Secure Access AD Connector 동기화 문제 해결

목차

문제

도메인 컨트롤러에 설치된 AD 커넥터가 Cisco Secure Access와 제대로 동기화되지 않습니다. 커넥터에 다음과 같은 여러 동기화 오류가 발생합니다.

- "액세스가 거부되었습니다." 오류가 있는 델타 동기화 실패(COMException 0x80070005)
- "UnauthorizedAccessException: 권한이 없는 작업을 수행하려고 했습니다."
- 매니페스트를 다운로드할 때 "잘못된 URI 형식"이 표시되는 클라우드 등록 문제
- 동기화 시도 중 특정 AssetID에 대한 HTTP 404 "object_not_found" 오류

커넥터가 Cisco Secure Access 클라우드 서비스에 연결된 것처럼 보이지만 Active Directory 권한 측면과 클라우드 등록 컨피그레이션에서 모두 실패합니다.

환경

- AD 커넥터를 사용하는 Cisco Secure Access
- AD Connector 버전 1.15.2
- 도메인 컨트롤러에 설치된 AD 커넥터
- 기본 Cisco_Connector 계정 대신 사용자 지정 서비스 계정(svcCiscoUmbrella)
- 테스트/파일럿 환경 설정

해결

해결에는 전체 재설치 프로세스를 통해 Active Directory 권한 문제 및 클라우드 등록 문제를 모두 해결하는 것이 포함됩니다.

1단계: 기존 AD 커넥터 항목 확인 및 정리

Secure Access(보안 액세스) 대시보드에서 호스트의 AD 커넥터 항목을 확인하고 동일한 서버에 대해 오래된 항목이나 중복된 항목이 있으면 제거합니다.

2단계: 전체 제거 확인

기존 AD 커넥터 서비스를 완전히 제거하여 등록 문제를 일으킬 수 있는 잔여 컨피그레이션이 남아 있지 않도록 합니다.

3단계: 도메인 컨트롤러 스크립트 실행

커넥터를 다시 설치하기 전에 적절한 도메인 컨트롤러 컨피그레이션 스크립트를 실행하여 적절한 권한이 설정되었는지 확인합니다. 커넥터 자체는 다른 도메인에 가입된 컴퓨터의 도메인 컨트롤러 외부에 있을 수 있지만, 스크립트는 해당되는 각 도메인 컨트롤러에서 실행해야 합니다.

4단계: 서비스 계정 권한 구성

서비스 계정에 필요한 Active Directory 권한을 부여합니다.

- AD 동기화 권한(적절한 도메인/루트 범위):
    - 읽기
    - 디렉토리 변경 복제
    - 디렉토리 변경 사항 모두 복제(환경에 필요한 경우)
    - 필터링된 집합에서 디렉토리 변경 복제(환경에 필요한 경우)
- 도메인 컨트롤러에서 이벤트 로그 액세스:
    - Event Log Readers 그룹에 서비스 계정을 추가합니다.
    - 보안 로그를 읽을 수 있는 동등한 정책 기반 권한을 확인합니다.

5단계: AD 커넥터 다시 설치

AD 커넥터 서비스를 다시 설치하여 새 매니페스트와 유효한 AssetID를 생성하여 올바른 클라우드 등록을 보장합니다.

6단계: 재시작 및 검증

설치 및 권한 구성 후:

1. AD 커넥터 서비스를 다시 시작합니다.
2. 커넥터 로그를 모니터링하여 액세스 거부 및 무단 오류 중지를 확인합니다.
3. 성공적인 동기화 항목이 로그에 표시되는지 확인합니다(예: "ADSync LDIF RESPONSE: 200 Success").

원인

동기화 문제는 두 가지 주요 요인으로 인해 발생했습니다.

1. Active Directory 권한이 부족합니다. 사용자 지정 서비스 계정(svcCiscoUmbrella)에 델타 동기화 및 DC 이벤트 로그 액세스에 필요한 AD 권한이 없어 "액세스가 거부되었습니다." 및 "UnauthorizedAccessException" 오류가 발생했습니다.
2. 클라우드 등록 문제: 커넥터 인스턴스가 잘못 등록되었거나 잘못된/이전 AssetID를 가리키고 있어 동기화 시도 중에 매니페스트 및 HTTP 404 "object_not_found" 오류를 다운로드할 때 "Invalid URI format" 오류가 발생했습니다.

이러한 문제는 커넥터 설치 전에 도메인 컨트롤러 컨피그레이션 스크립트가 제대로 실행되지 않는 불완전한 설치 절차로 인해 더욱 악화되었습니다.

관련 콘텐츠

- Cisco Secure Access AD Connector 컨피그레이션

- AD 커넥터 권한 요구 사항
- AD 커넥터 설치 가이드
- AD 커넥터 문제 해결
- AD 커넥터 서비스 계정 컨피그레이션
- Cisco 기술 지원 및 다운로드

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.