 짧거나 매우 길 수 있습니다. 예를 들어, 24시간 후에 S3 버킷에서 로그를 다운로드하여 오프라인으로 저장하거나 클라우드에서 로그를 무기한 보존할 수 있습니다.

기본적으로 Amazon은 데이터를 버킷에 무기한 저장하지만 무제한 스토리지는 버킷을 유지하는 비용을 높입니다. S3 주기에 대한 자세한 내용은 AWS 설명서를 참조하십시오.

버킷의 라이프사이클을 구성하려면

1. 등록 정보 > 주기를 선택합니다.

2. 규칙 추가를 선택한 다음 규칙을 전체 버켓(또는 하위 폴더가 구성된 경우 하위 폴더)에 적용합니다.

3. 객체에 대한 작업(예: 삭제 또는 아카이브)을 선택한 다음 기간 및 Amazon 비용 절감을 위해

Glacier 스토리지를 사용할지 여부를 선택합니다. Glacier는 "콜드" 오프라인 스토리지이므로 액세스가 느리지만 훨씬 저렴합니다.

다른 방법(예: 내부 백업 솔루션)으로 로그를 관리하려는 경우 S3에서 로그를 다운로드하고 다른 방법으로 보존하면 됩니다.

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.