修復Active Directory組檢索在Identity Services引擎上發出ERROR_TOKEN_GROUPS_INSUFFICIENT_PERMISSIONS

目錄

簡介

本文描述如何在驗證期間解決Active Directory(AD)組檢索問題，而即時日誌中會顯示此錯誤：

```
ERROR_TOKEN_GROUPS_INSUFFICIENT_PERMISSIONS
```

必要條件

需求

思科建議您瞭解以下主題：

- 思科身分識別服務引擎
- Microsoft Active Directory

採用元件

本文檔不限於身份服務引擎(ISE)的特定軟體版本。

問題

問題在於用於將ISE加入AD的使用者帳戶沒有獲取令牌組的正確許可權。如果使用域管理員帳戶將ISE加入AD，則不會發生這種情況。要解決此問題，您必須將ISE節點新增到使用者帳戶並為這些ISE節點提供這些許可權：

- 列出內容
- 讀取所有屬性
- 讀取許可權

即使使用者的許可權似乎正確(檢查ISE 1.3 AD身份驗證失敗並出現錯誤：「許可權不足，無法提取

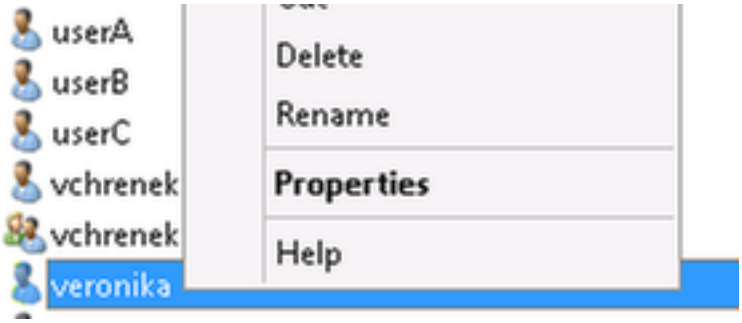
令牌組」)。 這些調試在ad-agent.log中可見：

```
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
```

