

Identity Services Engine에서 Active Directory 그룹 검색 문제 해결

ERROR_TOKEN_GROUPS_INCOMPLETE_PERMISSIONS

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[문제](#)

[솔루션](#)

소개

이 문서에서는 인증 중에 AD(Active Directory) 그룹 검색 문제를 해결하는 방법에 대해 설명하며 이 오류는 라이브 로그에 표시됩니다.

ERROR_TOKEN_GROUPS_INSUFFICIENT_PERMISSIONS

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Identity Services Engine
- Microsoft Active Directory

사용되는 구성 요소

이 문서는 ISE(Identity Services Engine)의 특정 소프트웨어 버전으로 제한되지 않습니다.

문제

문제는 ISE를 AD에 조인하는 데 사용된 사용자 계정에 tokenGroups를 가져올 올바른 권한이 없다는 것입니다. ISE를 AD에 조인하는 데 도메인 관리자 계정이 사용된 경우에는 이 오류가 발생하지 않습니다. 이 문제를 해결하려면 사용자 계정에 ISE 노드를 추가하고 ISE 노드에 해당 권한을 제공해야 합니다.

- 목록 내용
- 모든 속성 읽기

- 읽기 권한

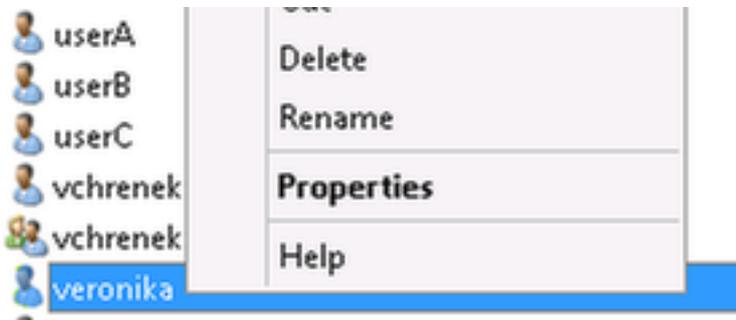
사용자에 대한 권한이 올바른 것처럼 보이지만 이 문제가 나타납니다([ISE 1.3 AD 인증 실패, 오류 발생:"토큰 그룹을 가져올 수 있는 권한이 없습니다."](#)) 이러한 디버그는 ad-agent.log에 표시됩니다.

```
28/08/2016 17:23:35,VERBOSE,140693934700288,Error code: 60173 (symbol: LW_ERROR_TOKEN_GROUPS_INSUFFICIENT_PERMISSIONS),lsass/server/auth-providers/ad-open-provider/provider-main.c:7409
28/08/2016 17:23:35,VERBOSE,140693934700288,Error code: 60173 (symbol: LW_ERROR_TOKEN_GROUPS_INSUFFICIENT_PERMISSIONS),lsass/server/api/api2.c:2572
```

