Conceder permiso mínimo a una cuenta de usuario de Active Directory utilizada por el agente de usuario de Sourcefire

Contenido

Introducción

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

Prerequisites

Requirements

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

Componentes Utilizados

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

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.

Configurar

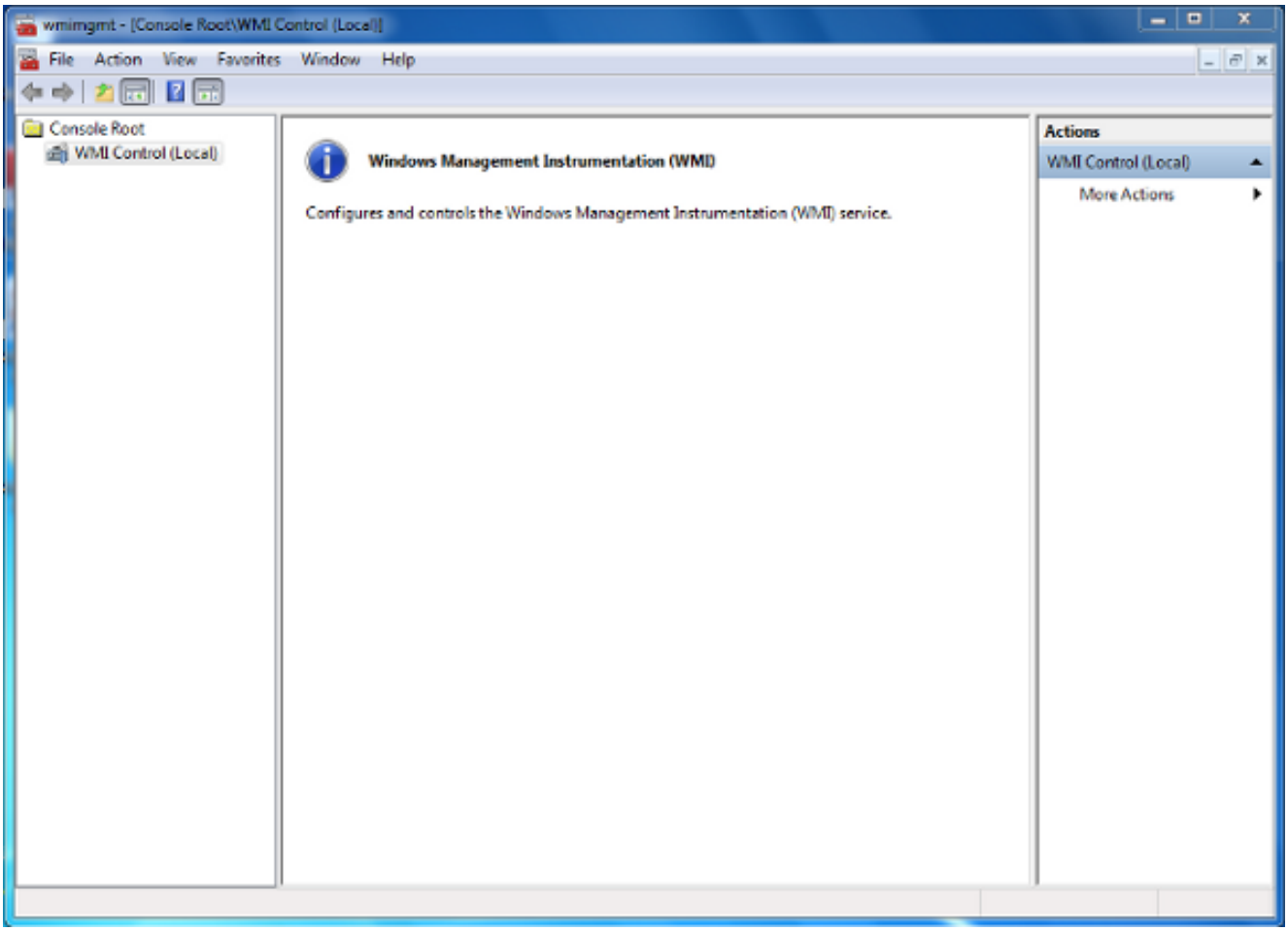
En primer lugar, un administrador debe crear un nuevo usuario AD específicamente para el acceso de agente de usuario. Si este nuevo usuario no es miembro del grupo de administradores de dominio (y no debería serlo), es posible que se deba conceder explícitamente al usuario permiso para acceder a los registros de seguridad de Windows Management Instrumentation (WMI). Para conceder permiso, complete estos pasos:

1. Abra la consola de control WMI:

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

   Haga clic en **Ejecutar** e ingrese **wmimgmt.msc**.

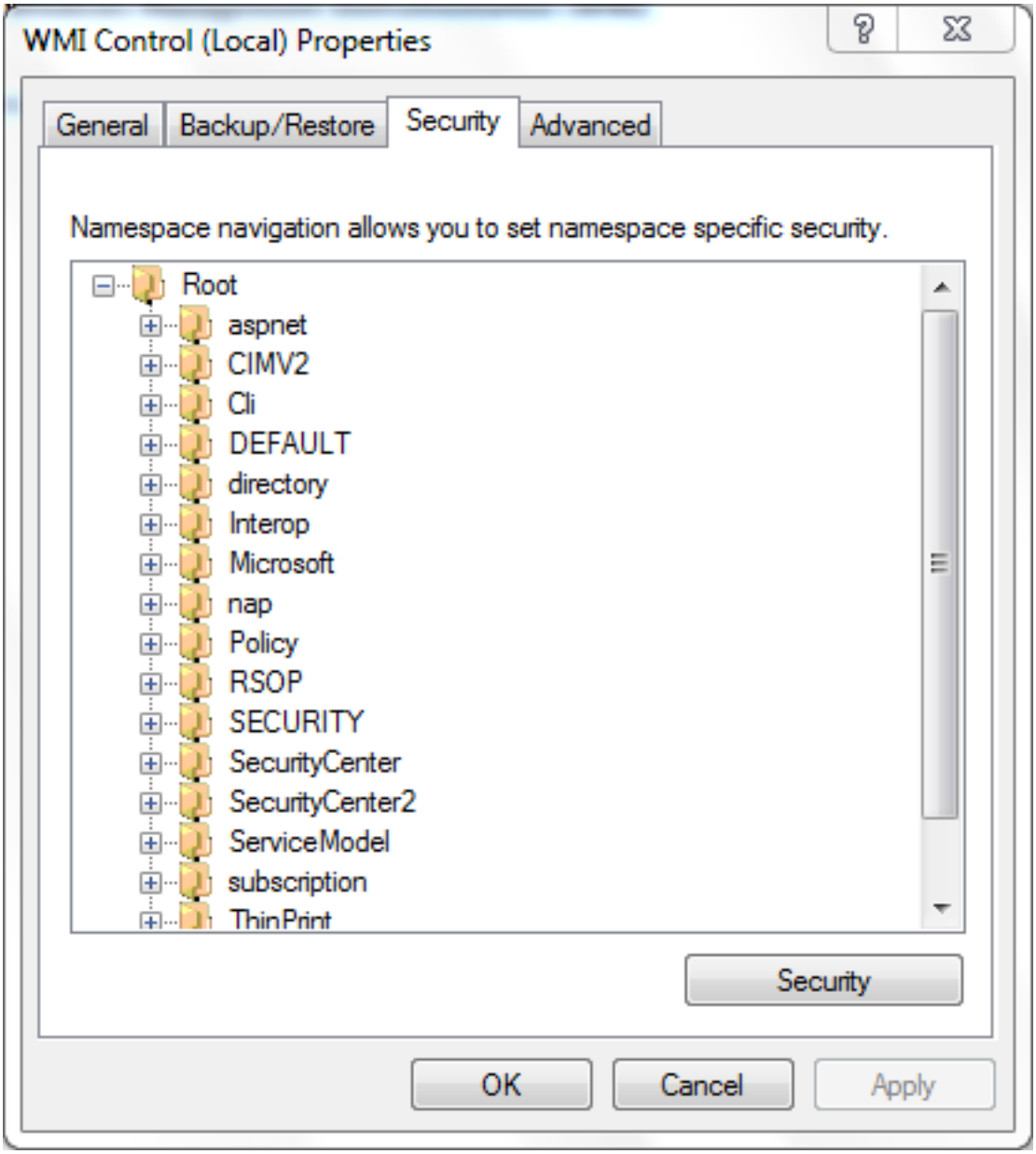
   Click OK. Aparece la consola de control WMI.



