Concedere autorizzazioni minime a un account utente di Active Directory utilizzato dall'agente utente Sourcefire

Sommario

Introduzione

In questo documento viene descritto come fornire a un utente di Active Directory (AD) le autorizzazioni minime necessarie per eseguire query sul controller di dominio AD. L'agente utente Sourcefire utilizza un utente AD per eseguire query sul controller di dominio AD. Per eseguire una query, un utente AD non richiede autorizzazioni aggiuntive.

Prerequisiti

Requisiti

Cisco richiede l'installazione dell'agente utente Sourcefire in un sistema Microsoft Windows e l'accesso al controller di dominio Active Directory.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

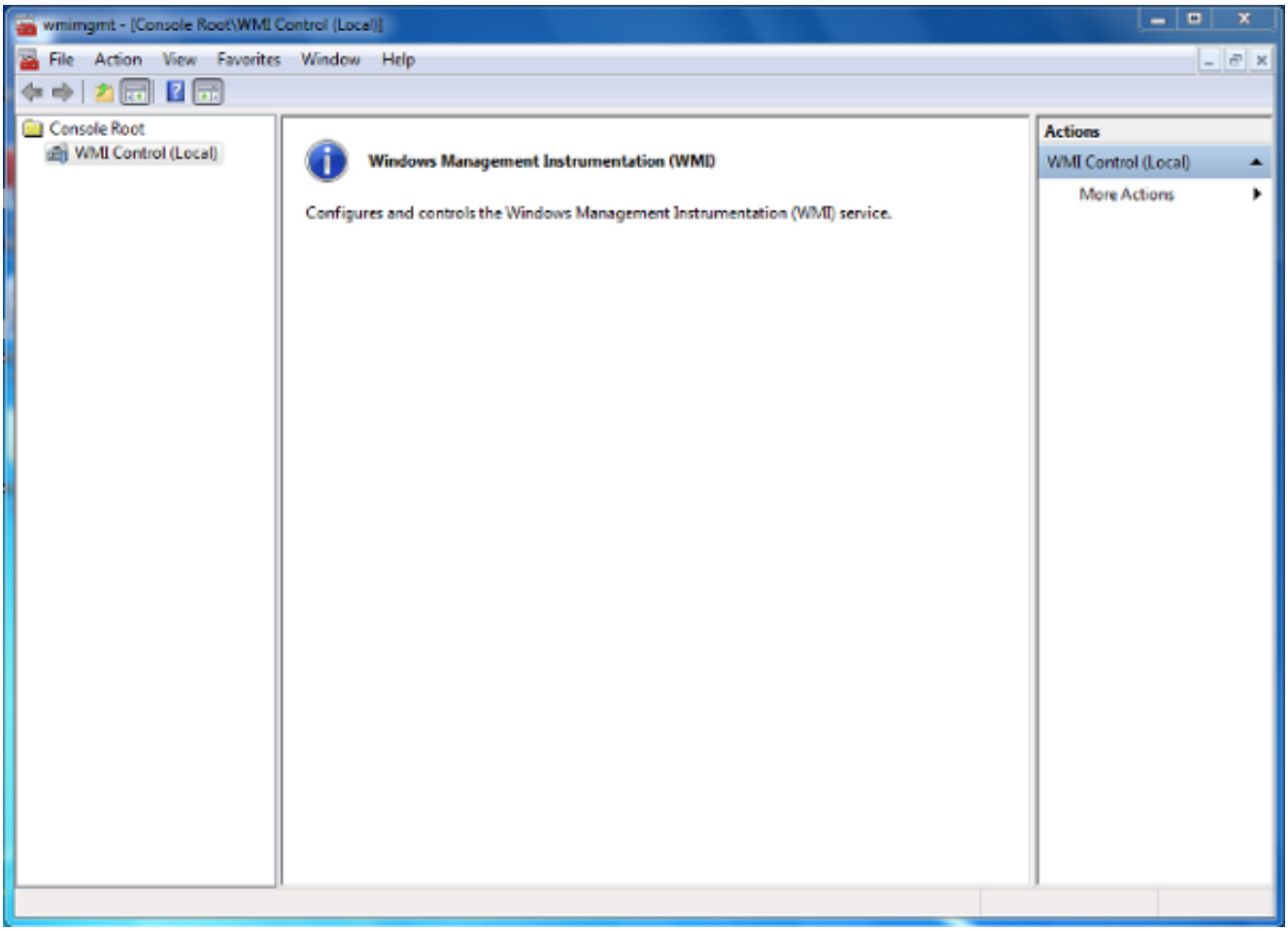
In primo luogo, un amministratore deve creare un nuovo utente AD specifico per l'accesso Agente utente. Se il nuovo utente non è membro del gruppo degli amministratori di dominio e non dovrebbe esserlo, potrebbe essere necessario concedere in modo esplicito all'utente l'autorizzazione ad accedere ai registri di protezione di Strumentazione gestione Windows (WMI). Per concedere l'autorizzazione, attenersi alla seguente procedura:

1. Aprire la console di controllo WMI:

   Sul server AD, scegliere il menu **Start**.

   Fare clic su **Esegui** e immettere **wmimgmt.msc**.

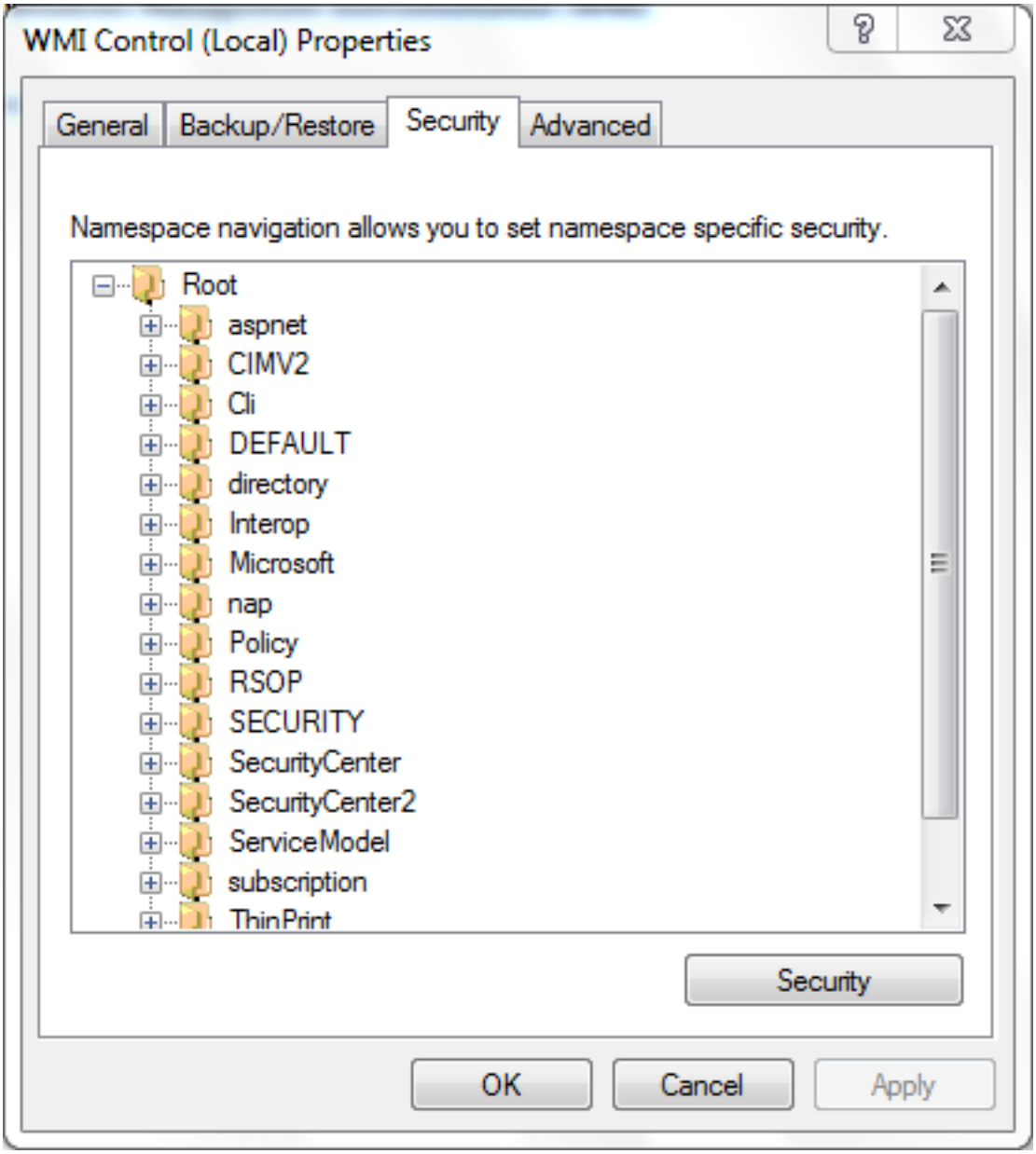
   Fare clic su **OK**. Verrà visualizzata la console di controllo WMI.