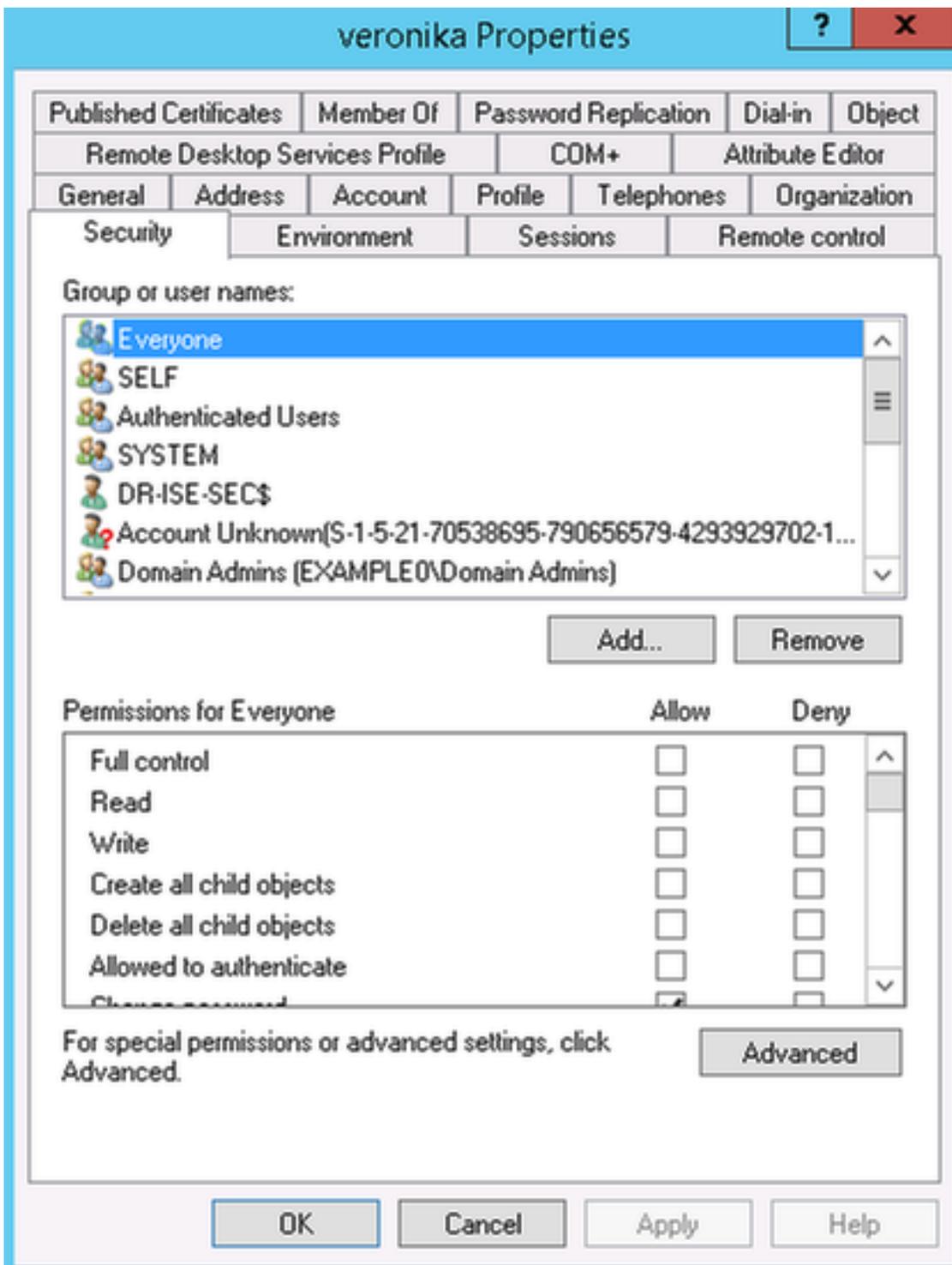
솔루션

사용자 계정에 필요한 권한을 제공하려면 다음 단계를 수행하십시오.

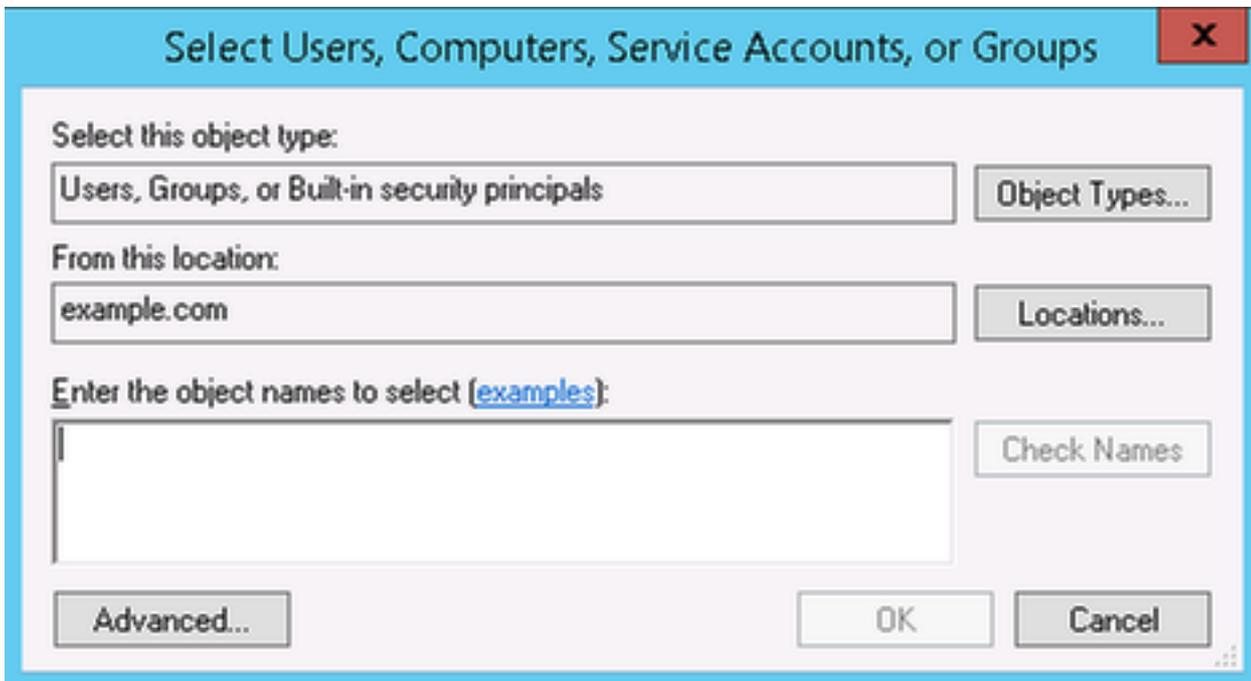
1.AD에서 AD 사용자 계정 속성으로 이동합니다.



