Minimale toestemming voor een actieve gebruikersaccount van de map die door de Sourcefire-gebruikersagent is gebruikt

Inhoud

Inleiding

Dit document beschrijft hoe een actieve gebruiker van de Map (AD) de minimale rechten moet krijgen om de AD-domeincontroller te vragen. De Sourcefire-gebruikersagent gebruikt een AD-gebruiker om de AD-domeincontroller te vragen. Om een query uit te voeren heeft een AD-gebruiker geen extra rechten nodig.

Voorwaarden

Vereisten

Cisco vereist dat u de Sourcefire User Agent op een Microsoft Windows-systeem installeert en toegang tot de AD-domeincontroller biedt.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

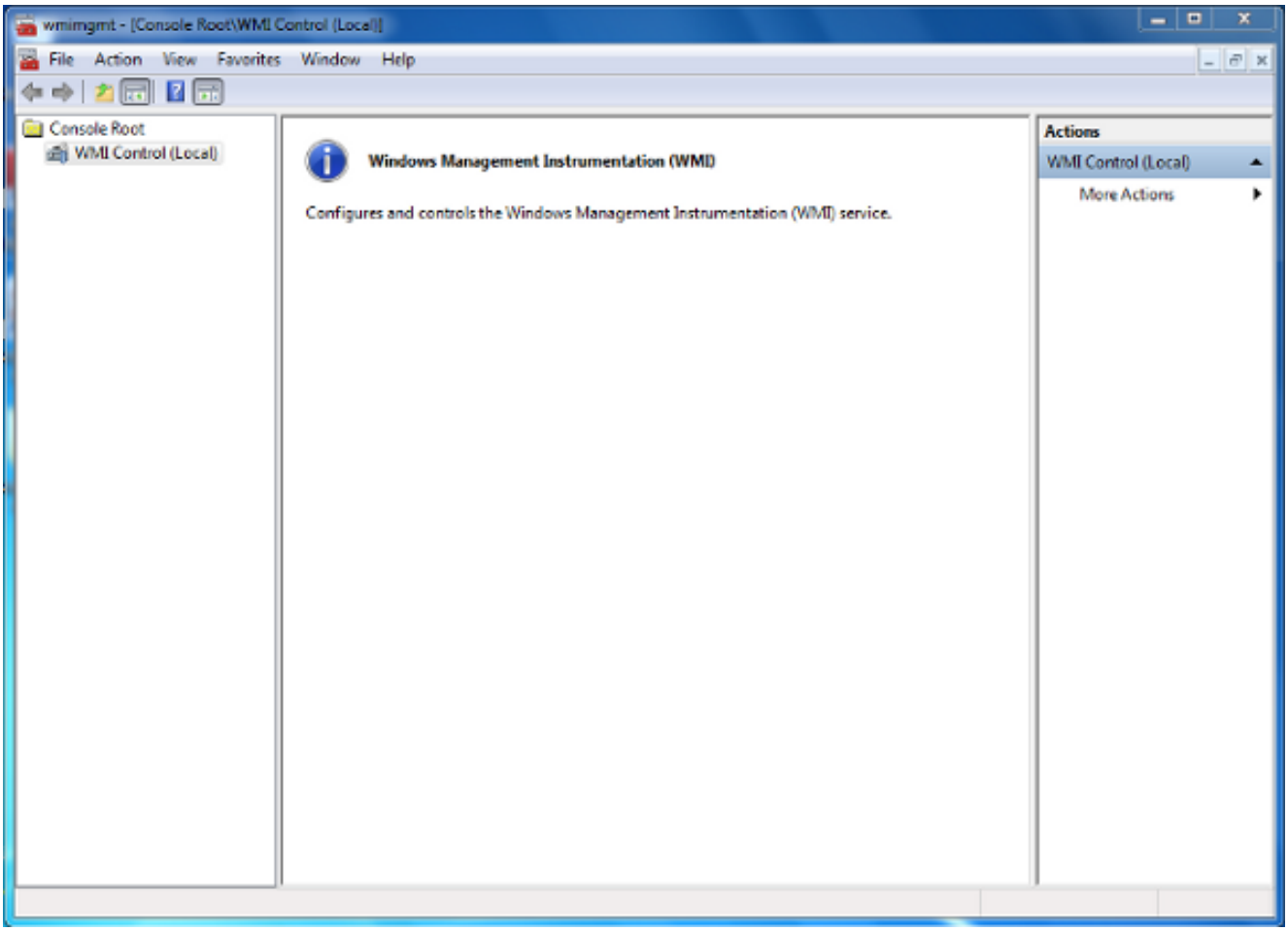
Eerst moet een beheerder een nieuwe AD gebruiker speciaal maken voor de toegang tot de gebruikersagent. Als deze nieuwe gebruiker geen lid is van de groep van de domeinbeheerders (en zij zouden niet moeten zijn), zou de gebruiker expliciet toestemming kunnen moeten worden verleend om tot de veiligheidslogbestanden van Windows Management Instrumentation (WMI) toegang te hebben. Voltooi de volgende stappen om toestemming te geven:

1. Open de WMI-beheerconsole:

   Kies in de AD server het menu **Start**.

   Klik op **Uitvoeren** en voer **wmimgmt.msc in**.

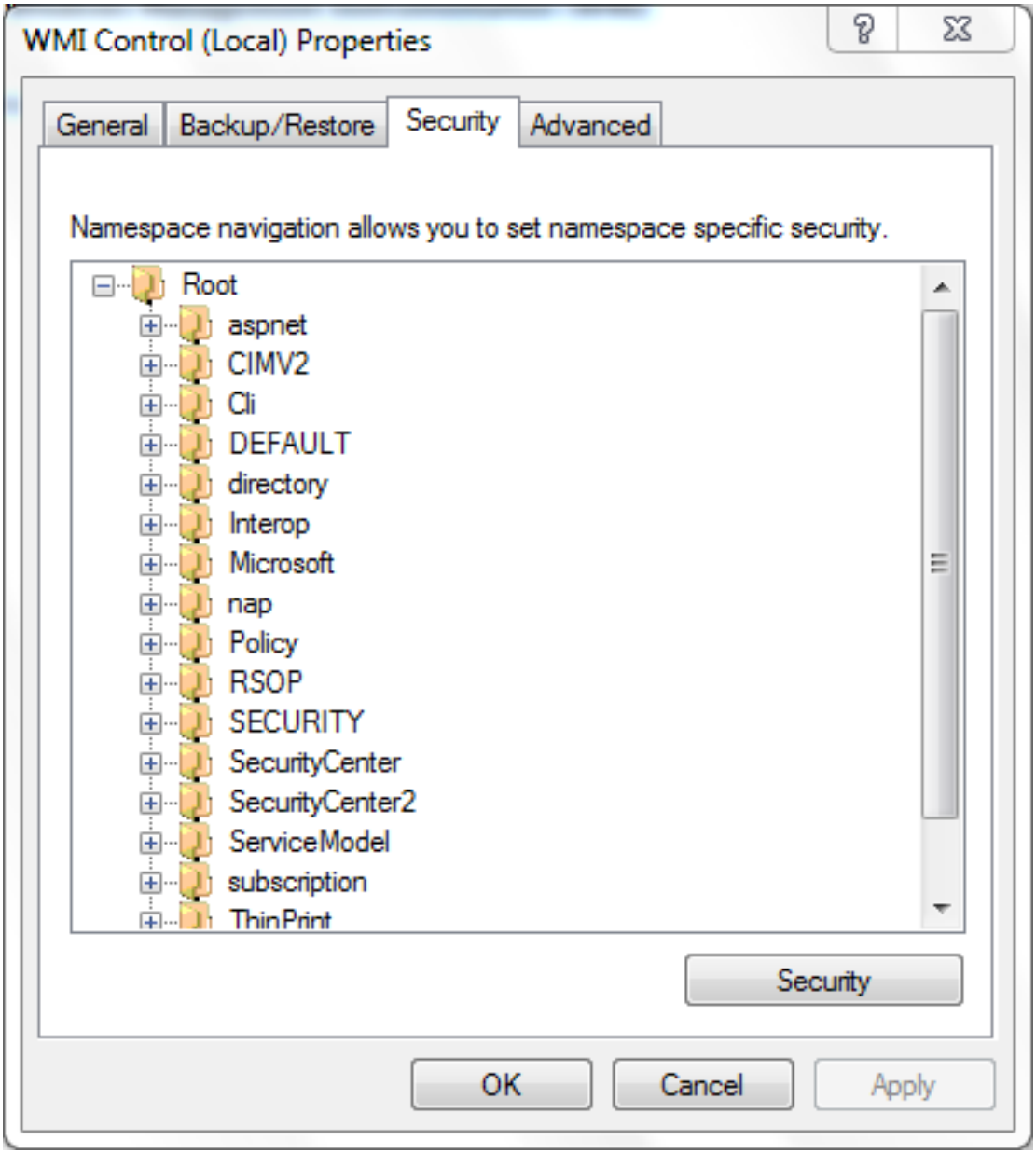
   Klik op **OK**. De WMI-Control Console verschijnt.