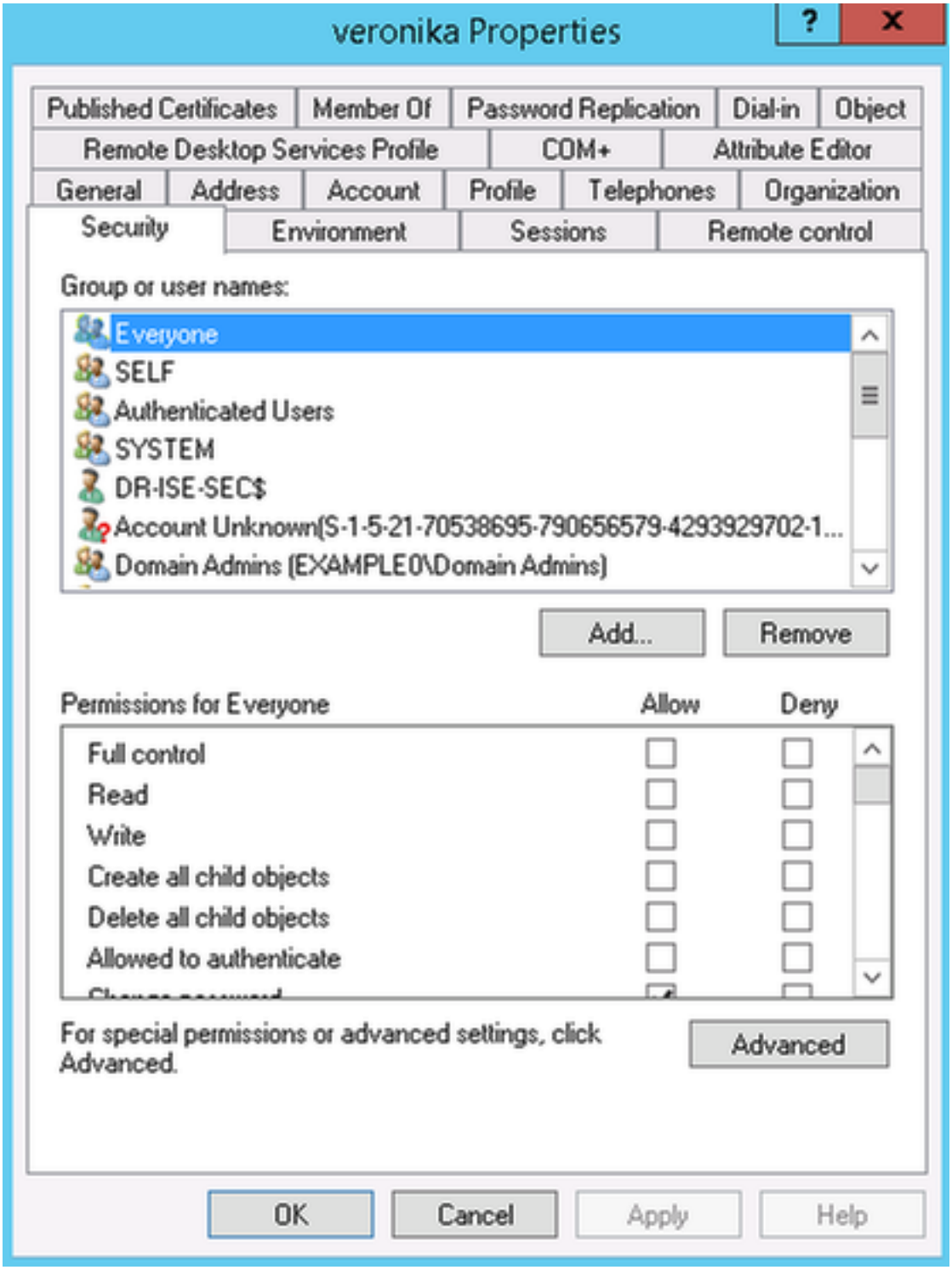
解決方案

要為使用者帳戶提供所需的許可權，請執行以下步驟：

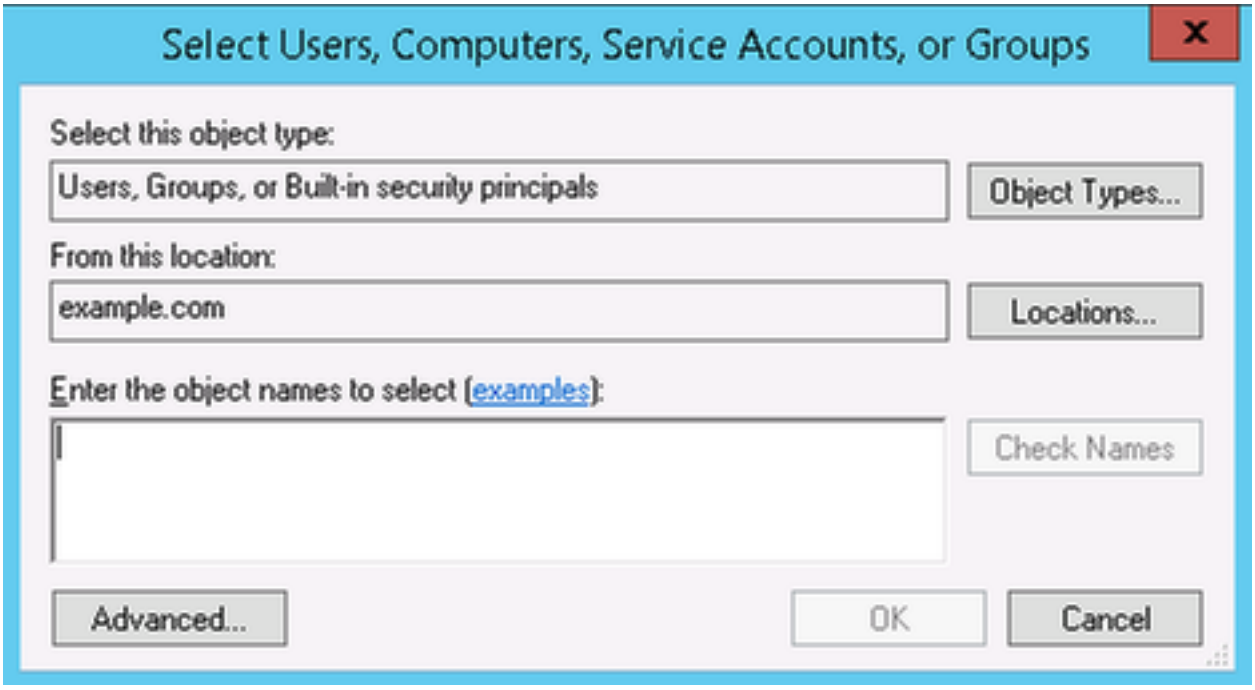
