Conceder permissão mínima para uma conta de usuário do Ative Diretory usada pelo agente de usuário da Sourcefire

Contents

Introduction

Este documento descreve como fornecer a um usuário do Ative Diretory (AD) as permissões mínimas necessárias para consultar o controlador de domínio do AD. O agente de usuário Sourcefire usa um usuário do AD para consultar o controlador de domínio do AD. Para realizar uma consulta, um usuário do AD não exige nenhuma permissão adicional.

Prerequisites

Requirements

A Cisco exige que você instale o Sourcefire User Agent em um sistema Microsoft Windows e forneça acesso ao controlador de domínio do AD.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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

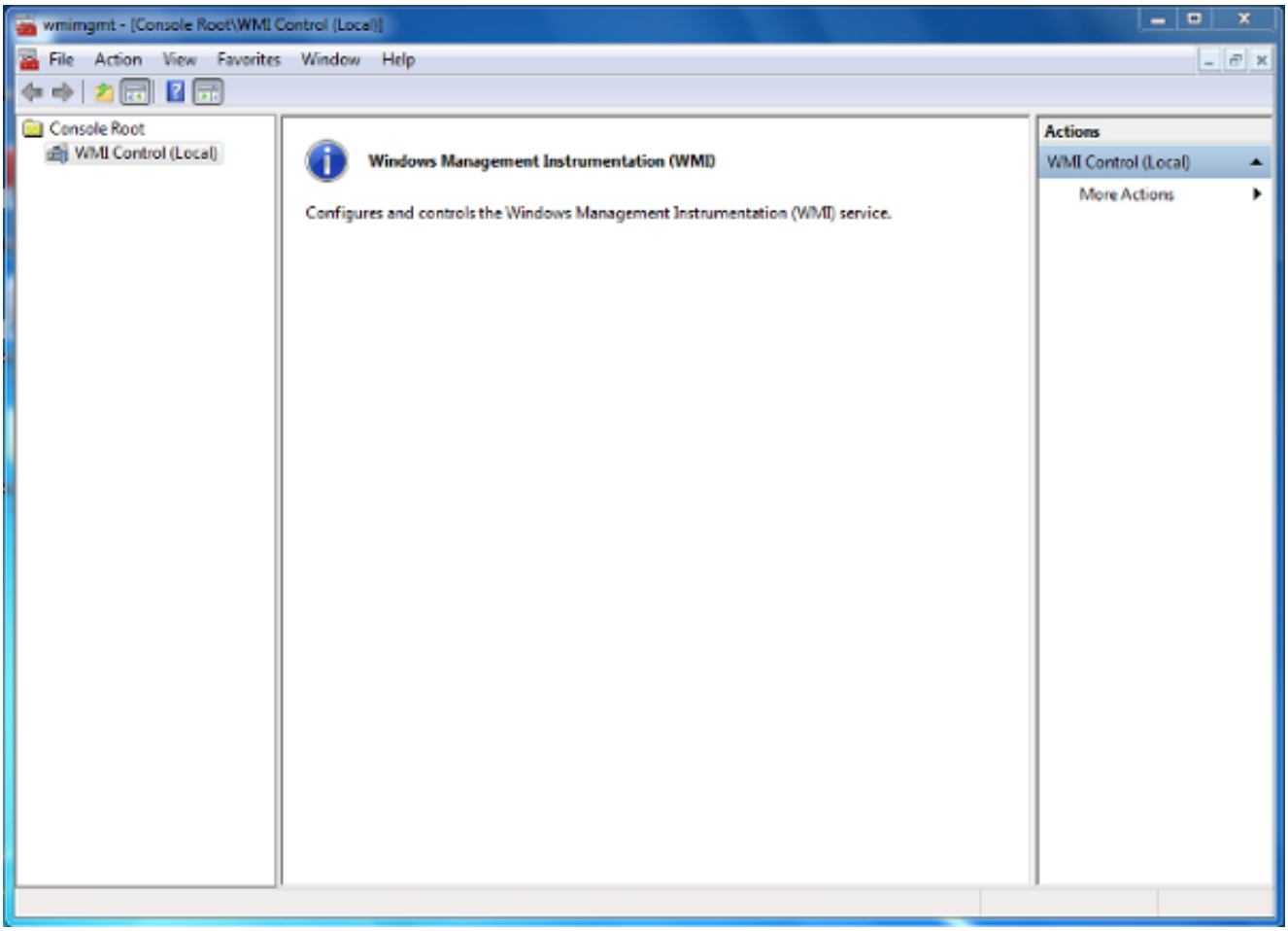
Primeiro, um administrador deve criar um novo usuário do AD especificamente para acesso ao Agente de usuário. Se esse novo usuário não for membro do grupo de administradores de domínio (e eles não devem ser), talvez seja necessário conceder explicitamente ao usuário permissão para acessar os logs de segurança da Instrumentação de Gerenciamento do Windows (WMI). Para conceder permissão, faça o seguinte:

1. Abra o Console de controle WMI:

   No servidor AD, escolha o menu **Iniciar**.