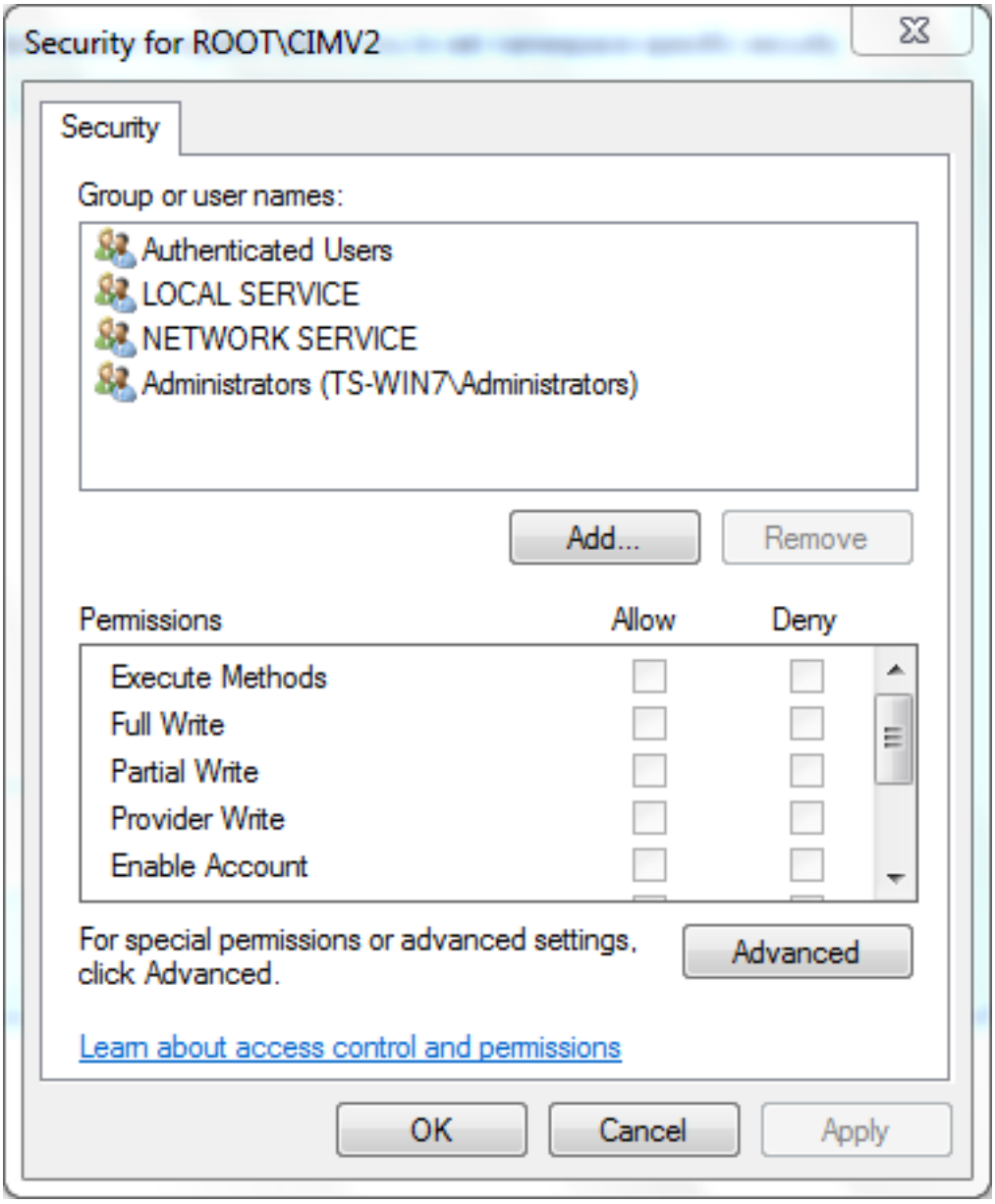
2. Klik in de WMI-console-boom met de rechtermuisknop op **WMI-regeling** en klik vervolgens op **Eigenschappen**.

