修正活动目录组在身份服务引擎的检索问题ERROR_TOKEN_GROUPS_INSUFFICIENT_PERMISSIONS

目录

简介

本文描述如何对应急方案与激活目录(AD)组检索的问题在验证时，而此错误在实际日志被看到：

```
ERROR_TOKEN_GROUPS_INSUFFICIENT_PERMISSIONS
```

先决条件

要求

Cisco 建议您了解以下主题：

- 思科身份服务引擎
- Microsoft Active Directory

使用的组件

本文没有限制对特定软件版本身份服务引擎(ISE)。

问题

问题是用于的用户帐户加入ISE到AD没有正确权限获得tokenGroups。如果域管理帐户用于加入ISE到AD，这不会发生。要调整此问题，您必须添加ISE节点到用户帐户和提供那些权限给ISE节点：

- 列表内容
- 读所有属性
- 读权限

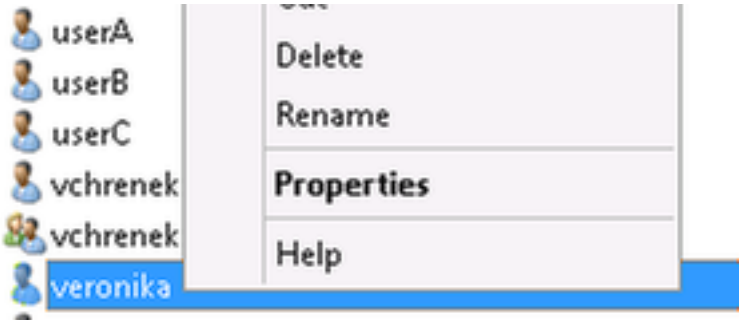
此问题被看到，即使用户的权限似乎正确(ISE的检查1.3 AD认证失效与Error:“不足的权限拿来标记组”)。那些调试在ad-agent.log被看到：

```
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
```

