Octroi d'une autorisation minimale à un compte d'utilisateur Active Directory utilisé par l'agent d'utilisateur Sourcefire

Contenu

Introduction

Ce document décrit comment fournir à un utilisateur Active Directory (AD) les autorisations minimales nécessaires pour interroger le contrôleur de domaine AD. L'agent utilisateur Sourcefire utilise un utilisateur AD afin d'interroger le contrôleur de domaine AD. Pour exécuter une requête, un utilisateur AD ne nécessite aucune autorisation supplémentaire.

Conditions préalables

Conditions requises

Cisco exige que vous installiez l'agent utilisateur Sourcefire sur un système Microsoft Windows et que vous fournissiez l'accès au contrôleur de domaine AD.

Components Used

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

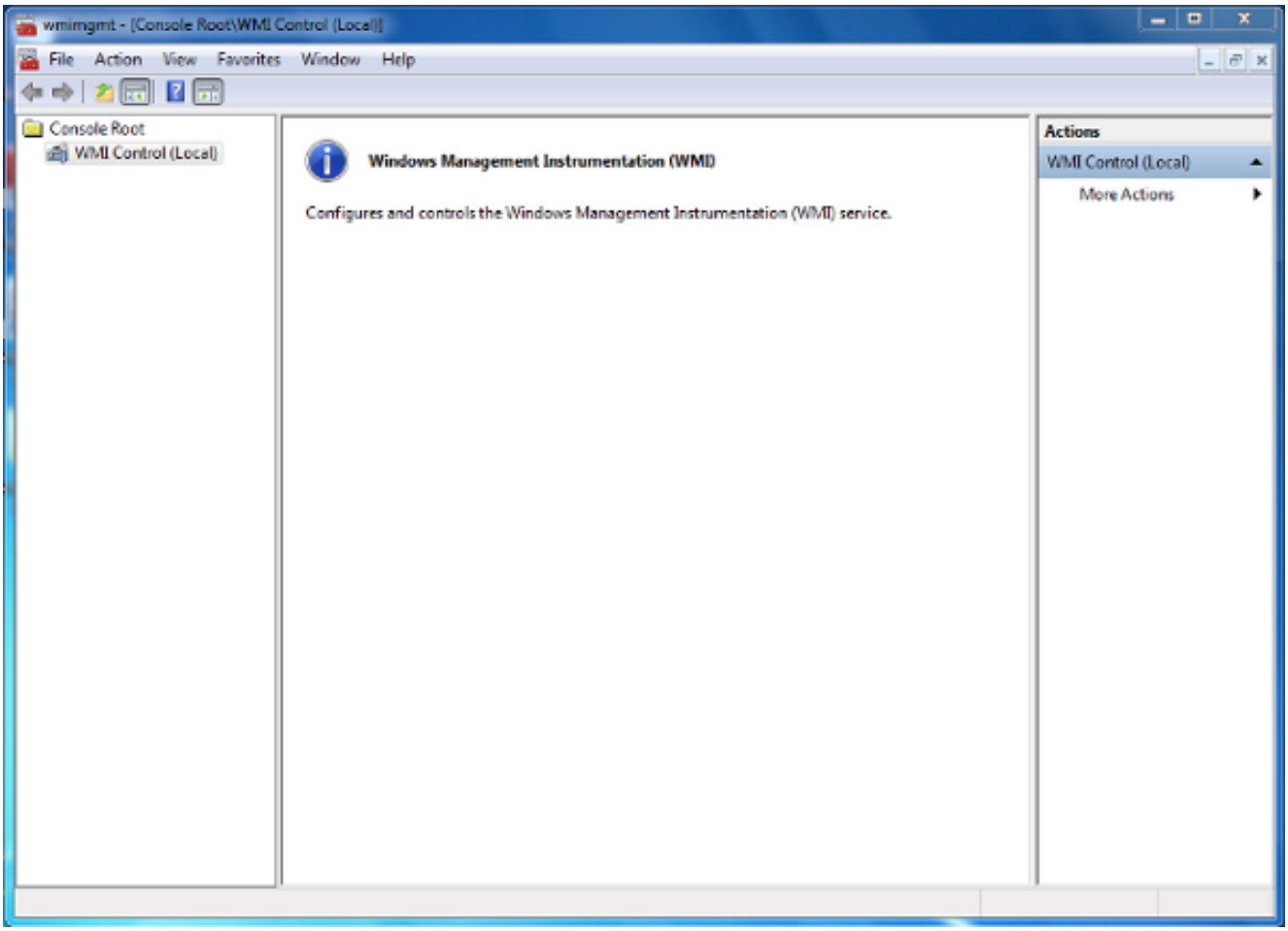
Tout d'abord, un administrateur doit créer un nouvel utilisateur AD spécifiquement pour l'accès à l'Agent utilisateur. Si ce nouvel utilisateur n'est pas membre du groupe d'administrateurs de domaine (et qu'il ne le devrait pas), il peut être explicitement nécessaire d'accorder à l'utilisateur l'autorisation d'accéder aux journaux de sécurité WMI (Windows Management Instrumentation). Pour accorder l'autorisation, procédez comme suit :