3. Klik op het tabblad **Beveiliging**.

4. Selecteer de naamruimte waarvoor u een gebruiker of groep toegang wilt geven (`Root\CIMV2`) en klik vervolgens op **Beveiliging**.



5. Klik in het dialoogvenster Beveiliging op **Toevoegen**.



6. In het dialoogvenster Gebruikers, computers of groepen selecteren voert u de naam in van het object (gebruiker of groep) dat u wilt toevoegen. Klik op **Naam controleren** om de ingang te controleren en vervolgens op **OK** te klikken. U kunt de locatie moeten wijzigen of op **Geavanceerd** klikken om naar objecten te vragen. Zie de Context-gevoelige help (**?**) voor meer informatie.

7. In het dialoogvenster Beveiliging kiest u in het gedeelte Toestemmingen **Toestaan** of **ontkennen** om de nieuwe gebruiker of groep toestemming te geven (waarmee u het gemakkelijkst alle toegangsrechten kunt geven). De gebruiker moet ten minste de toestemming **Remote Enable** hebben gegeven.

8. Klik op **Toepassen** om wijzigingen op te slaan. Sluit het venster.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

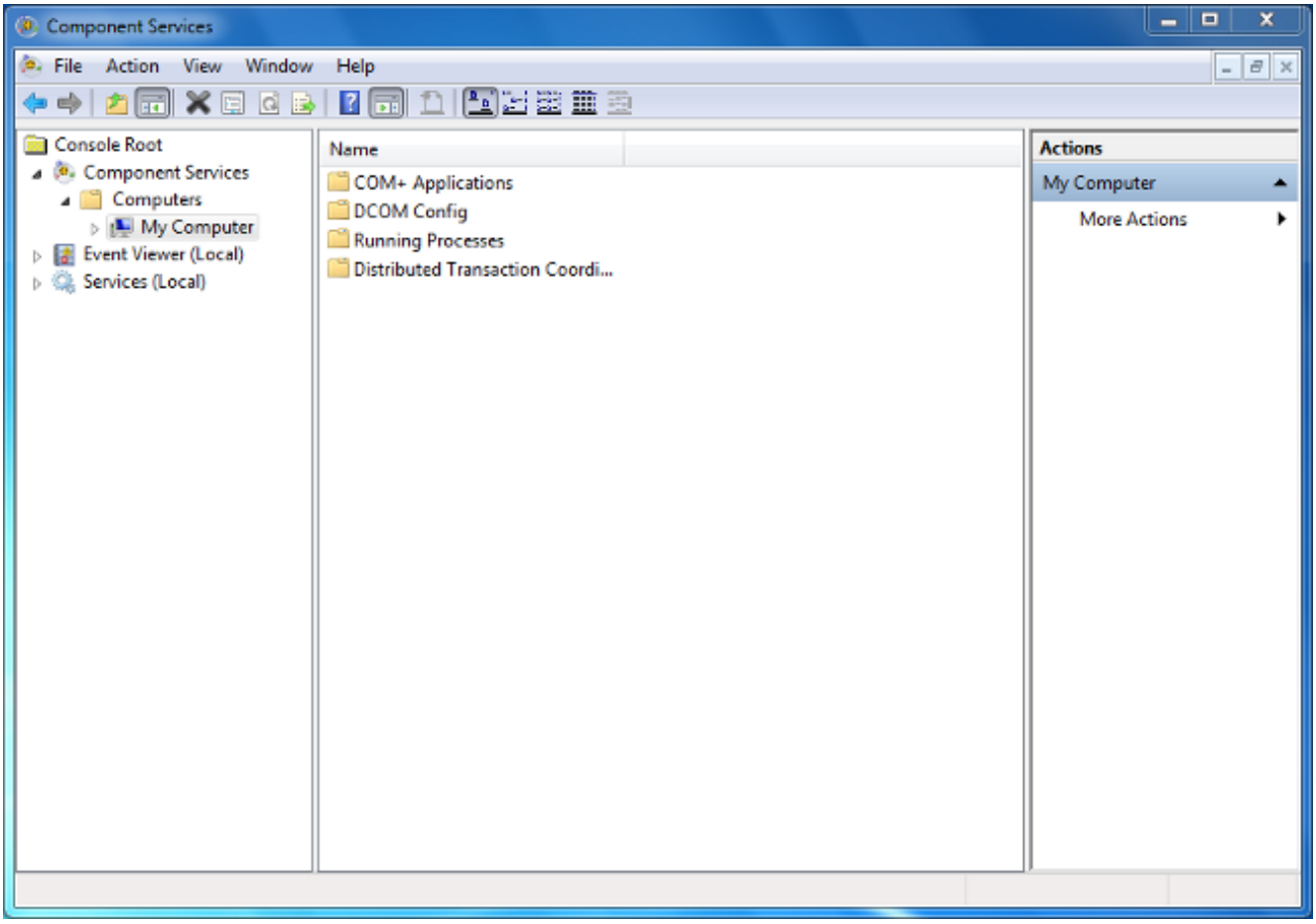
Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Als een probleem blijft bestaan na het wijzigen van de configuratie, update de instellingen van het Gedistribueerde Component Object Model (DCOM) om toegang op afstand mogelijk te maken:

1. Kies het menu **Start**.

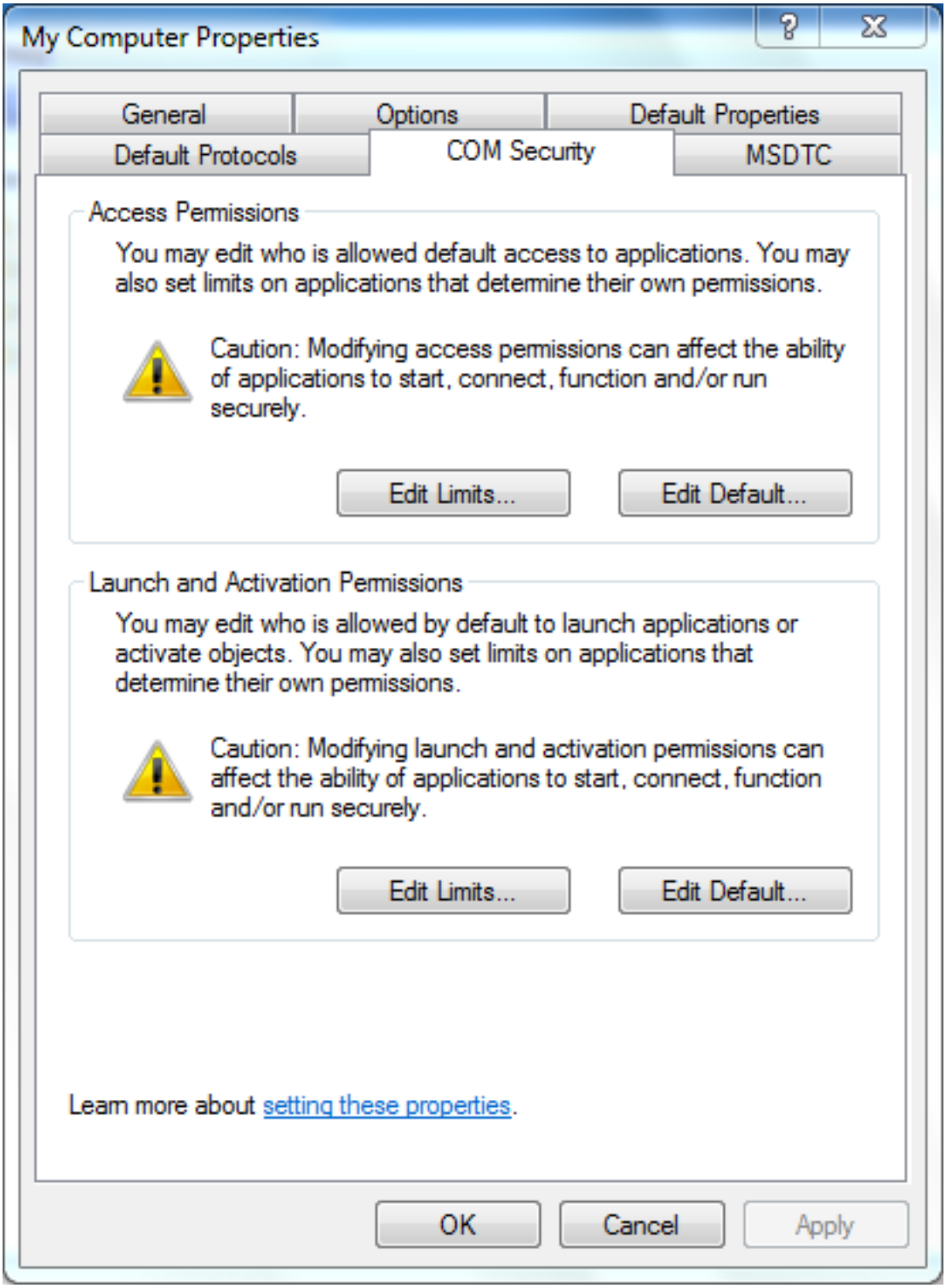
2. Klik op **Uitvoeren** en voer **DCOMCNFG in**.

