

Identity Services Engine の修正 Active Directory グループ検索問題 ERROR_TOKEN_GROUPS_INSUFFICIENT_PERMISSIONS

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[問題](#)

[解決策](#)

概要

このエラーはライブ ログで見られるがどのように回避策に認証かの中の Active Directory (AD) グループ検索における問題この資料に記述されています、 :

ERROR_TOKEN_GROUPS_INSUFFICIENT_PERMISSIONS

前提条件

要件

次の項目に関する知識が推奨されます。

- Cisco Identity Services Engine
- Microsoft Active Directory

使用するコンポーネント

この資料は Identity Services Engine (ISE) の特定のソフトウェア バージョンに制限 されません。

問題

問題は ISE に AD に加入するのに使用されるユーザアカウントが tokenGroups を得る正しい特権がないことです。これは ISE に AD に加入すればのにドメイン 管理者アカウントが使用された場合起こりません。この問題を解決するために、ユーザアカウントに ISE ノードを追加し、ISE ノードにそれらの権限を提供しなければなりません:

- リスト コンテンツ

- すべてのプロパティを読んで下さい
- 読み取り権限

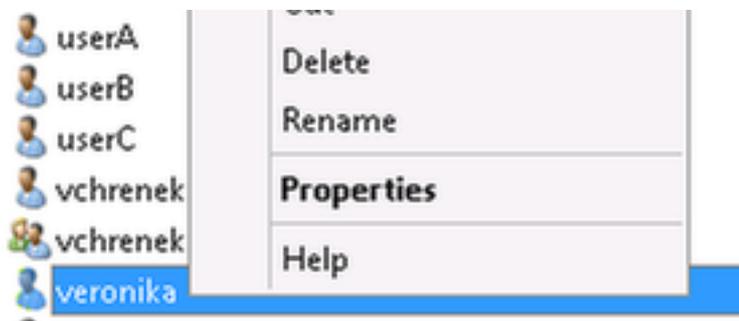
この問題はユーザ向けの権限が正しいようであるのに、見られます ([ISE 1.3 AD 認証](#) に対するチェックは [エラーと失敗します: 「トークングループ」を取出す不十分な特権](#))。それらのデバッグは ad-agent.log で参照されます:

```
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
```

