Réparez la question ERROR_TOKEN_GROUPS_INSUFFICIENT_PERMISSIONS de récupération de groupe de Répertoire actif sur le Cisco Identity Services Engine

Contenu

Introduction

Ce document décrit comment au contournement le problème avec la récupération de groupe de Répertoire actif (AD) pendant l'authentification, alors que cette erreur est vue dans les logs vivants :

```
ERROR_TOKEN_GROUPS_INSUFFICIENT_PERMISSIONS
```

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Logiciel Cisco Identity Services Engine
- Microsoft Active Directory

Composants utilisés

Ce document n'est pas limité aux versions de logiciel spécifiques du Cisco Identity Services Engine (ISE).

Problème

Le problème est que le compte utilisateur utilisé pour joindre ISE à l'AD n'a pas des privilèges corrects d'obtenir des tokenGroups. Ceci ne se produirait pas si le compte d'admin de domaine était utilisé pour joindre ISE à l'AD. Pour réparer cette question, vous devez ajouter des noeuds

ISE au compte utilisateur et fournir ces autorisations aux noeuds ISE :

- Contenu de liste
- Lisez toutes les propriétés
- Lisez les autorisations

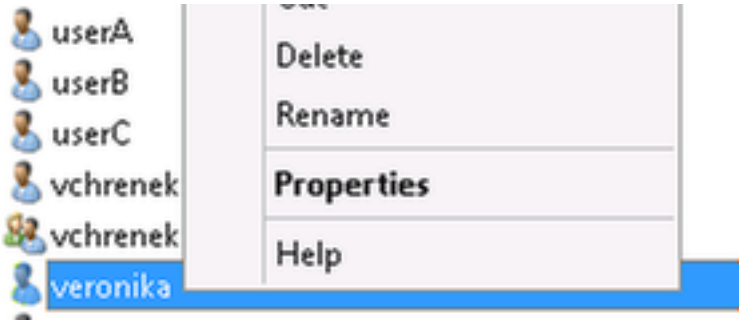
Cette question est vue, quoique les autorisations pour l'utilisateur semble être correctes (le contrôle contre des authentifications d'AD ISE 1.3 échouent avec l'erreur : « Privilège insuffisant de chercher les groupes symboliques »). Ces débogages sont vus dans ad-agent.log :

```
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
```