   Clique em **Executar** e digite **wmimgmt.msc**.

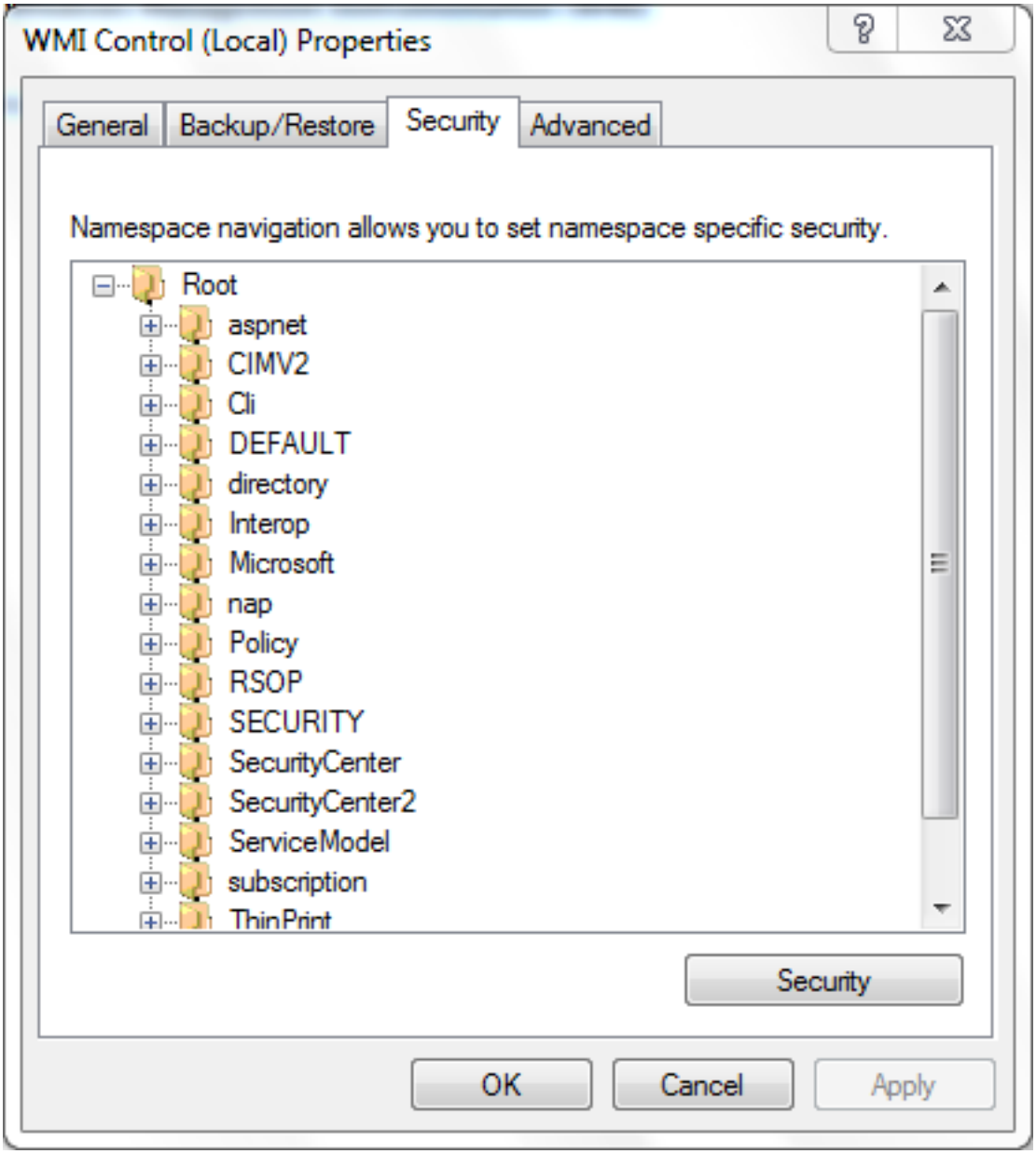
   Click **OK**. O Console de controle WMI é exibido.



