

Fix Active Directory-groepsophalen FOUT_TOKEN_GROUPS_INSUFFICIENT_PER MISSIONS op Identity Services Engine

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Probleem](#)

[Oplossing](#)

Inleiding

Dit document beschrijft hoe u het probleem met het ophalen van een AD-groep (Active Directory) tijdens verificatie kunt oplossen, terwijl deze fout in live logs wordt gezien:

ERROR_TOKEN_GROUPS_INSUFFICIENT_PERMISSIONS

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Identity Services Engine
- Microsoft Active Directory

Gebruikte componenten

Dit document is niet beperkt tot specifieke softwareversies van Identity Services Engine (ISE).

Probleem

Het probleem is dat gebruikersaccount dat wordt gebruikt om zich aan te sluiten bij ISE in AD geen juiste rechten heeft om symbolische groepen te krijgen. Dit zou niet gebeuren als de Domain Admin account werd gebruikt om zich bij ISE aan AD aan te sluiten. Om dit probleem te repareren, moet u ISE-knooppunt(s) aan de gebruikersaccount toevoegen en de rechten aan ISE-knooppunt(s) geven:

- Lijstinhoud
- Alle eigenschappen lezen
- Lezen van rechten

Dit probleem wordt gezien, ook al lijkt de permissies voor gebruiker correct (controle tegen [ISE 1.3 AD Authenticaties Falt met fout: "Onvoldoende voorrecht om Token Groepen te proeven"](#)). Deze diepten worden gezien in ad-agent.log:

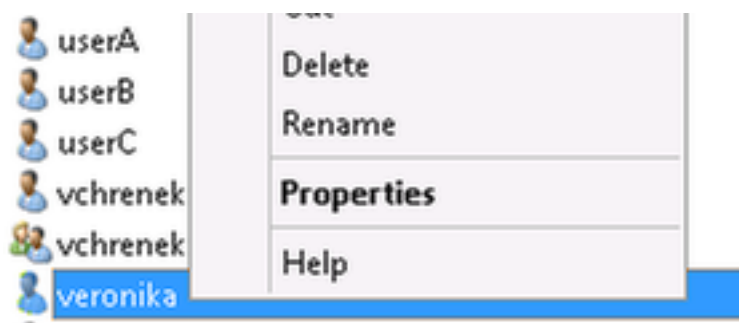
```
28/08/2016 17:23:35,VERBOSE,140693934700288,Error code: 60173 (symbol: LW_ERROR_TOKEN_GROUPS_INSUFFICIENT_PERMISSIONS),lsass/server/auth-providers/ad-open-provider/provider-main.c:7409
```

```
28/08/2016 17:23:35,VERBOSE,140693934700288,Error code: 60173 (symbol: LW_ERROR_TOKEN_GROUPS_INSUFFICIENT_PERMISSIONS),lsass/server/api/api2.c:2572
```