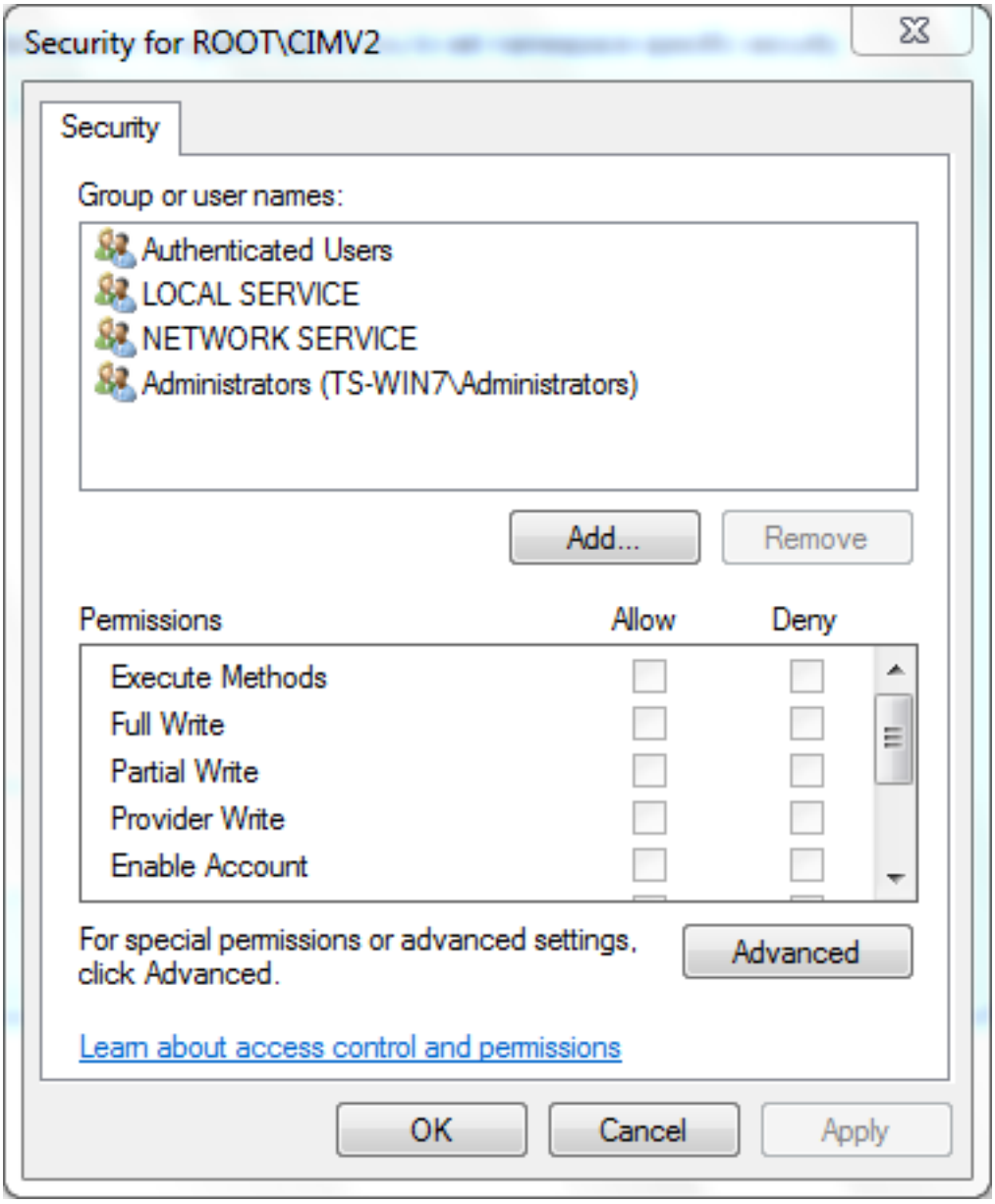
2. En el árbol de la consola WMI, haga clic con el botón secundario del mouse en **Control WMI** y, a continuación, haga clic en **Propiedades**.