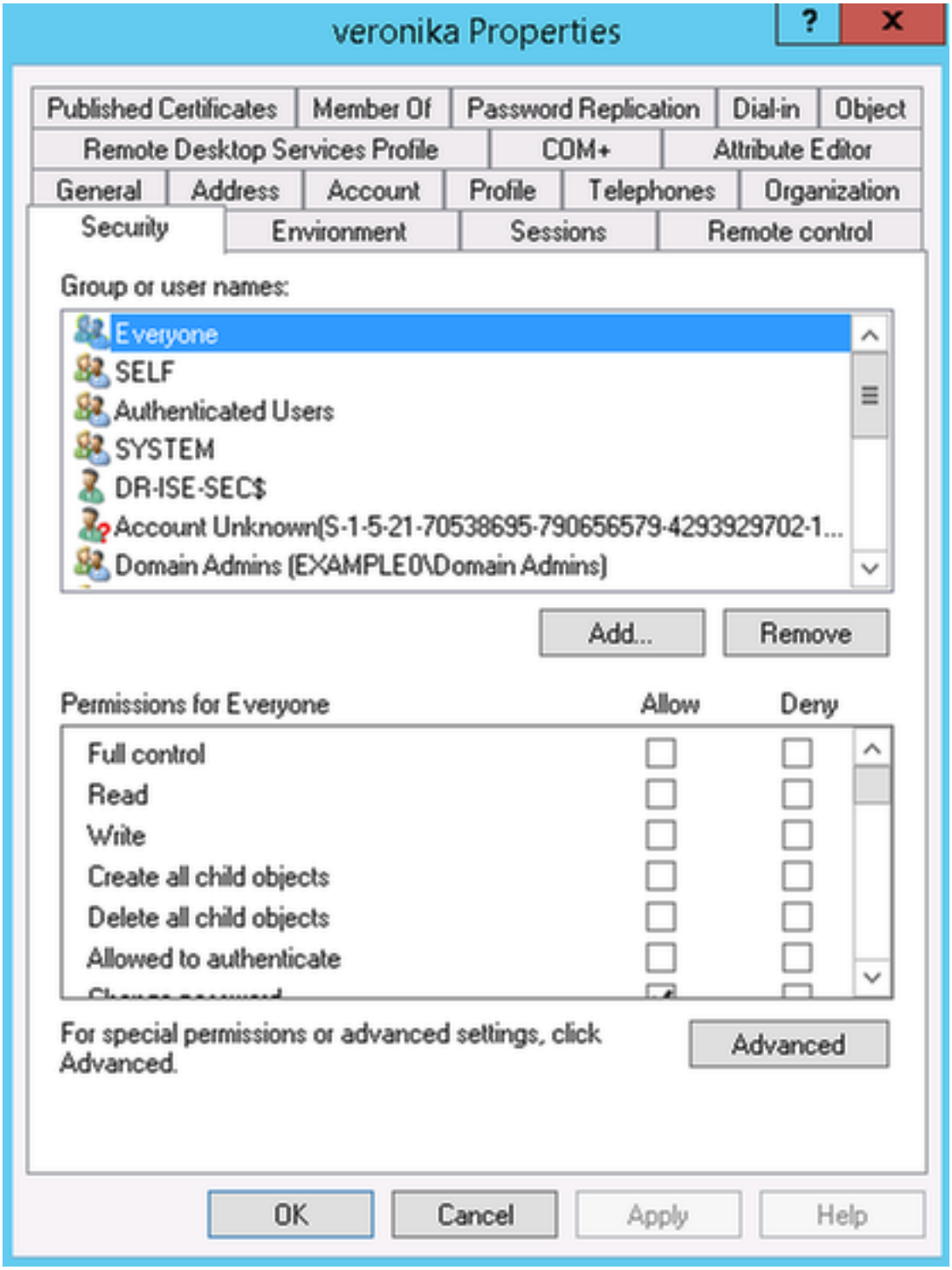
解决方案

要提供需要的权限给用户帐户，请执行那些步骤：

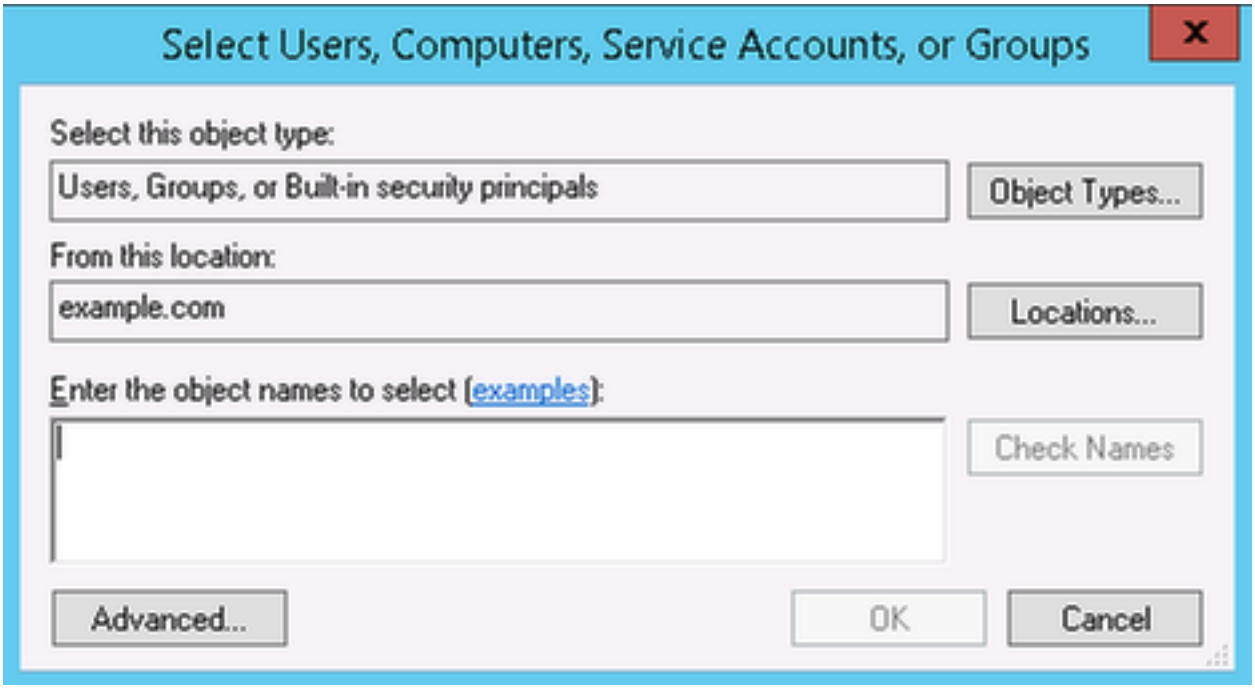