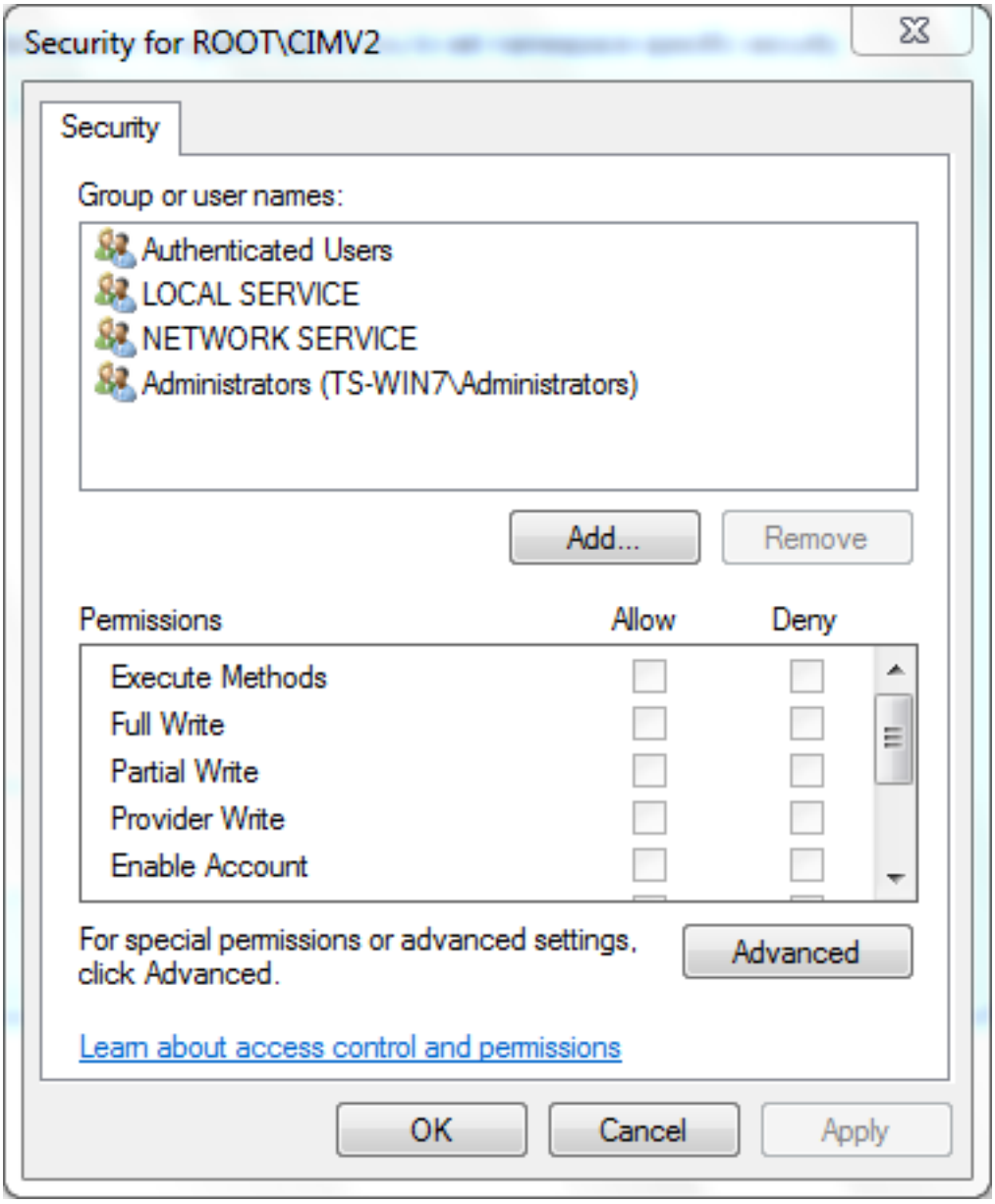
2. Nell'albero della console WMI fare clic con il pulsante destro del mouse su **Controllo WMI** e quindi scegliere **Proprietà**.

