Permiso mínimo de Grant a una cuenta de usuario del Active Directory usada por el agente de usuario de Sourcefire

Contenido

Introducción

Este documento describe cómo proporcionar a un usuario del Active Directory (AD) con los permisos mínimos necesarios para preguntar el controlador de dominio AD. El agente de usuario de Sourcefire utiliza a un usuario AD para preguntar el controlador de dominio AD. Para realizar una interrogación, un usuario AD no requiere ningunos permisos adicionales.

Prerrequisitos

Requisitos

Cisco requiere que usted instale el agente de usuario de Sourcefire en un sistema de Microsoft Windows y proporcione el acceso al controlador de dominio AD.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

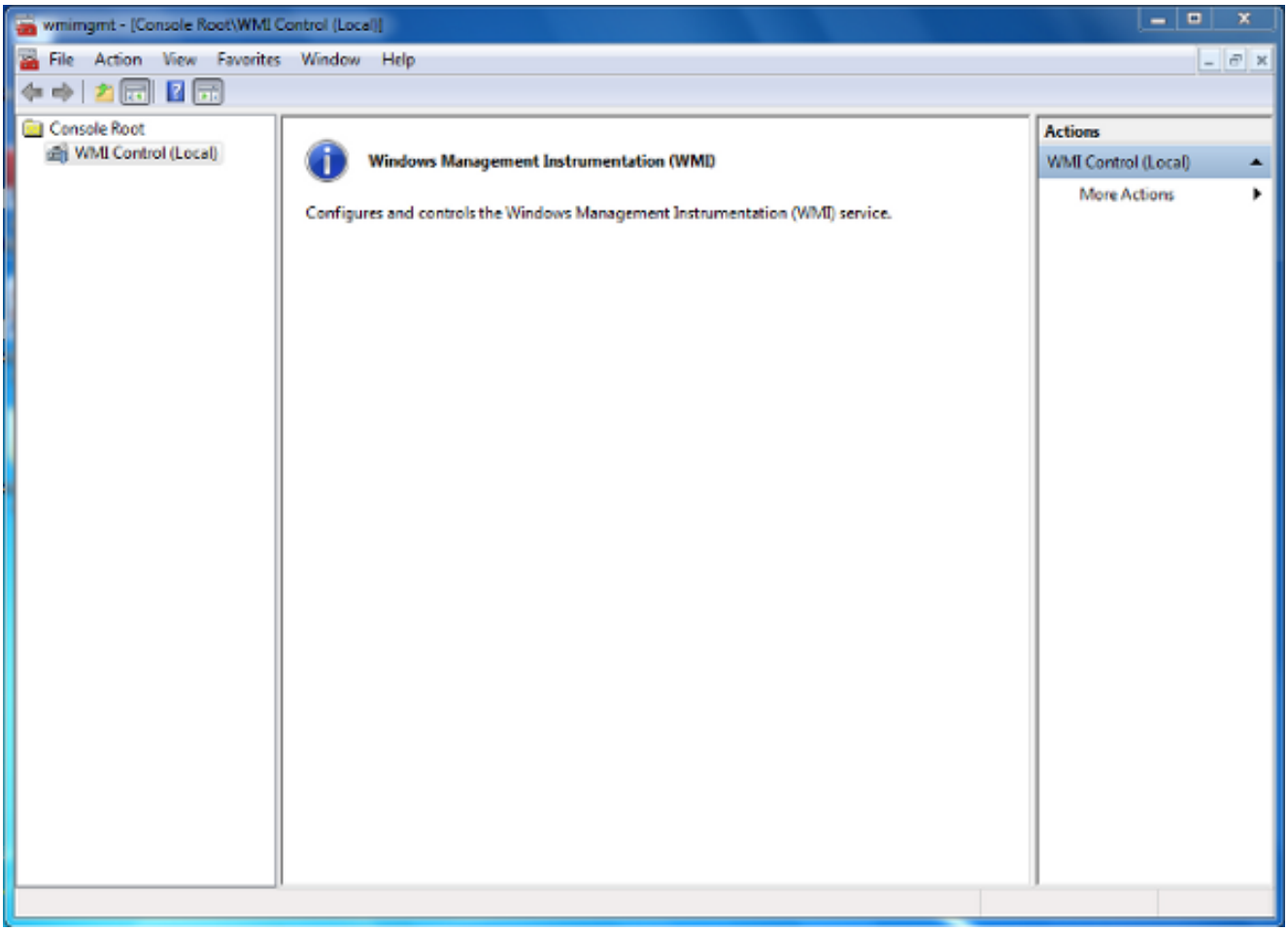
Primero, un administrador debe crear a un nuevo usuario AD específicamente para el acceso del agente de usuario. Si este usuario nuevo no es un miembro del grupo de los administradores de dominio (y ellos no debe ser), el usuario pudo tener que ser concedido explícitamente el permiso para acceder los registros de seguridad de Windows Management Instrumentation (WMI). Para conceder el permiso, complete estos pasos:

1. Abra la consola de control WMI:

   En el servidor AD, elija el **menú Inicio**.

   Haga clic el **funcionamiento** y ingrese **wmimgmt.msc.**

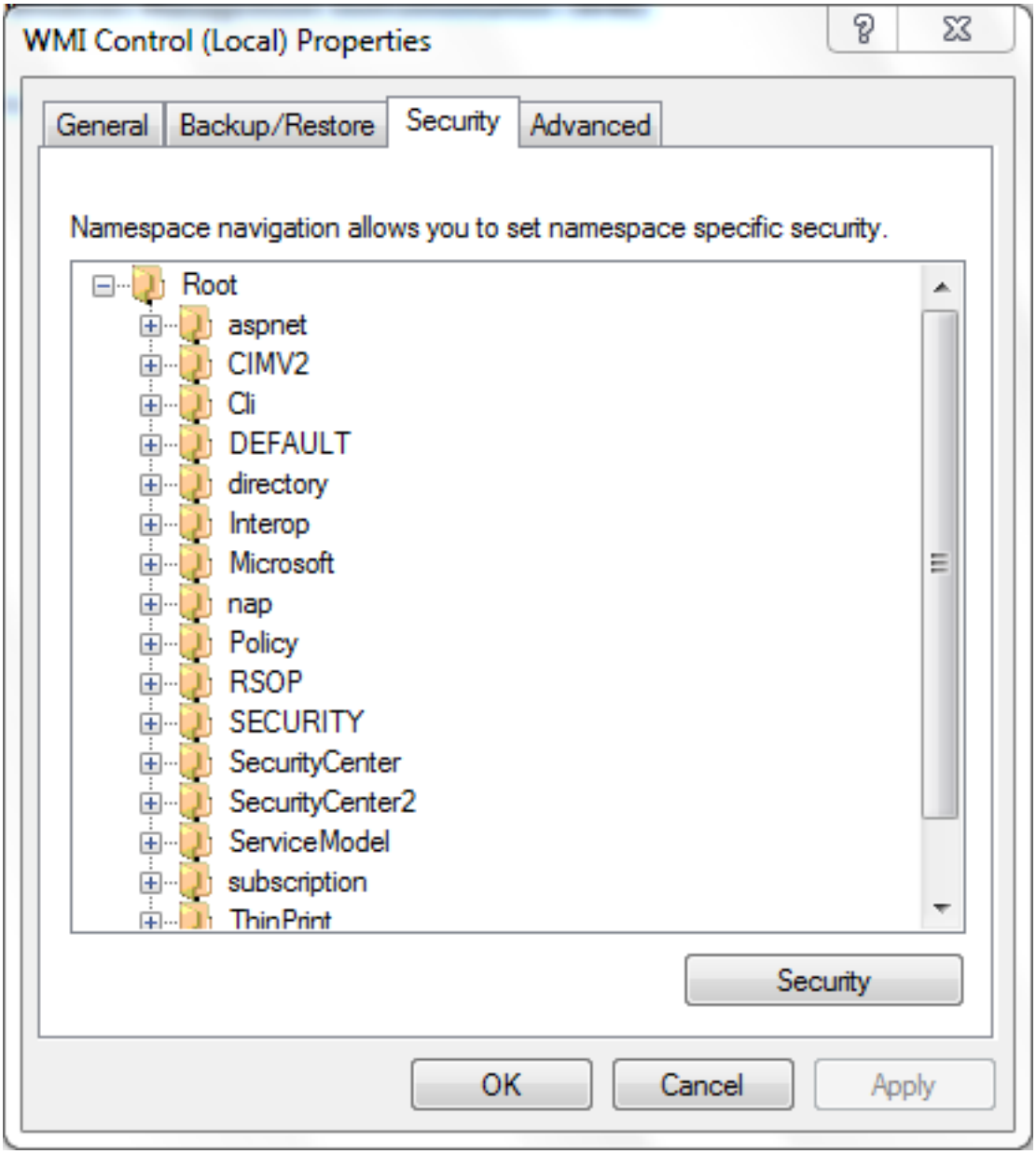
   Haga clic en OK. La consola de control WMI aparece.