1. 在AD请导航对AD用户帐户的**属性**：



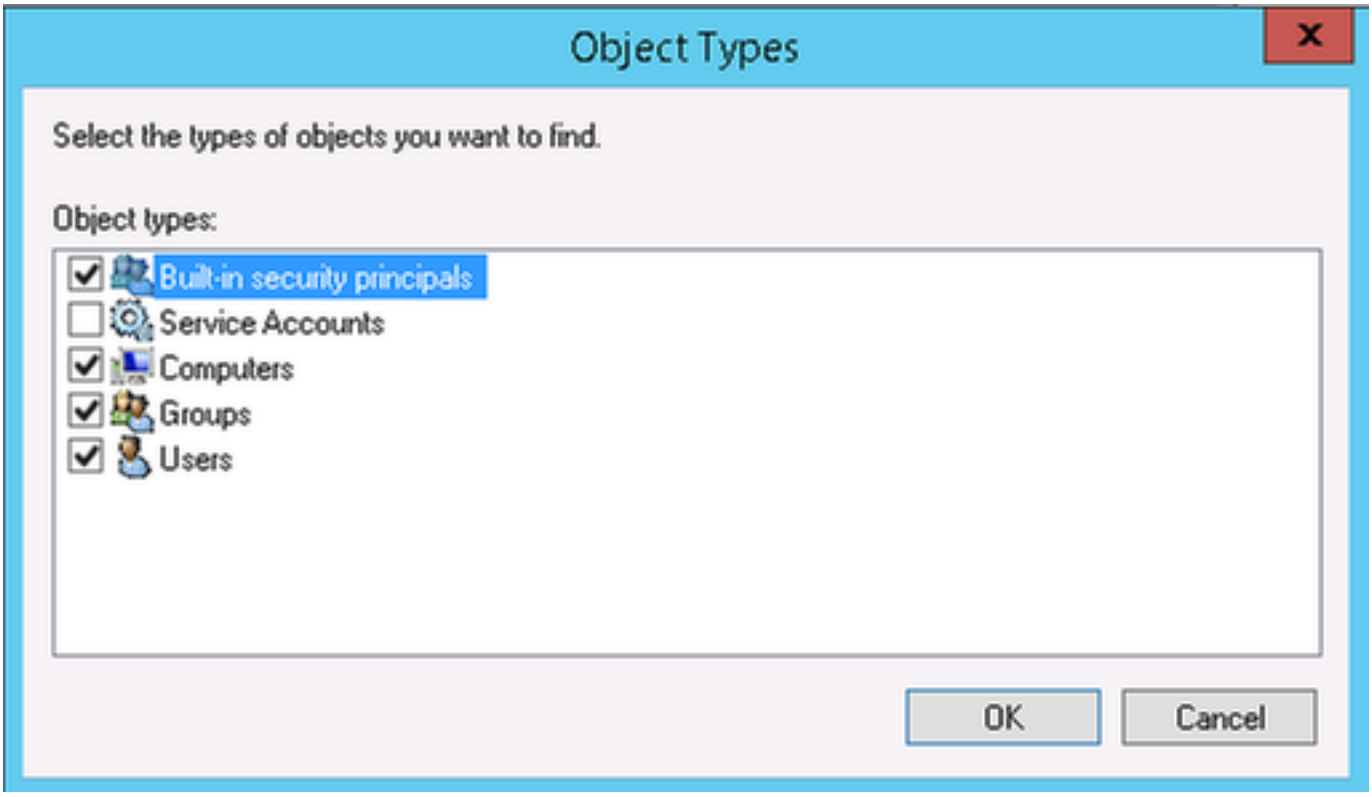
2. 选择**安全选项卡**并且单击**添加**：


