문제 해결(&Quot; 액세스 거부(&Quot;) Umbrella AD 커넥터의 경고

목차

소개

이 문서에서는 Cisco Umbrella Active Directory(AD) Connector가 경고 또는 오류 상태인 경우 "액세스 거부" 트러블슈팅에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

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.

문제

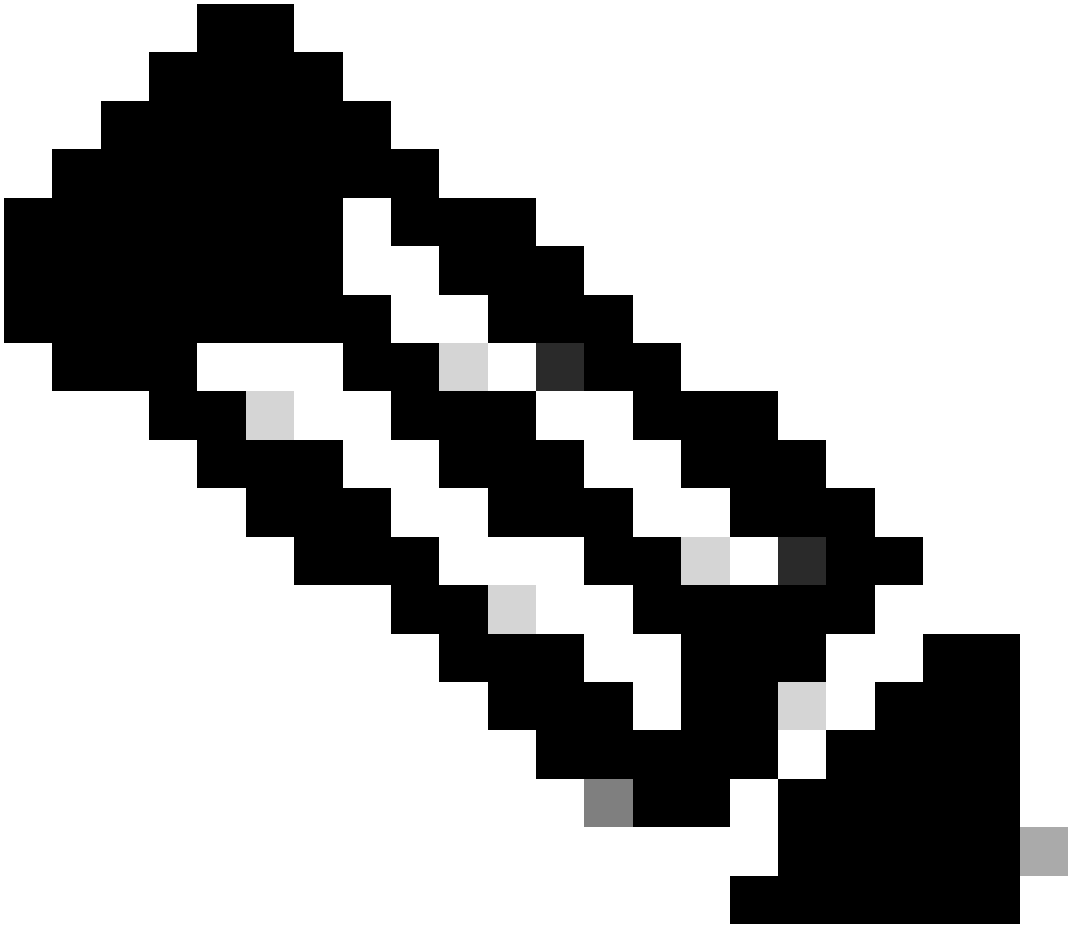
AD 커넥터가 알림 또는 오류 상태를 표시하며, 알림 위에 마우스를 올려 놓으면 나열된 메시지에 등록된 AD 서버 중 하나에 대한 "액세스 거부됨"이 포함됩니다.

솔루션

OpenDNS_Connector 사용자가 다음 AD 그룹의 멤버인지 확인하십시오.