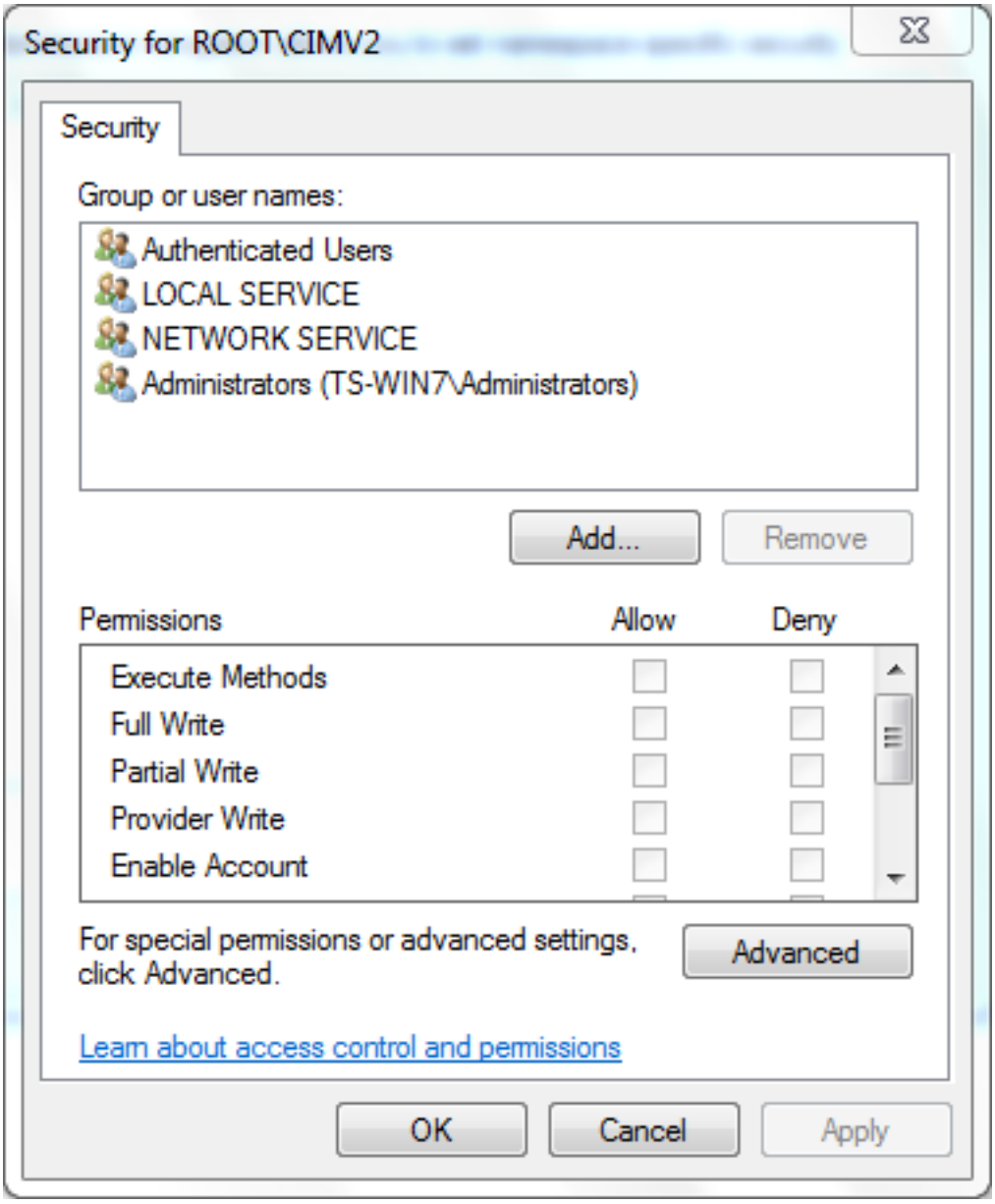
2. En el árbol de la consola WMI, el **control del** click derecho **WMI** y entonces hace clic las **propiedades**.