1. Ouvrez la console de contrôle WMI :

   Sur le serveur AD, sélectionnez le menu **Démarrer**.

   Cliquez sur **Exécuter** et saisissez **wmimgmt.msc**.

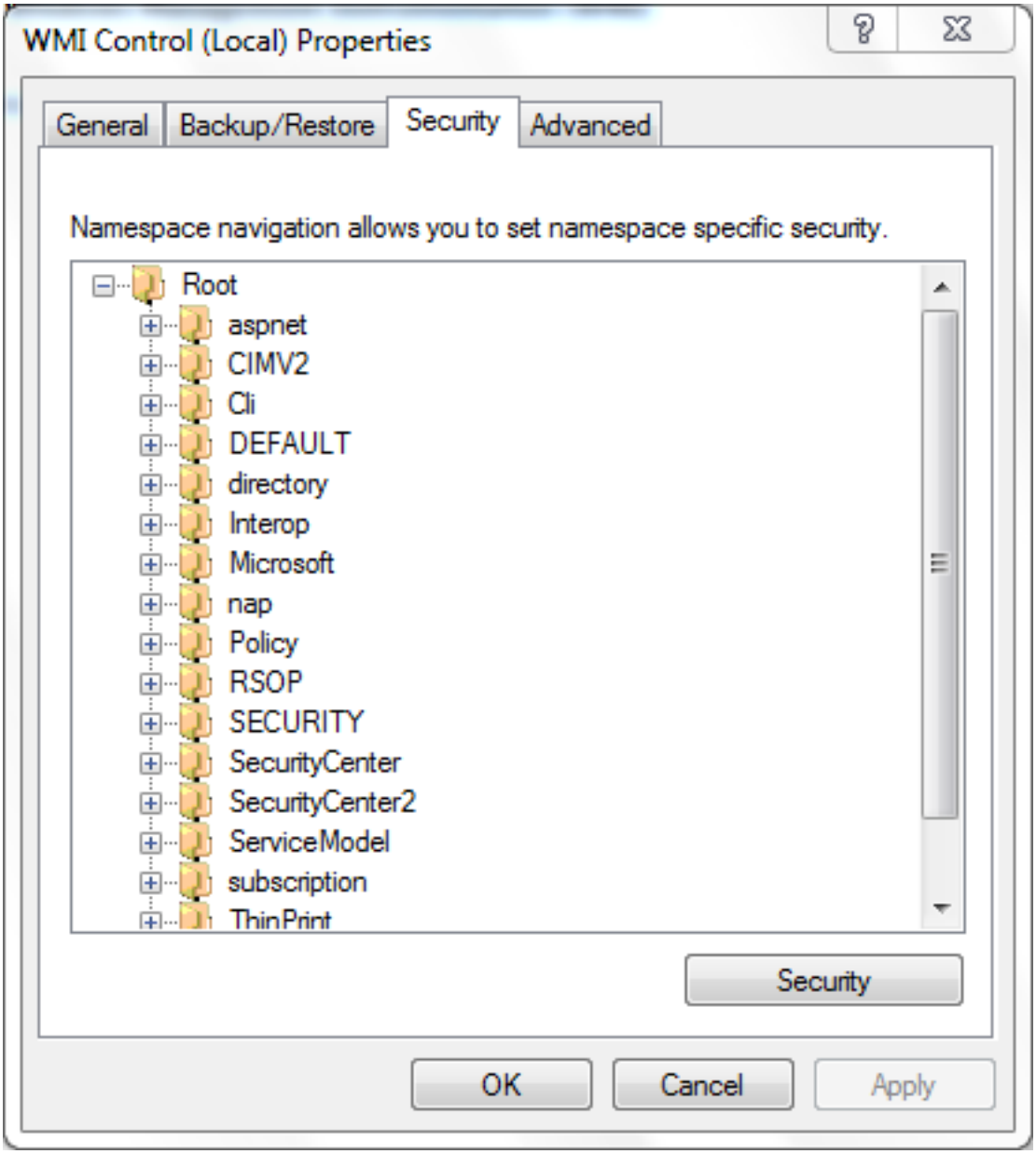
   Click OK. La console de contrôle WMI apparaît.