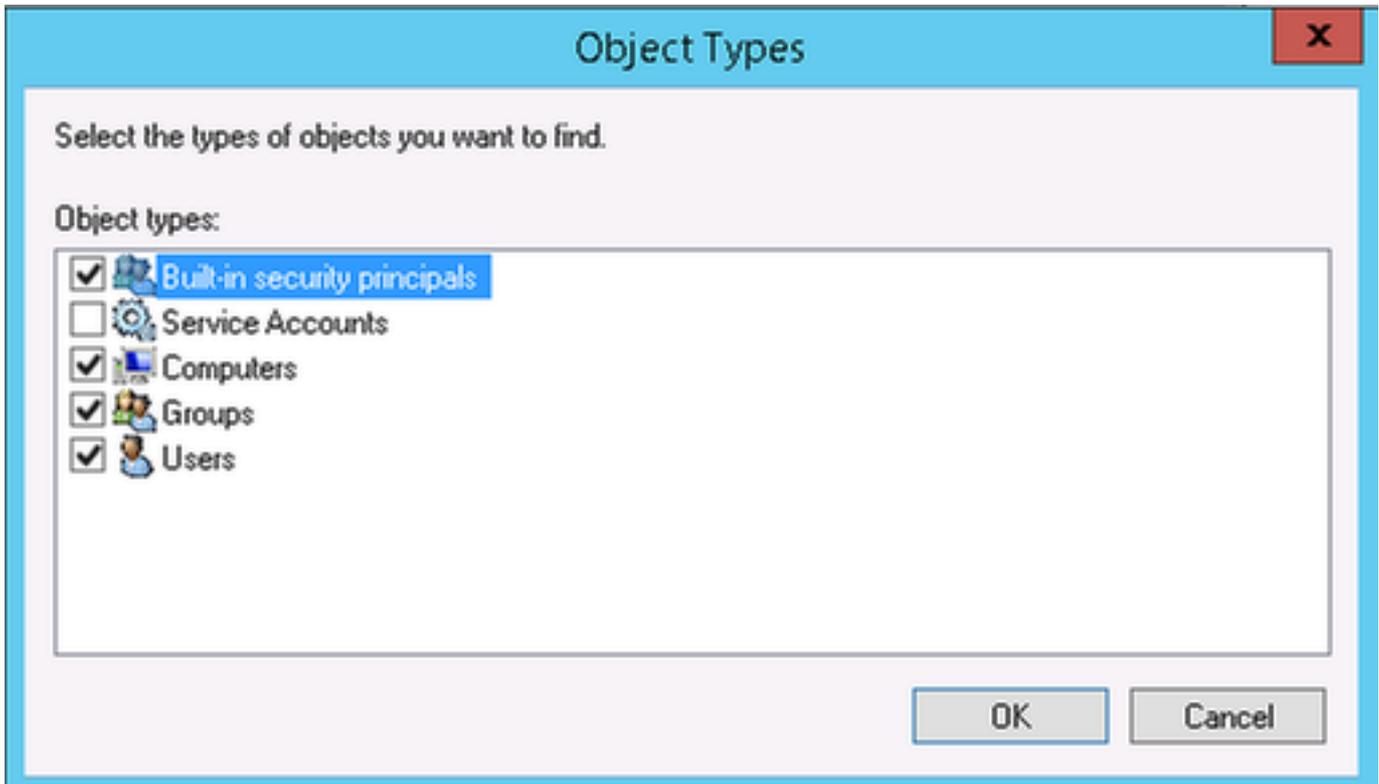
2. 보안 탭을 선택하고 추가를 클릭합니다.



