Sourcefire ユーザ エージェントが使用する Active Directory ユーザ アカウントに最小限の権限を付与する

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[設定](#)
[確認](#)
[トラブルシュート](#)

概要

このドキュメントでは、ADドメインコントローラーのクエリに必要な最小限のアクセス許可をActive Directory (AD)ユーザーに与える方法について説明します。Sourcefire User Agentは、ADドメインコントローラーのクエリにADユーザーを使用します。クエリーを実行するには、AD ユーザに追加の権限は必要ありません。

前提条件

要件

Microsoft Windows システムに Sourcefire ユーザ エージェントをインストールし、AD ドメインコントローラへのアクセスを提供する必要があります。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

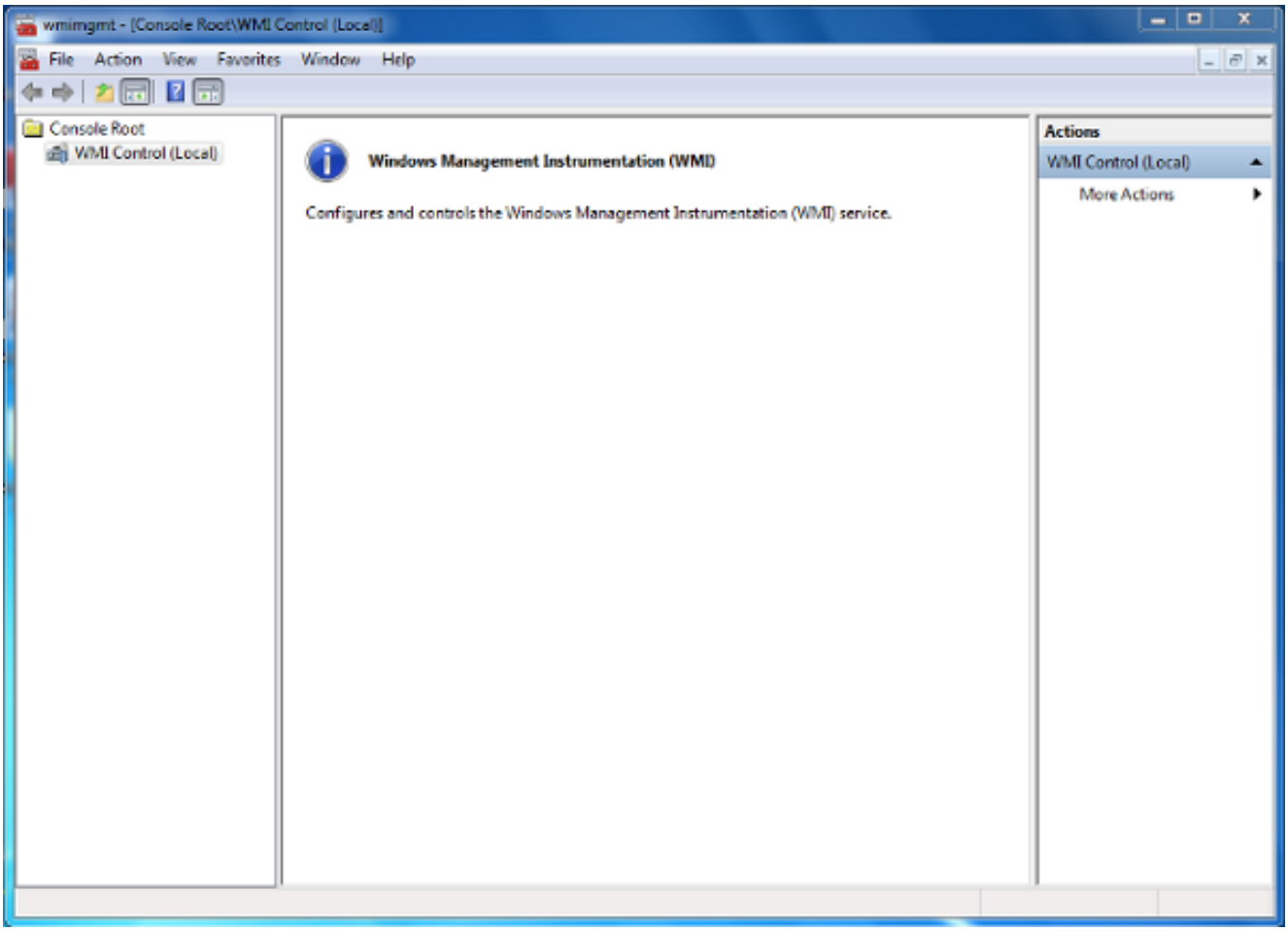
最初に、管理者がユーザ エージェント アクセス専用の新しい AD ユーザを作成する必要があります。この新しいユーザがドメイン管理者グループのメンバでない場合（およびメンバであってはならない場合）、Windows Management Instrumentation（WMI）セキュリティ ログへのアクセス権限をユーザに明示的に与える必要が生じることがあります。権限を付与するには、次の手順を完了します。