3. Haga clic en la ficha Security (Seguridad).

4. Seleccione el namespace para el cual usted quiere dar un acceso del usuario o del grupo (`Root\CIMV2`), y después haga clic la **Seguridad**.



5. En el cuadro de diálogo de la Seguridad, haga click en Add



6. En la casilla de diálogo Seleccionar usuarios, computadoras o grupos, ingrese el nombre del objeto (usuario o grupo) ese usted quieren agregar. Haga clic los **nombres del control** para verificar su entrada y después hacer clic la **AUTORIZACIÓN**. Usted puede ser que tenga que cambiar la ubicación o hacer clic **avanzado** para preguntar para los objetos. Vea la ayuda sensible al contexto (**?**) para más detalle.

7. En el cuadro de diálogo de la Seguridad, en la sección de los permisos, elija **permiten** o **niegan** para conceder los permisos al usuario nuevo o al grupo (más fácil dar todos los permisos). El usuario debe ser dado por lo menos el permiso **remoto del permiso**.

8. El tecleo **se aplica** para salvar los cambios. Cerrar ventana

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

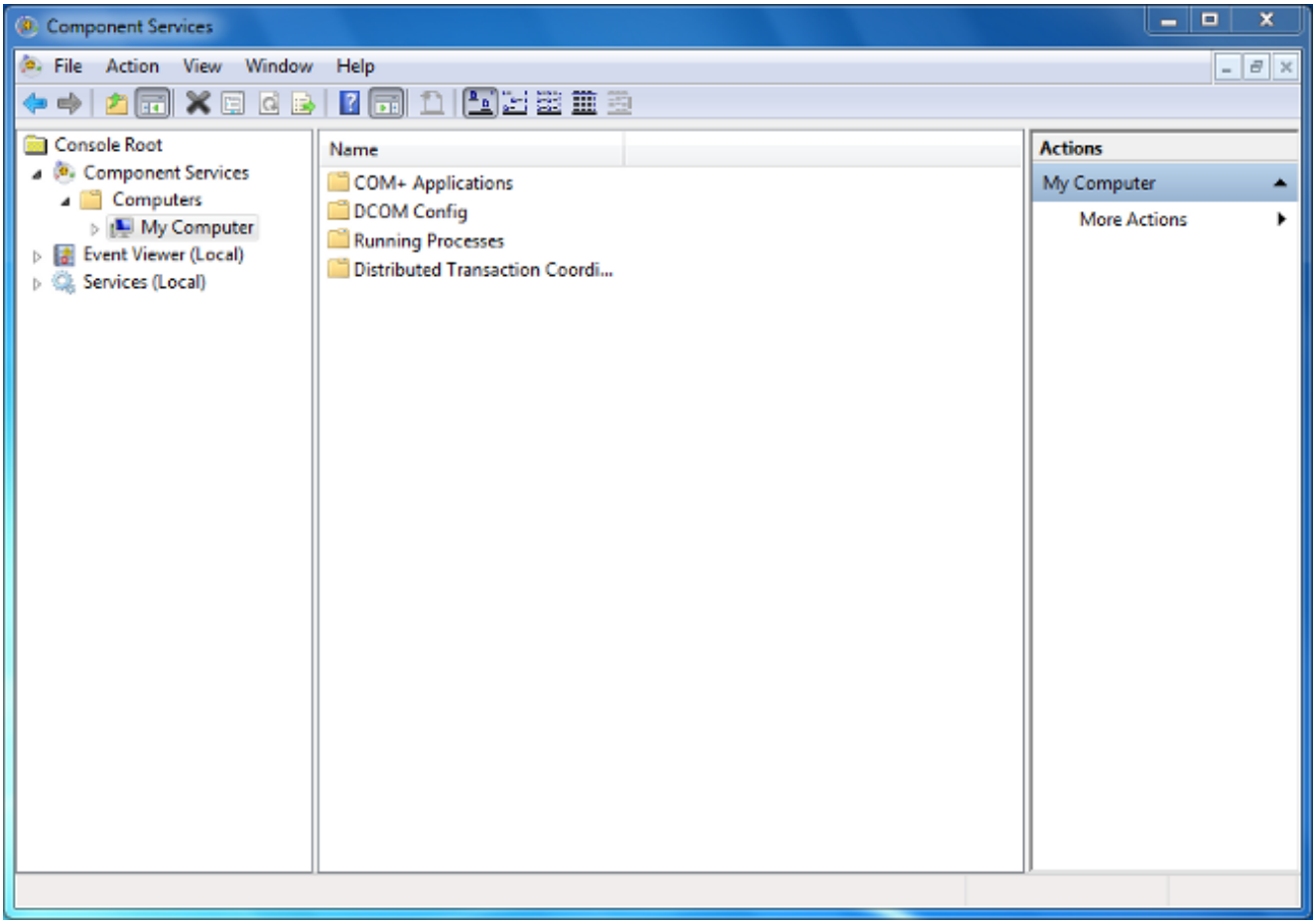
En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Si un problema persiste después de los cambios de configuración, ponga al día las configuraciones del Modelo de objeto de componente distribuido (DCOM) para permitir el Acceso Remoto:

1. Elija el **menú Inicio**.

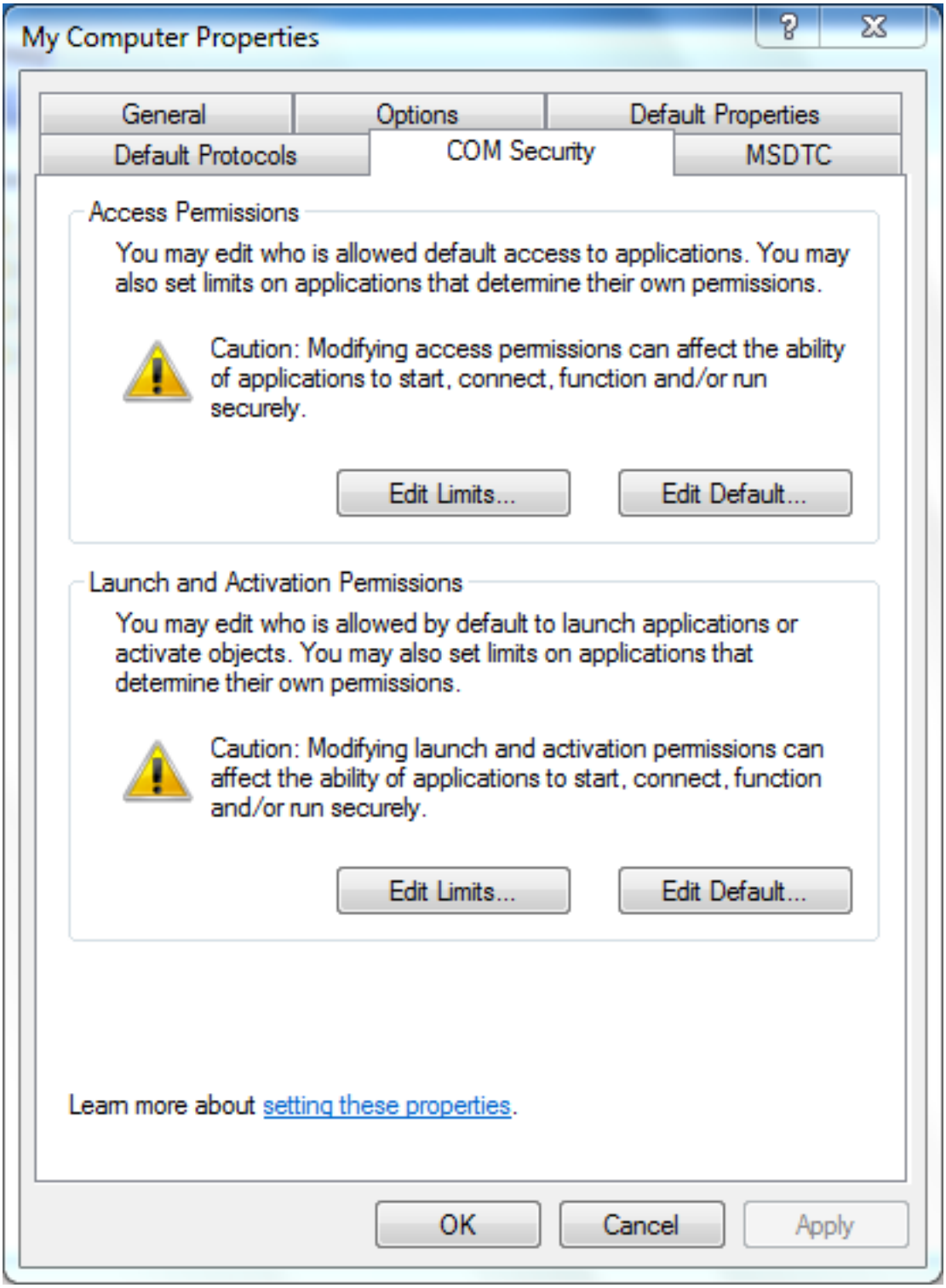
2. Haga clic el **funcionamiento** y ingrese **DCOMCNFG**.