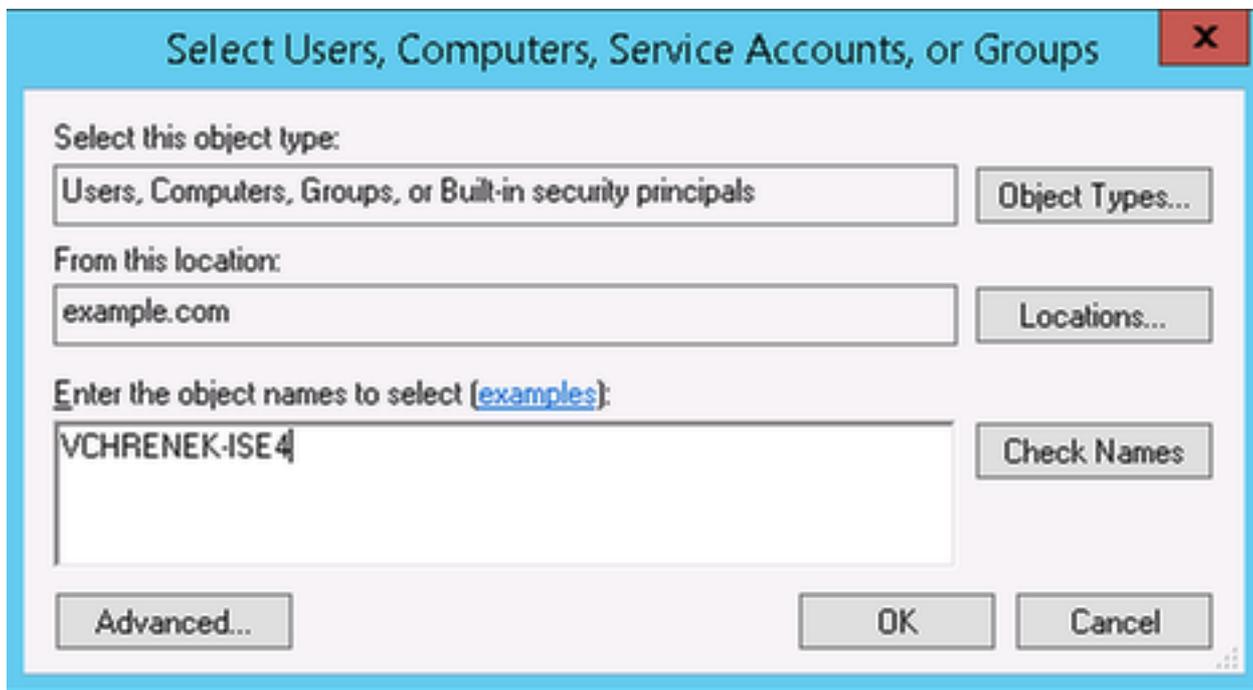
3. 객체 유형 선택:



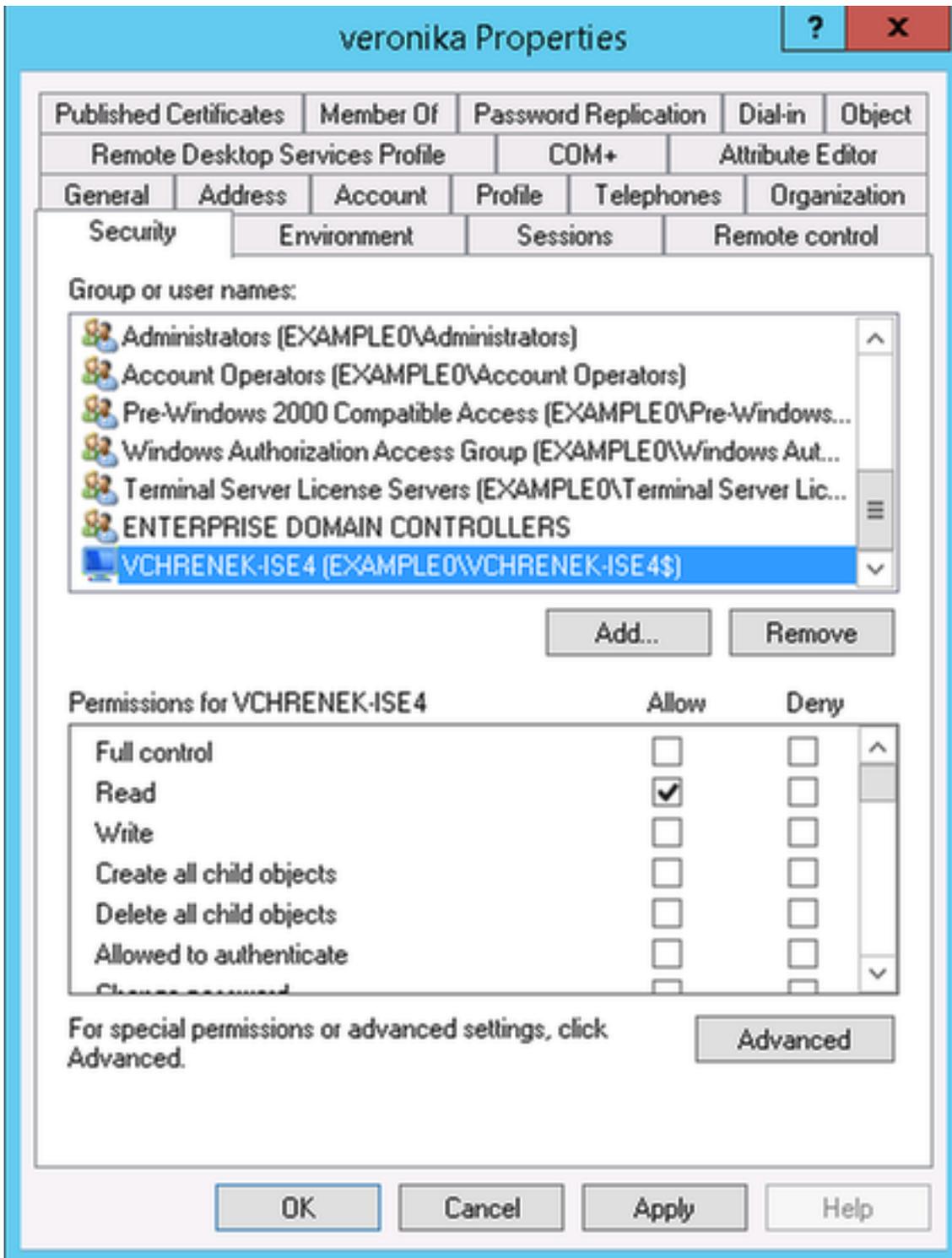
4. 컴퓨터를 선택하고 확인을 클릭합니다.