1.在AD上，導航到**Properties** for AD使用者帳戶：



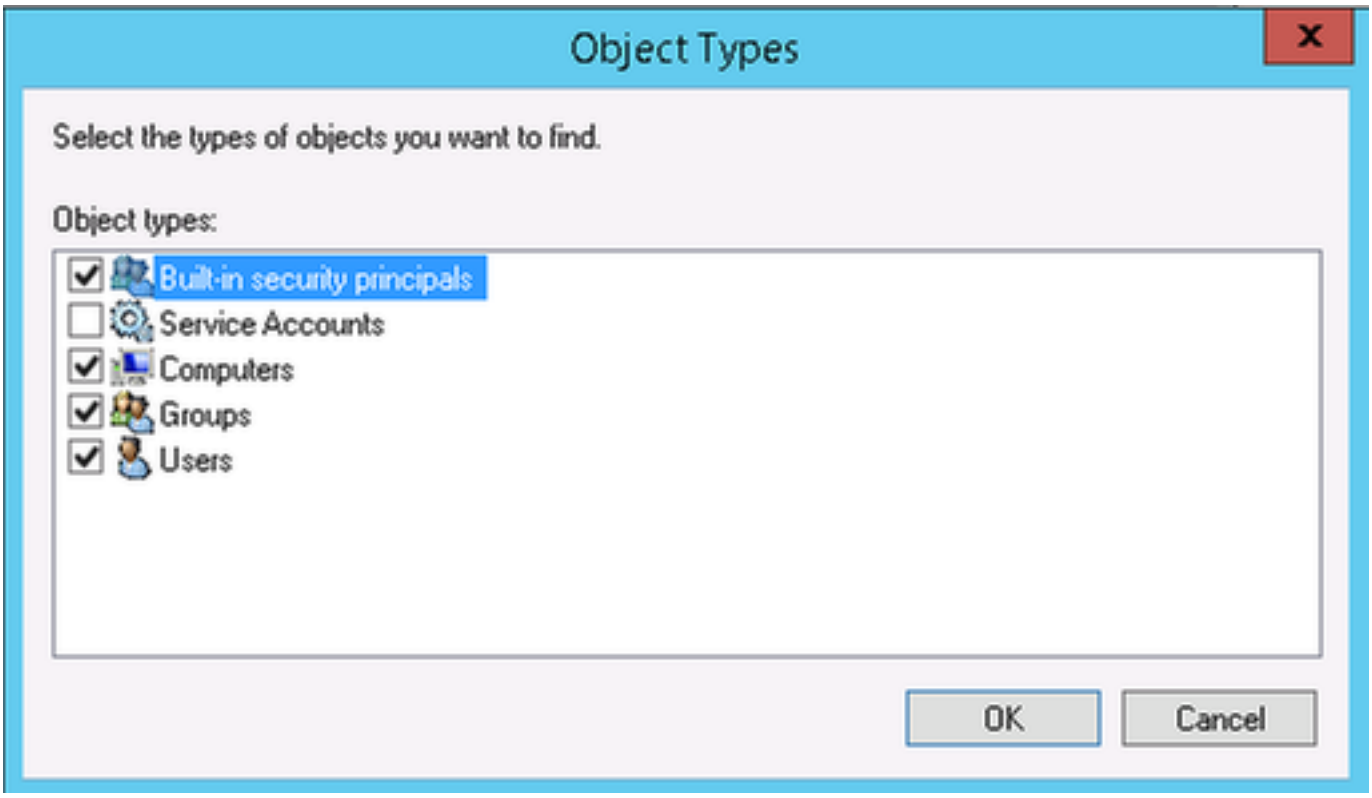
2.選擇**Security**頁籤，然後按一下**Add**:


veronika Properties
Published Certificates
Member Of
Password Replication
Dial-in
Object
Remote Desktop Services Profile
COM+
Attribute Editor
General
Address
Account
Profile
Telephones
Organization
Security
Environment
Sessions
Remote control
Group or user names:
Everyone
SELF
Authenticated Users
SYSTEM
DR-ISE-SEC$
Account Unknown(S-1-5-21-70538695-790656579-4293929702-1...
Domain Admins (EXAMPLE0\Domain Admins)
Add...
Remove
Permissions for Everyone
Allow
Deny
Full control
Read
Write
Create all child objects
Delete all child objects
Allowed to authenticate
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
Help

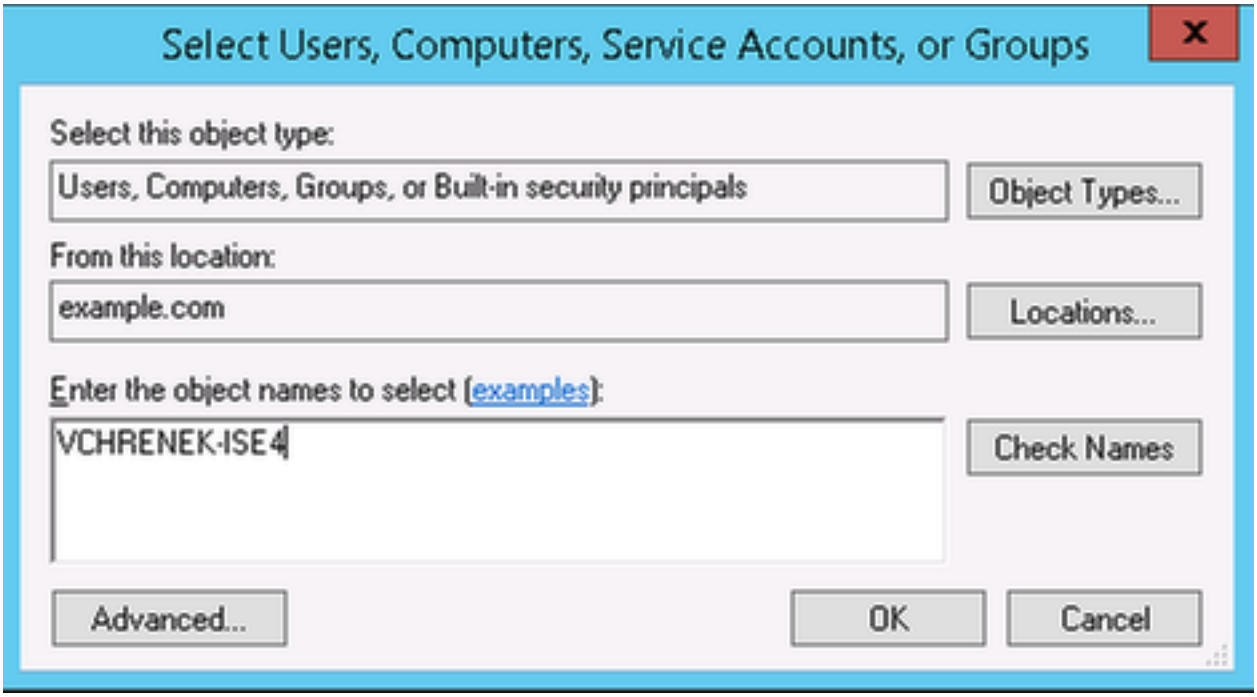
3.選擇**對象型別**:



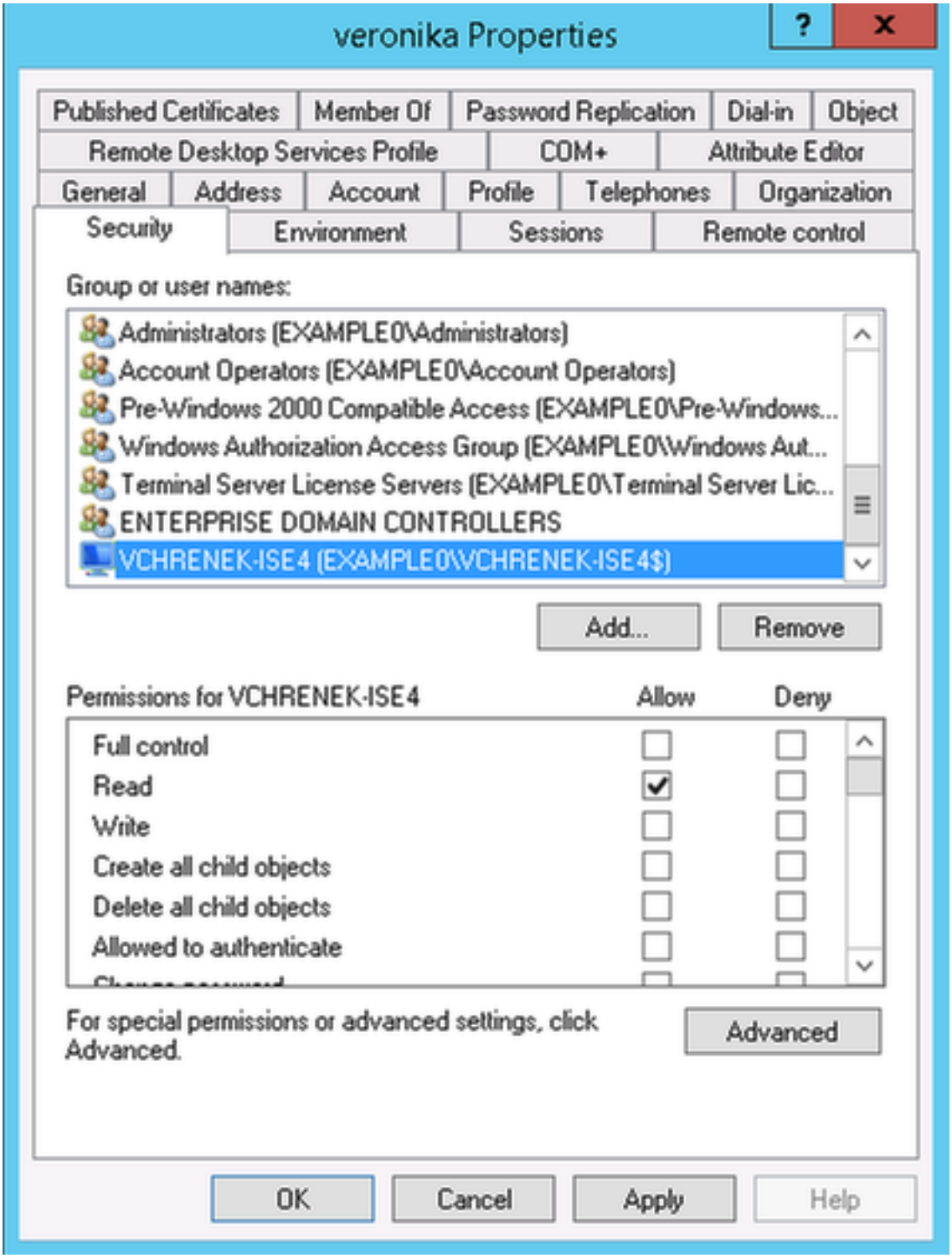
4.選擇**Computers**，然後按一下**OK**:



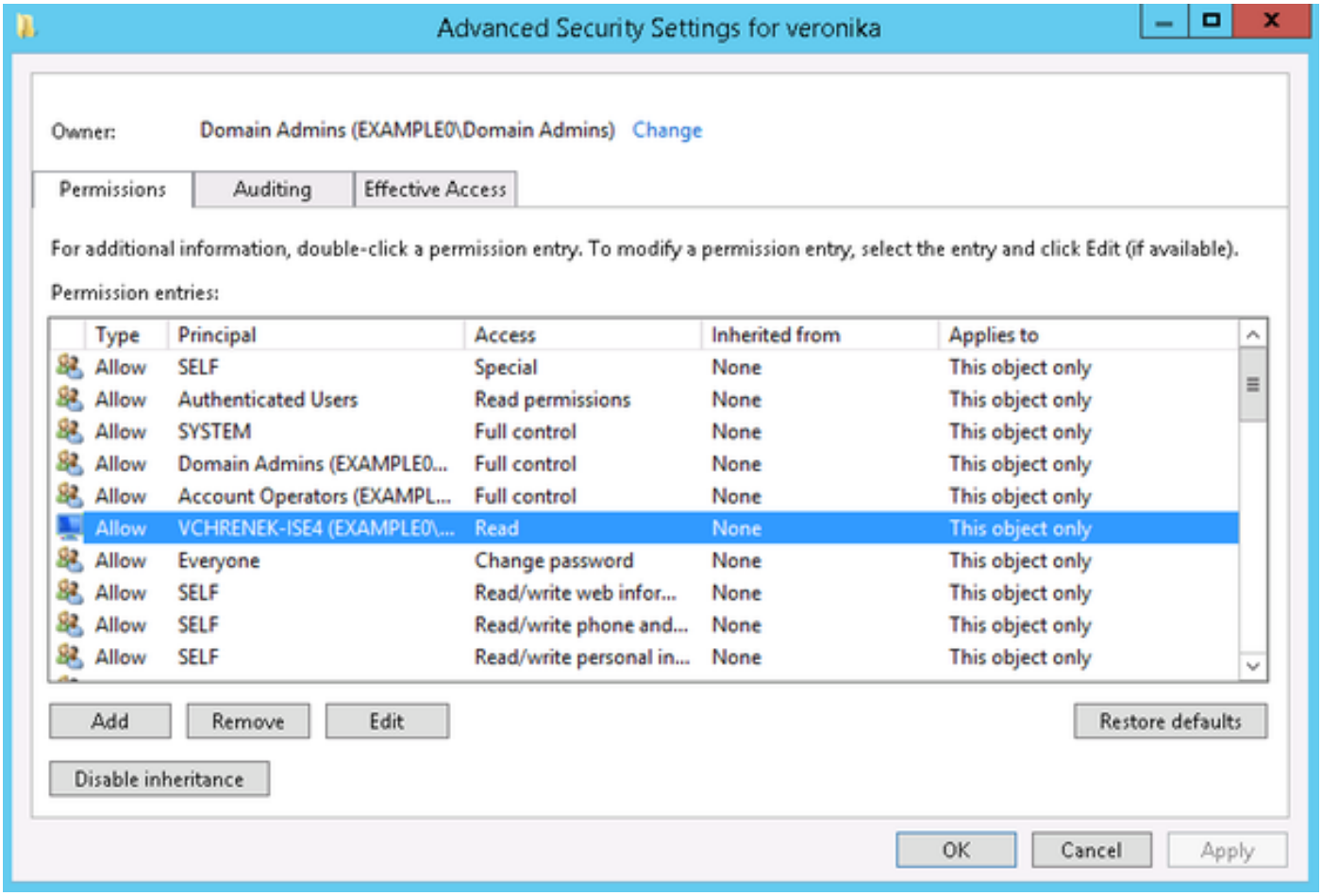
5.插入ISE主機名（在本示例中為VCHRENEK-ISE4），然後按一下**OK**:



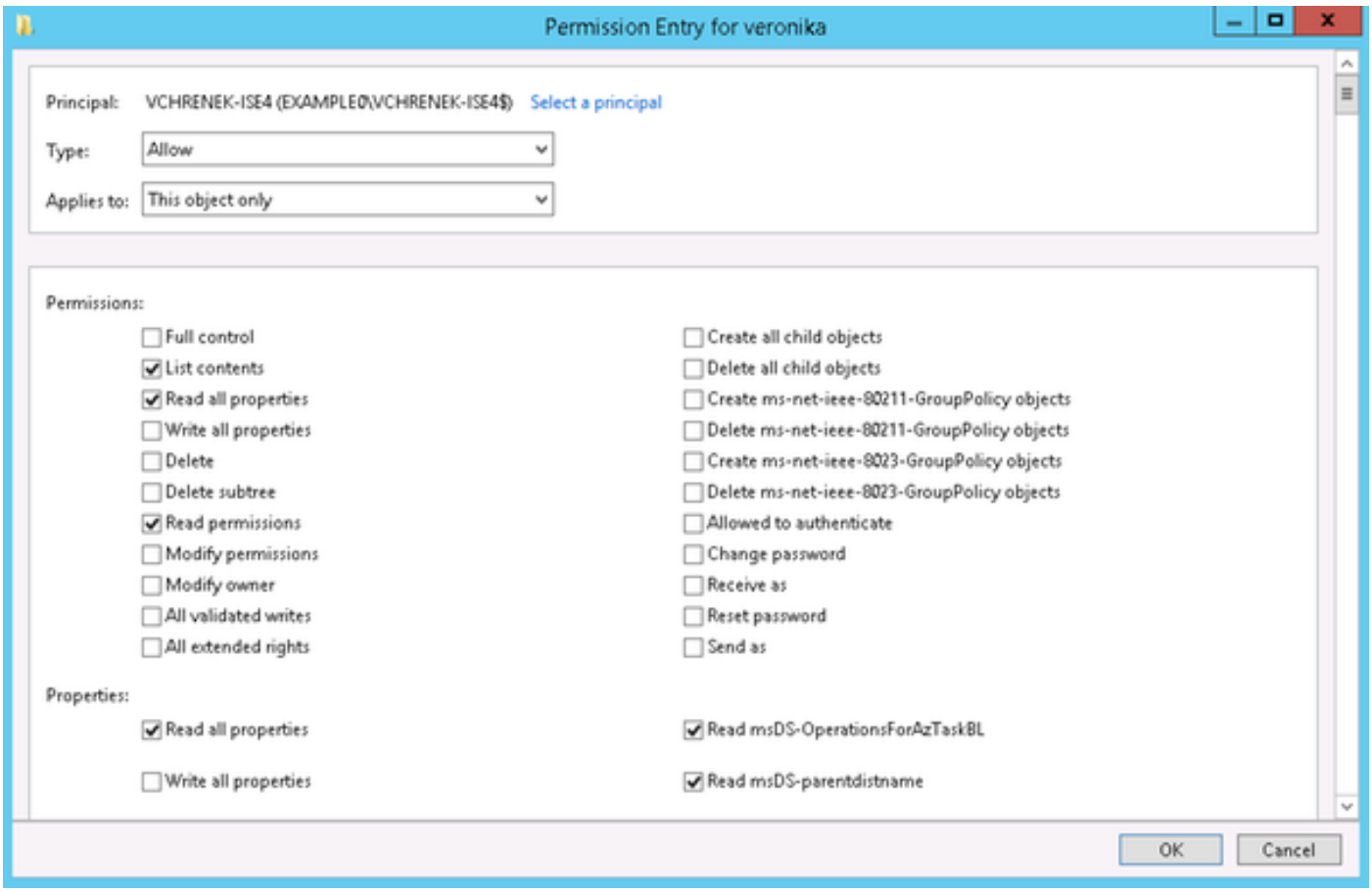
6.選擇ISE節點，然後按一下**Advanced**:



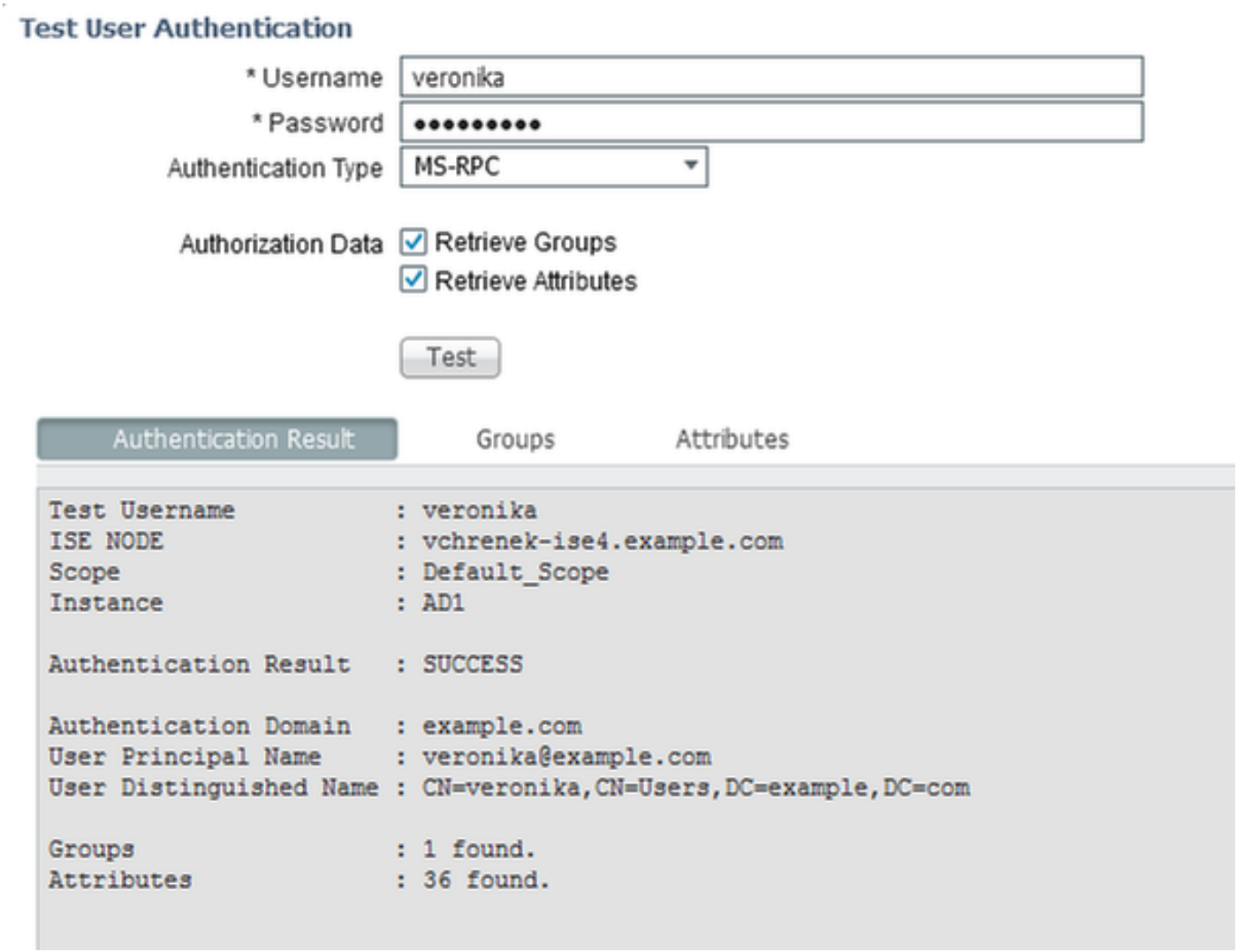
7.從「高級安全設定」中選擇ISE電腦帳戶，然後按一下**編輯**:



8.向ISE電腦帳戶提供這些許可權，然後按一下**OK**:



進行這些更改後，應在不出現任何問題的情況下檢索AD組：



必須對所有使用者執行該操作，並且更改應複製到域中的所有域控制器。