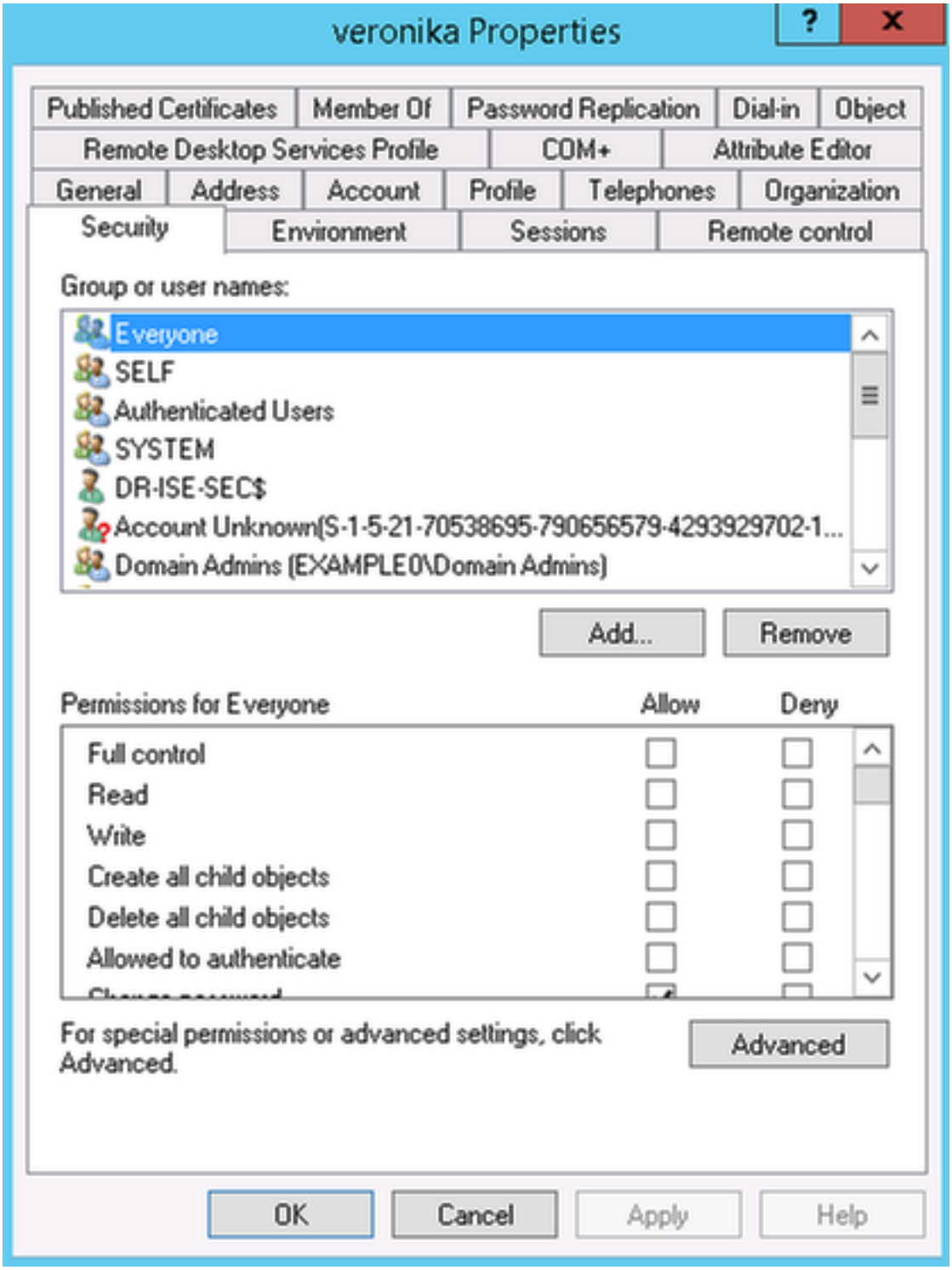
Solution

Pour fournir des autorisations requises au compte utilisateur, exécutez ces étapes :

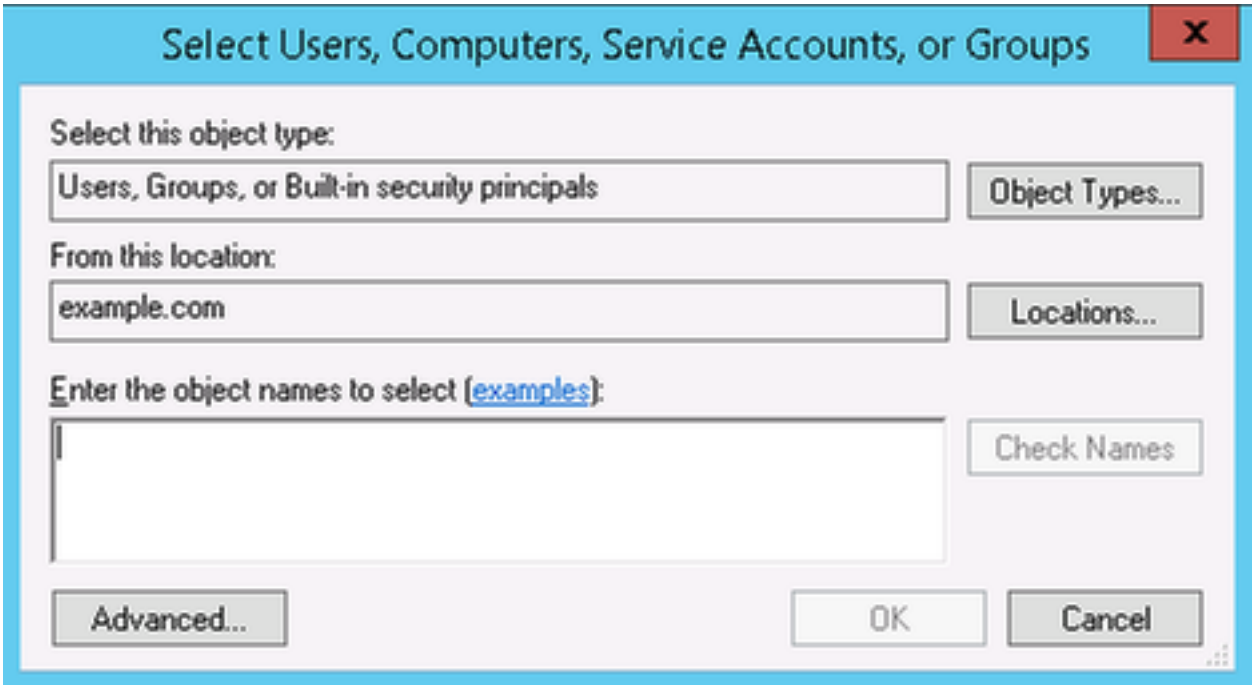
1. sur l'AD naviguez vers **Properties** pour le compte utilisateur d'AD :



