Autorisation minimum de Grant à un compte utilisateur de Répertoire actif utilisé par l'agent d'utilisateur de Sourcefire

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Configurez](#)
[Vérifiez](#)
[Dépannez](#)

Introduction

Ce document décrit comment fournir à un utilisateur de Répertoire actif (AD) les autorisations minimales requises pour questionner le contrôleur de domaine d'AD. L'agent d'utilisateur de Sourcefire utilise un utilisateur d'AD afin de questionner le contrôleur de domaine d'AD. Afin d'exécuter une requête, un utilisateur d'AD n'a besoin d'aucune autorisation supplémentaire.

Conditions préalables

Conditions requises

Cisco exige que vous installez l'agent d'utilisateur de Sourcefire sur un système de Microsoft Windows et permettez d'accéder au contrôleur de domaine d'AD.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

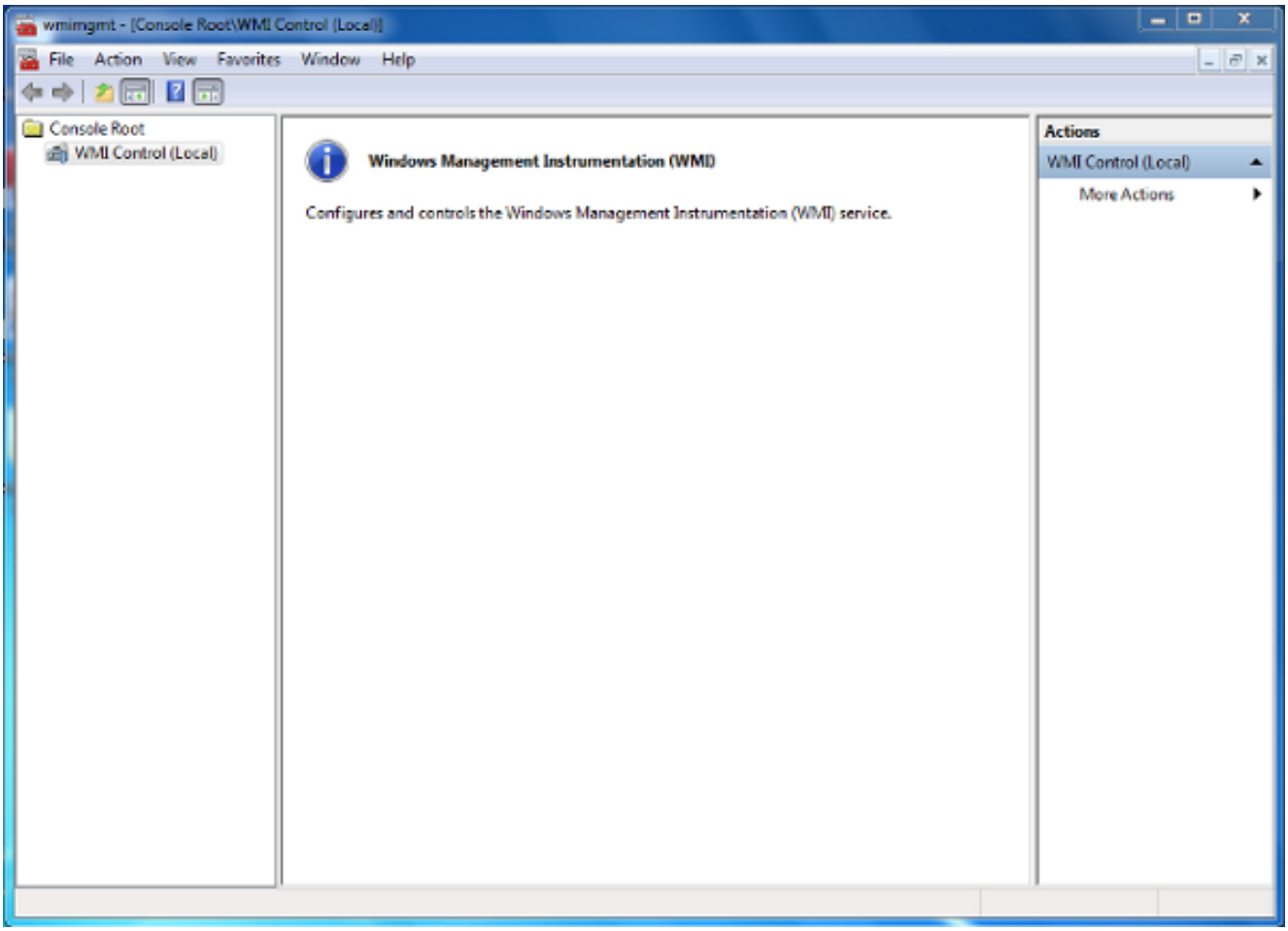
D'abord, un administrateur doit créer un nouvel utilisateur d'AD spécifiquement pour l'accès d'agent d'utilisateur. Si ce nouvel utilisateur n'est pas un membre du groupe d'administrateurs de domaine (et eux ne devrait pas être), on doit accorder explicitement l'utilisateur pourrait l'autorisation d'accéder aux logs de sécurité des Windows Management Instrumentation (WMI). Afin d'accorder l'autorisation, terminez-vous ces étapes :