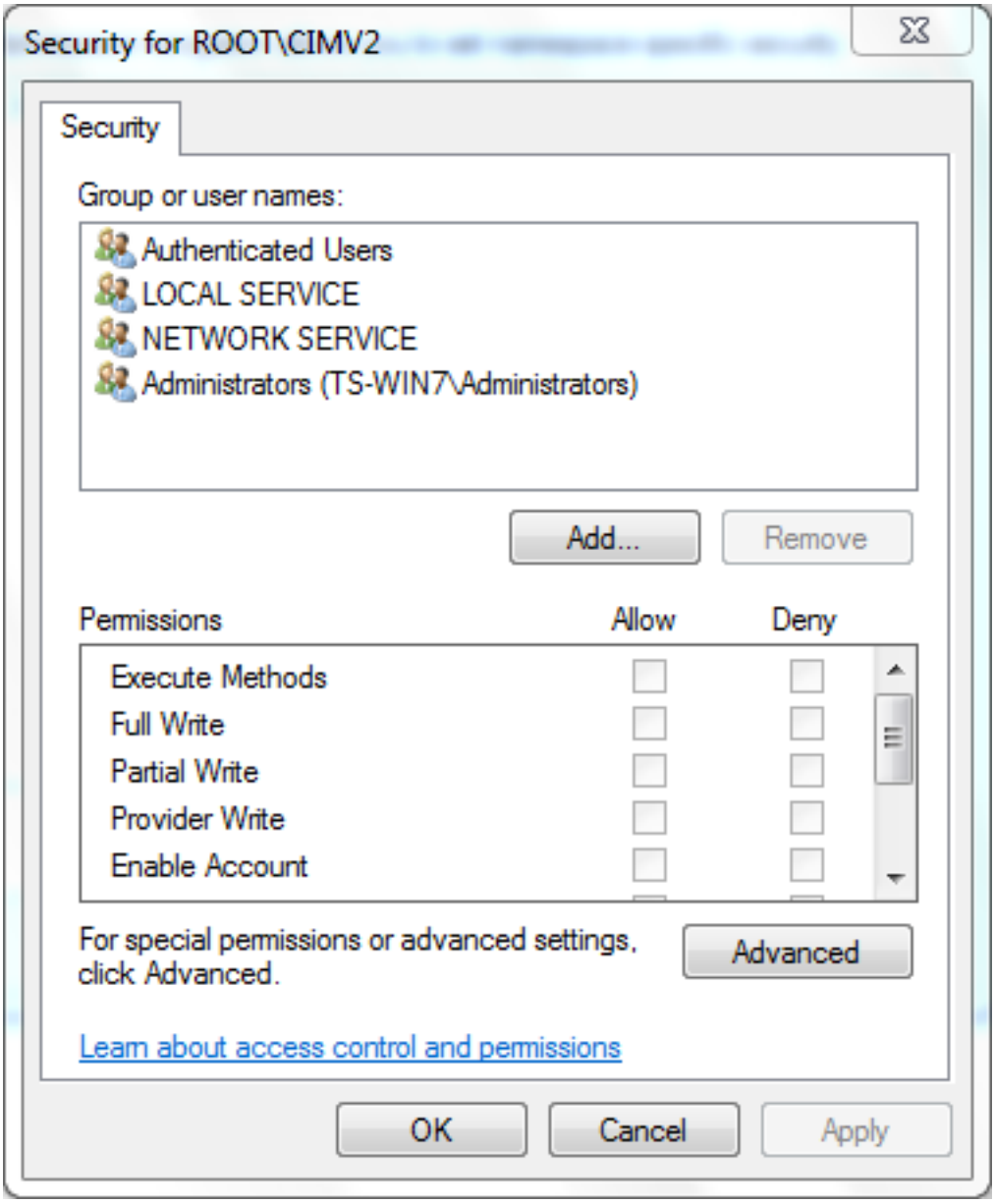
2. Dans l'arborescence de la console WMI, cliquez avec le bouton droit sur **Contrôle WMI**, puis cliquez sur **Propriétés**.