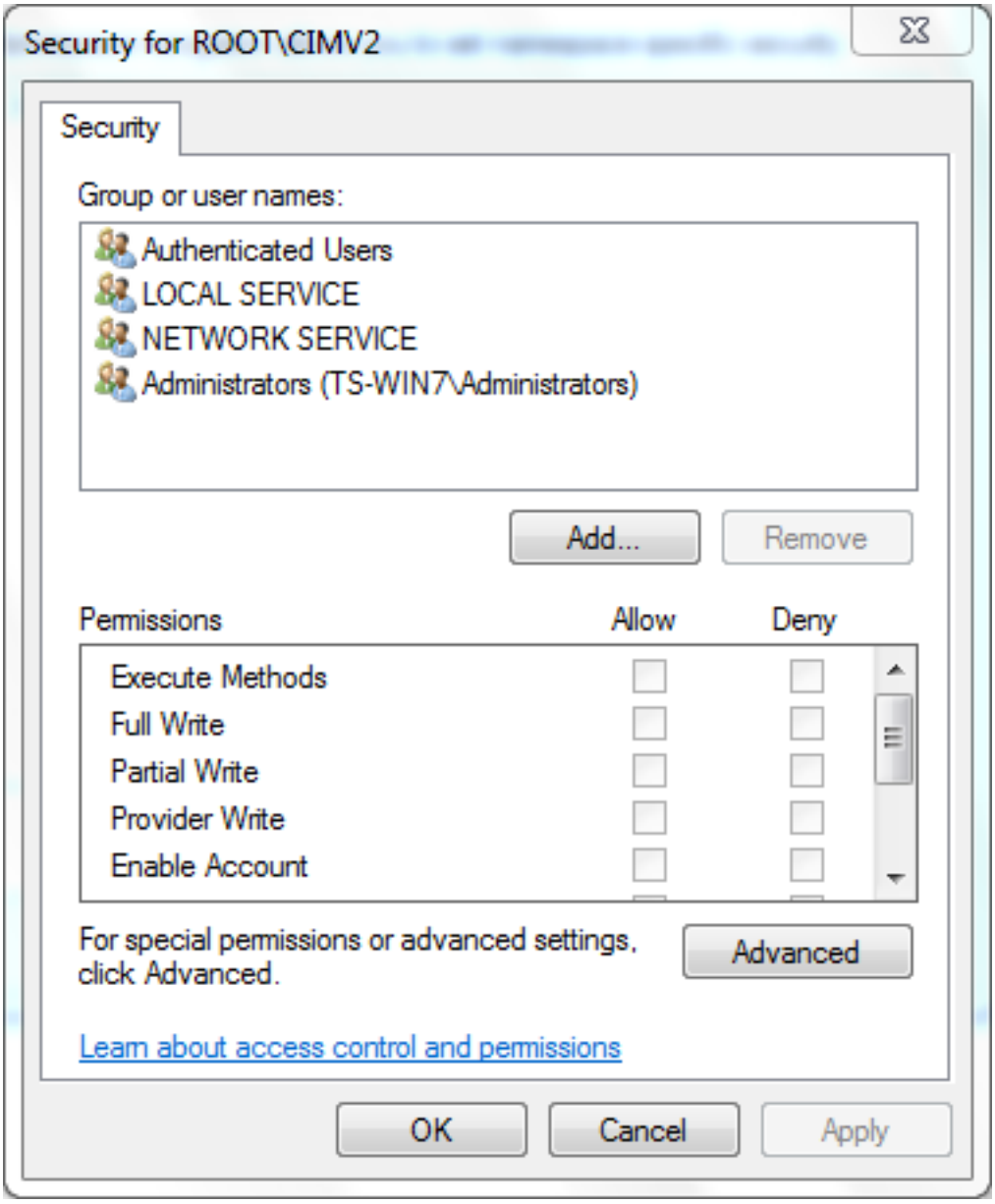
2. Na árvore do console WMI, clique com o botão direito do mouse em **Controle WMI** e clique em **Propriedades**.

3. Clique na guia Security.

4. Selecione o espaço de nomes para o qual pretende conceder a um utilizador ou grupo acesso (`Raiz\CIMV2`) e, em seguida, clique em **Segurança**.



5. Na caixa de diálogo Segurança, clique em **Adicionar**.



6. Na caixa de diálogo Selecionar usuários, computadores ou grupos, digite o nome do objeto (usuário ou grupo) que deseja adicionar. Clique em **Verificar nomes** para verificar sua entrada e clique em **OK**. Talvez seja necessário alterar o local ou clicar em **Avançado** para procurar objetos. Consulte a Ajuda sensível ao contexto (**?**) para obter mais detalhes.