1. Ouvrez le pupitre de commande WMI :

   Sur le serveur d'AD, choisissez le **menu de démarrage**.

   Cliquez sur Run et écrivez **wmimgmt.msc.**

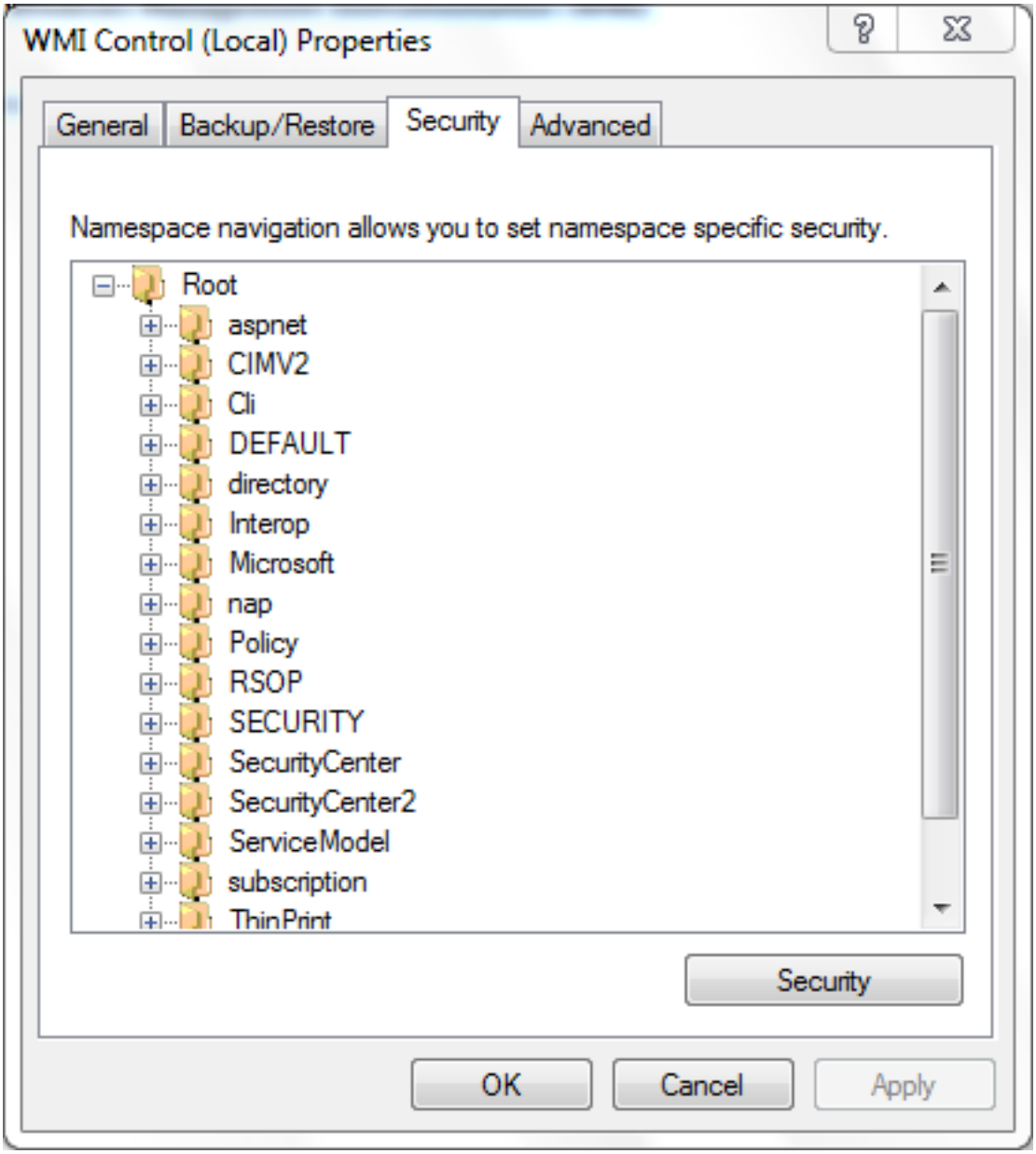
   Cliquez sur **OK**. Le pupitre de commande WMI apparaît.