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

4. Sélectionnez l'espace de noms pour lequel vous souhaitez accorder un accès utilisateur ou de groupe (`Root\CIMV2`), puis cliquez sur **Sécurité**.



5. Dans la boîte de dialogue Sécurité, cliquez sur **Ajouter**.



6. Dans la boîte de dialogue Sélectionner des utilisateurs, des ordinateurs ou des groupes, saisissez le nom de l'objet (utilisateur ou groupe) à ajouter. Cliquez sur **Vérifier les noms** afin de vérifier votre entrée, puis cliquez sur **OK**. Vous devrez peut-être modifier l'emplacement ou cliquer sur **Avancé** pour rechercher des objets. Consultez l'aide contextuelle (**?**) pour plus de détails.

7. Dans la boîte de dialogue Sécurité, dans la section Autorisations, sélectionnez **Autoriser** ou **Refuser** afin d'accorder des autorisations au nouvel utilisateur ou au nouveau groupe (plus facile de donner toutes les autorisations). L'utilisateur doit disposer au moins de l'autorisation **Remote Enable**.

8. Cliquez sur **Apply** afin d'enregistrer les modifications. Fermez la fenêtre.

Vérification

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

Dépannage

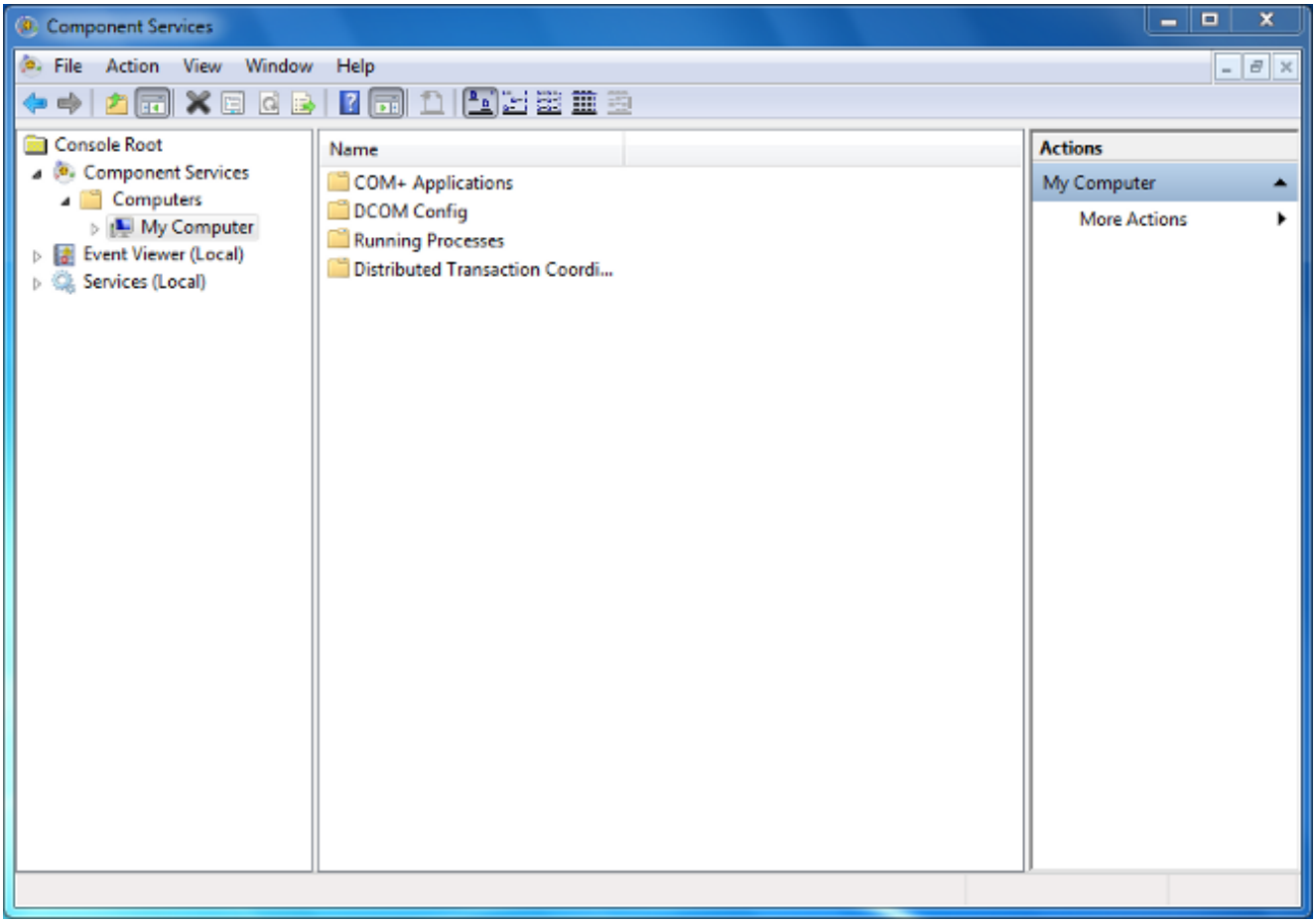
Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Si un problème persiste après les modifications de configuration, mettez à jour les paramètres DCOM (Distributed Component Object Model) afin d'autoriser l'accès à distance :