3. Fare clic sulla scheda **Protezione**.

4. Selezionare lo spazio dei nomi per il quale si desidera concedere a un utente o a un gruppo l'accesso (`Root\CIMV2`), quindi fare clic su **Protezione**.



5. Nella finestra di dialogo Protezione fare clic su **Aggiungi**.



6. Nella finestra di dialogo Seleziona utenti, computer o gruppi immettere il nome dell'oggetto (utente o gruppo) che si desidera aggiungere. Fare clic su **Controlla nomi** per verificare la voce immessa, quindi fare clic su **OK**. Per eseguire una query sugli oggetti, potrebbe essere necessario modificare il percorso o fare clic su **Avanzate**. Vedere la Guida sensibile al contesto (**?**) per ulteriori informazioni.

7. Nella sezione Autorizzazioni della finestra di dialogo Protezione scegliere **Consenti** o **Nega** per concedere le autorizzazioni al nuovo utente o gruppo (operazione più semplice). All'utente deve essere concessa almeno l'autorizzazione **Abilitazione remota**.

8. Per salvare le modifiche, fare clic su **Apply** (Applica). Chiudete la finestra.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

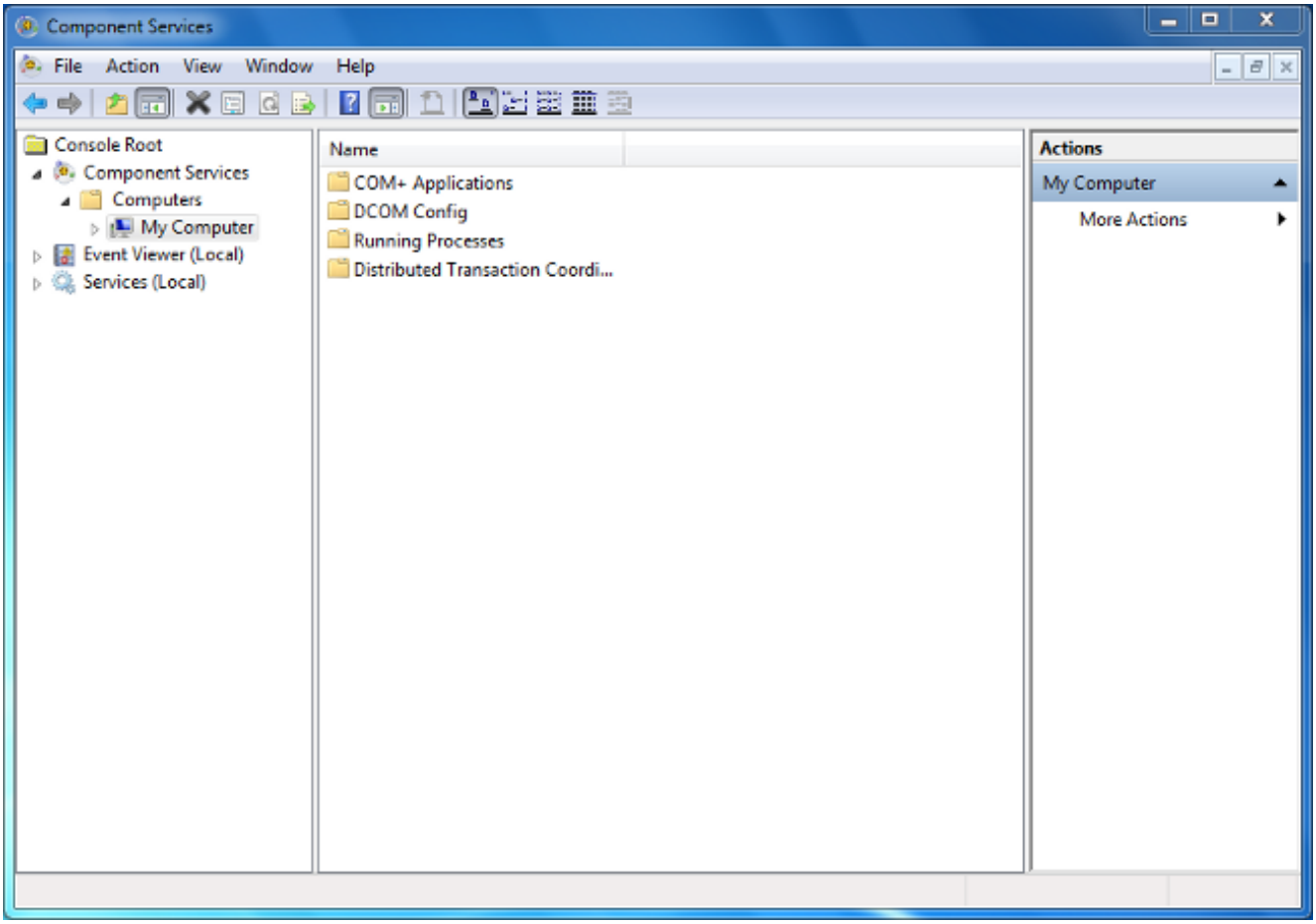
Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Se il problema persiste dopo la modifica della configurazione, aggiornare le impostazioni DCOM (Distributed Component Object Model) per consentire l'accesso remoto:

1. Scegliere il menu **Start**.

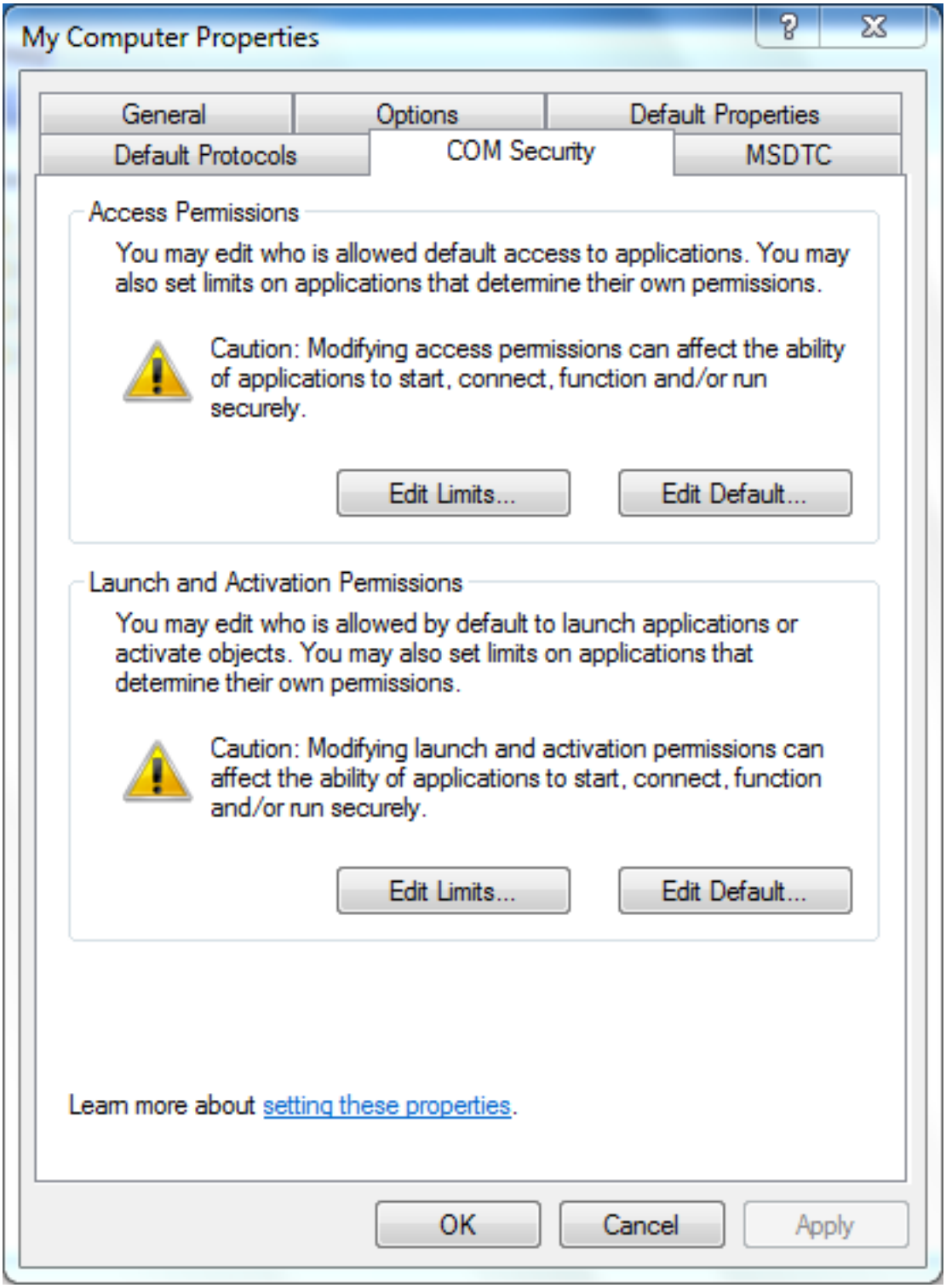
2. Fare clic su **Esegui** e immettere **DCOMCNFG**.