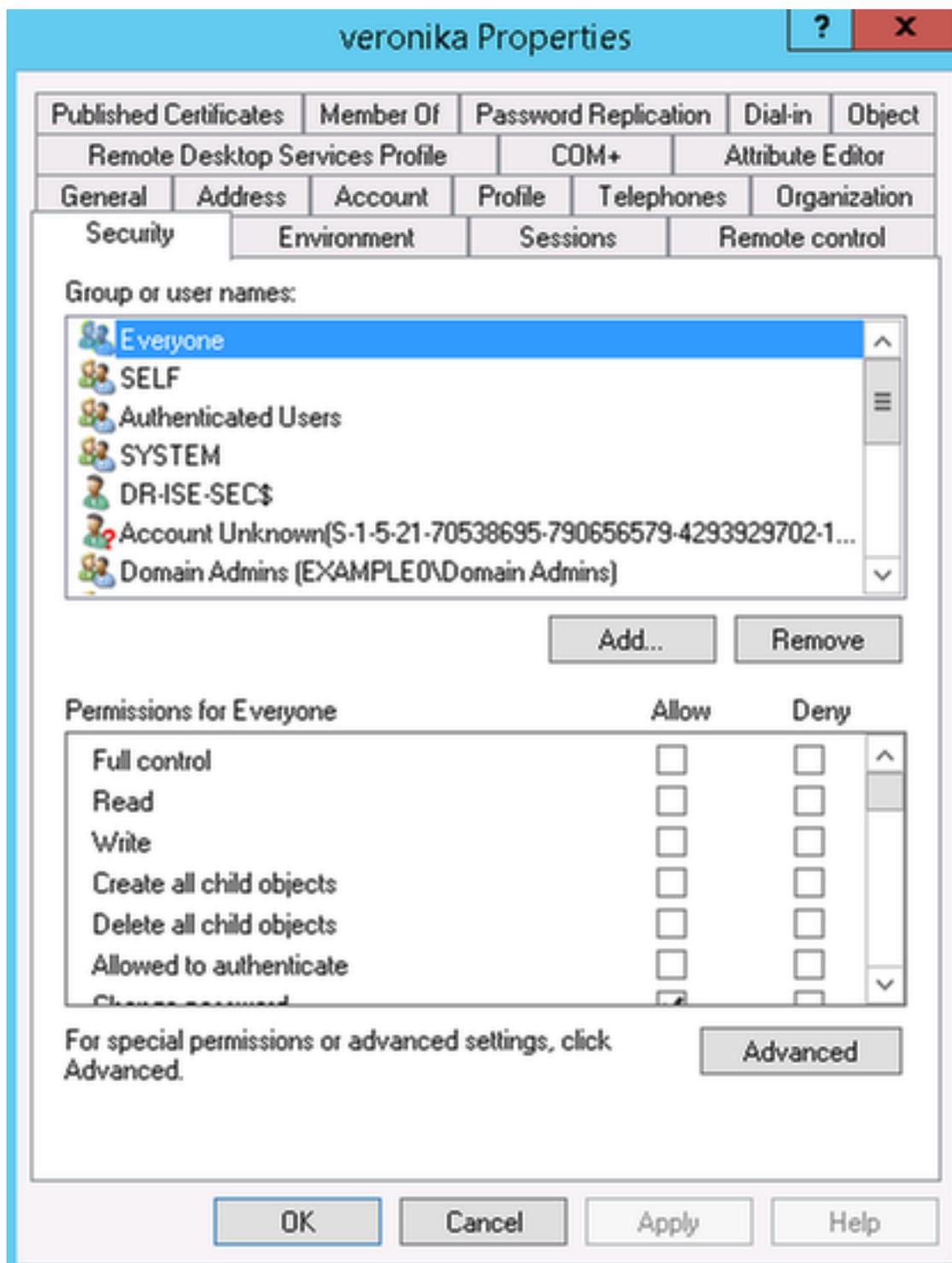
解決策

必要なアクセス許可をユーザアカウントに提供するために、それらのステップを実行して下さい:

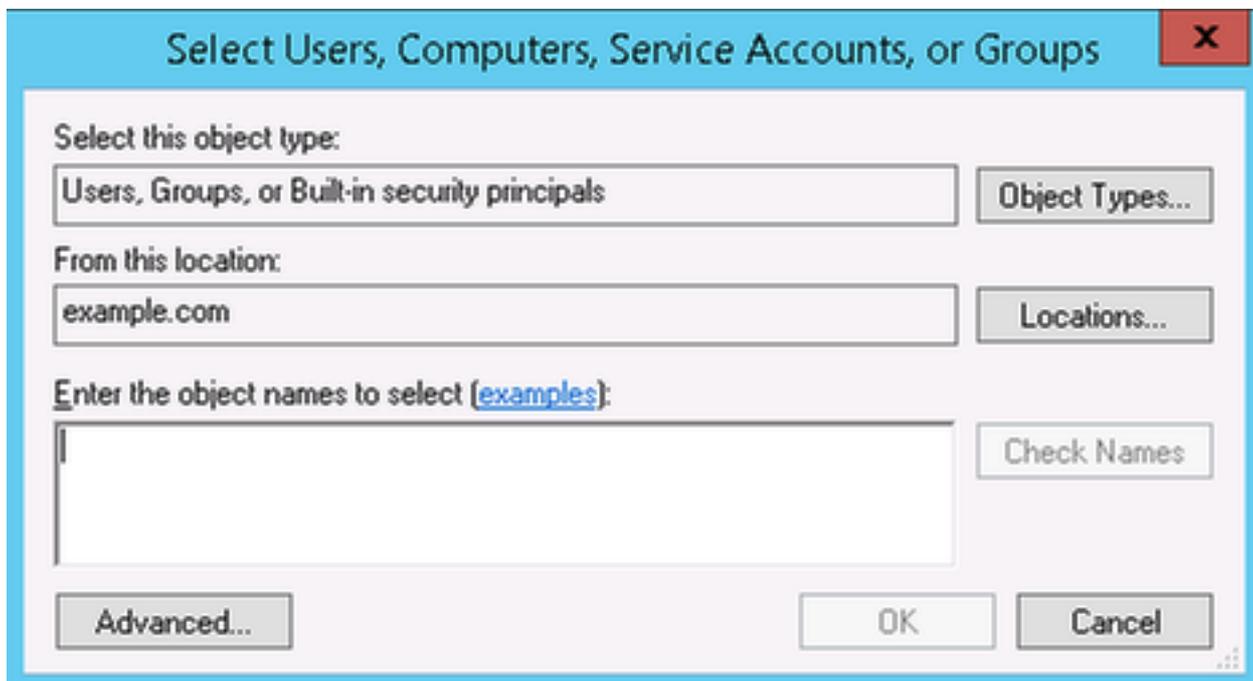
1. AD で AD ユーザアカウントのための **Properties** にナビゲートして下さい:



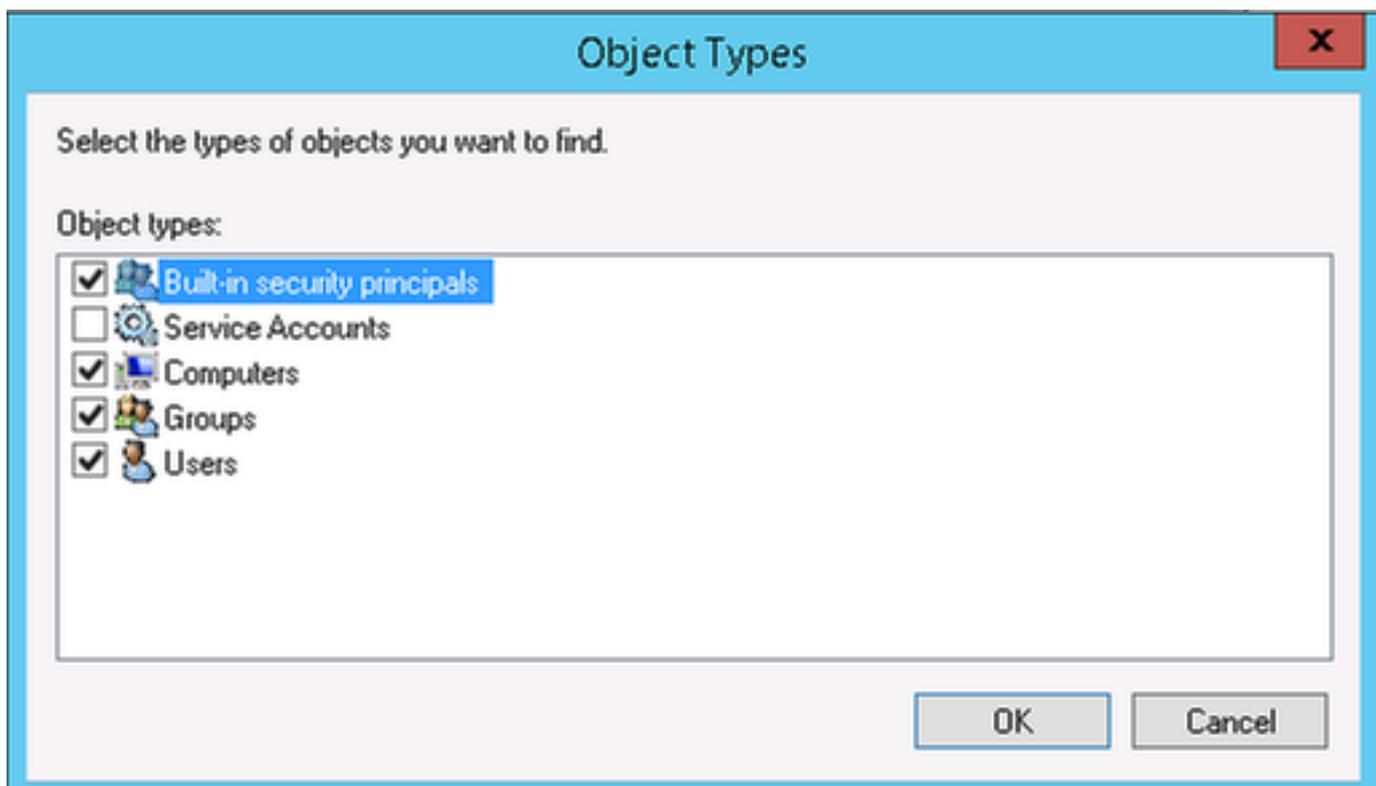
2. タブを『Security』を選択し、『Add』をクリックして下さい:



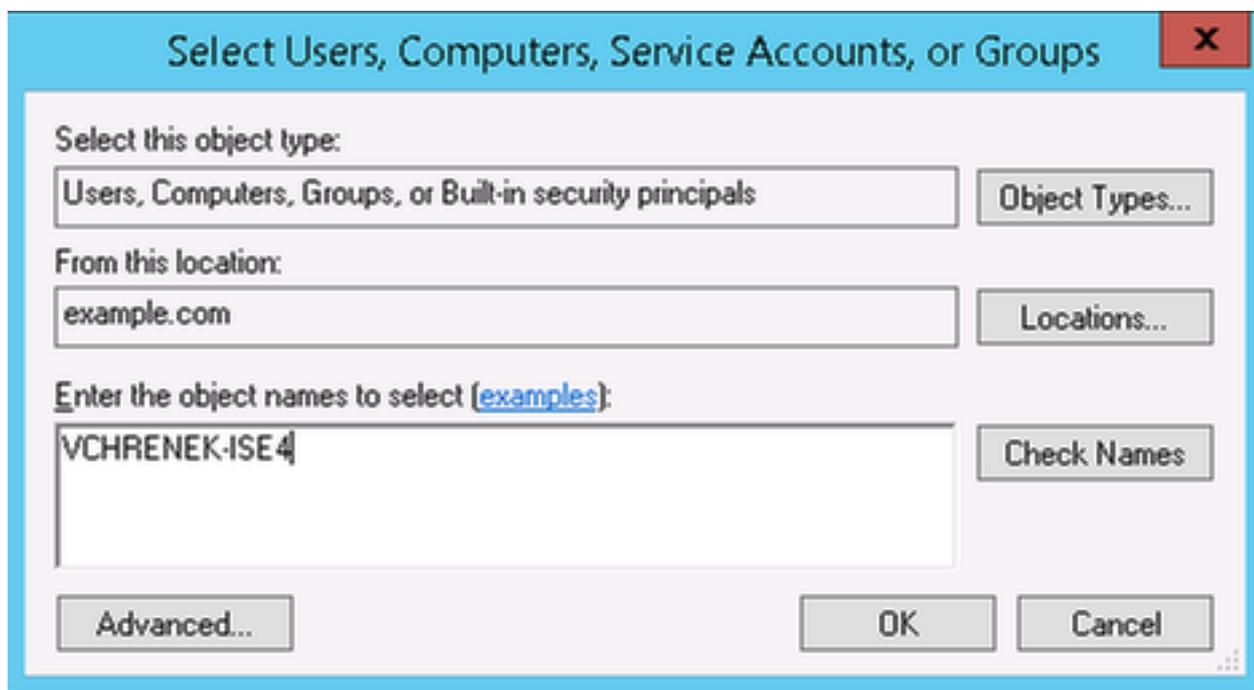
3. オブジェクト タイプを選択して下さい:



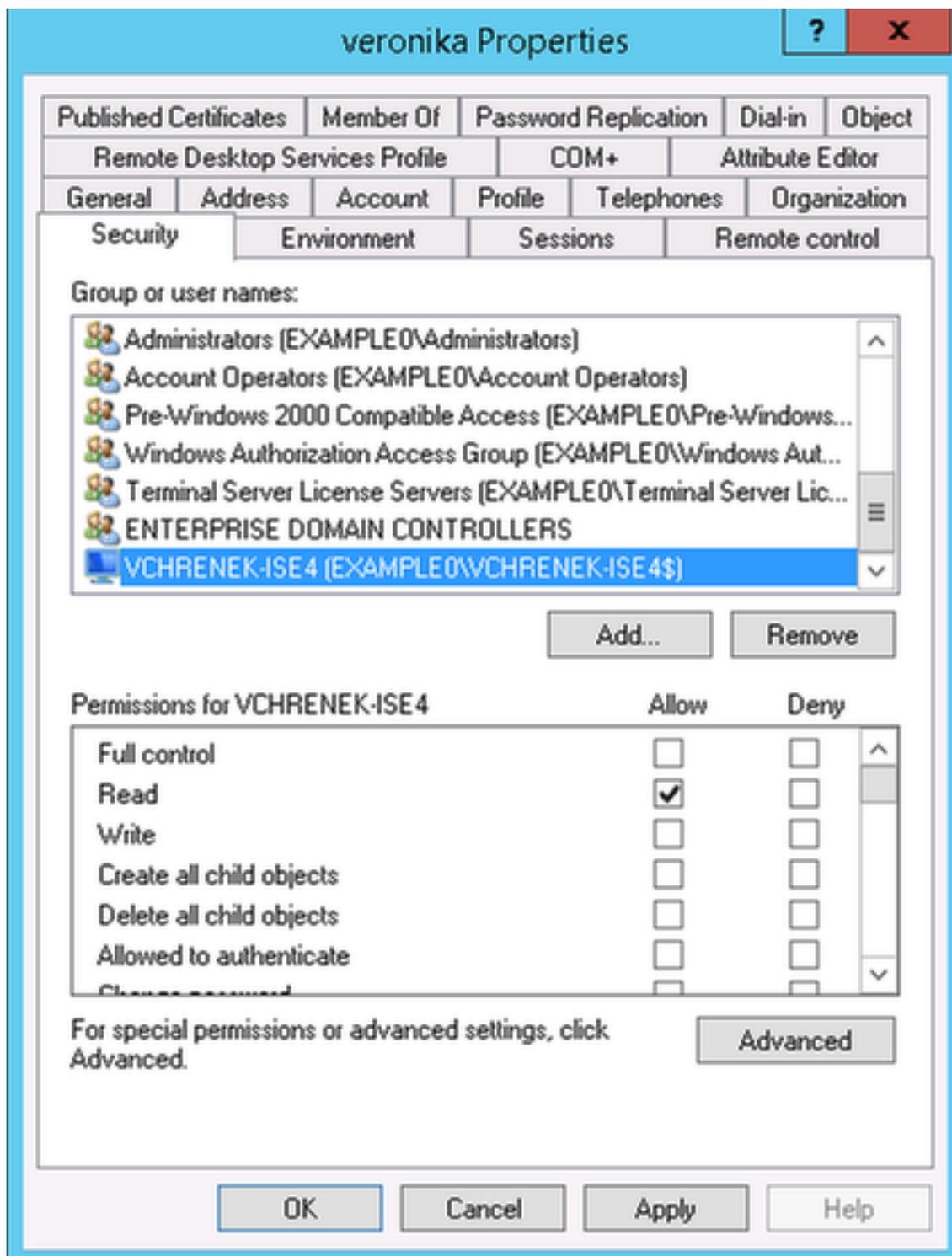
4. コンピュータを選択し、『OK』をクリックして下さい:



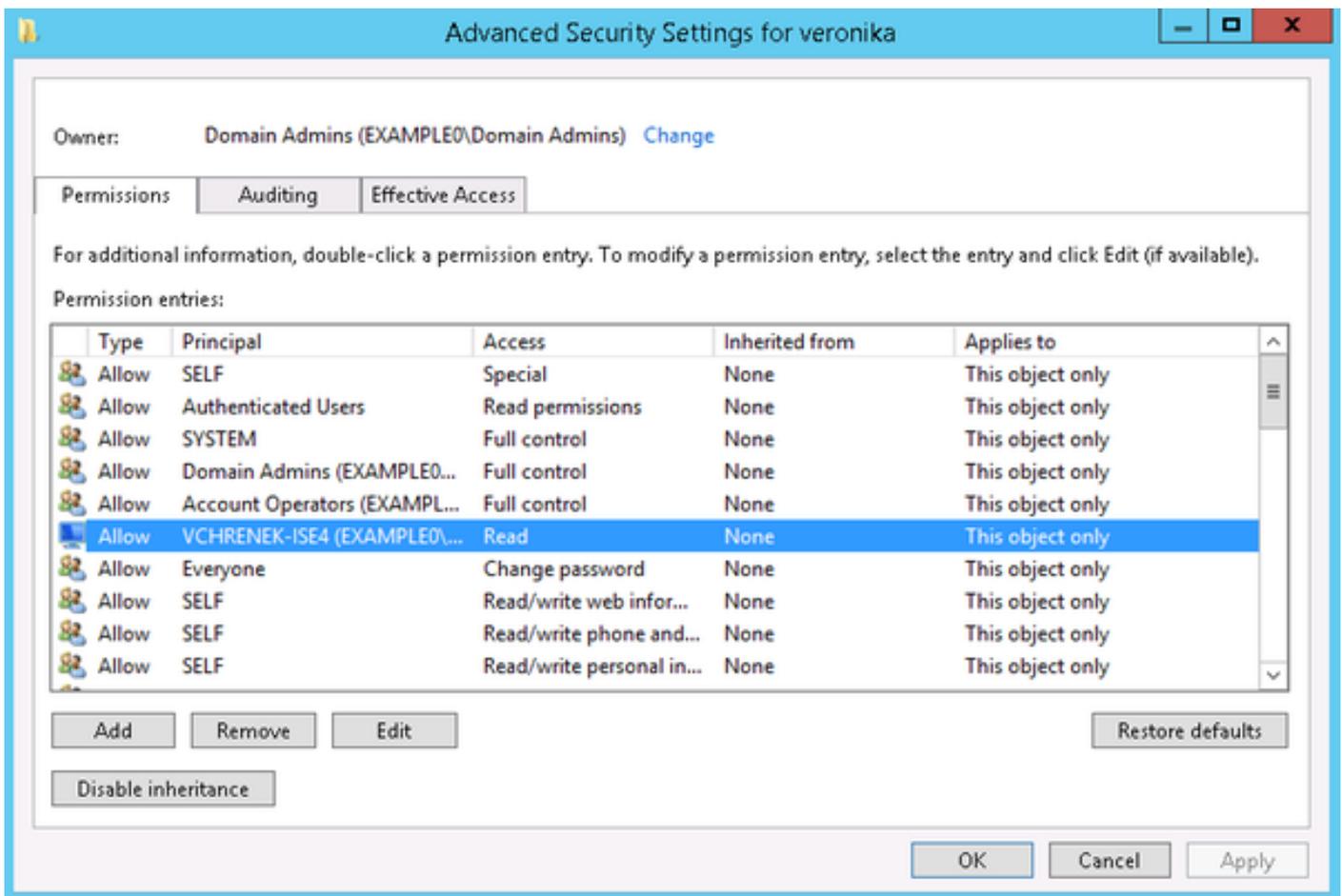
5. ISE ホスト名 (この例の VCHRENEK-ISE4) を挿入し、『OK』をクリックして下さい:



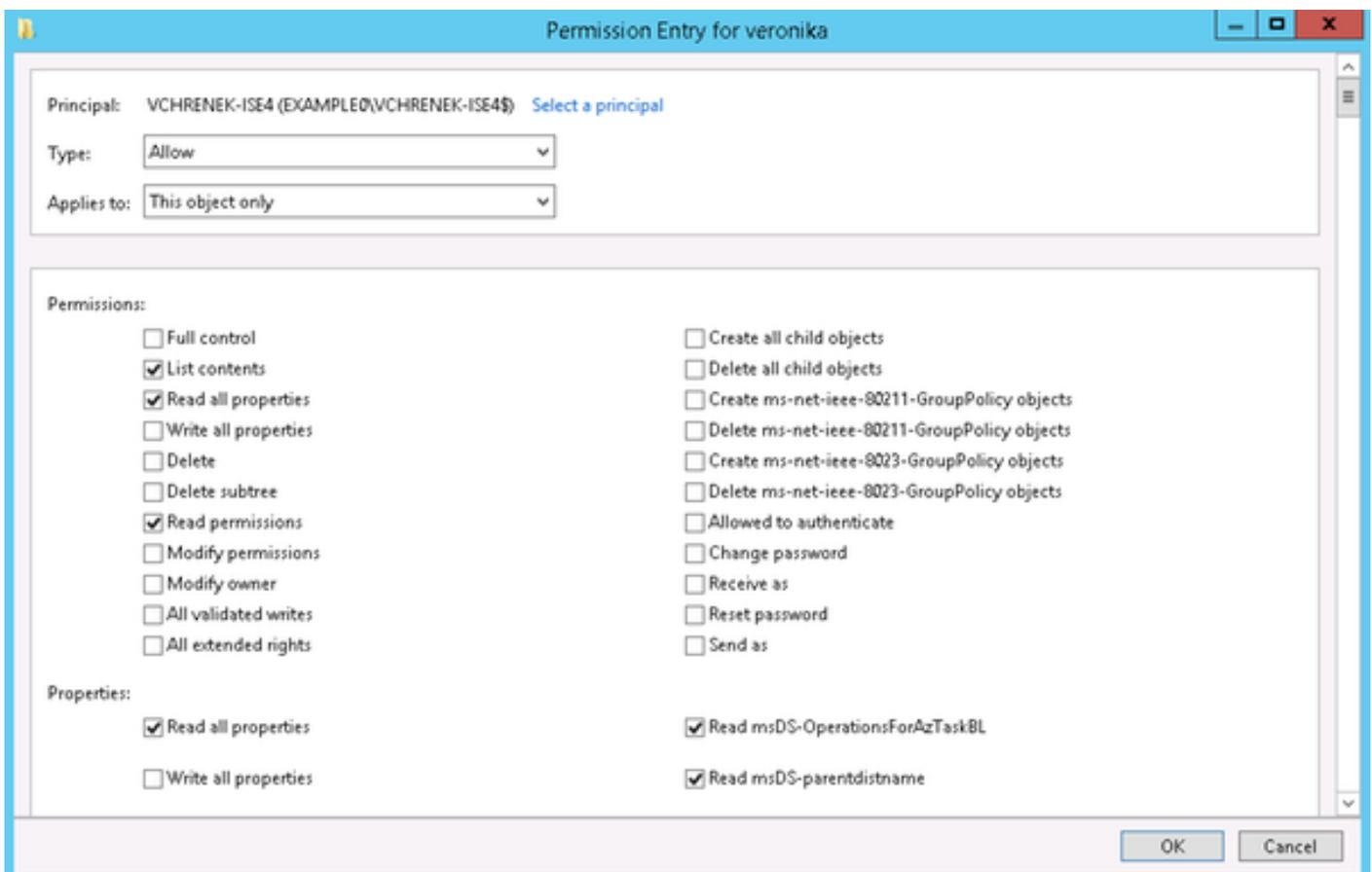
6. ISE ノードを選択し、『Advanced』をクリックして下さい:



7. 拡張セキュリティ設定から ISE コンピューター アカウントを選択し、『Edit』 をクリックして下さい:



8. それらの権限を ISE コンピューター アカウントに提供し、『OK』をクリックして下さい:



これらの変更が問題なしで、AD グループ取得する必要があった後:

Test User Authentication

* Username	<input type="text" value="veronika"/>
* Password	<input type="password" value="••••••••"/>
Authentication Type	<input type="text" value="MS-RPC"/>
Authorization Data	<input checked="" type="checkbox"/> Retrieve Groups <input checked="" type="checkbox"/> Retrieve Attributes
	<input type="button" value="Test"/>

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.	

これはすべてのユーザ向けに実行されたなり、ドメインのすべてのドメインコントローラへの変更は複製する必要があります。