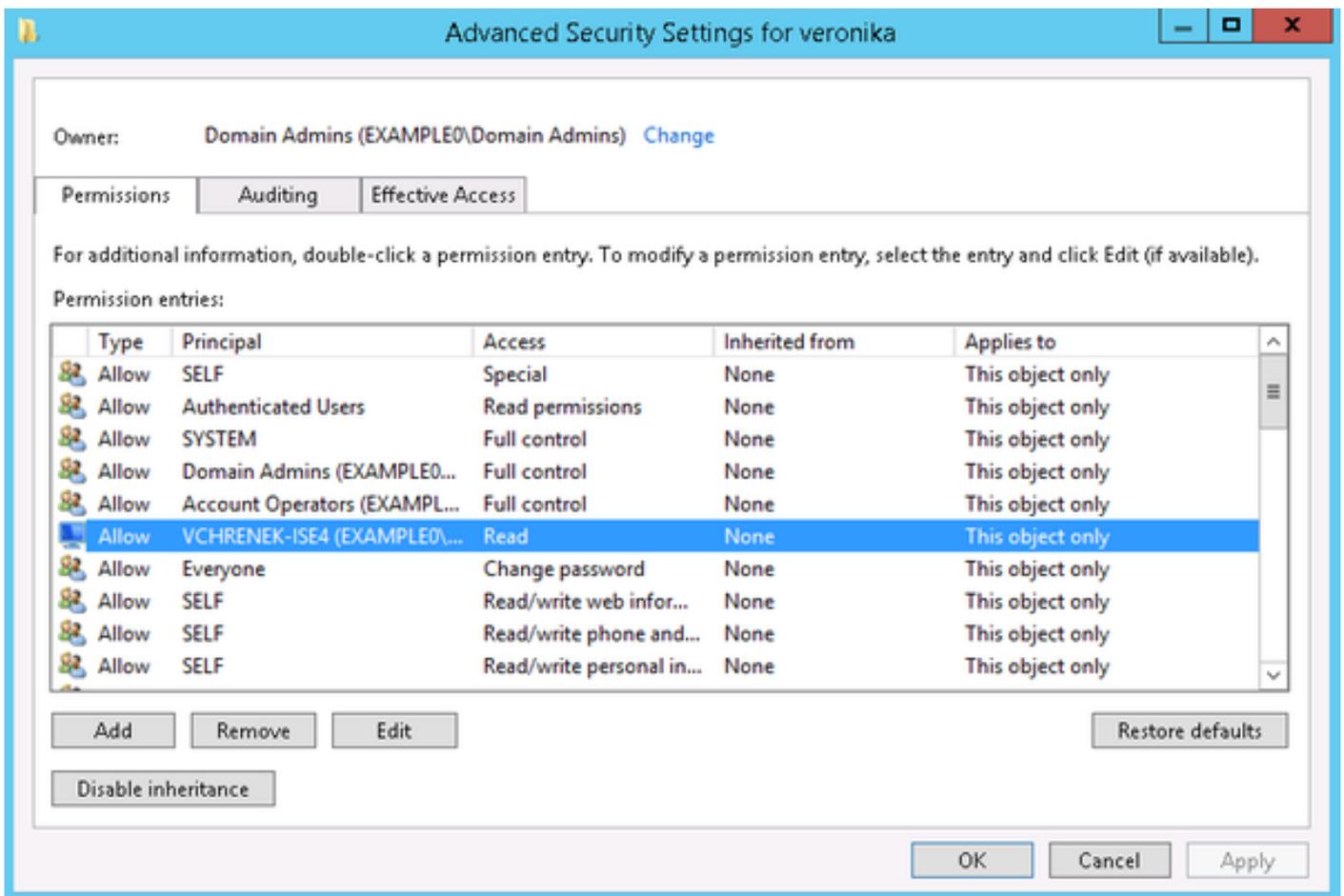
5. ISE 호스트 이름(이 예에서는 VCHRENK-ISE4)을 삽입하고 OK를 클릭합니다.