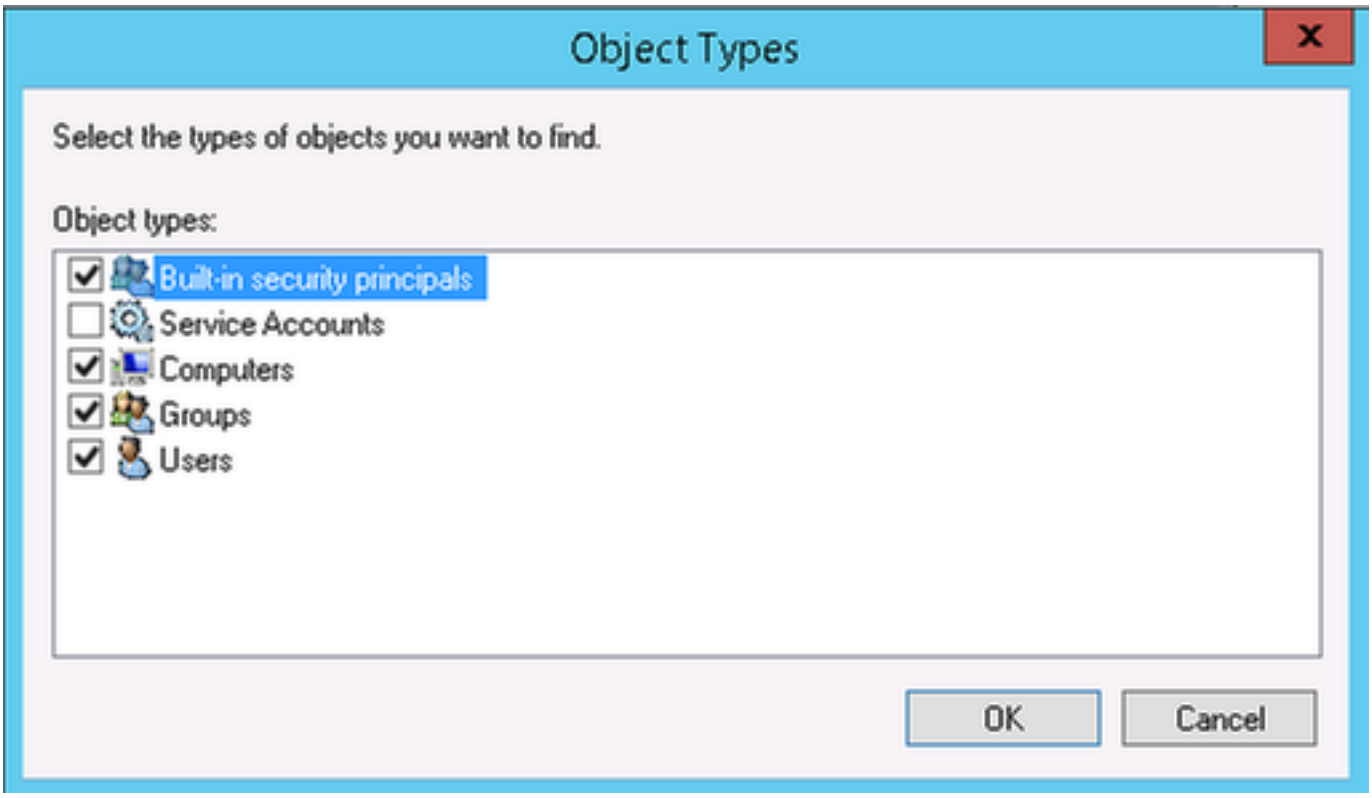
2. Choisissez l'**onglet Sécurité** et cliquez sur Add :