3. Fare clic su **OK**. Verrà visualizzata la finestra di dialogo Servizi componenti.



4. Nella finestra di dialogo Servizi componenti espandere **Servizi componenti**, **Computer**, fare clic con il pulsante destro del mouse su **Risorse del computer** e scegliere **Proprietà**.

5. Nella finestra di dialogo Proprietà - Risorse del computer fare clic sulla scheda **Protezione COM**.



6. In Autorizzazioni di avvio e attivazione fare clic su **Modifica limiti**.

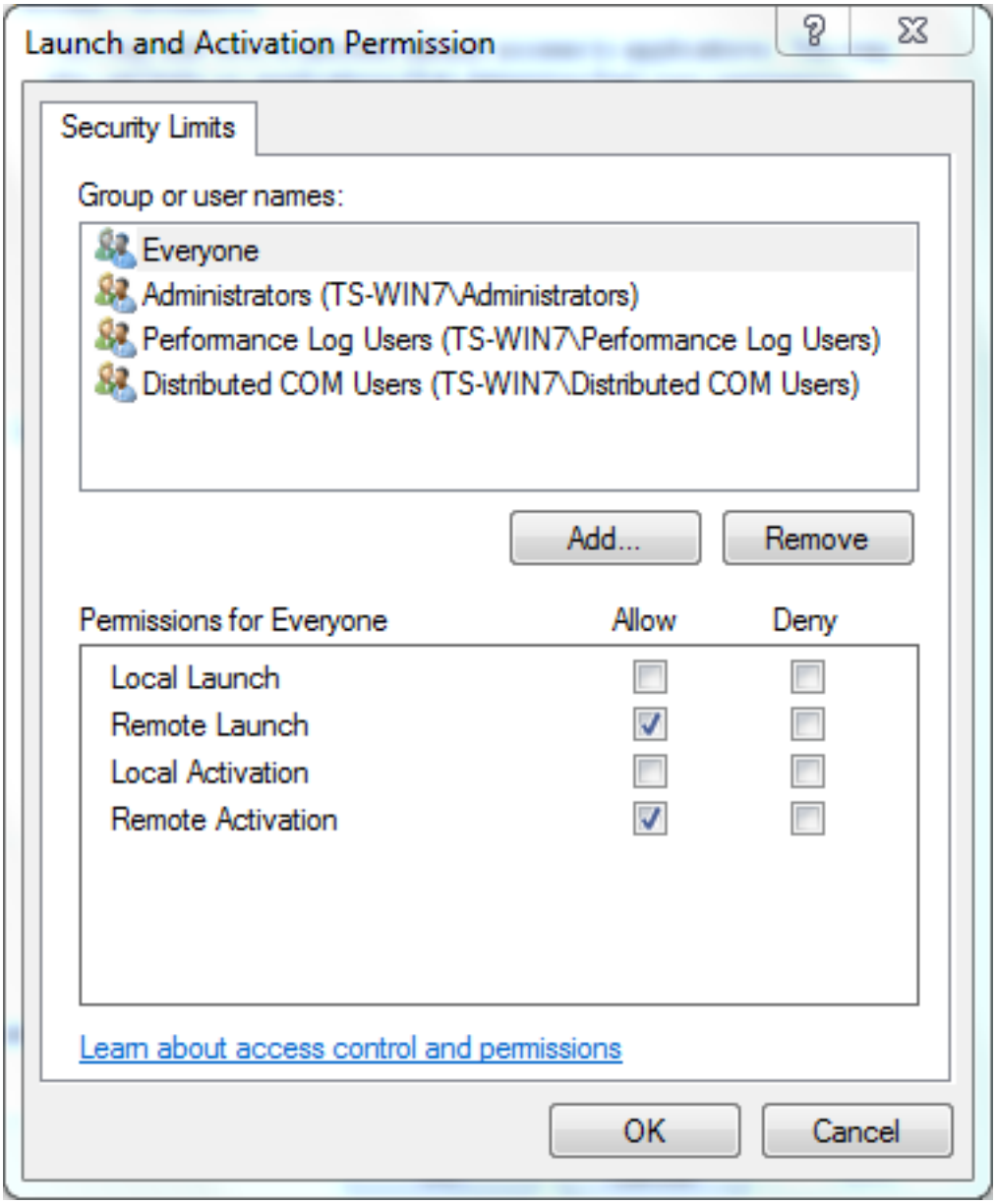
7. Nella finestra di dialogo Autorizzazioni di avvio e attivazione eseguire la procedura seguente se il proprio nome o il proprio gruppo non è visualizzato nell'elenco Gruppi o nomi utente:

   Nella finestra di dialogo Autorizzazioni di avvio e attivazione fare clic su **Aggiungi**.

   Nella finestra di dialogo Seleziona utenti, computer o gruppi immettere il proprio nome e il gruppo nel campo Immettere i nomi degli oggetti da selezionare e quindi fare clic su **OK**.

8. Nella finestra di dialogo Autorizzazione di avvio e attivazione selezionare l'utente e il gruppo

nella sezione **Utenti e gruppi**.



9. Nella colonna Consenti in Autorizzazioni per l'utente selezionare le caselle di controllo **Avvio remoto** e **Attivazione remota** e quindi fare clic su **OK**.**Nota:** Un nome utente deve disporre dei diritti per eseguire query sui dati di accesso utente in un server AD. Per eseguire l'autenticazione con un utente tramite proxy, immettere un nome utente completo. Per impostazione predefinita, il campo Dominio viene compilato automaticamente dal dominio dell'account utilizzato per accedere al computer in cui è stato installato l'agente. Se l'utente specificato è membro di un dominio diverso, aggiornare il dominio per le credenziali utente fornite.
10. Se il problema persiste, nel controller di dominio provare ad aggiungere l'utente nel criterio Gestione registro di controllo e di protezione. Per aggiungere l'utente, attenersi alla seguente procedura:

    Scegliere l'**Editor Gestione Criteri di gruppo**.

    Scegliere Configurazione computer > **Impostazioni di Windows** > **Impostazioni protezione** > **Criteri locali** > **Assegnazione diritti utente**.

Scegliere **Gestisci registro di controllo e di protezione**.

Aggiungere l'utente.