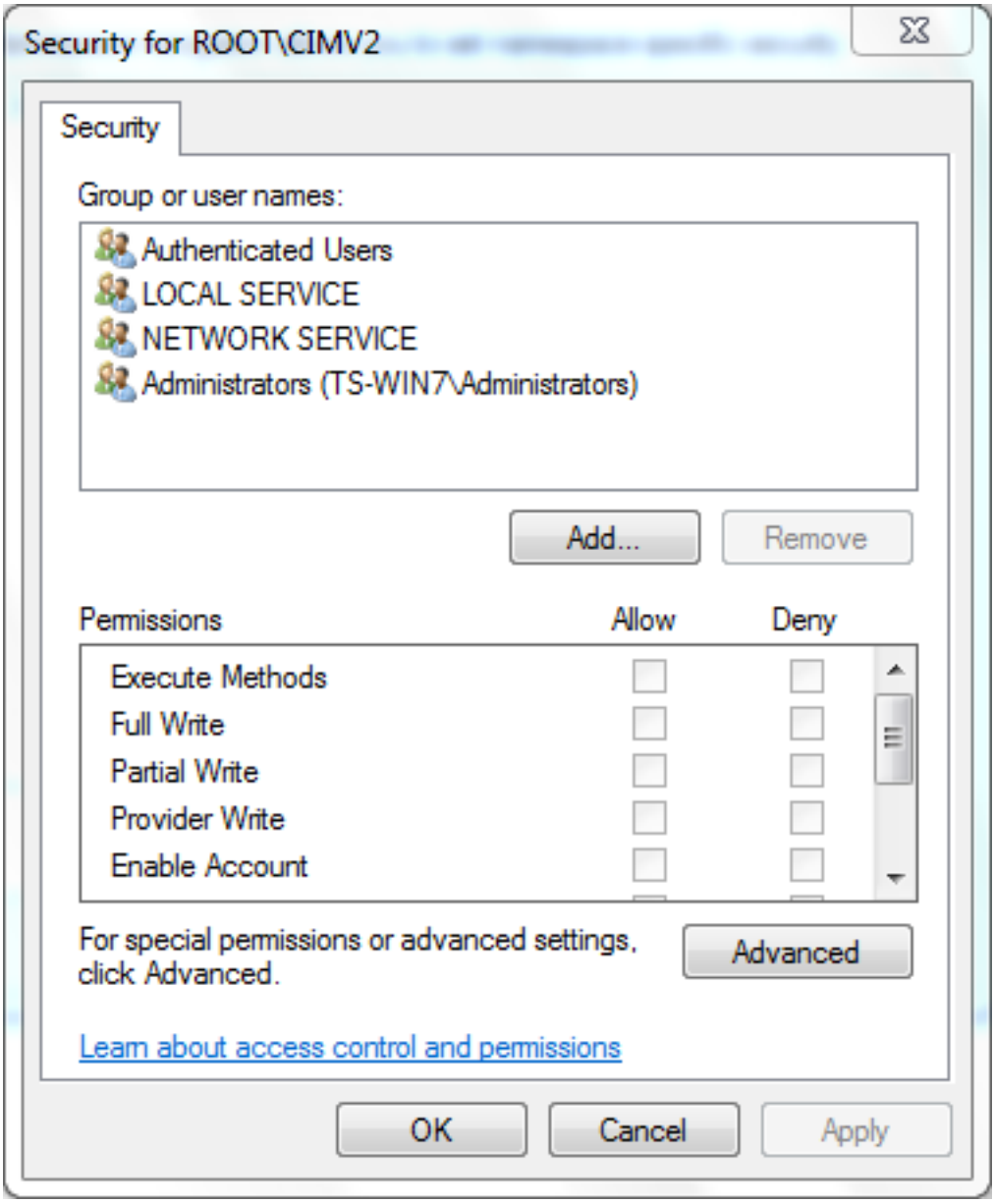
2. Sur l'arborescence de la console WMI, le **contrôle du** clic droit **WMI** et cliquent sur alors **Properties**.