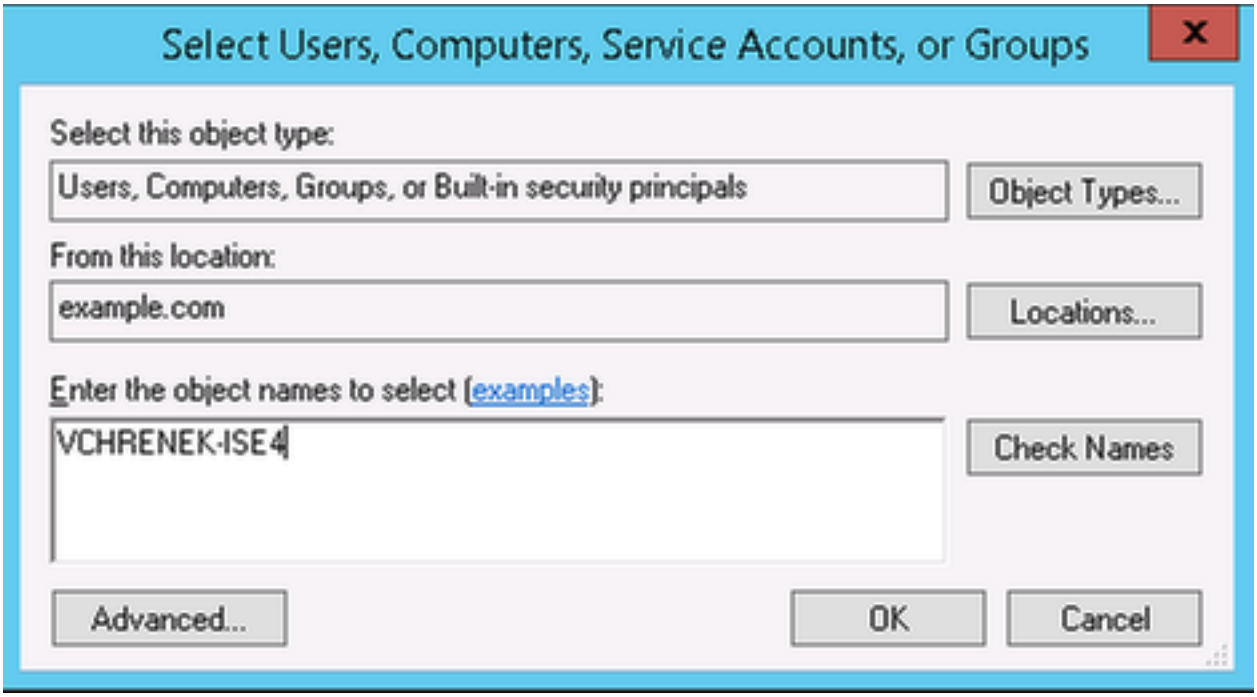
3. **Types d'objet** choisis :