1. 次のように WMI コントロール コンソールを開きます。

   AD サーバで [Start] **メニューを選択します。**

   [Run] をクリックして **wmimgmt.msc と入力します。**

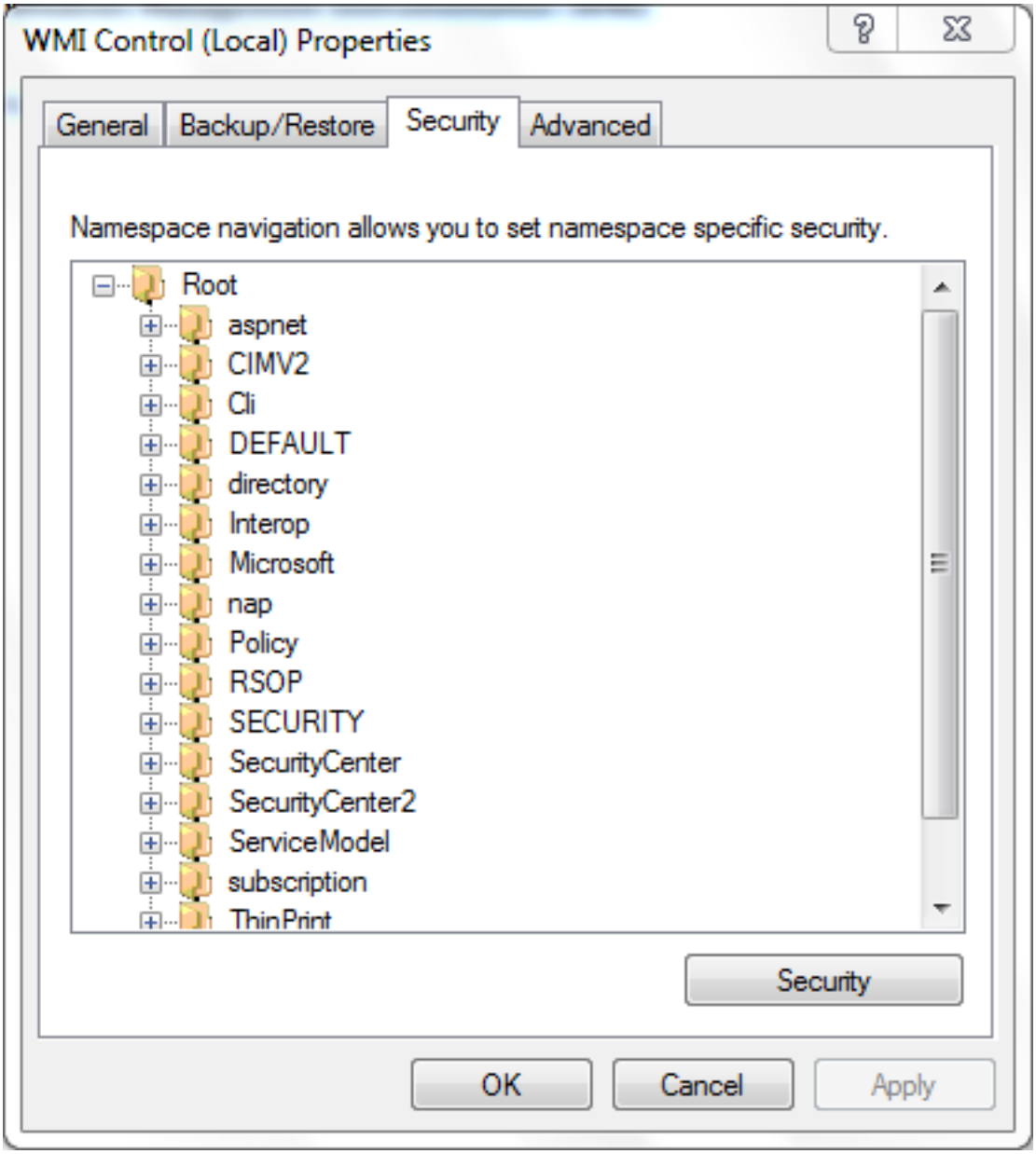
   [OK] をクリックします。WMI コントロール コンソールが表示されます。