3. Cliquez sur l'onglet **Security**.

4. Sélectionnez l'espace de noms pour lequel vous voulez donner un accès d'utilisateur ou de groupe (**`Root\CIMV2`**), et puis cliquez sur Security.



5. Dans la boîte de dialogue de Sécurité, cliquez sur Add.



6. Dans les utilisateurs choisis, la boîte de dialogue d'ordinateurs, ou de groupes, écrivent le nom de l'objet (utilisateur ou groupe) que vous voulez ajouter. Cliquez sur les **noms de contrôle** afin de vérifier votre entrée et puis cliquer sur OK. Vous pourriez devoir changer l'emplacement ou cliquer sur **avancé** afin de questionner pour des objets. Voyez l'aide contextuelle (**?**) pour plus de détail.

7. Dans la boîte de dialogue de Sécurité, dans la section d'autorisations, choisissez **laissent** ou **refusent** afin d'accorder des autorisations au nouveau utilisateur ou groupe (le plus facile de donner toutes les autorisations). L'utilisateur doit être donné au moins l'autorisation **distante d'enable**.

8. Cliquez sur Apply afin de sauvegarder des modifications. Fermez la fenêtre.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

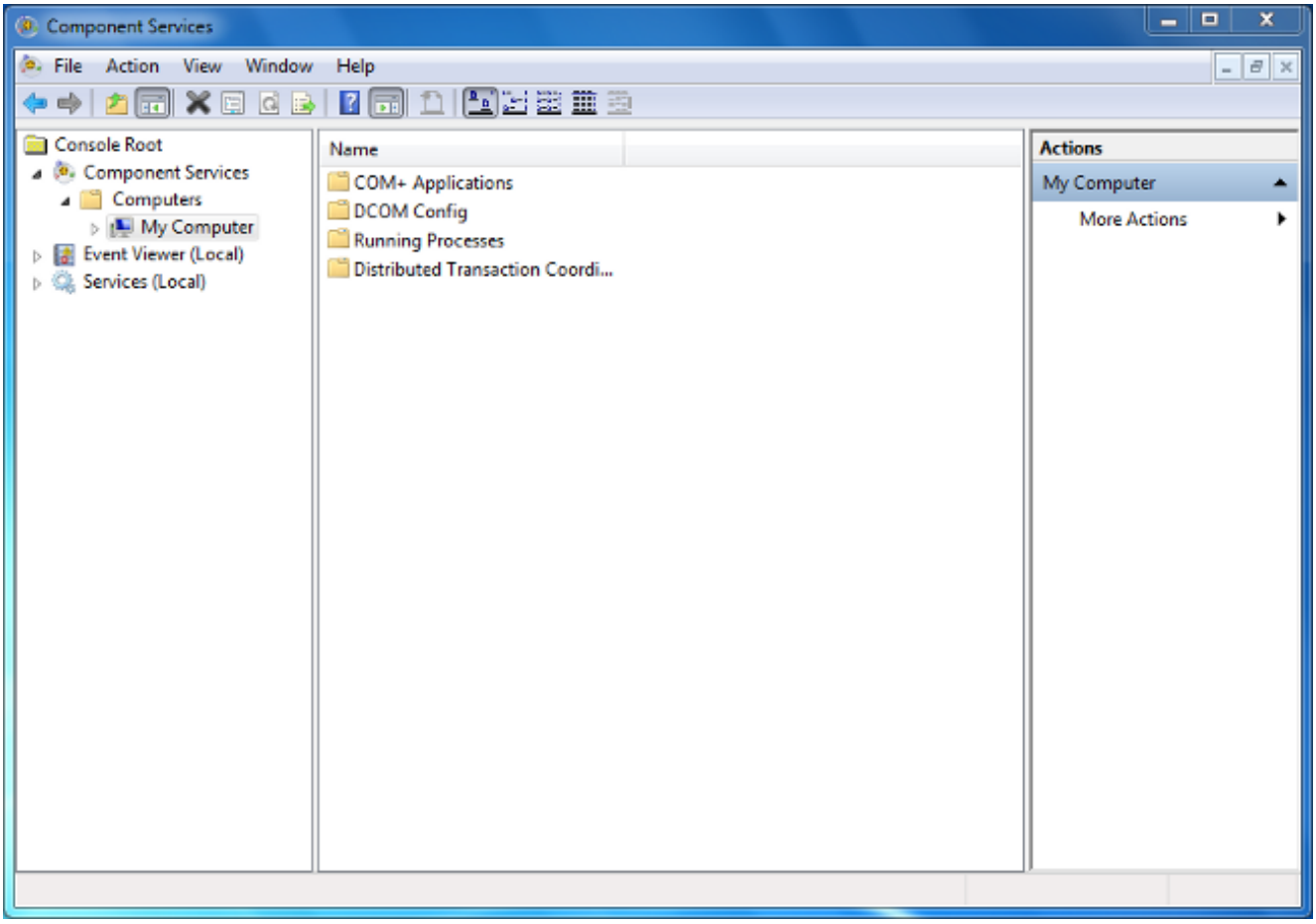
Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Si une question persiste après les modifications de configuration, mettez à jour les configurations composantes distribuées du modèle objet (DCOM) afin de permettre l'Accès à distance :