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

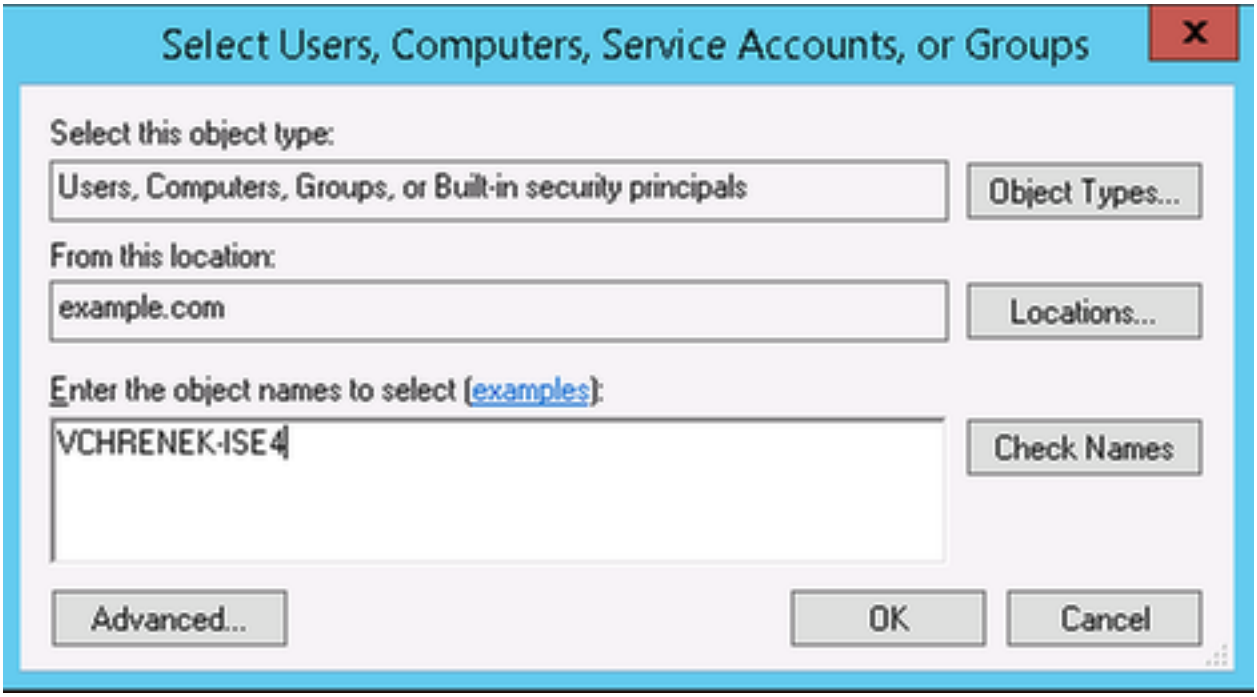