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

4. Seleccione el espacio de nombres para el que desea otorgar acceso a un usuario o grupo (`Root\CIMV2`) y, a continuación, haga clic en **Security**.



5. En el cuadro de diálogo Seguridad, haga clic en **Agregar**.



6. En el cuadro de diálogo Seleccionar usuarios, equipos o grupos, introduzca el nombre del objeto (usuario o grupo) que desea agregar. Haga clic en **Verificar nombres** para verificar su entrada y luego haga clic en **Aceptar**. Puede que tenga que cambiar la ubicación o hacer clic en **Avanzadas** para consultar los objetos. Consulte la ayuda contextual (**?**) para obtener más información.

7. En el cuadro de diálogo Seguridad, en la sección Permisos, elija **Permitir** o **Denegar** para conceder permisos al nuevo usuario o grupo (lo más fácil es otorgar todos los permisos). Se debe dar al usuario al menos el permiso **Remote Enable**.

8. Haga clic en **Aplicar** para guardar los cambios. Cerrar ventana

Verificación

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

Troubleshoot

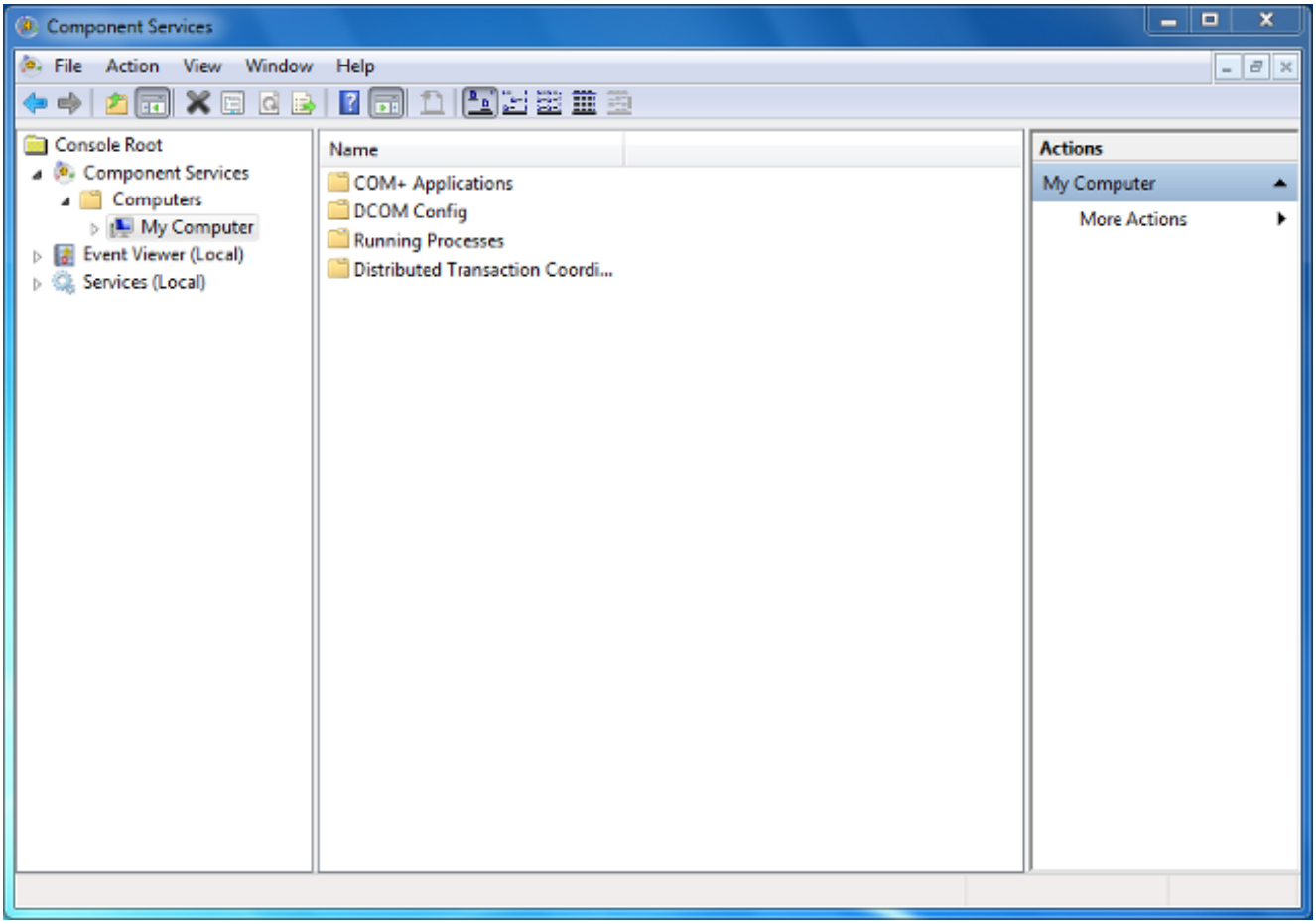
En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Si un problema persiste después de los cambios de configuración, actualice la configuración del Modelo de objetos componentes distribuidos (DCOM) para permitir el acceso remoto:

1. Elija el menú **Inicio**.

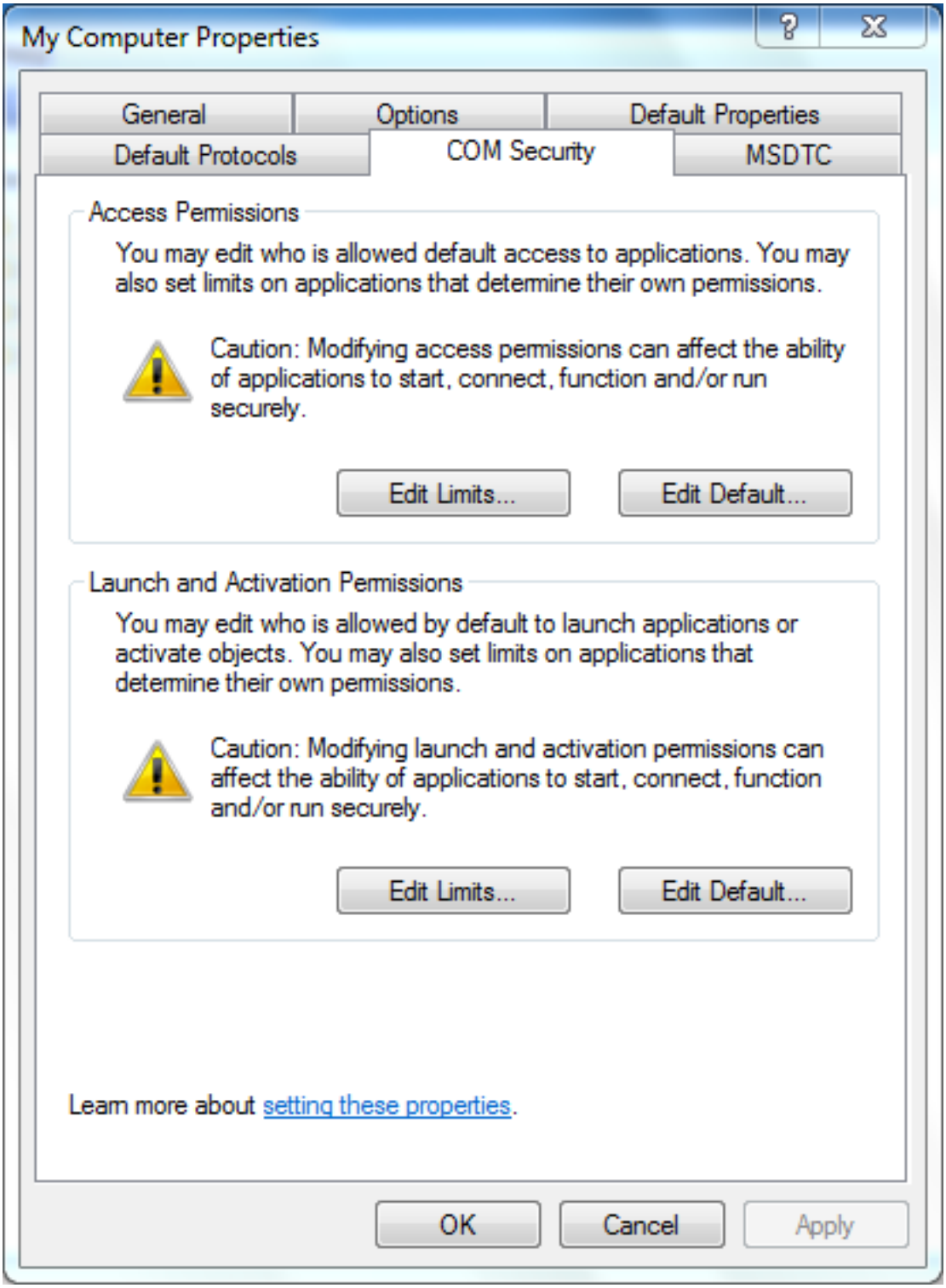
2. Haga clic en **Ejecutar** e introduzca **DCOMCNFG**.