1. Choisissez le **menu de démarrage**.

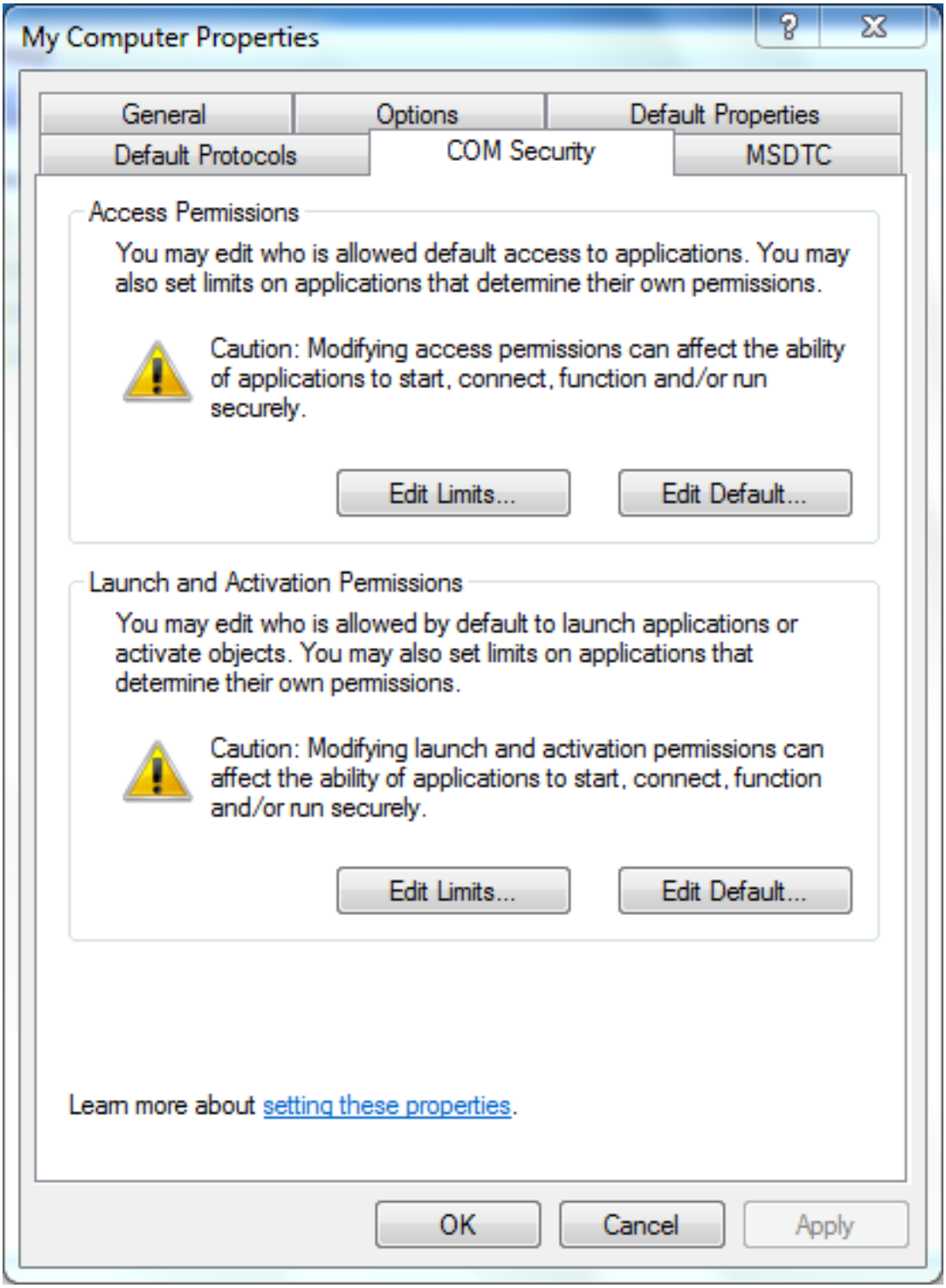
2. Cliquez sur Run et écrivez **DCOMCNFG**.