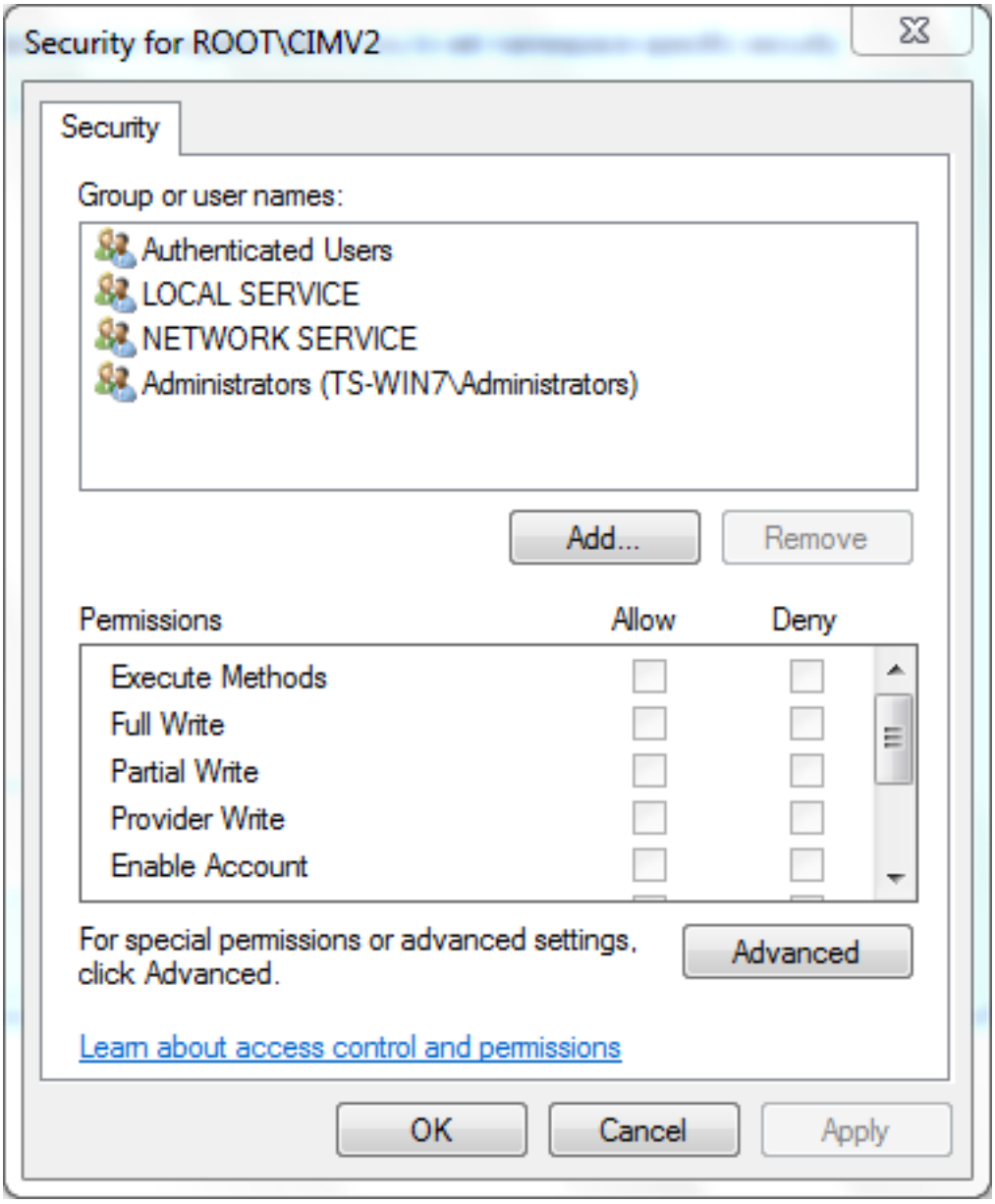
2. WMI コンソール ツリーで [WMI Control] **を右クリックして、[Properties] をクリックします。**