3. Click OK. Aparecerá el cuadro de diálogo Servicios de componentes.



4. En el cuadro de diálogo Servicios de componentes, expanda **Servicios de componentes**, expanda **Equipos** y, a continuación, haga clic con el botón derecho en **Mi PC** y elija **Propiedades**.

5. En el cuadro de diálogo Propiedades de mi equipo, haga clic en la ficha **Seguridad COM**.



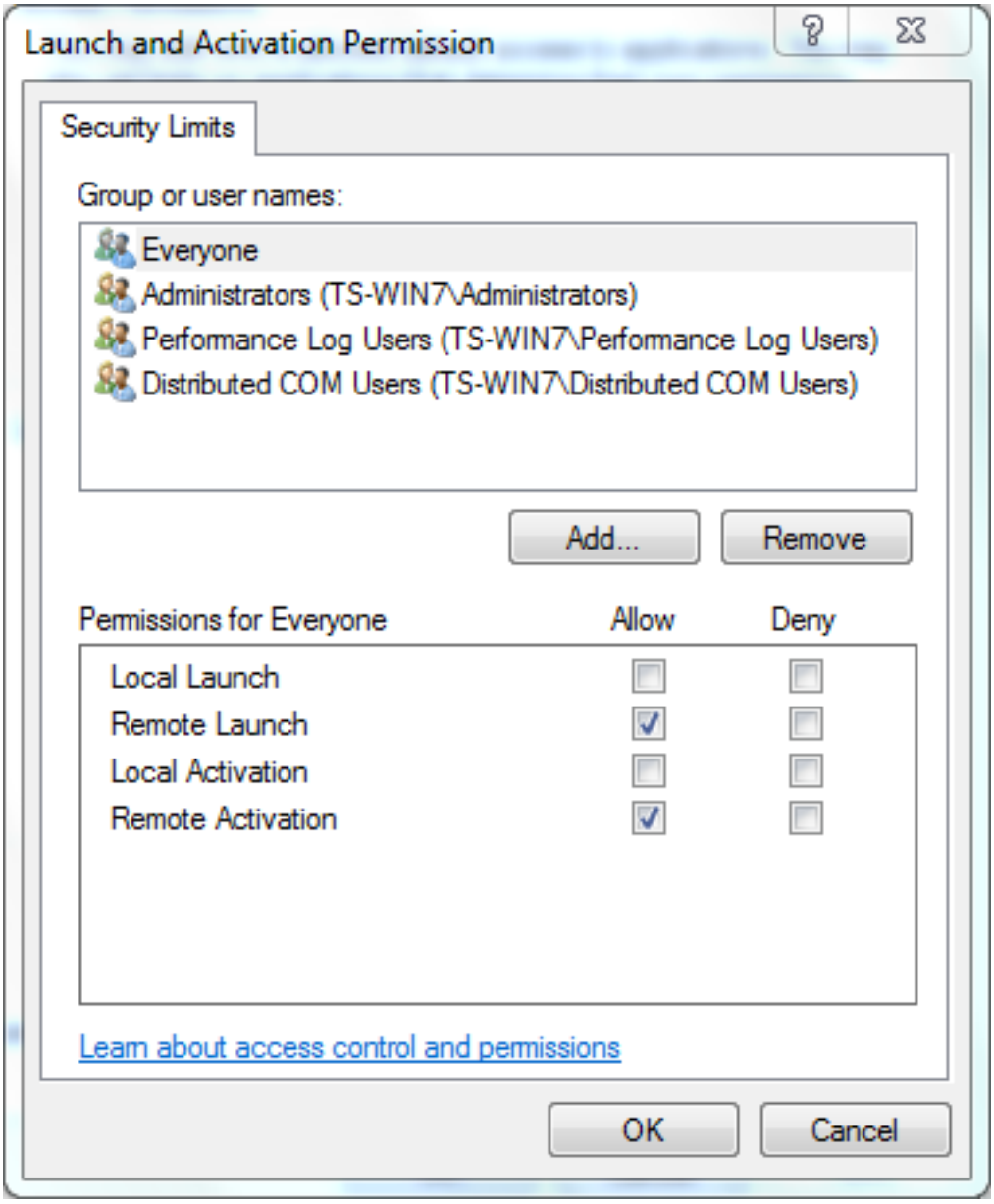
6. En Permisos de inicio y activación, haga clic en **Editar límites**.

7. En el cuadro de diálogo Permiso de inicio y activación, complete estos pasos si su nombre o grupo no aparece en la lista Grupos o nombres de usuario:

   En el cuadro de diálogo Permiso de inicio y activación, haga clic en **Agregar**.

   En el cuadro de diálogo Seleccionar usuarios, equipos o grupos, introduzca su nombre y el grupo en el campo Introducir los nombres de objeto para seleccionar y, a continuación, haga clic en **Aceptar**.

8. En el cuadro de diálogo Permiso de inicio y activación, seleccione su usuario y grupo en la sección **Nombres de grupo o de usuario**.



9. En la columna Permitir en Permisos para usuario, active las casillas de verificación **Inicio remoto** y **Activación remota** y, a continuación, haga clic en **Aceptar**.**Nota:** Un nombre de usuario debe tener derechos para consultar los datos de inicio de sesión del usuario en un servidor AD. Para autenticarse con un usuario a través de proxy, ingrese un nombre de usuario completamente calificado. De forma predeterminada, el dominio de la cuenta que utilizó para iniciar sesión en el equipo donde instaló el agente rellena automáticamente el campo Dominio. Si un usuario proporcionado es miembro de un dominio diferente, actualice el dominio para las credenciales de usuario proporcionadas.
10. Si el problema persiste, en el controlador de dominio intente agregar el usuario en la política Administrar auditoría y registro de seguridad. Para agregar el usuario, complete estos pasos:

    Elija el **Editor de administración de directivas de grupo**.

    Elija Computer Configuration **>Windows Settings > Security Settings > Local Policies >**

User Rights Assignment.

Elija **Administrar auditoría y registro de seguridad**.

Agregue el usuario.