3. Cliquez sur **OK**. La boîte de dialogue de services de composant apparaît.



4. Dans la boîte de dialogue de services de composant, développez les **services composants**, développez les **ordinateurs**, et puis cliquez avec le bouton droit **mon ordinateur** et choisissez Properties.

5. Dans la ma boîte de dialogue Properties d'ordinateur, cliquez sur l'**onglet Sécurité COM**.



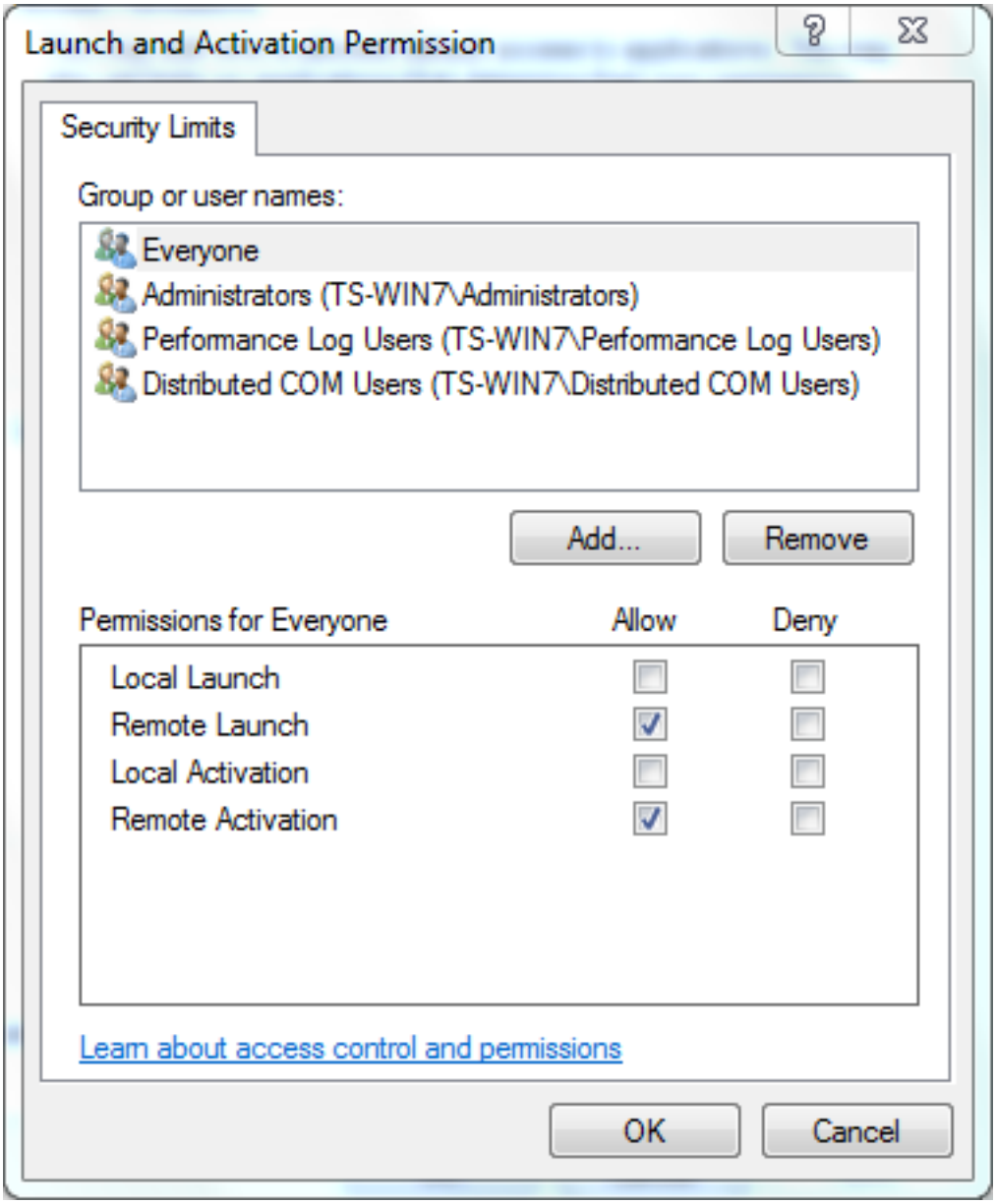
6. Sous des autorisations de lancement et de lancement, cliquez sur Edit les **limites**.

7. Dans la boîte de dialogue d'autorisation de lancement et de lancement, terminez-vous ces étapes si votre nom ou votre groupe n'apparaît pas dans les groupes ou les noms d'utilisateur les répertorient :

   Dans la boîte de dialogue d'autorisation de lancement et de lancement, cliquez sur Add.

   Dans les utilisateurs choisis, la boîte de dialogue d'ordinateurs, ou de groupes, présentent votre nom et le groupe dans l'entrer les noms d'objet pour sélectionner le champ, et puis cliquent sur OK.

8. Dans la boîte de dialogue d'autorisation de lancement et de lancement, sélectionnez votre utilisateur et groupe dans le **groupe ou la** section de **noms d'utilisateur**.