- 이벤트 로그 판독기
- 분산 COM 사용자
- 엔터프라이즈 읽기 전용 도메인 컨트롤러

해결 방법은 DCOM, WMI 및 감사 및 보안 로그 관리가 문제의 AD 서버에서 올바르게 설정되었는지 확인하는 것입니다.



> 참고: 여러 도메인 또는 여러 포리스트는 기본적으로 지원되지 않습니다. Umbrella 공지에서 다중 AD 도메인 지원을 참조하십시오. 이러한 문제가 발생할 경우 Umbrella Support에 문의하여 지원을 받을 수도 있습니다.

WMI 권한을 확인하려면

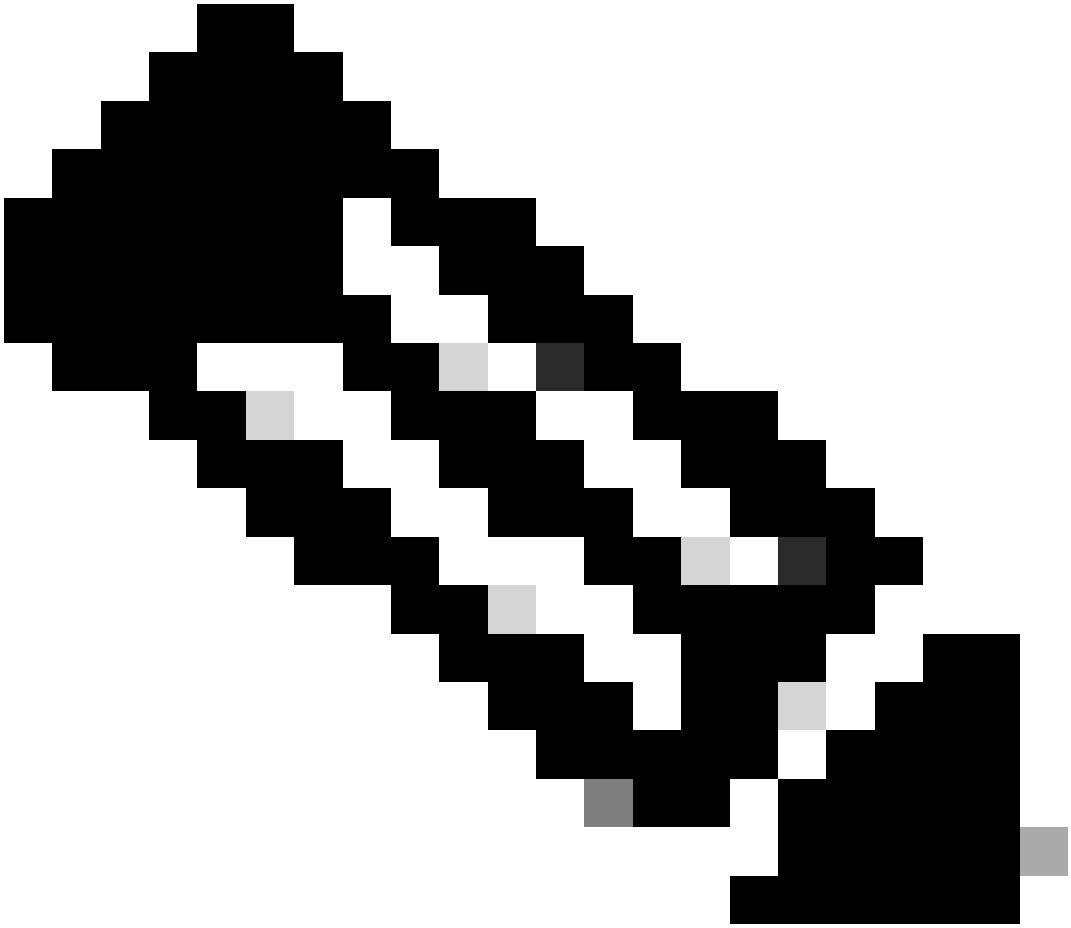
1. 시작 > 실행 > wmimgmt.msc를 선택하여 Windows Management Infrastructure Control 콘솔에 액세스합니다.
2. WMI Control(WMI 제어) > Properties(속성) > Security(보안) 탭을 마우스 오른쪽 버튼으로 클릭합니다.