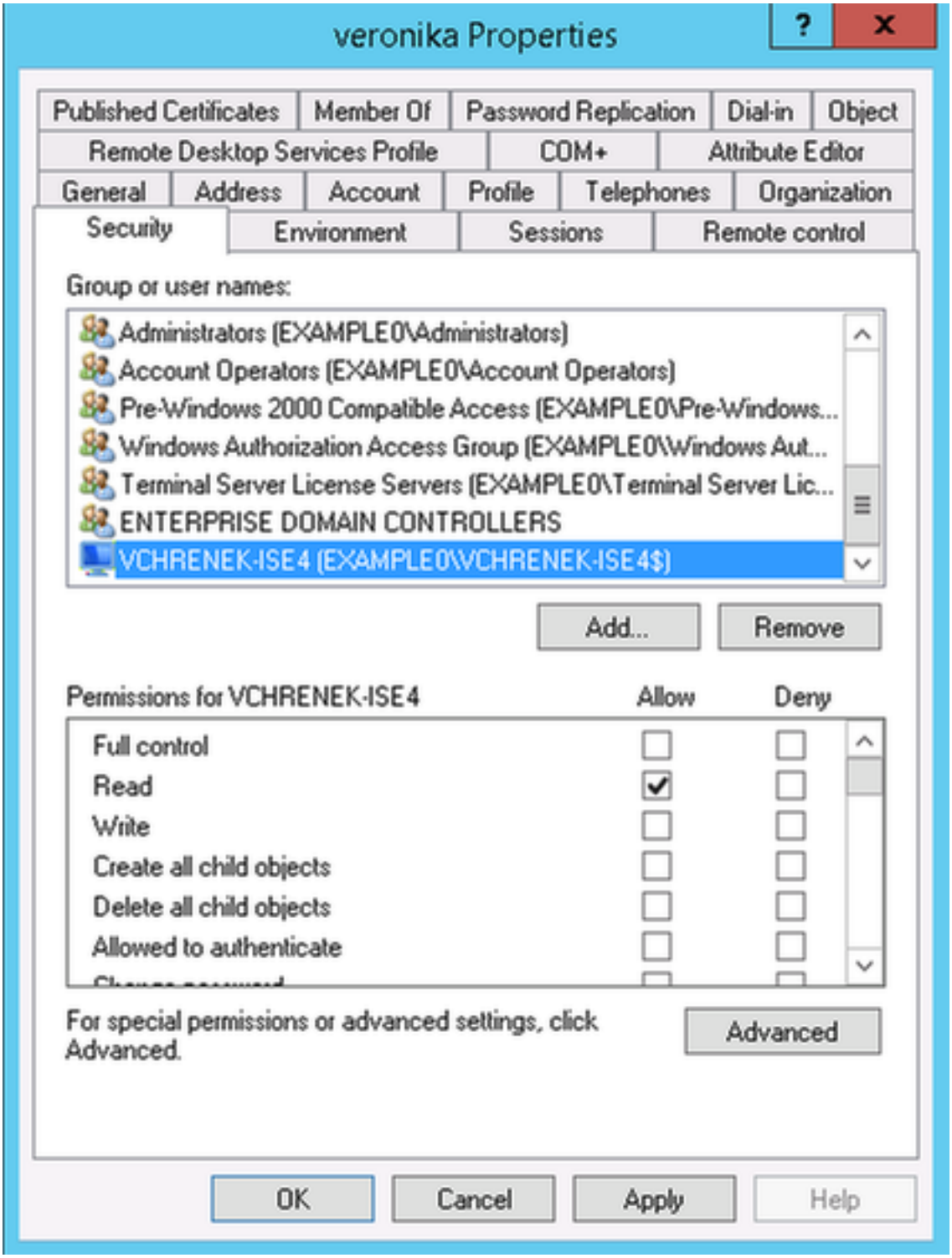
4. **Les ordinateurs** choisis et cliquent sur OK :