3. Haga clic en OK. El cuadro de diálogo de los servicios del componente aparece.



4. En el cuadro de diálogo de los servicios del componente, amplíe los **servicios del componente**, amplíe las **Computadoras**, y entonces haga clic con el botón derecho del ratón el **mi PC** y elija las **propiedades**.

5. En el cuadro de diálogo Propiedades del mi PC, haga clic la **ficha de seguridad COM**.



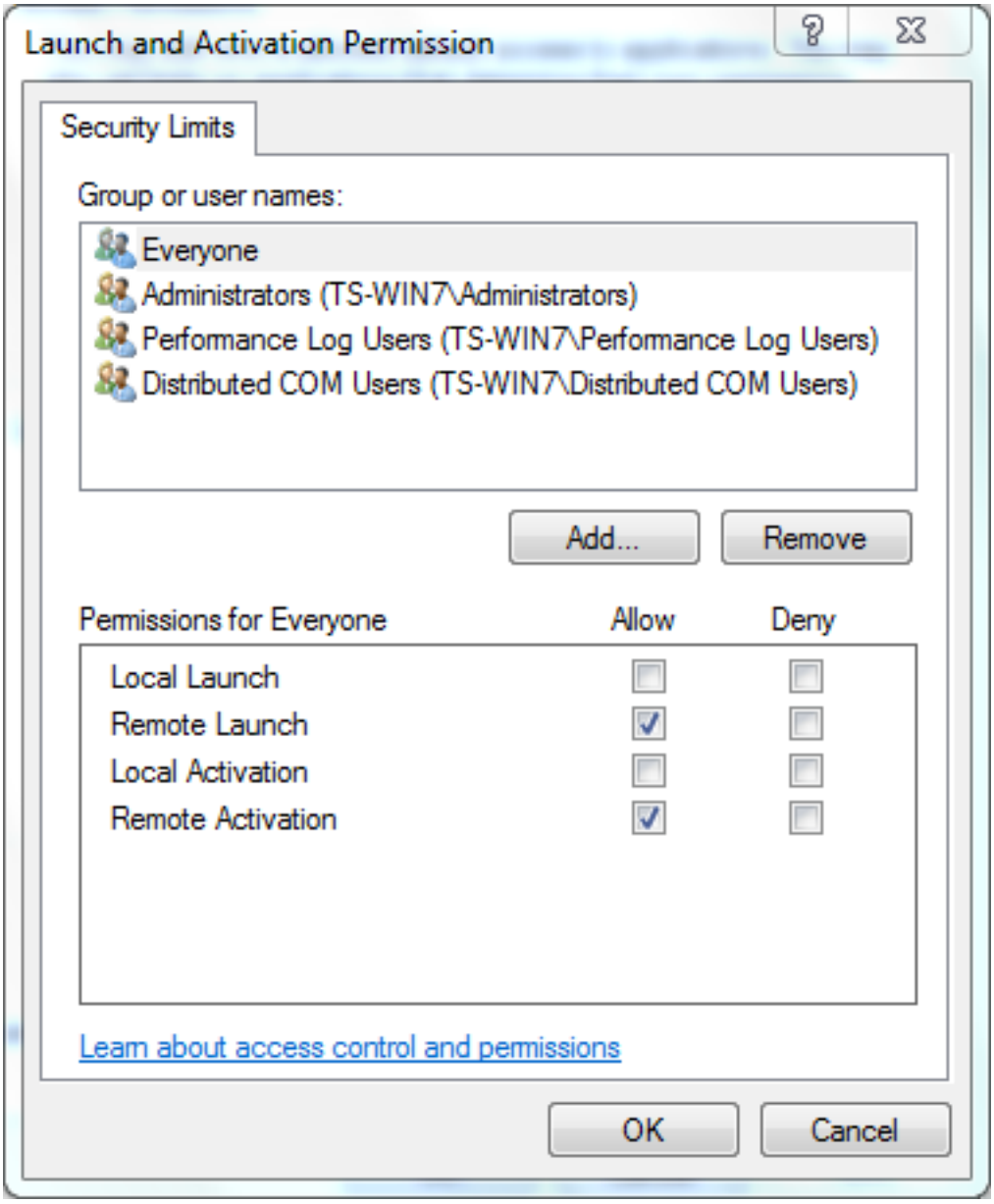
6. Conforme a los permisos del lanzamiento y de la activación, el tecleo **edita los límites**.

7. En el lanzamiento y el cuadro de diálogo del permiso de la activación, complete estos pasos si su nombre o su grupo no aparece en los grupos o la lista de Nombres de usuario:

   En el lanzamiento y el cuadro de diálogo del permiso de la activación, haga click en Add

   En la casilla de diálogo Seleccionar usuarios, computadoras o grupos, ingrese su nombre y al grupo en el ingresar los nombres del objeto para seleccionar el campo, y después haga clic la **AUTORIZACIÓN**.

8. En el lanzamiento y el cuadro de diálogo del permiso de la activación, seleccione a su usuario y agrúpelo en el **grupo o la** sección de los **Nombres de usuario**.



9. En la columna de la permit bajo los permisos para el usuario, marque las casillas de verificación **remotas de la activación del lanzamiento** y del **telecontrol**, y después haga clic la **AUTORIZACIÓN**.Nota: Un Nombre de usuario debe tener derechos de preguntar para los datos del ingreso del usuario al sistema sobre un servidor AD. Para autenticar con un usuario vía el proxy, ingrese un Nombre de usuario calificado completamente. Por abandono, el dominio para la cuenta que usted registraba en el ordenador donde usted instaló el agente auto-puebla el campo del dominio. Si un usuario que usted suministra es un miembro de un diverso dominio, pone al día el dominio para los credenciales de usuario suministrados.
10. Si persiste el problema, en el intento del controlador de dominio para agregar al usuario en la directiva del registro de seguridad y auditoría del manejo. Para agregar al usuario, complete estos pasos:

    Elija el **editor de la Administración de políticas del grupo**.

Elija el **Computer Configuration (Configuración de la computadora) > Windows Settings (Configuración de Windows) > Security Settings (Configuración de seguridad)** > las **políticas locales** > la **asignación de derechos de usuario**.

Elija **manejan el registro de seguridad y auditoría**.

Agregue al usuario.