1. Sélectionnez le menu **Démarrer**.

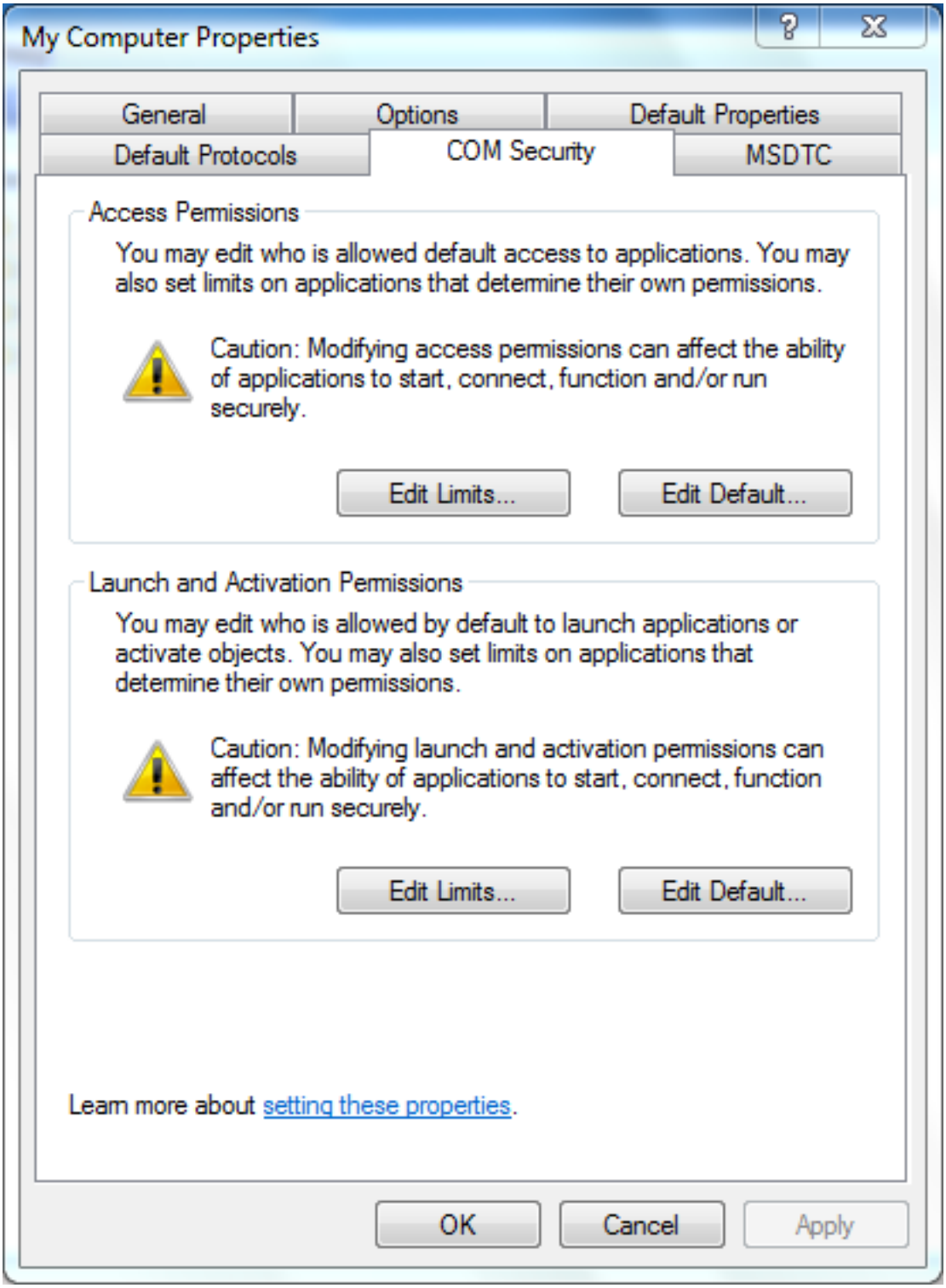
2. Cliquez sur **Exécuter** et saisissez **DCOMCNFG**.