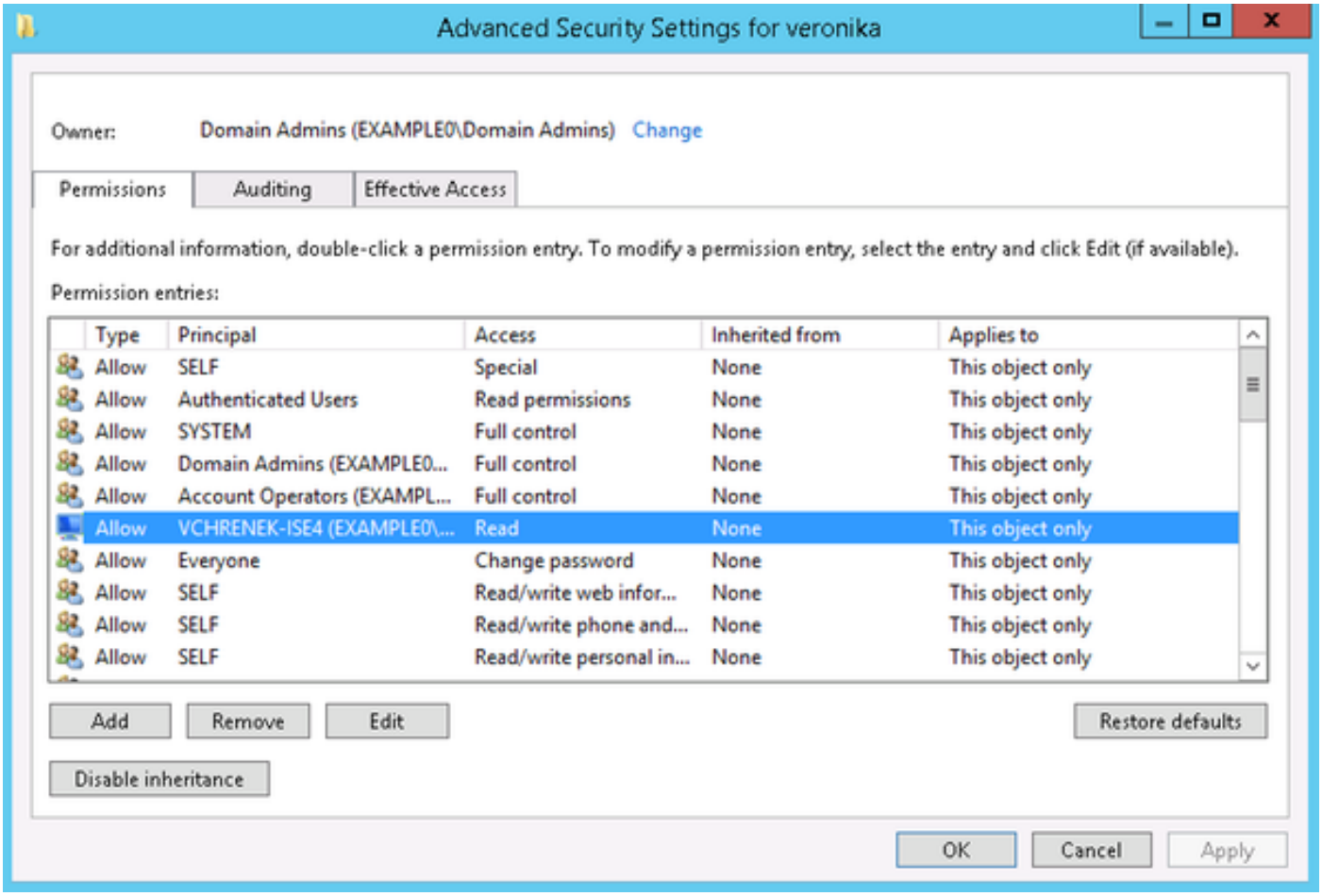
5. Insérez l'adresse Internet ISE (VCHRENEK-ISE4 dans cet exemple) et cliquez sur OK :



