사용자 트래픽을 탐지하지 못하는 Umbrella Insights AD 통합 문제 해결

목차

소개

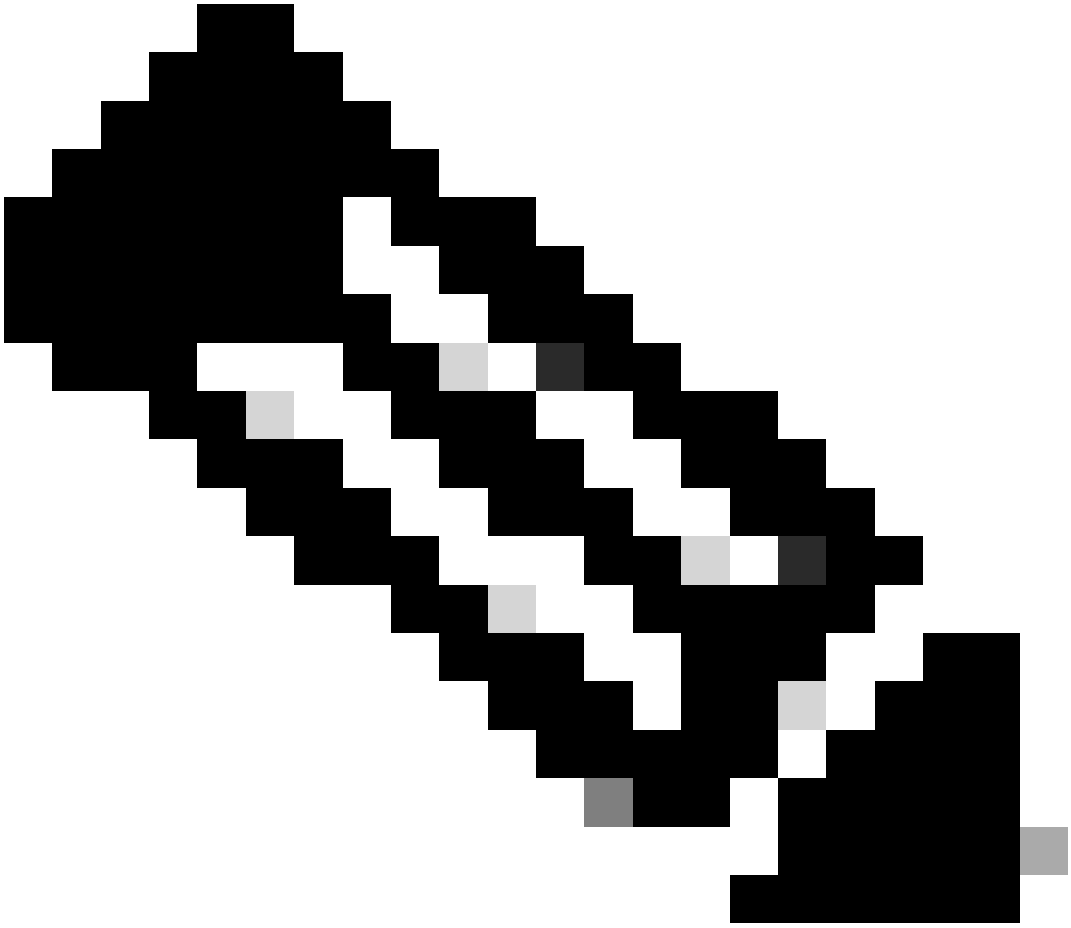
이 문서에서는 사용자 트래픽을 탐지하지 못하는 Umbrella Insights AD 통합의 문제를 해결하는 방법에 대해 설명합니다.

개요

Umbrella Insights를 설치하고 커넥터 및 가상 어플라이언스를 설정하고 도메인 컨트롤러를 등록했습니다. 모든 구성 요소가 녹색으로 표시되고 구축 —> 사이트 및 Active Directory의 대시보드에서 작동합니다. 그러나 AD 사용자 또는 그룹 객체를 사용하도록 구성된 정책이 있지만 대시보드나 정책에 보고된 사용자 활동이 올바르게 적용되지 않습니다.

이 항목이 OpenDNSAuditClient.log 파일에서 반복된다는 것을 알 수도 있습니다.

`1970-01-01 00:00:00에 수신된 마지막 이벤트`



참고: 로그 파일은 C:\Program Files (x86)\OpenDNS\OpenDNS Connector\<VERSION>\\에 있습니다
VERSION = Connector 서비스의 실제 설치된 버전(예: v1.1.22)

설명

이러한 문제가 발생하는 주된 이유는 감사 로그온 이벤트가 Active Directory 도메인에 구성되지 않았을 수 있기 때문입니다. 로그 메시지는 커넥터가 설치된 이후 단일 사용자 이벤트가 하나도 없음을 나타냅니다. 현재 대시보드에 오류가 발생하는 것은 아닙니다.