3. Click OK. La boîte de dialogue Services de composants s'affiche.



4. Dans la boîte de dialogue Services de composants, développez **Services de composants**, développez **Ordinateurs**, puis cliquez avec le bouton droit sur **Poste de travail** et choisissez **Propriétés**.

5. Dans la boîte de dialogue Propriétés du Poste de travail, cliquez sur l'onglet **Sécurité COM**.



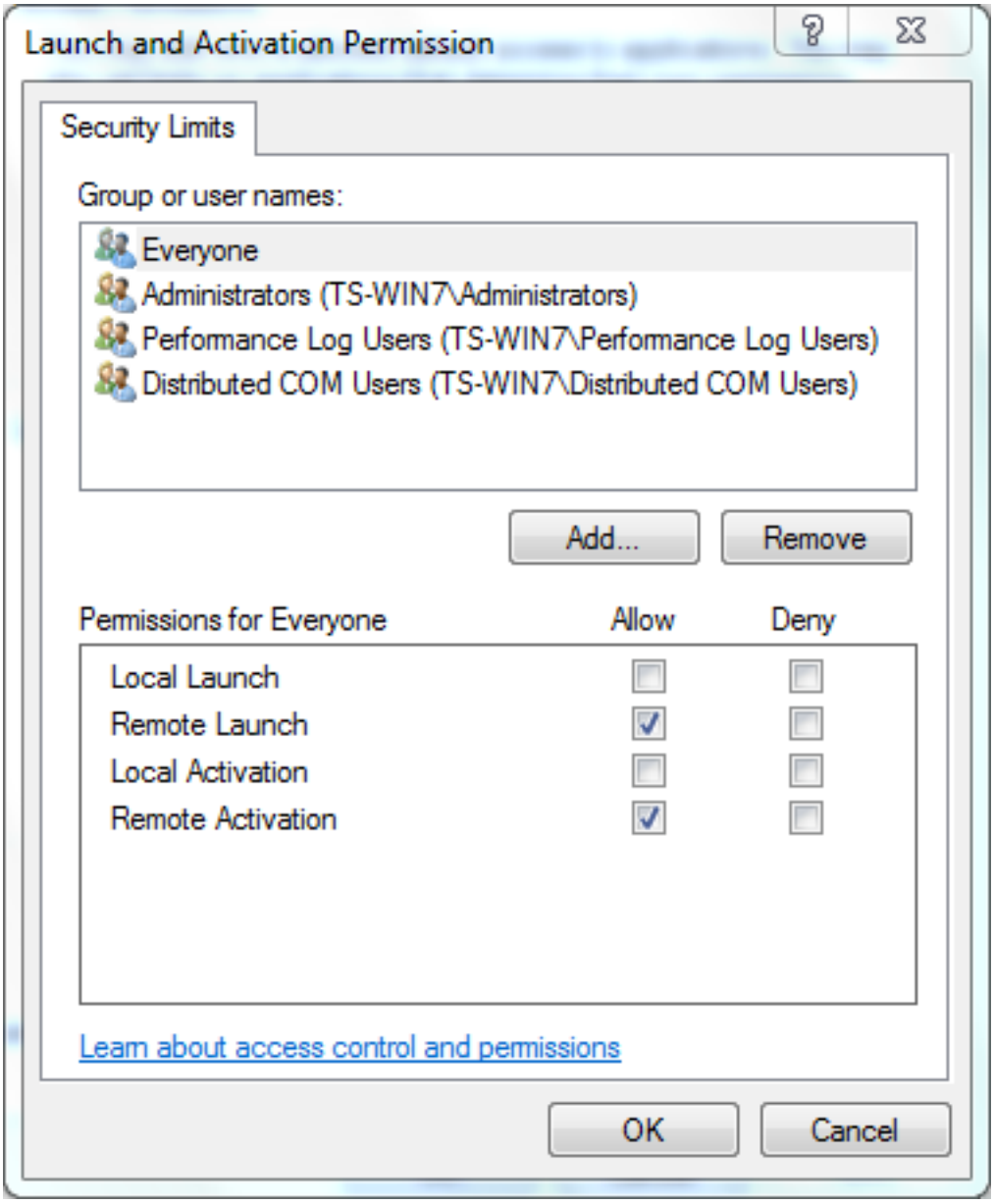
6. Sous Autorisations de lancement et d'activation, cliquez sur **Modifier les limites**.

7. Dans la boîte de dialogue Autorisation de lancement et d'activation, procédez comme suit si votre nom ou votre groupe n'apparaît pas dans la liste Groupes ou noms d'utilisateur :

   Dans la boîte de dialogue Autorisation de lancement et d'activation, cliquez sur **Ajouter**.

   Dans la boîte de dialogue Sélectionner des utilisateurs, des ordinateurs ou des groupes, entrez votre nom et le groupe dans le champ Entrez les noms d'objet à sélectionner, puis cliquez sur **OK**.

8. Dans la boîte de dialogue Autorisation de lancement et d'activation, sélectionnez votre utilisateur et votre groupe dans la section **Nom du groupe ou des utilisateurs**.