3. 选择**对象类型**：



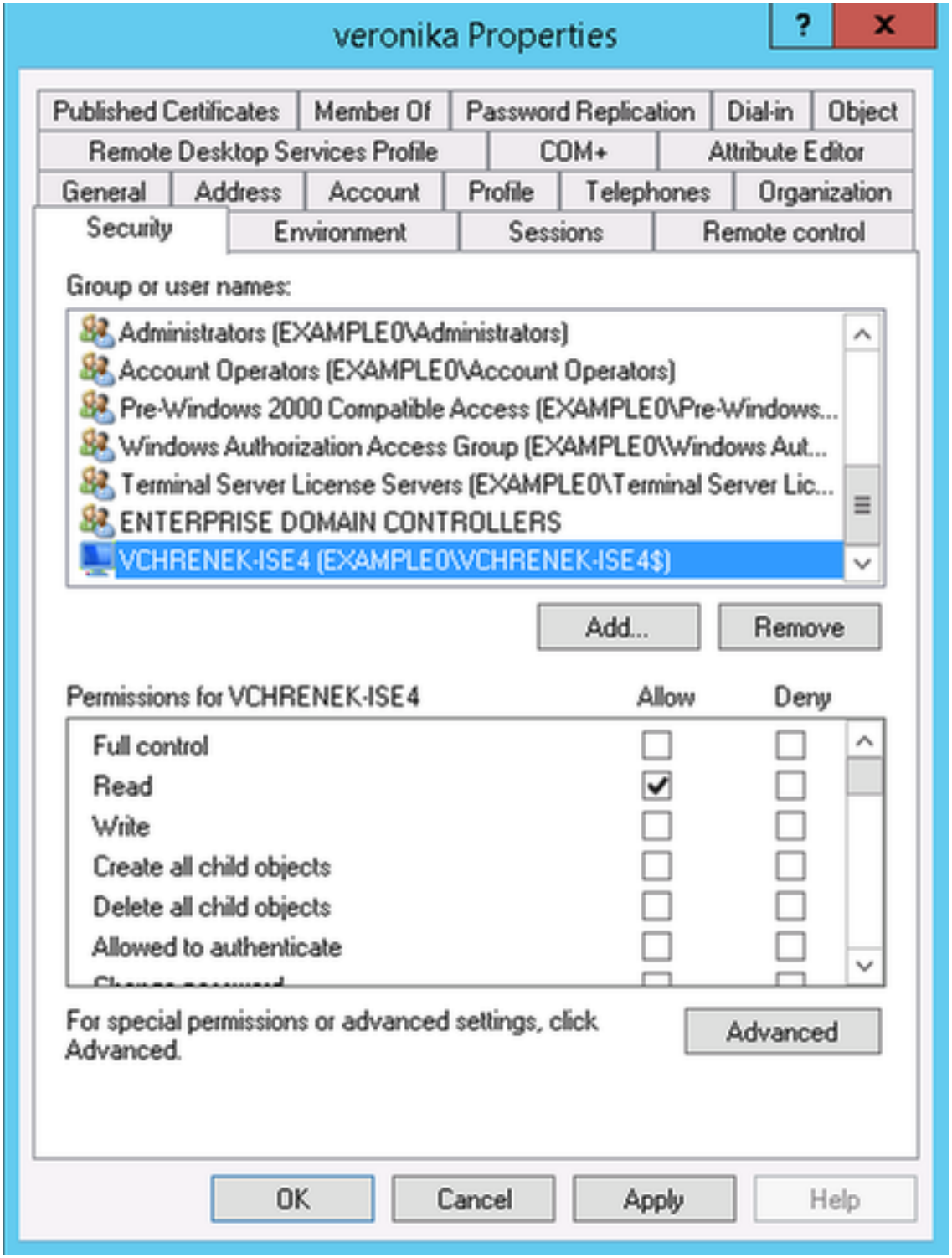
4. 选择**计算机**并且点击OK键：