해결

AD 그룹 정책에서 올바른 감사 정책 컨피그레이션을 확인해야 합니다.

1. Domain Controller(도메인 컨트롤러)에서 Administrative *Tools(관리 툴)* 내에 있는 Group Policy Management(그룹 정책 관리) 패널을 열고 도메인 컨트롤러에 적용할 정책을 선택합니다(Default

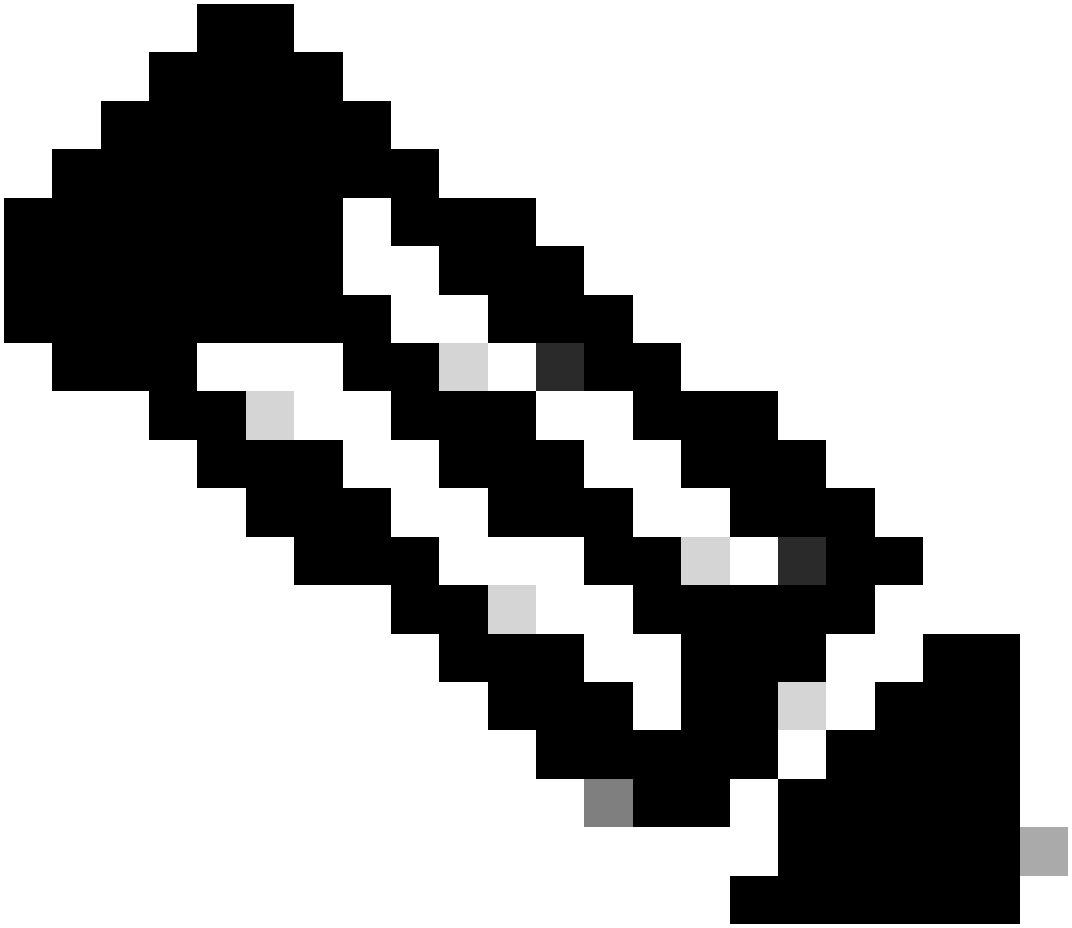
Domain Controller Policy(기본 도메인 컨트롤러 정책)가 후보가 될 수 있음).

2. 해당 정책을 마우스 오른쪽 단추로 클릭하고 Edit(편집)를 선택하여 Group Policy Management Editor(그룹 정책 관리 편집기)를 표시합니다.

3. "Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy" 폴더로 이동한 다음 Audit logon events를 선택하여 해당 속성을 봅니다.

4. 이 정책은 성공 시도를 감사하기 위한 것이어야 합니다.

5. gpupdate 명령을 실행하여 정책을 적용합니다.



참고: "Default Domain Controllers and the Default Domain Policy(기본 도메인 컨트롤러 및 기본 도메인 정책)" 둘 다 해당 설정을 구성해야 하는 경우가 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.