

# Correggere il problema di recupero del gruppo di Active Directory ERROR\_TOKEN\_GROUPS\_INSufficient\_PERMISSIONS su Identity Services Engine

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Problema](#)

[Soluzione](#)

## Introduzione

In questo documento viene descritto come risolvere il problema relativo al recupero del gruppo di Active Directory (AD) durante l'autenticazione, mentre l'errore viene visualizzato nei log attivi:

ERROR\_TOKEN\_GROUPS\_INSUFFICIENT\_PERMISSIONS

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Identity Services Engine
- Microsoft Active Directory

### Componenti usati

Il documento può essere consultato per tutte le versioni software di Identity Services Engine (ISE).

## Problema

Il problema è che l'account utente utilizzato per aggiungere ISE ad AD non dispone dei privilegi corretti per ottenere tokenGroups. Ciò non si verifica se per aggiungere ISE ad AD è stato utilizzato l'account Domain Admin. Per risolvere il problema, aggiungere uno o più nodi ISE all'account utente e fornire le autorizzazioni ai nodi ISE:

- Contenuto elenco
- Leggi tutte le proprietà

- Autorizzazioni di lettura

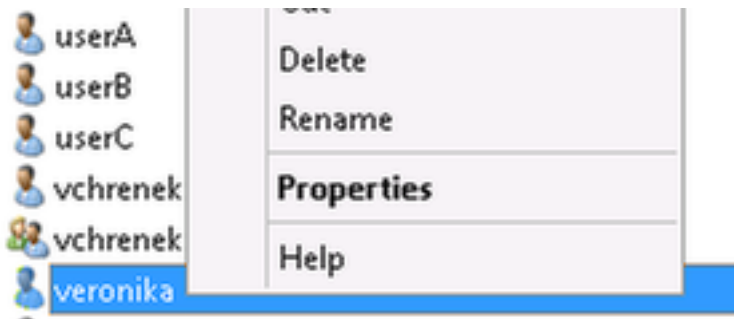
Questo problema si verifica, anche se le autorizzazioni per l'utente sembrano essere corrette (verificare rispetto a [ISE 1.3 AD Authentication Fail with Error: "Privilegio insufficiente per recuperare i gruppi di token"](#)). Tali debug sono riportati in ad-agent.log:

```
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
```