9. Dans la colonne d'autoriser sous des autorisations pour l'utilisateur, vérifiez les cases **distantes de lancement de lancement** et de **distant**, et puis cliquez sur OK.Remarque: Un nom d'utilisateur doit avoir des droits de questionner pour des données d'ouverture de session utilisateur sur un serveur d'AD. Afin d'authentifier avec un utilisateur par l'intermédiaire du proxy, écrivez le nom d'utilisateur qualifié a entièrement -. Par défaut, le domaine pour le compte que vous vous connectiez dans l'ordinateur où vous avez installé l'agent automatique-remplit champ Domain. Si un utilisateur que vous fournissez est un membre d'un domaine différent, mettent à jour le domaine pour les identifiants utilisateurs fournis.
10. Si le problème persiste, sur l'essai de contrôleur de domaine pour ajouter l'utilisateur dans la stratégie de auditer et de log de sécurité du gérer. Afin d'ajouter l'utilisateur, terminez-vous ces étapes :

    Choisissez l'**éditeur de Gestion de stratégie de groupe**.

Choisissez la **configuration de l'ordinateur** > les **paramètres de windows** > les **paramètres de sécurité** > **affectation locale de stratégies** > de **droits des utilisateurs**.

Choisissez **gèrent auditer et log de sécurité**.

Ajoutez l'utilisateur.