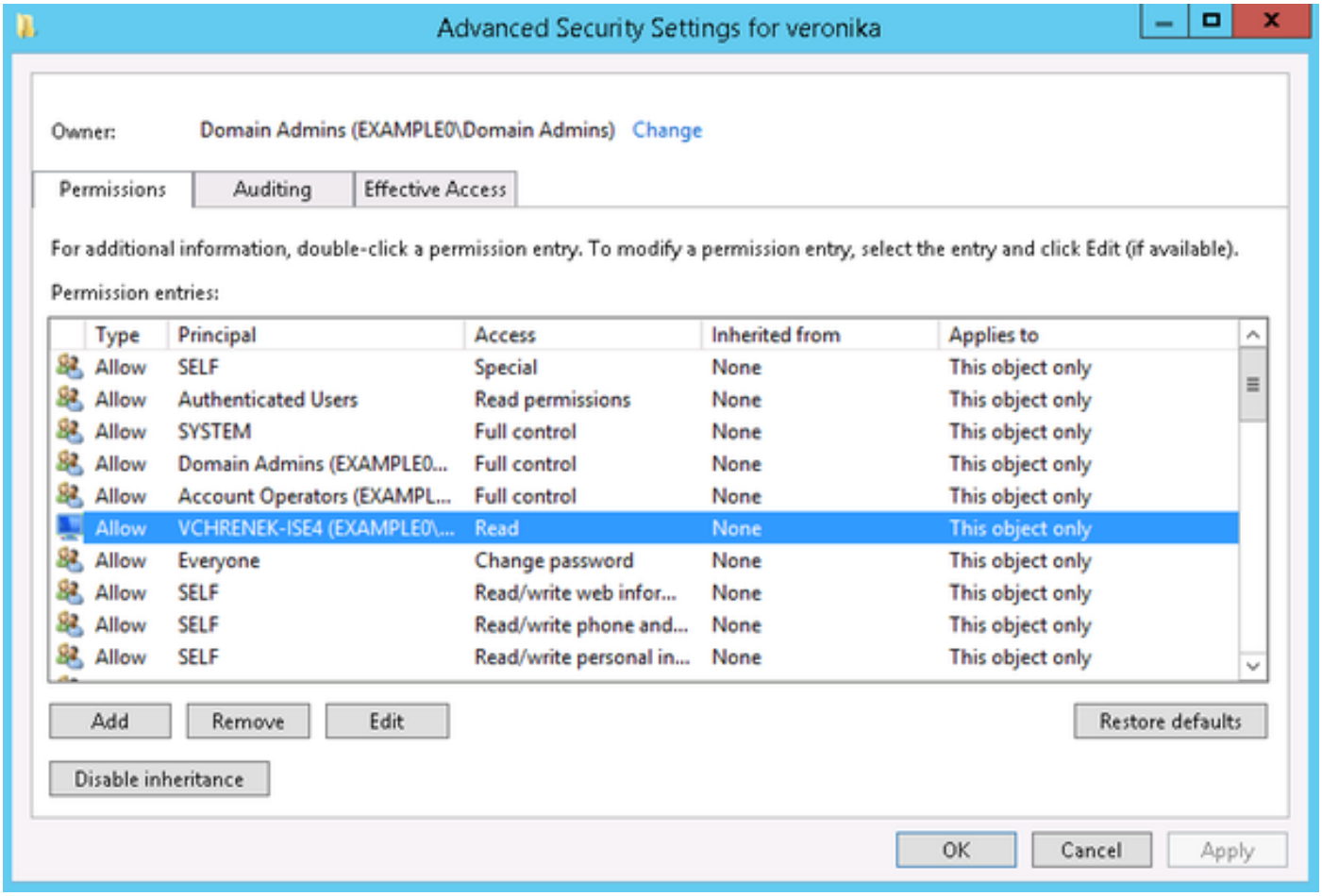
5. 插入ISE主机名(在本例中的VCHRENEK-ISE4)并且点击OK键：



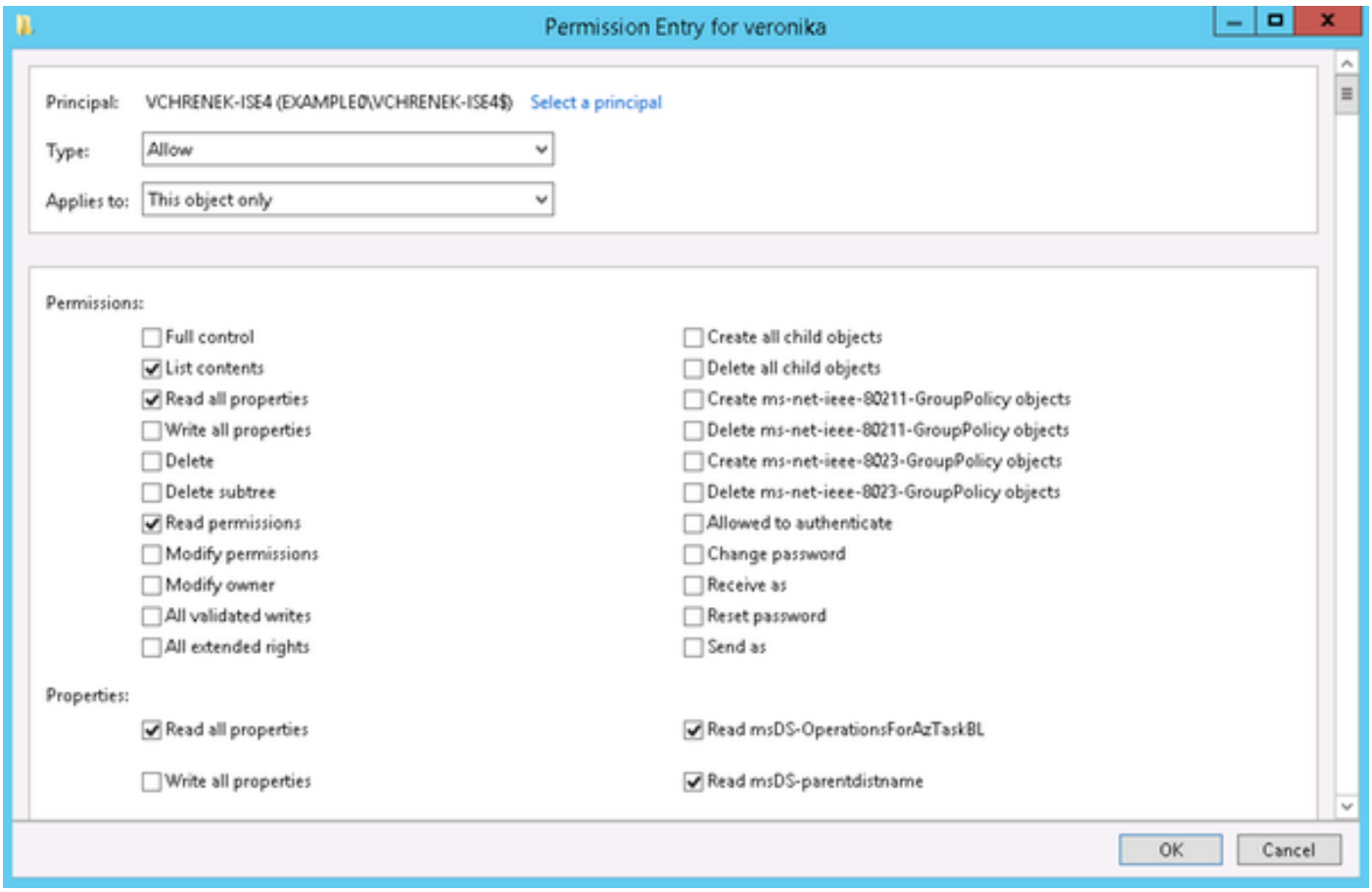