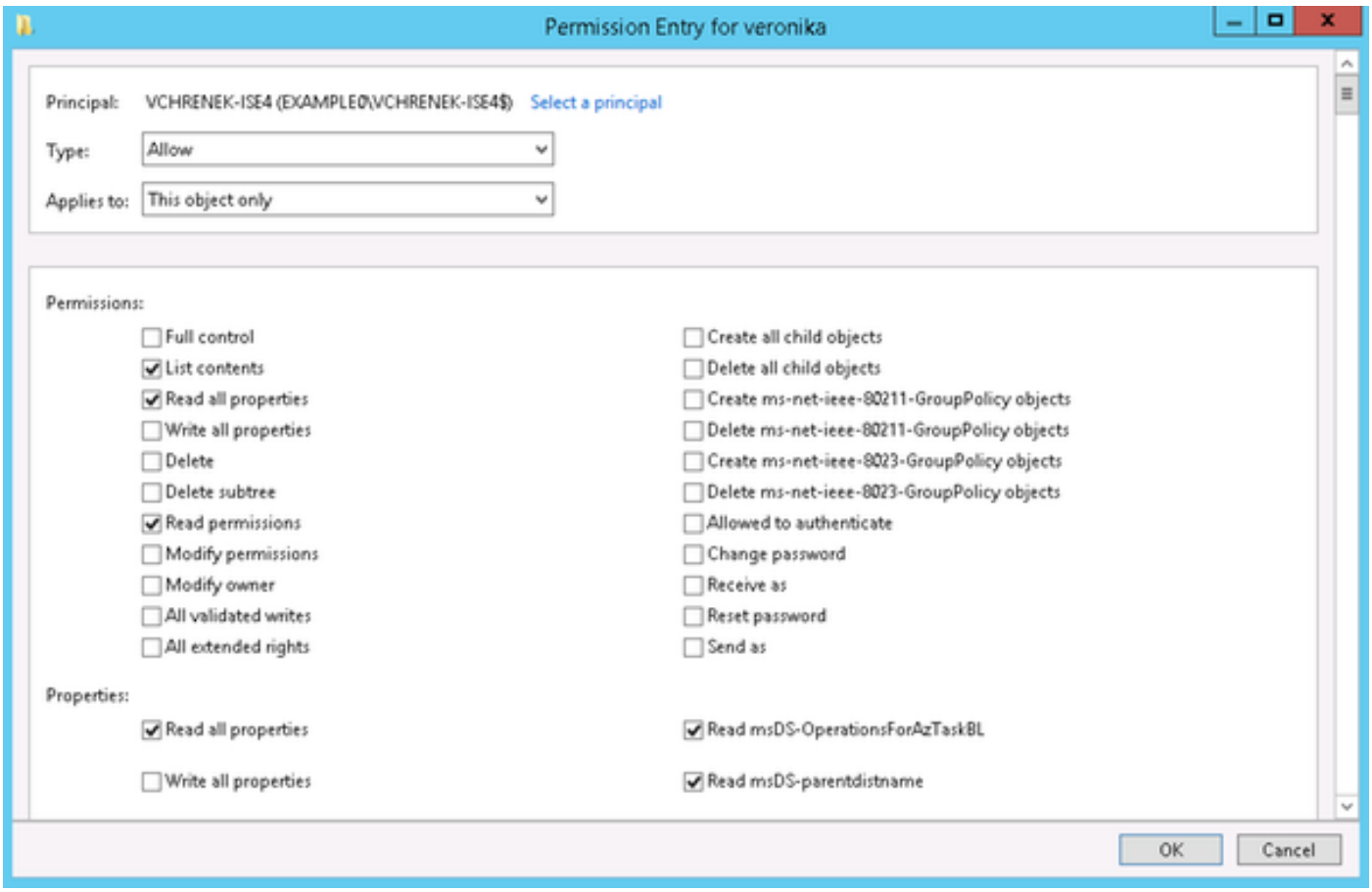
6. Noeud choisi et clic ISE **avancés** :



