Active Directory 서비스 계정을 차단하는 Umbrella 커넥터 문제 해결

목차

[소개](#)

[개요](#)

[차단된 계정 목록](#)

[추가 정보](#)

소개

이 문서에서는 Active Directory 서비스 계정이 Umbrella Connector에 의해 차단된 이유를 해결하는 방법을 설명합니다.

개요

Umbrella Connector 서비스는 로그인 이벤트 정보를 읽기 위해 동일한 [Umbrella 사이트](#)에 속한 등록된 DC(도메인 컨트롤러)의 이벤트 로그에 WMI를 연결합니다. 그런 다음 이러한 로그인 이벤트를 구문 분석하여 동일한 Umbrella 사이트의 모든 VA(Virtual Appliance)에 업로드합니다. 그런 다음 VA는 해당 사용자 이름/소스 IP 주소에 대한 임시 User-to-IP 매핑을 생성합니다. 주목할 만한 몇 가지 사항이 있습니다.

- Umbrella Insights는 한 번에 IP당 한 명의 로그인된 사용자만 지원할 수 있습니다
- 소스 IP에서 가장 최근에 처리된 로그인 이벤트 'wins'

모든 로그인 이벤트가 동일하기 때문에 커넥터에는 이벤트가 무시되는 공통 AD 서비스 계정의 하드 코딩된 목록이 있습니다. 커넥터 로그 파일에서 선택한 이러한 계정의 로그인 이벤트를 볼 수 있습니다. 예를 들면 다음과 같습니다.

블랙리스트 사용자의 이벤트가 무시되었습니다. OpenDNS_커넥터

이는 표준 사용자가 DC 보안 이벤트 로그에서 로그인 이벤트를 생성하는 것과 마찬가지로 서비스 계정이 실제 로그인한 사용자의 User-to-IP 매핑을 재정의하지 못하도록 하기 위한 것입니다.

대규모 환경에서는 서비스 계정이 사용되는 프로세스/응용 프로그램에 따라 1분마다 수천 개의 로그인 이벤트를 생성할 수도 있습니다. 이는 또한 커넥터에 대한 추가 로드로서, 사용자 로그인과 올바른 정책 적용 사이의 지연 또는 나중에 손실되는 올바른 정책으로 나타날 수 있습니다.

차단된 계정 목록

- _vmware_user_
- 관리자

- 익명
- 익명 로그인
- 아스프넷
- 로컬 서비스
- McAfeeMVSUser
- MHC제어
- 네트워크 서비스
- 네트릭스
- OpenDNS_커넥터
- peersyncsvc
- s-pcadmin
- SophosUpdateMgr
- SophosUpdMgr
- svc-altiris
- svc.iCreate

추가 정보

다른 AD 계정 로그인 이벤트를 커넥터에서 처리하지 못하도록 제외할 수도 있습니다. 자세한 내용은 이 문서를 참조하십시오.

<https://support.umbrella.com/hc/en-us/articles/231266088>

또한 커넥터의 AD 동기화에서 제외할 수 있는 AD 그룹이 있습니다. 이는 대시보드 정책 영역에 AD 사용자, 컴퓨터 및 그룹 목록을 채우기 위해 수행됩니다. 다음 위치에서 찾을 수 있습니다.

<https://support.umbrella.com/hc/en-us/articles/115005206526>

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.