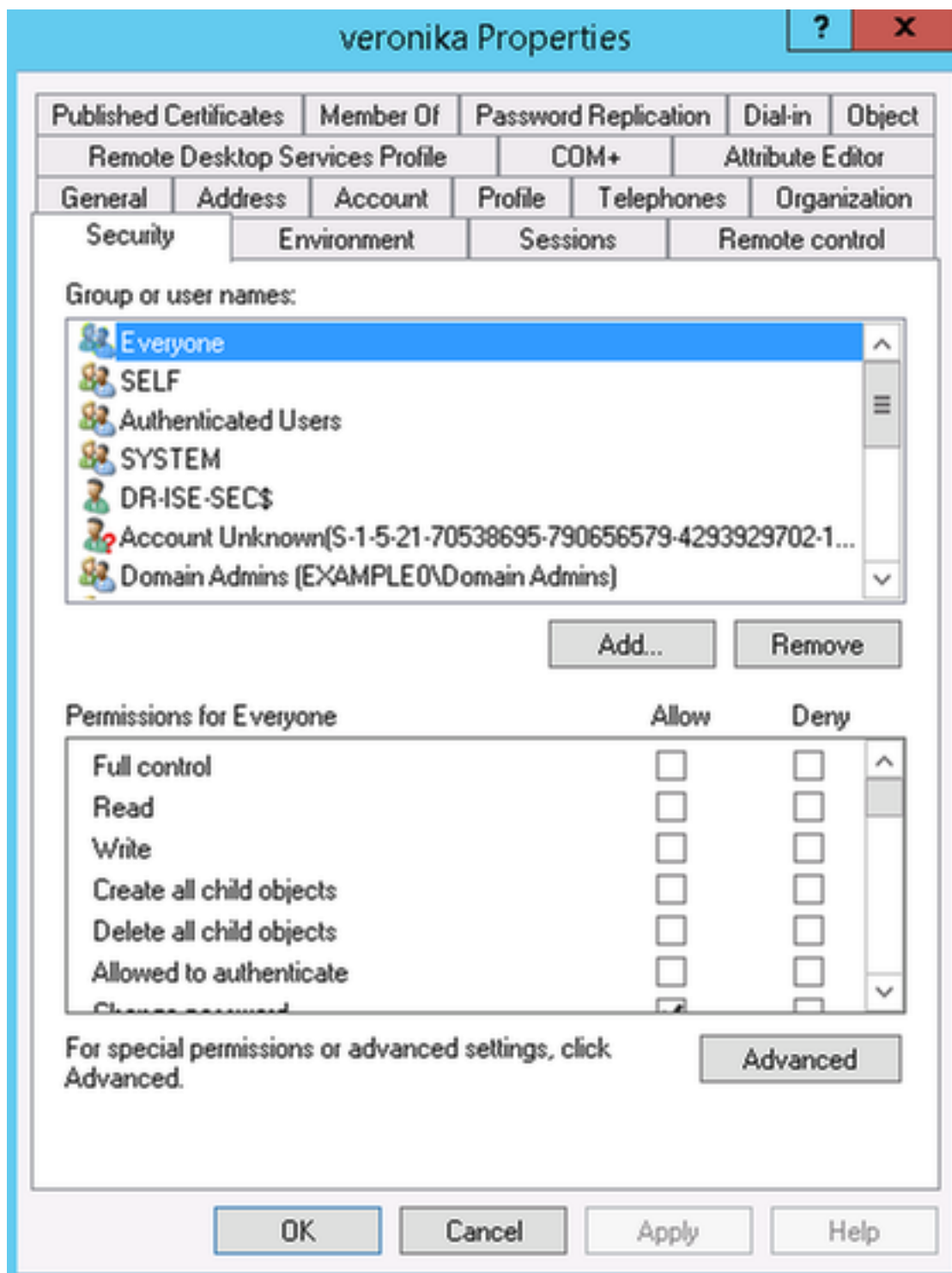
## Soluzione

Per fornire le autorizzazioni necessarie per l'account utente, effettuare le seguenti operazioni:

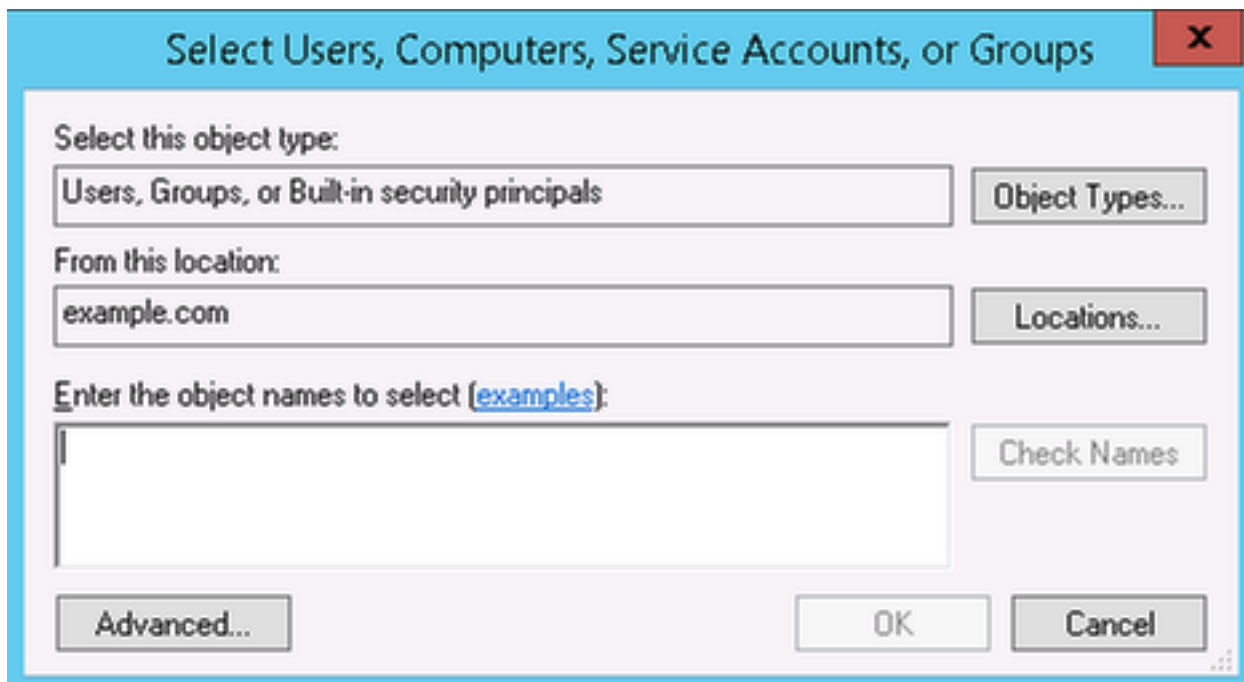
1. in Active Directory passare a **Proprietà** per l'account utente AD:



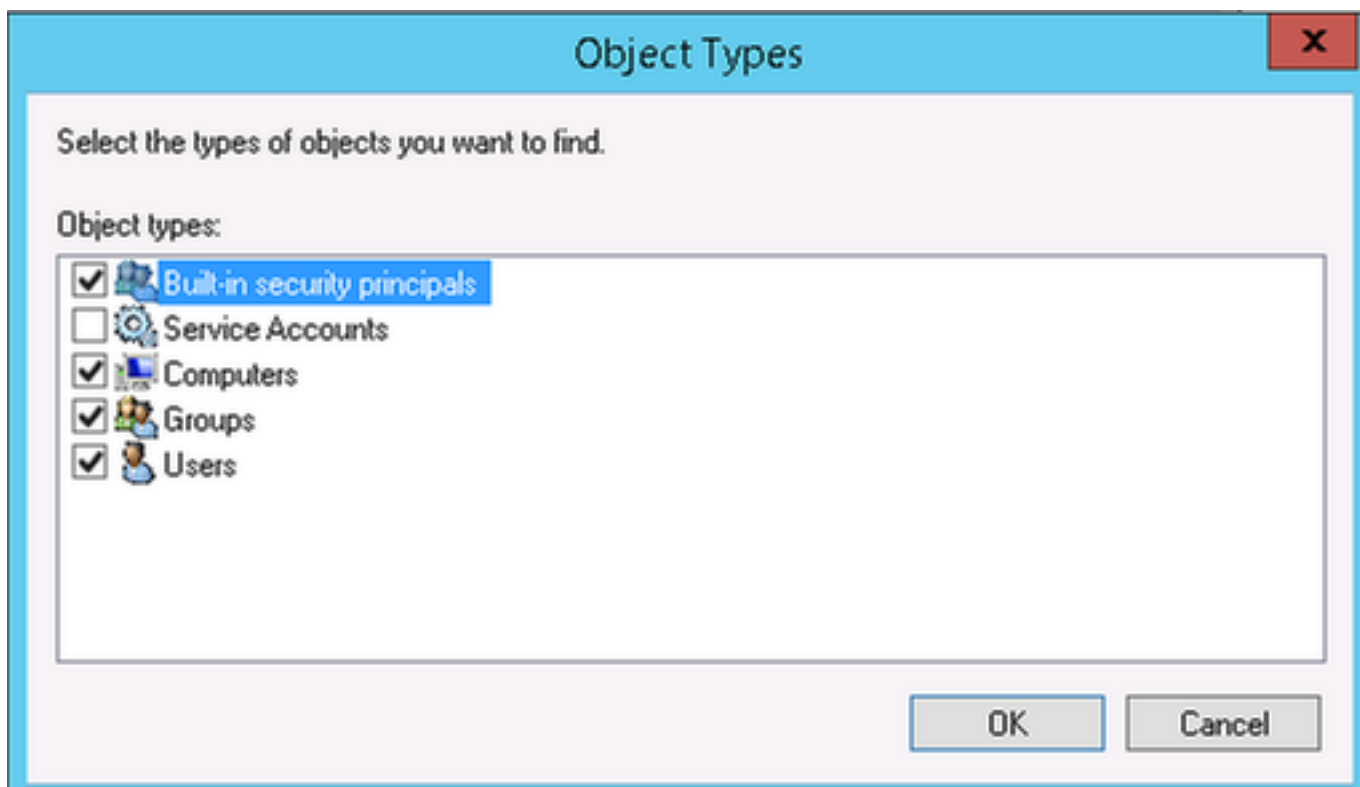
2. Scegliere la scheda **Protezione** e fare clic su **Aggiungi**:



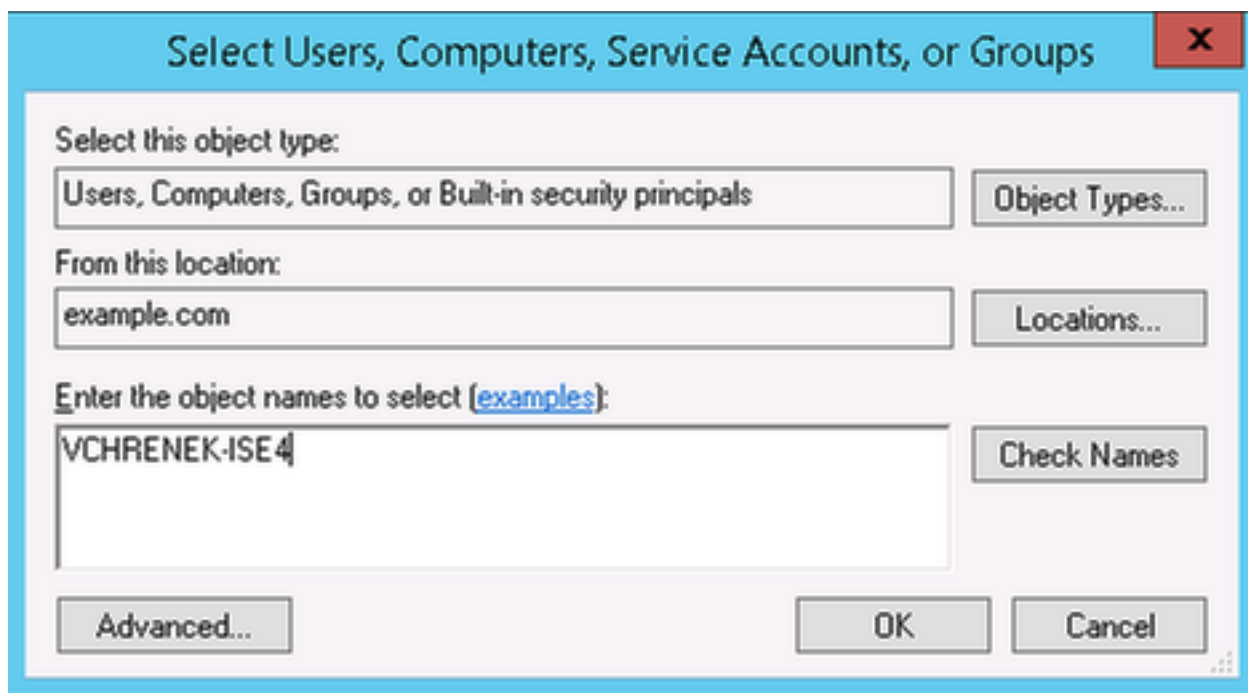
3. Selezionare i tipi di oggetto:



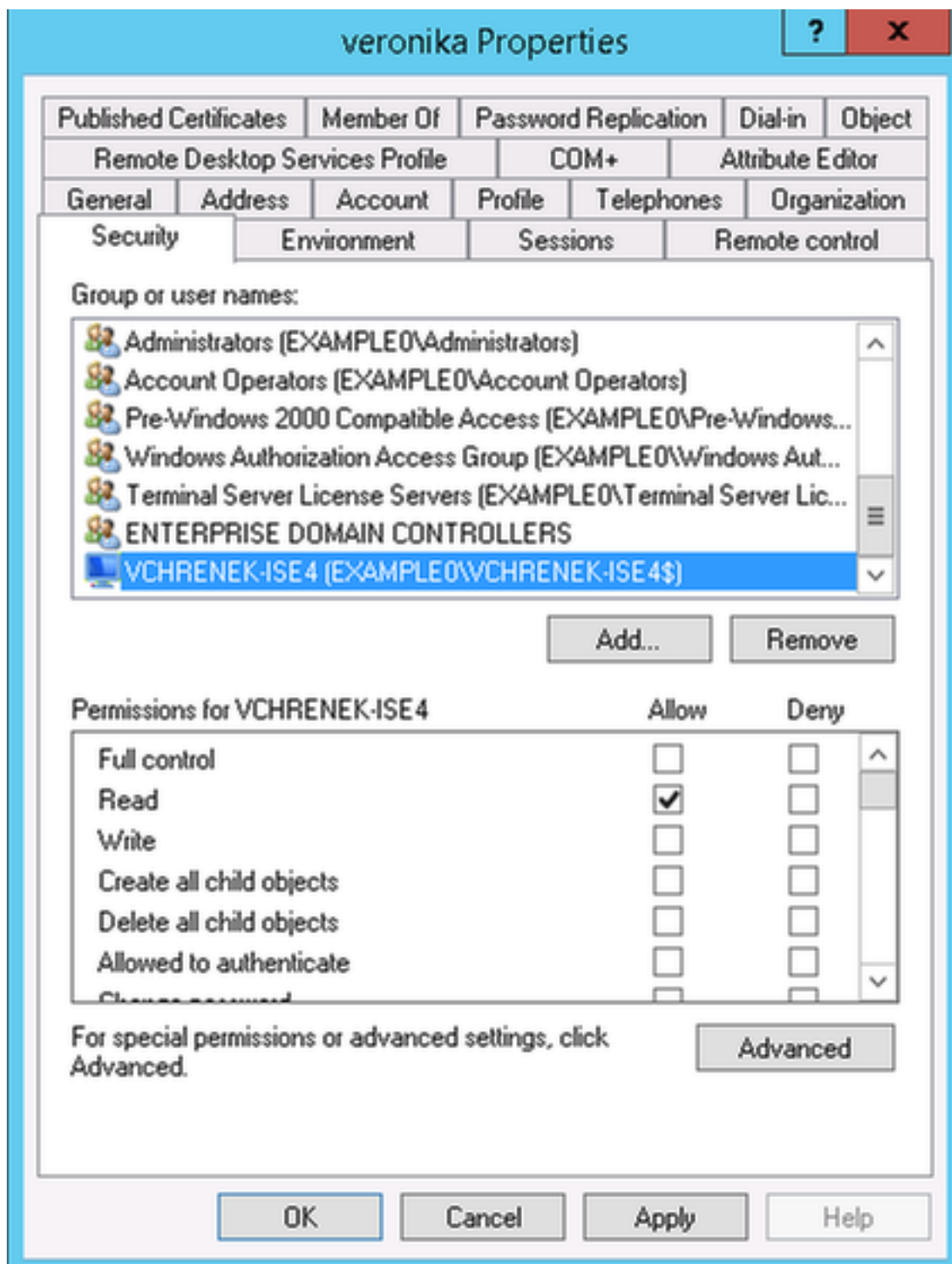
4. Selezionare **Computer** e fare clic su **OK**:



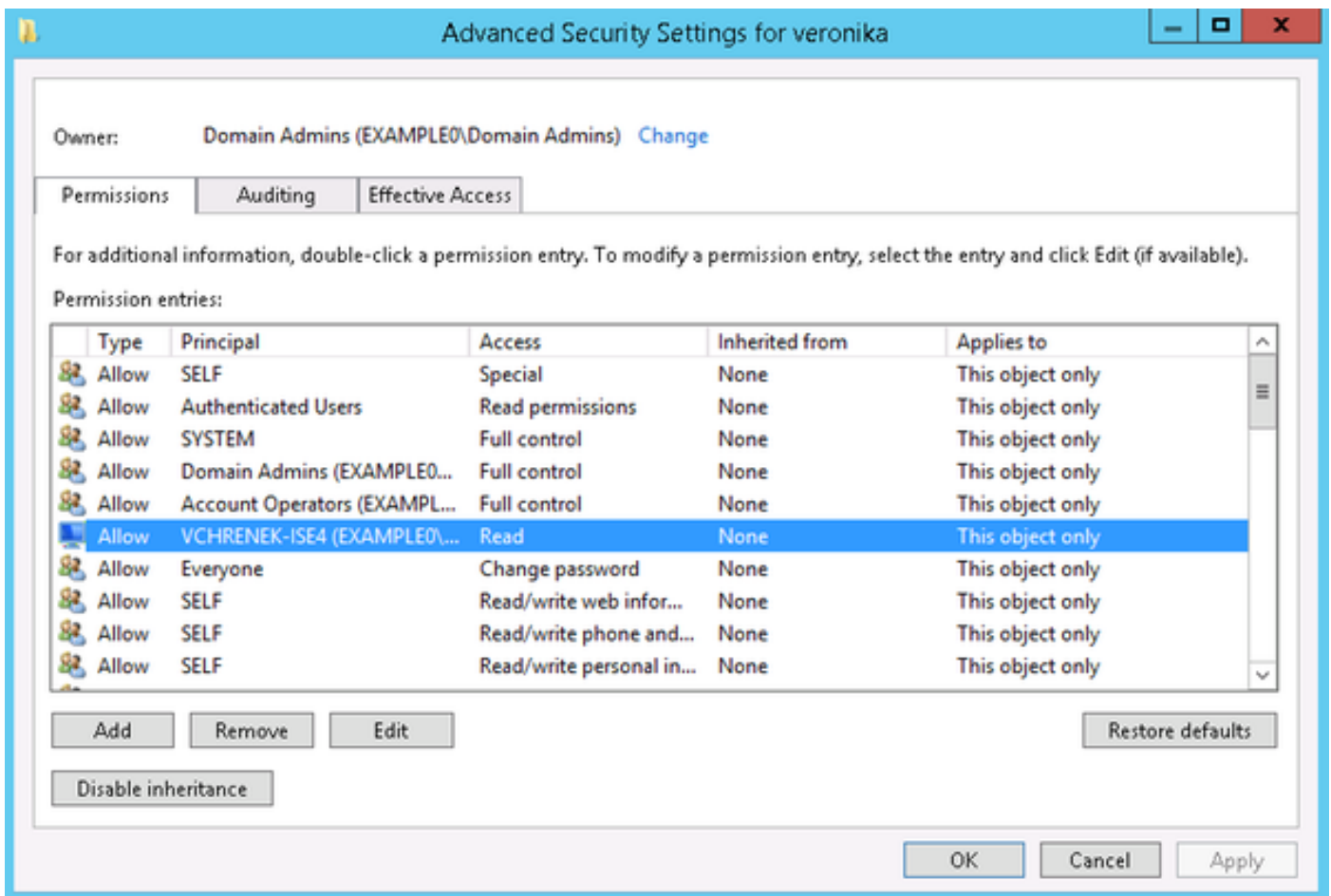
5. Inserire il nome host ISE (VCHRENEK-ISE4 nell'esempio) e fare clic su **OK**:



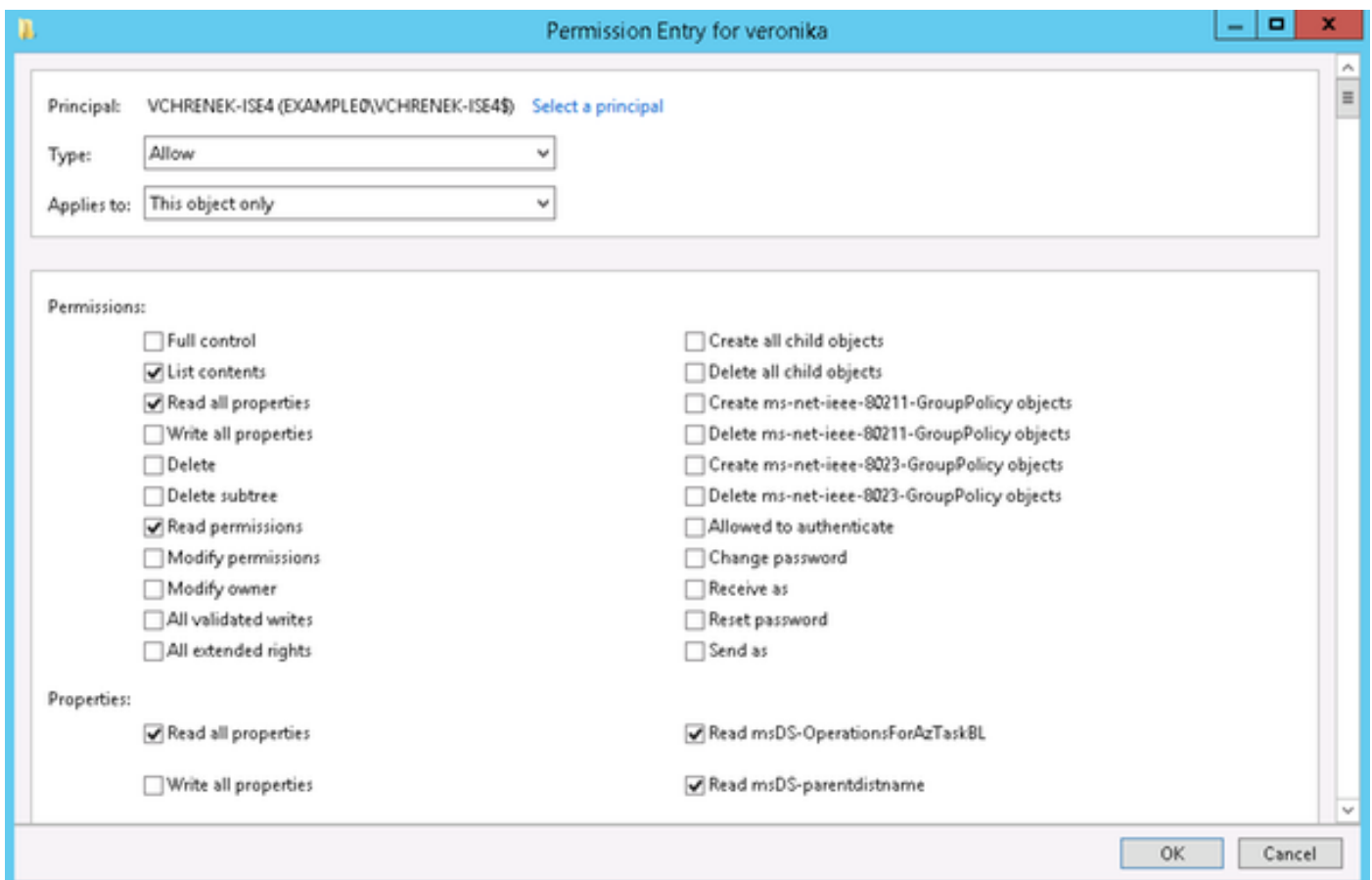
6. Selezionare il nodo ISE e fare clic su **Advanced**:



7. Da Advanced Security Settings selezionare ISE machine account e fare clic su **Edit**:



8. Fornire queste autorizzazioni all'account del computer ISE e fare clic su **OK**:



Dopo queste modifiche, i gruppi AD devono essere recuperati senza problemi:

## 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.	

Questa operazione deve essere eseguita per tutti gli utenti e le modifiche devono essere replicate in tutti i controller di dominio del dominio.