3. [Security] タブをクリックします。

4. ユーザまたはグループにアクセスを与える対象の名前空間を選択して（`Root\CIMV2`）、[Security] をクリックします。



5. [Security] ダイアログボックスで [Add] をクリックします。



6. [Select Users, Computers, or Groups] ダイアログボックスでは、追加するオブジェクト（ユーザまたはグループ）の名前を入力します。入力内容を検証するために [Check Names] **をクリックして、[OK] をクリックします。**オブジェクトをクエリーするために、場所を変更するか [Advanced] をクリックする必要が生じることもあります。詳しくは、状況依存ヘルプ（**？**）を参照してください。

7. [Security] ダイアログボックスの [Permissions] セクションで、新しいユーザまたはグループに権限を与えるために [Allow] **または [Deny] を選択します（すべての権限を与えるのが最も簡単です）。** 少なくとも [Remote Enable] 権限をユーザに与える必要があります。

8. 変更を保存するには [Apply] をクリックします。ウィンドウを閉じます。

確認

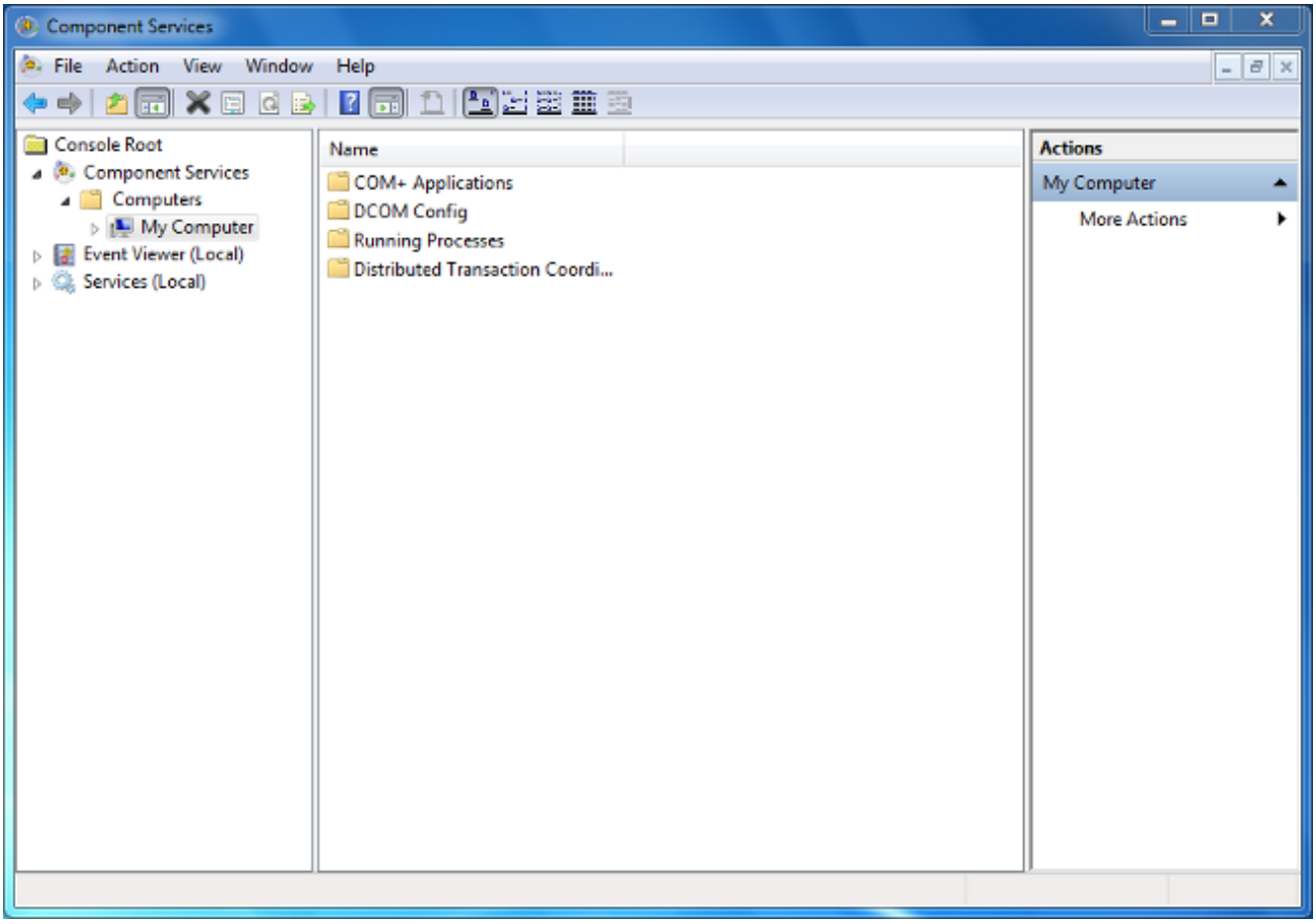
現在、この設定に使用できる確認手順はありません。

トラブルシュート

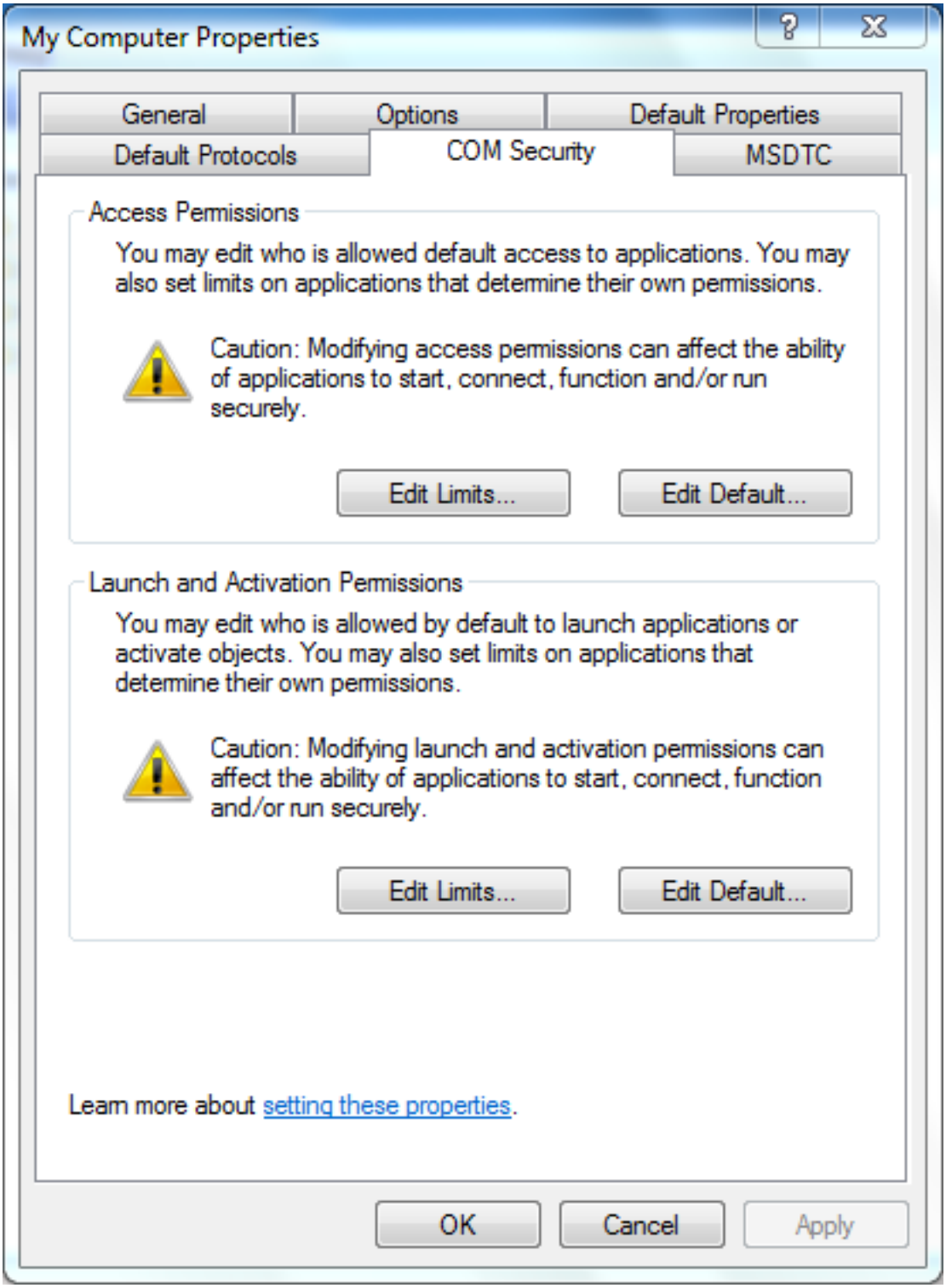
ここでは、設定のトラブルシューティングに使用できる情報を示します。

設定を変更した後に引き続き問題が発生する場合は、リモート アクセスを許可するために分散 COM（DCOM）設定を更新してください。

1. [Start] **メニューを選択します。**
2. [Run] をクリックして **DCOMCNFG** と入力します。
3. [OK] をクリックします。[Component Services] ダイアログボックスが表示されます。



4. [Component Services] ダイアログボックスで、[Component Services] および [Computers] の順に展開し、[My Computer] **を右クリックして [Properties] を選択します。**
5. [My Computer Properties] ダイアログボックスで、[COM Security] **タブをクリックします。**