3. 루트 > CIMV2 네임 공간을 선택하고 보안 버튼을 선택합니다.
4. OpenDNS_Connector 사용자를 추가하고 다음 권한을 허용합니다.

- 계정 사용
- 원격 사용
- 보안 읽기

DCOM 권한을 확인하려면

1. 명령줄에서 dcomcnfg를 실행합니다.
2. Console Root(콘솔 루트) > Component Services(구성 요소 서비스) > Computers(컴퓨터)로 이동합니다.
3. [내 컴퓨터]를 마우스 오른쪽 단추로 클릭하고 [속성]을 선택합니다.
4. 내 컴퓨터 속성에서 COM 보안 탭을 선택합니다.
5. 시작 및 활성화 권한 섹션에서 한도 편집을 선택합니다.
6. OpenDNS_Connector 사용자를 추가하고 원격 실행 및 원격 활성화 권한을 허용합니다.
7. 확인을 선택하여 내 컴퓨터 등록 정보를 확인하고 닫습니다.



참고: 대부분의 경우 DCOM이 변경되면 해당 DC를 재부팅해야 변경 사항이 적용됩니다.

Windows 2003 서버에서 "감사 및 보안 로그 관리"를 확인하려면

1. 도메인 컨트롤러에서 명령 프롬프트를 열고 이 명령을 입력합니다(Windows 2003을 실행하는 경우 /r을 /v로 대체).

```
gpresult /scope computer /r
```

2. Applied Group Policy Objects(적용된 그룹 정책 개체) 줄을 확인합니다. 그 아래에는 해당 도메인 컨트롤러에 적용된 정책의 목록이 나와 있습니다. 모든 도메인 컨트롤러에 적용할 수 있는 하나를 기록해 둡니다.
(예: "기본 도메인 컨트롤러 정책"). 존재하지 않는 경우 하나를 만들어 적용해야 합니다.

올바른 정책을 수정하려면

3. [그룹 정책 관리] 패널을 엽니다(시작/관리 도구 사용). 원하는 정책을 선택합니다. "Domain Controllers(도메인 컨트롤러)" 폴더에 있는 항목을 선택할 수 있습니다.

4. 해당 정책을 마우스 오른쪽 단추로 누르고 편집을 선택하여 그룹 정책 관리 편집기를 표시합니다.

5. Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment 폴더로 이동한 후 Manage audit and security log를 선택하여 해당 속성을 봅니다.

6. 이러한 정책 설정 정의 > 사용자 또는 그룹 추가를 선택합니다. OpenDNS_Connector 사용자를 찾아 선택합니다.

7. 도메인 컨트롤러에서 "gpupdate /force" 명령을 실행하여 정책이 적용되었는지 확인합니다.

원인

이 오류는 일반적으로 OpenDNS_Connector 사용자가 작업을 수행할 수 있는 권한이 부족함을 나타냅니다.

Windows 커넥터 스크립트는 일반적으로 OpenDNS_Connector 사용자에 필요한 권한을 설정합니다. 그러나 엄격한 AD 환경에서는 일부 관리자가 도메인 컨트롤러에서 VB 스크립트를 실행할 수 없으므로 Windows 구성 스크립트의 작업을 수동으로 복제해야 합니다.

추가 정보

이 문제 해결에 대한 자세한 내용은 액세스 거부 해결에 대한 전체 항목을 참조하십시오.

앞서 언급한 설정을 확인/변경한 후에도 대시보드에 "액세스 거부" 메시지가 표시되면 이 문서에 설

명된 대로 Support the Connector logs(커넥터 지원 로그)를 보내십시오. Provide Support with AD Connector Logs(AD 커넥터 로그를 사용하여 지원 제공).

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.