6. 选择ISE节点并且点击**先进**：



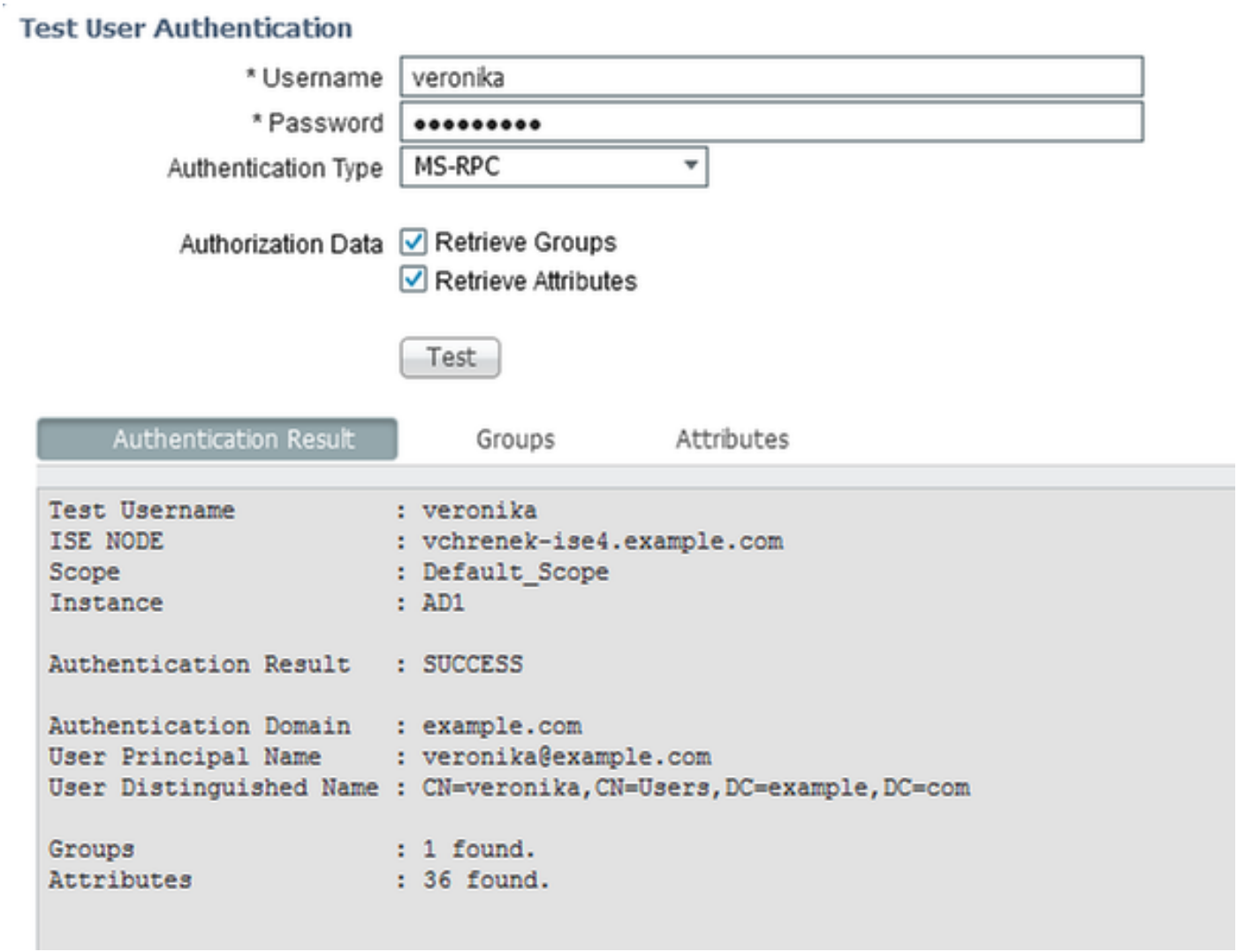
7. 从高级安全设置请选择ISE计算机帐户并且单击**编辑**：



8. 提供那些权限给ISE计算机帐户并且点击OK键：



在应该获取这些更改， AD组，不用任何问题后：



这必须为所有用户执行，并且应该复制变化对所有域控制器在域上。