

ISE 3.5 EntraID 외부 그룹 쿼리 성능 문제 및 Microsoft Graph API 권한 확인

목차

문제

EntraID REST ID Store 컨피그레이션이 있는 Cisco ISE 3.5 patch2는 EntraID.ExternalGroups를 쿼리할 때 EAP-TLS 인증 중에 상당한 인증 지연을 경험합니다. 쿼리된 PIP - EntraID.ExternalGroups 단계가 완료되는 데 30초 이상 걸려서 EAP 클라이언트가 시간 초과되고 인증을 다시 시작하여 성공적인 세션 완료를 방지합니다.

또한 EntraID REST ID Store 컨피그레이션에서 그룹 특성을 저장하려고 하면 다음 오류 메시지가 나타납니다.

```
java.rmi.RemoteException: null; nested exception is: java.lang.NullPointerException
```

인증 로그에는 외부 그룹 조회 프로세스 중에 비동기 PIP 오류 및 정책 엔진 중단이 표시됩니다. 이 문제는 클라이언트가 확장 된 쿼리 시간 때문에 EAP 세션을 완료 할 수 없는 실패 한 인증 워크플로로 표시 됩니다.

환경

- Cisco ISE(Identity Services Engine) 버전 3.5.0.527(패치 2 포함)
- REST ID 저장소를 통한 Microsoft EntraID(Azure Active Directory) 통합
- EAP-TLS 인증이 구성됨
- 그룹 특성 검색으로 EntraID에 대해 구성된 REST 소스
- ISE 3.4 patch4/patch5 및 ISE 3.5 patch2/patch3에서 관찰된 문제

해결

해결 방법에는 ISE EntraID REST ID 저장소 통합에서 사용하는 Azure 응용 프로그램에 올바른 Microsoft Graph API 권한을 부여하는 것이 포함됩니다.

1단계: 필요한 Microsoft Graph API 권한 부여

Azure 포털로 이동하여 ISE 통합에 사용되는 애플리케이션 등록을 찾습니다. 이 애플리케이션 유형 API 권한 부여:

Directory.Read.All

이 권한에 대한 관리자 동의가 허용되었는지 확인합니다.

2단계: ISE 서비스 다시 시작

Directory.Read.All 권한을 부여한 후 모든 ISE 노드에서 서비스를 다시 시작하여 새 권한이 적용되도록 합니다.

3단계: 해결 확인

인증 프로세스를 테스트하여 쿼리된 PIP - EntraID.ExternalGroups 단계가 허용되는 시간 내에 완료되고 그룹 특성이 오류 없이 저장될 수 있는지 확인합니다.

확인 로그는 AsynchronousPIPEError 없이 성공적으로 완료되었음을 표시해야 합니다.

2026-05-26 14:21:47,981 DEBUG [I/O dispatcher 1][[]] cisco.ise.ropc.utilities.HttpClientWrapper -:::--

원인

이 문제는 ISE 3.5 패치 3 및 관련 버전에 영향을 미치는 Cisco 버그 ID CSCwu13703에 의해 발생합니다. 이 버그는 EntraID 통합에 대한 Microsoft Graph API 권한이 충분하지 않은 것과 관련이 있습니다. 적절한 Directory.Read.All 권한이 없으면 ISE가 EntraID에서 외부 그룹을 효율적으로 쿼리할 수 없으므로 시간 초과 조건이 발생하고 AsynchronousPIPError 예외를 통해 정책 엔진이 일시 중단됩니다.

각 평가 실패 때문에 정책 엔진이 AsynchronousPIPError를 throw하고 인증 워크플로를 일시 중단하여 쿼리 시간이 길어지고 최종 클라이언트 시간 초과가 발생하기 때문에 인증 프로세스가 실패합니다.

관련 콘텐츠

- [Cisco 버그 ID CSCwu13703](#)
- [Microsoft Active Directory를 사용하는 Cisco ISE INTRA ID 및 Intune 컨피그레이션 가이드](#)

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.