9. Dans la colonne Autoriser sous Autorisations utilisateur, cochez les cases **Lancement à distance** et **Activation à distance**, puis cliquez sur **OK**.**Note**: Un nom d'utilisateur doit avoir les droits de requête pour les données de connexion utilisateur sur un serveur AD. Afin de s'authentifier auprès d'un utilisateur via un proxy, saisissez un nom d'utilisateur complet. Par défaut, le domaine du compte que vous avez utilisé pour vous connecter à l'ordinateur sur lequel vous avez installé l'agent remplit automatiquement le champ Domaine. Si un utilisateur que vous fournissez est membre d'un autre domaine, mettez à jour le domaine pour les informations d'identification de l'utilisateur fournies.
10. Si le problème persiste, sur le contrôleur de domaine, essayez d'ajouter l'utilisateur dans la stratégie Gérer l'audit et le journal de sécurité. Pour ajouter l'utilisateur, procédez comme suit :

    Sélectionnez l'**Éditeur de gestion des stratégies de groupe**.

    Choisissez Configuration de l'ordinateur > **Paramètres Windows** > **Paramètres de sécurité** >

Stratégies locales > Affectation De Droits D'Utilisateur.

Choisissez **Gérer le journal d'audit et de sécurité**.

Ajoutez l'utilisateur.