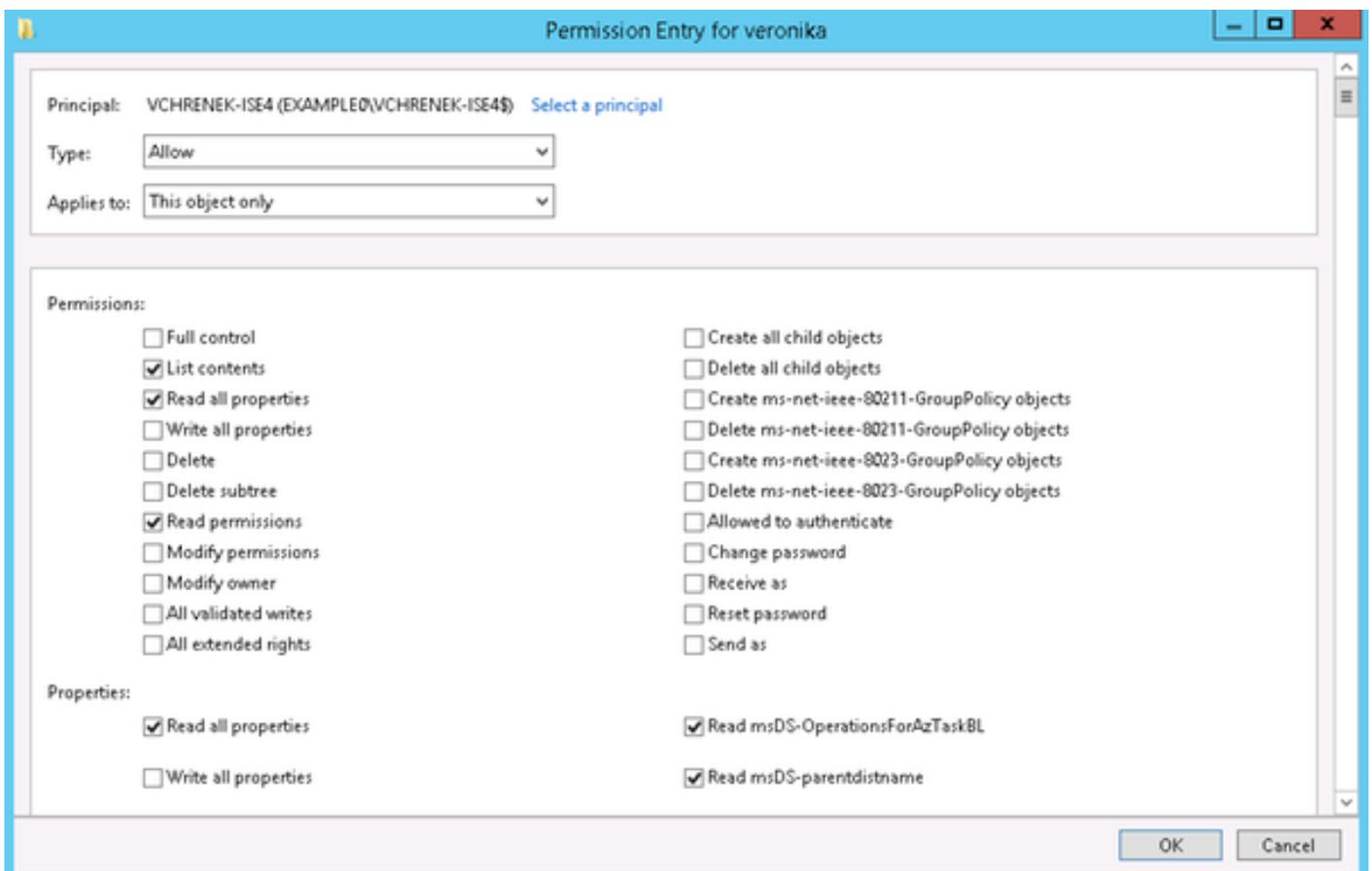
6. ISE 노드를 선택하고 **Advanced**(고급)를 클릭합니다.



7. 고급 보안 설정에서 ISE 머신 계정을 선택하고 편집을 클릭합니다.



8. ISE 시스템 계정에 대한 권한을 제공하고 OK(확인)를 클릭합니다.



이러한 변경 후, 문제 없이 AD 그룹을 검색해야 합니다.

Test User Authentication

* Username

* Password

Authentication Type

Authorization Data Retrieve Groups
 Retrieve Attributes

Authentication Result	Groups	Attributes
Test Username	: veronika	
ISE NODE	: vchrenek-ise4.example.com	
Scope	: Default_Scope	
Instance	: AD1	
Authentication Result	: SUCCESS	
Authentication Domain	: example.com	
User Principal Name	: veronika@example.com	
User Distinguished Name	: CN=veronika,CN=Users,DC=example,DC=com	
Groups	: 1 found.	
Attributes	: 36 found.	

이 작업은 모든 사용자에게 대해 수행되어야 하며 변경 내용은 도메인의 모든 도메인 컨트롤러에 복제되어야 합니다.