6. [Launch and Activation Permissions] の下で、[Edit Limits] をクリックします。

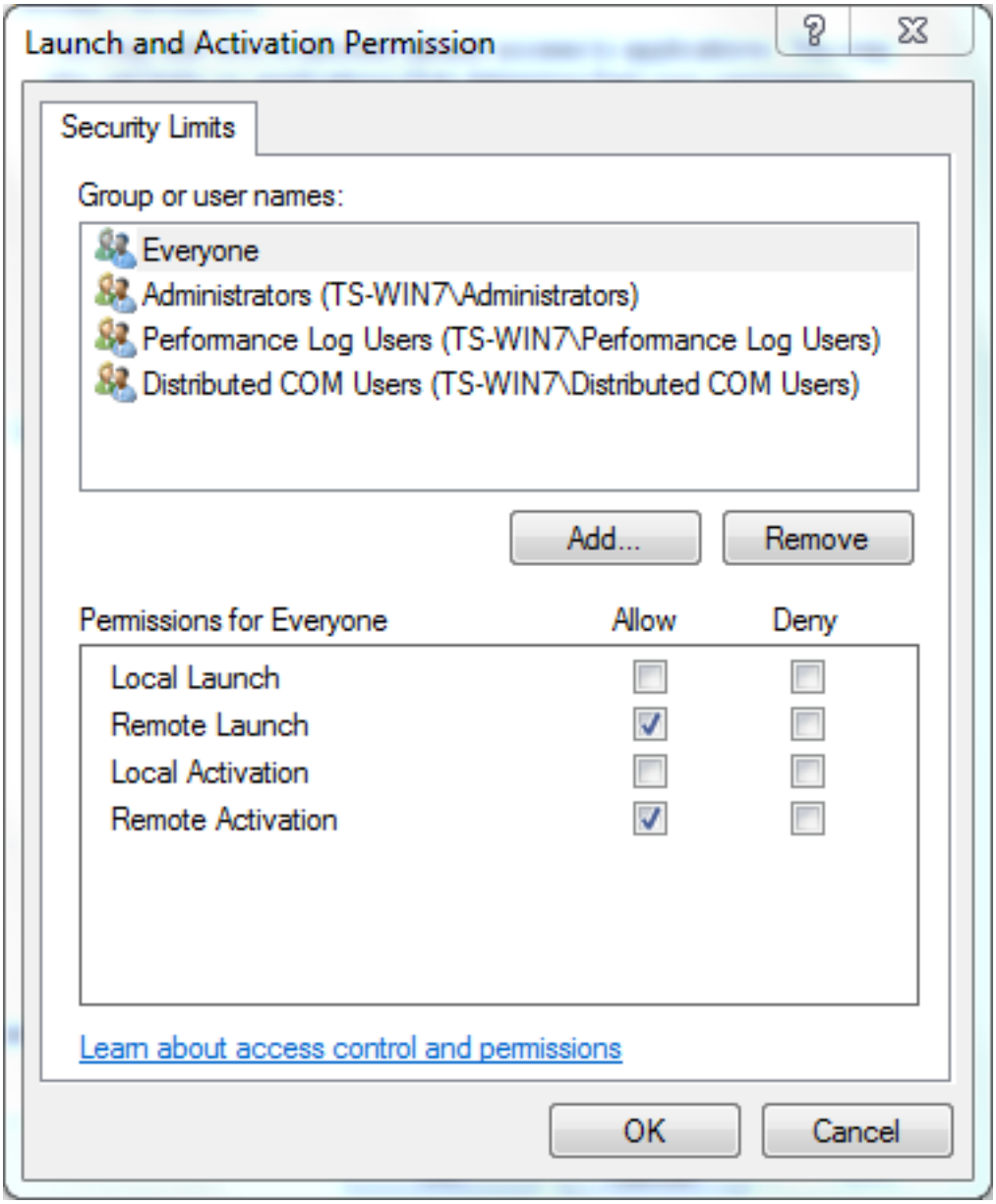
7. [Launch and Activation Permission] ダイアログボックスで、グループまたはユーザ名のリストに名前やグループが表示されない場合には次の手順を完了します。

   [Launch and Activation Permission] ダイアログボックスで [Add] をクリックします。

   [Select Users, Computers, or Groups] ダイアログボックスで、[Enter the object names to select] フィールドに名前とグループを入力して、[OK] をクリックします。

8. [Launch and Activation Permission] ダイアログボックスの [Group or user names] **セクショ**

ンでユーザとグループを選択します。



9. [Permissions for User] の下の [Allow] カラムで、[Remote Launch] **および [Remote Activation] チェックボックスをオンにして [OK] をクリックします。注：**ユーザ名には、AD サーバでユーザ ログイン データをクエリーする権限が必要です。プロキシを介してユーザを認証するには、完全修飾ユーザ名を入力します。デフォルトでは、エージェントのインストール場所のコンピュータへのログインで使用したアカウントのドメインが [Domain] フィールドに自動的に入力されます。異なるドメインのメンバーをユーザとして指定する場合、提供するユーザ クレデンシャルのドメインを更新してください。
10. 問題が引き続き発生する場合、ドメイン コントローラで、[Manage auditing and security log] ポリシーにユーザを追加してみてください。ユーザを追加するには、次の手順を完了します。

    [Group Policy Management Editor] を選択します。

    [Computer Configuration] > [Windows Settings] > [Security Settings] > [Local Policies] > [User Rights Assignment] を選択します。

[Manage auditing and security log] を選択します。

ユーザを追加します。