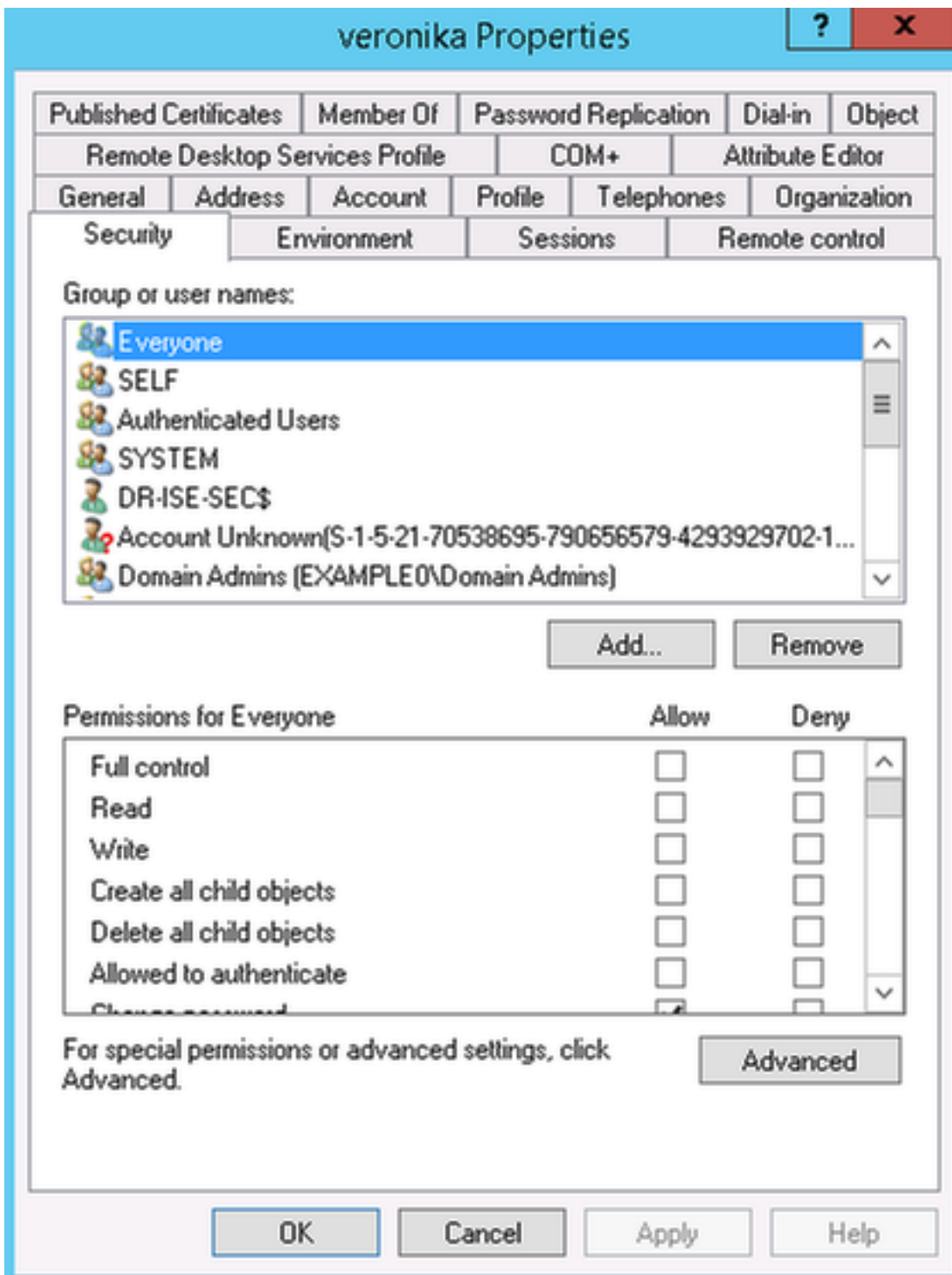
Oplossing

Om de vereiste permissies voor gebruikersaccount te geven, voert u deze stappen uit:

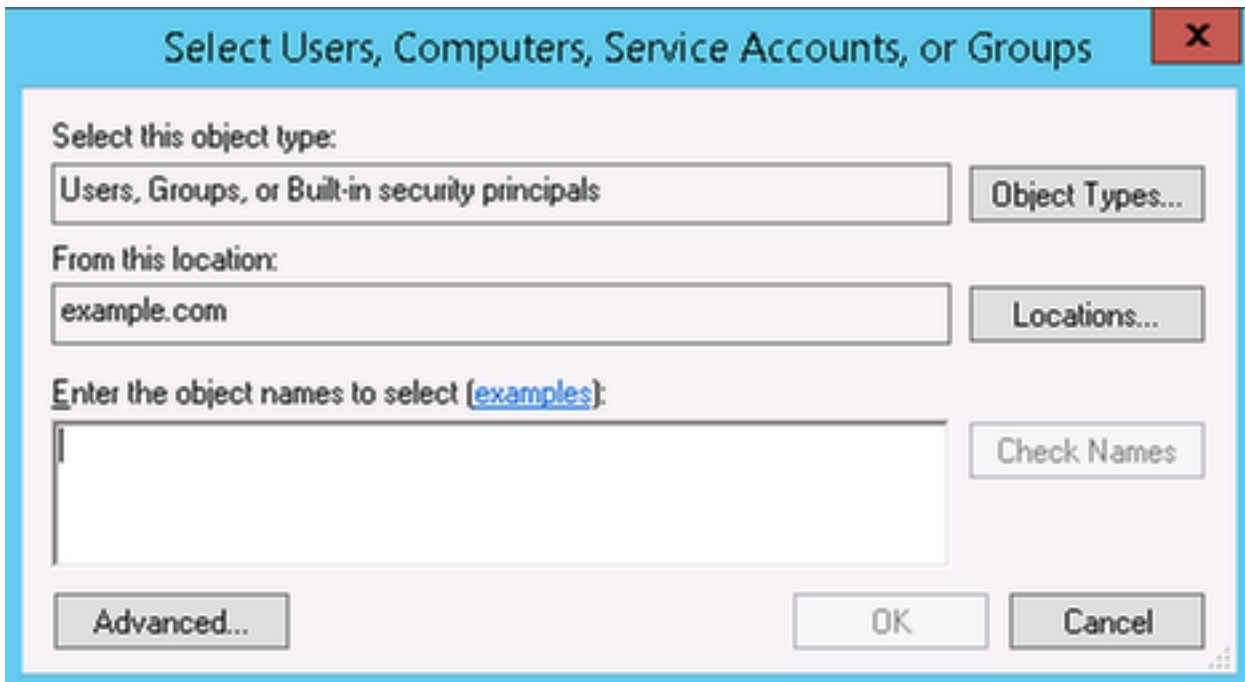
1. navigeer op AD naar **Properties** voor AD user account:



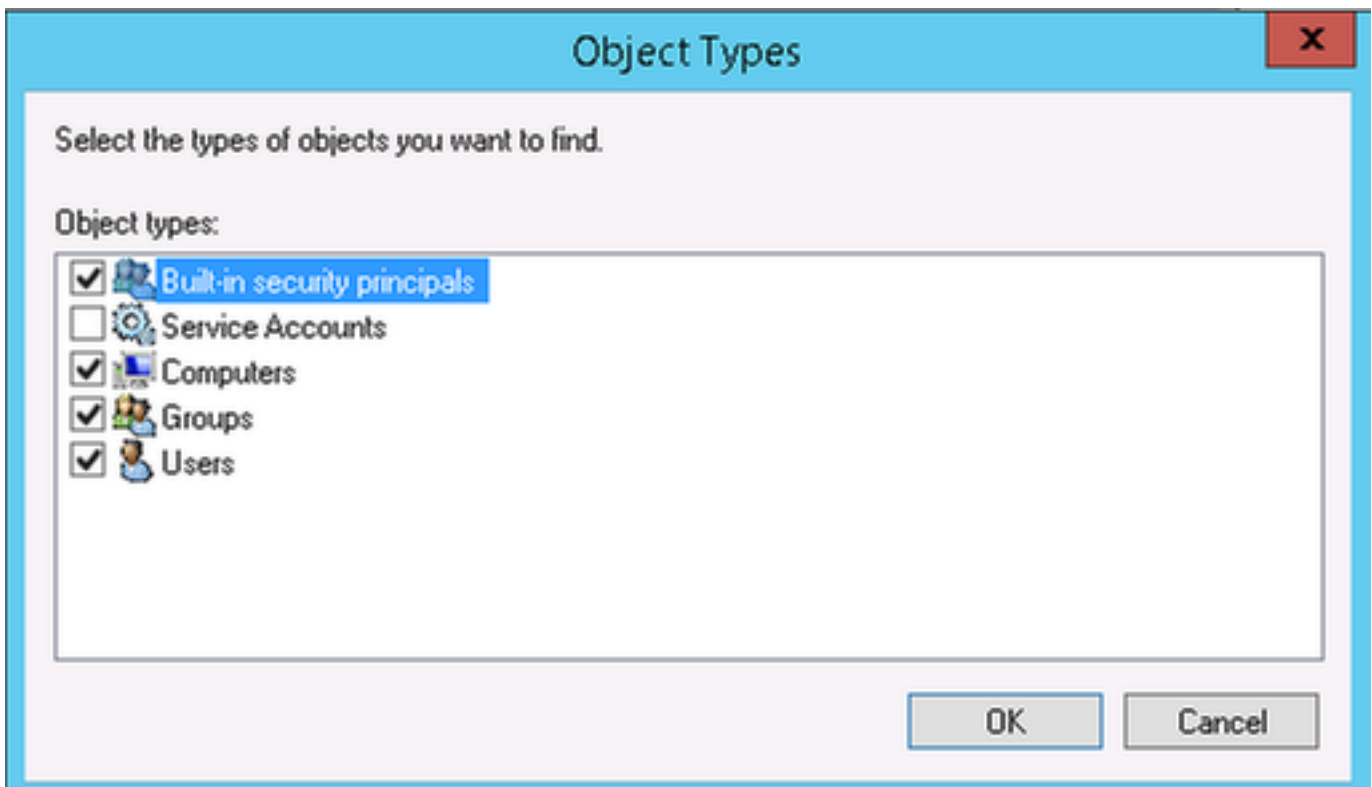
2. Kies het tabblad **Beveiliging** en klik op **Toevoegen**:



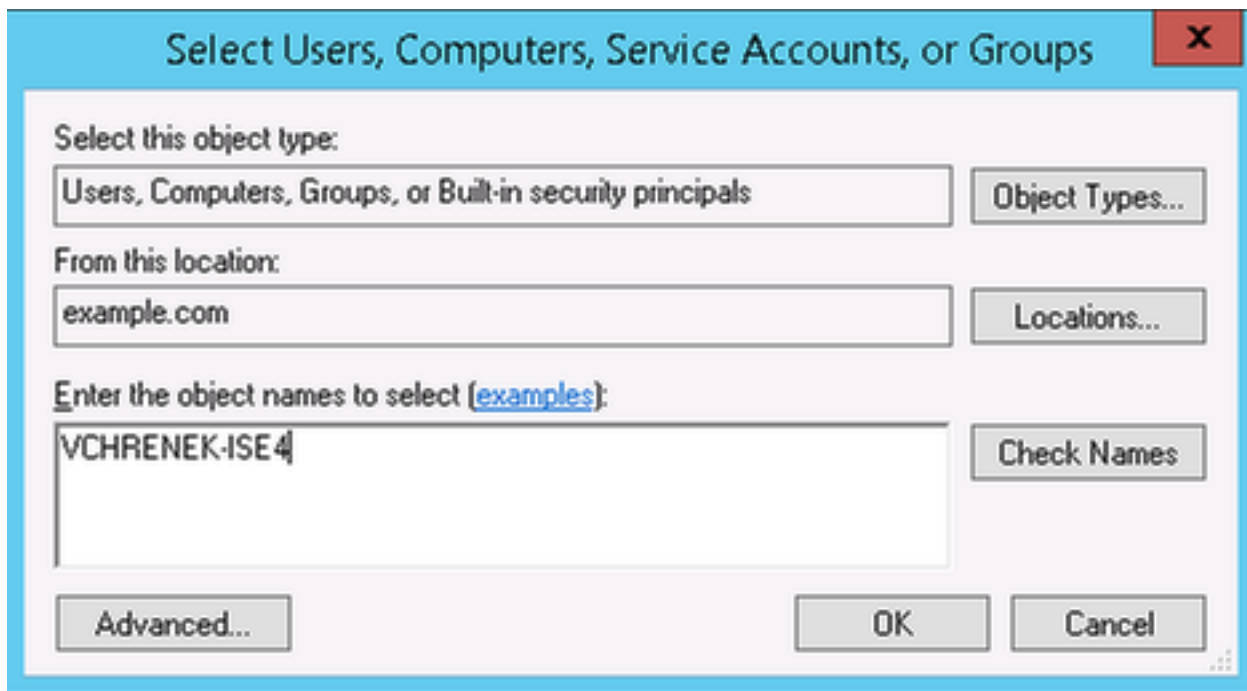
3. Selecteer Objecttypen:



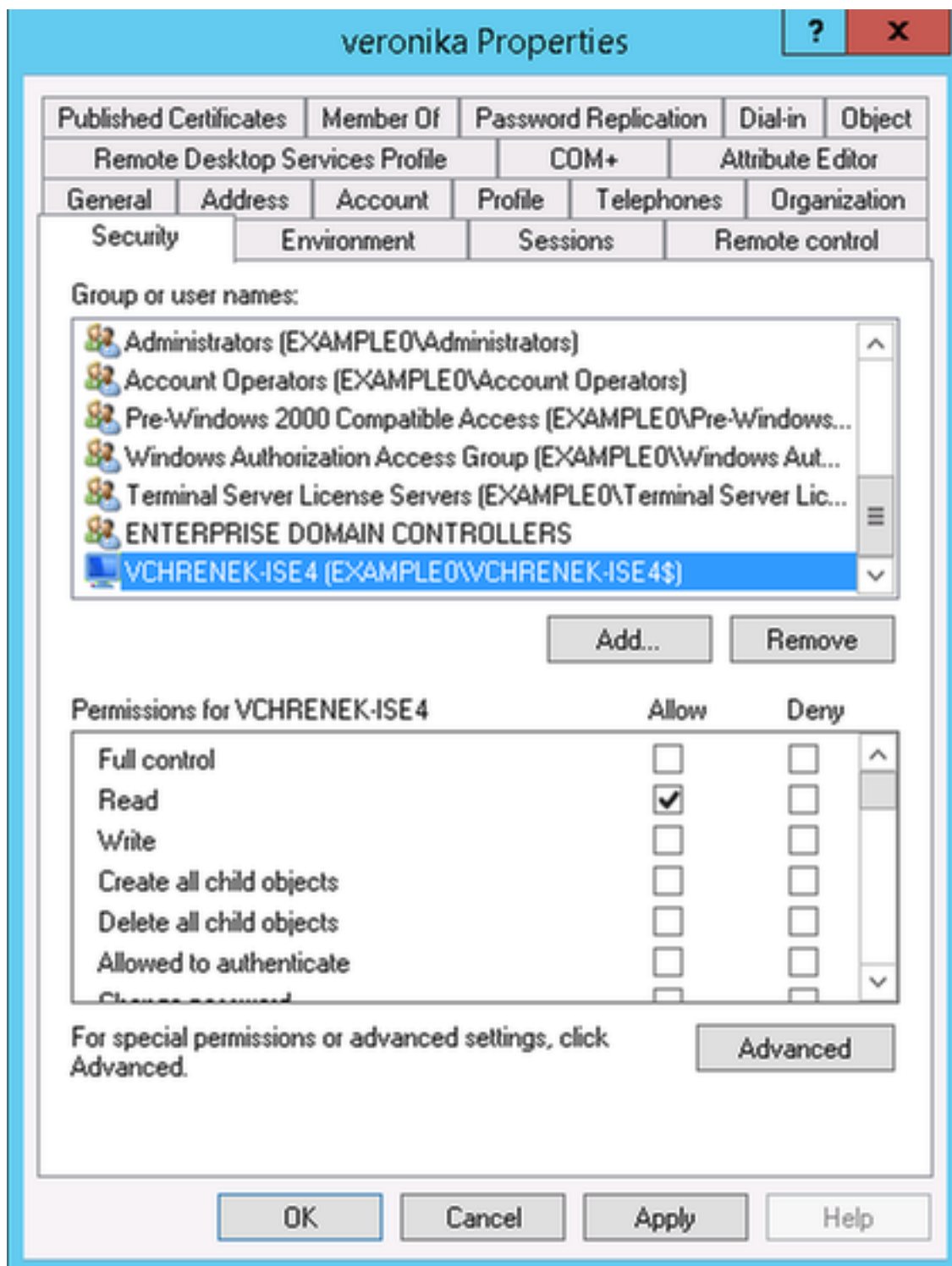
4. Selecteer **Computers** en klik op **OK**:



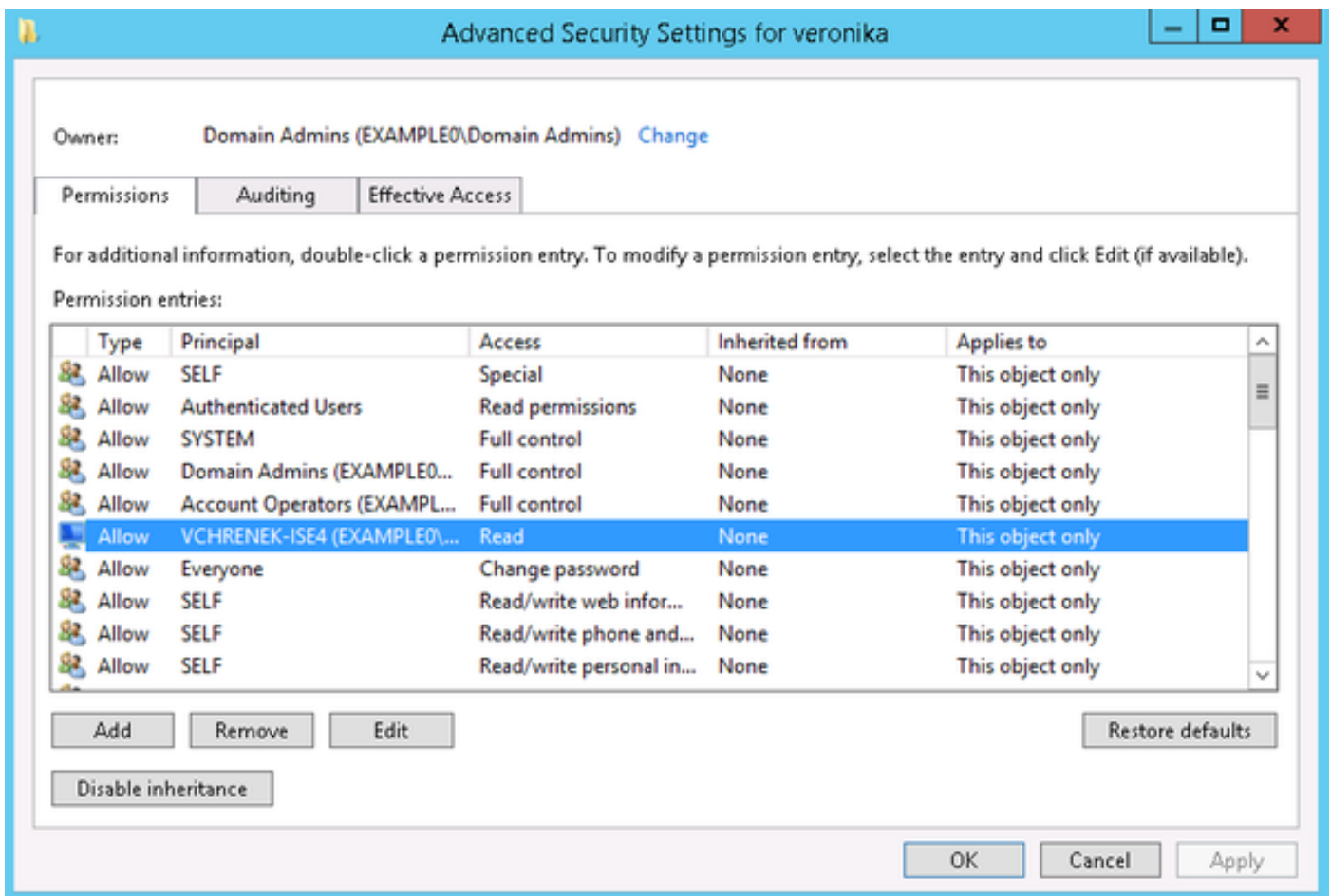
5. Typ ISE-hostname (VCHRENEK-ISE4 in dit voorbeeld) en klik op **OK**:



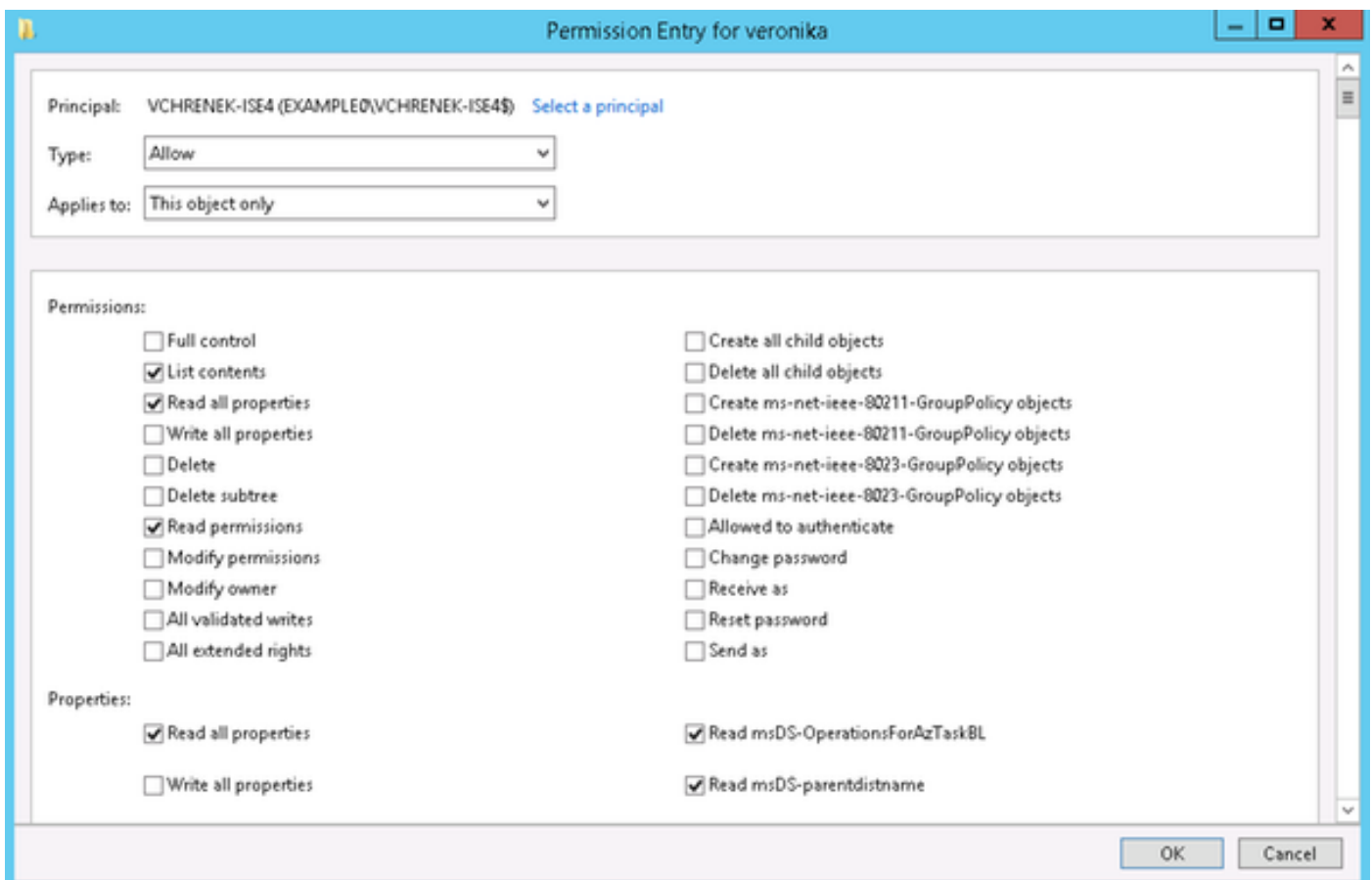
6. Selecteer ISE-knooppunt en klik op **Geavanceerd**:



7. Selecteer ISE-computeraccount met geavanceerde beveiligingsinstellingen en klik op **Bewerken**:



8. Typ die toestemming aan ISE machine account en klik op OK:



Na deze veranderingen moeten AD-groepen worden opgeroepen zonder problemen:

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.	

Dit moet voor alle gebruikers worden uitgevoerd en wijzigingen moeten worden herhaald voor alle Domain Controllers in het domein.