7. De la sécurité avancée les configurations sélectionnent le compte d'ordinateur ISE et cliquent sur Edit :

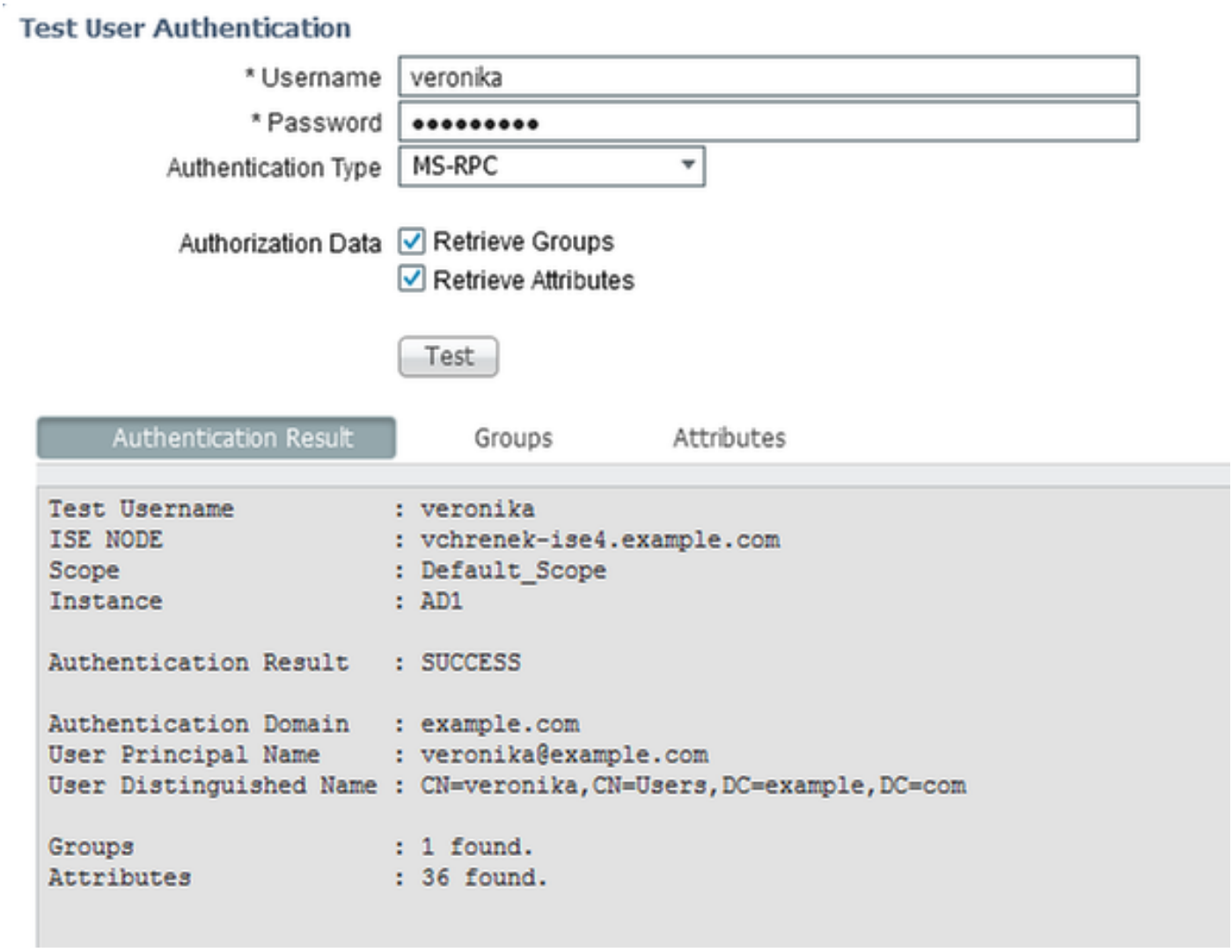


8. Fournissez ces autorisations au compte d'ordinateur ISE et cliquez sur OK :



Après que ces modifications, des groupes d'AD devraient n'être récupérées sans aucune question

:



Ceci doit être exécuté pour tous les utilisateurs et des changements devraient être répliqués vers tous les contrôleurs de domaine du domaine.