3. Klik op **OK**. Het dialoogvenster Component-services verschijnt.



4. Wilt u in het dialoogvenster **Component Services** uitvouwen, **Component Services** uitvouwen, **Computers** uitvouwen en dan met de rechtermuisknop op **Mijn computer** en **Eigenschappen** kiezen.

5. Klik in het dialoogvenster Mijn computereigenschappen op het tabblad **COM Security**.



6. Klik onder **Limieten** starten en activeren op **Bewerken**.

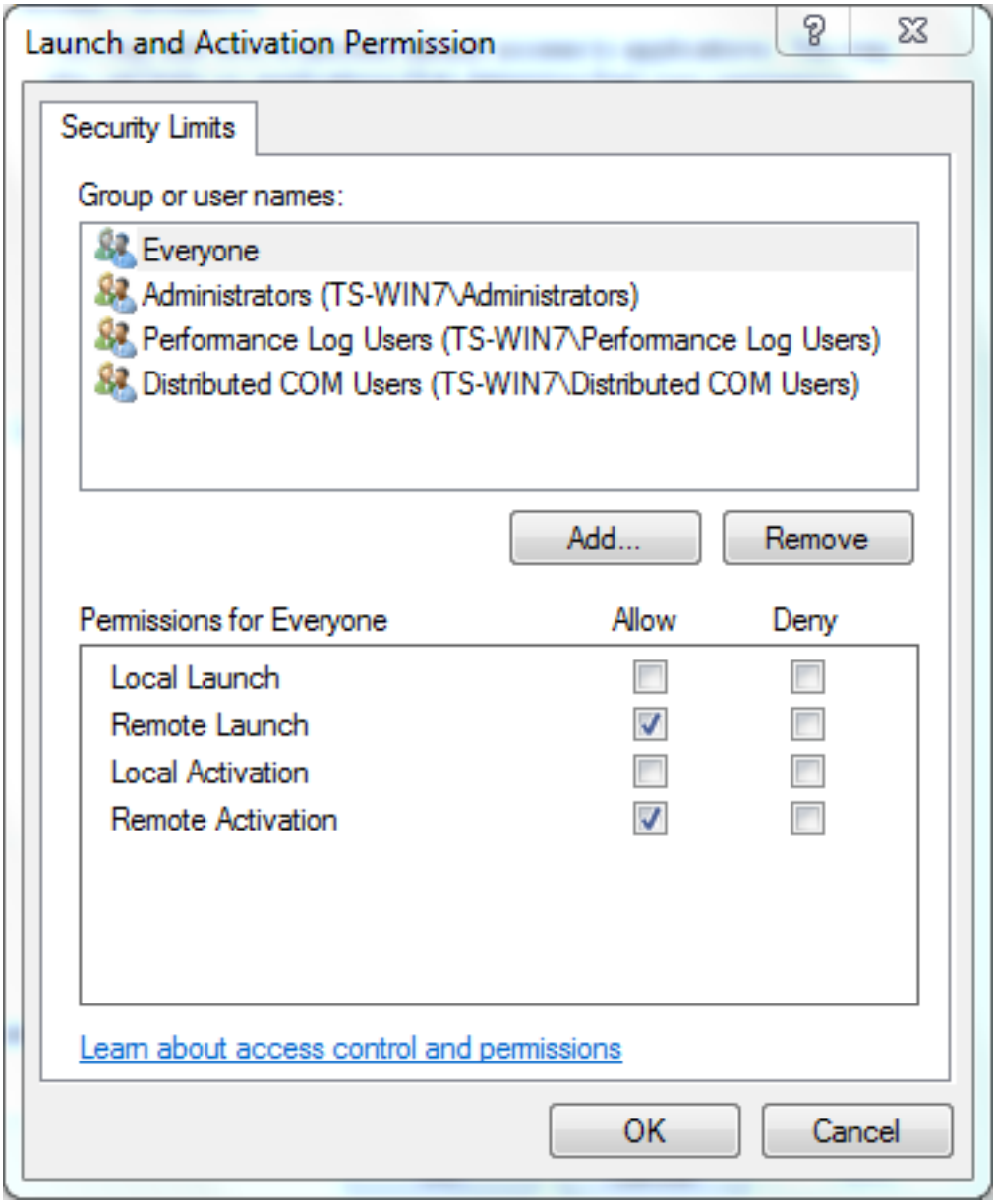
7. Voltooi de volgende stappen in het dialoogvenster Start en Activeringsvergunning als uw naam of uw groep niet in de lijst Groepen of gebruikersnamen verschijnt:

   Klik in het dialoogvenster Toegang starten en activeren op **Toevoegen**.

   Typ in het dialoogvenster Gebruikers, computers of groepen selecteren uw naam en de groep in het veld Voer de doelnamen in om het veld te selecteren en klik vervolgens op **OK**.

8. Selecteer uw gebruiker en groep in het gedeelte **Group of** de **gebruikersnamen** in het

dialoogvenster Toegang tot **de** computer **en** activering.



9. In de kolom Accessoire onder Instellingen voor gebruiker, controleer de vinkjes **Afstandsbediening** en **Afstandsactivering** en klik vervolgens op **OK**.Opmerking: Een gebruikersnaam moet rechten hebben om gebruikersloggegevens op een AD-server te kunnen vragen. Als u een gebruiker via proxy wilt authenticeren, voert u een volledig gekwalificeerde gebruikersnaam in. Standaard wordt het domein van de account dat u aan de computer hebt gebruikt waarop u de Agent hebt geïnstalleerd, automatisch ingevuld. Als een gebruiker die u levert een lid van een ander domein is, update het domein voor de meegeleverde gebruikersreferenties.
10. Als het probleem zich blijft voordoen, probeert u op de Domain Controller de gebruiker toe te voegen in het beleid voor het beheren van de audit en het veiligheidslogboek. Voltooi de volgende stappen om de gebruiker toe te voegen:

    Kies de **redacteur voor groepsbeheer**.

    Kies **computerconfiguratie >Windows-instellingen > beveiligingsinstellingen > Lokaal beleid > toewijzing van gebruikersrechten.**

Kies **Auditing en beveiligingslogbestand beheren**.

Voeg de gebruiker toe.