7. Na caixa de diálogo Segurança, na seção Permissões, escolha **Permitir** ou **Negar** para conceder permissões ao novo usuário ou grupo (mais fácil de conceder todas as permissões). O usuário deve receber pelo menos a permissão **Remote Enable**.

8. Clique em **Apply** para salvar as alterações. Feche a janela.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

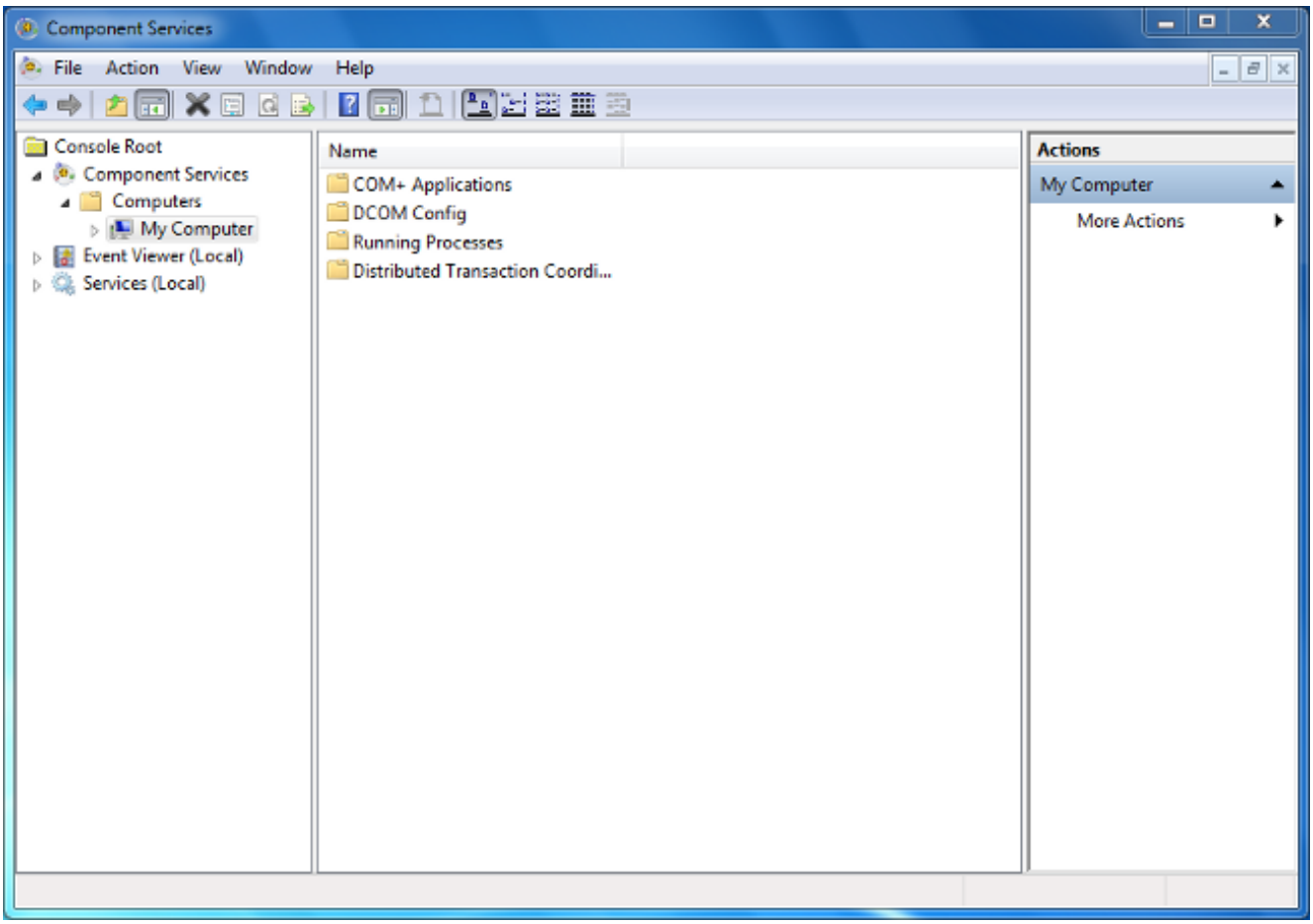
Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Se um problema persistir após as alterações de configuração, atualize as configurações do Distributed Component Object Model (DCOM) para permitir acesso remoto:

1. Escolha o menu **Iniciar**.

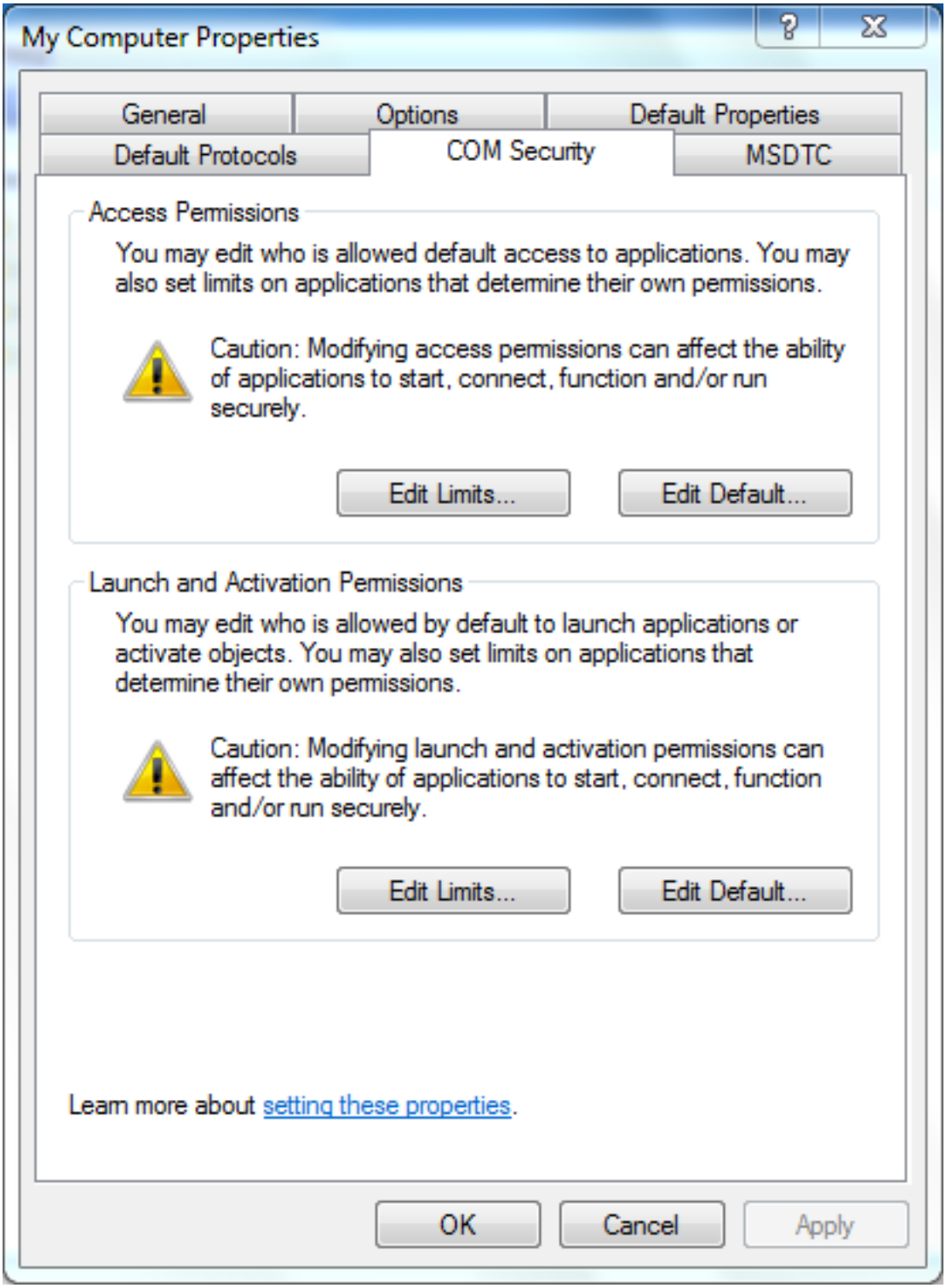
2. Clique em **Executar** e digite **DCOMCNFG**.

3. Click **OK**. A caixa de diálogo Serviços de Componentes é exibida.



4. Na caixa de diálogo Serviços de componente, expanda **Serviços de componente**, expanda **Computadores** e clique com o botão direito do mouse em **Meu computador** e escolha **Propriedades**.

5. Na caixa de diálogo Propriedades do meu computador, clique na guia **Segurança COM**.



6. Em Permissões de inicialização e ativação, clique em **Editar limites**.

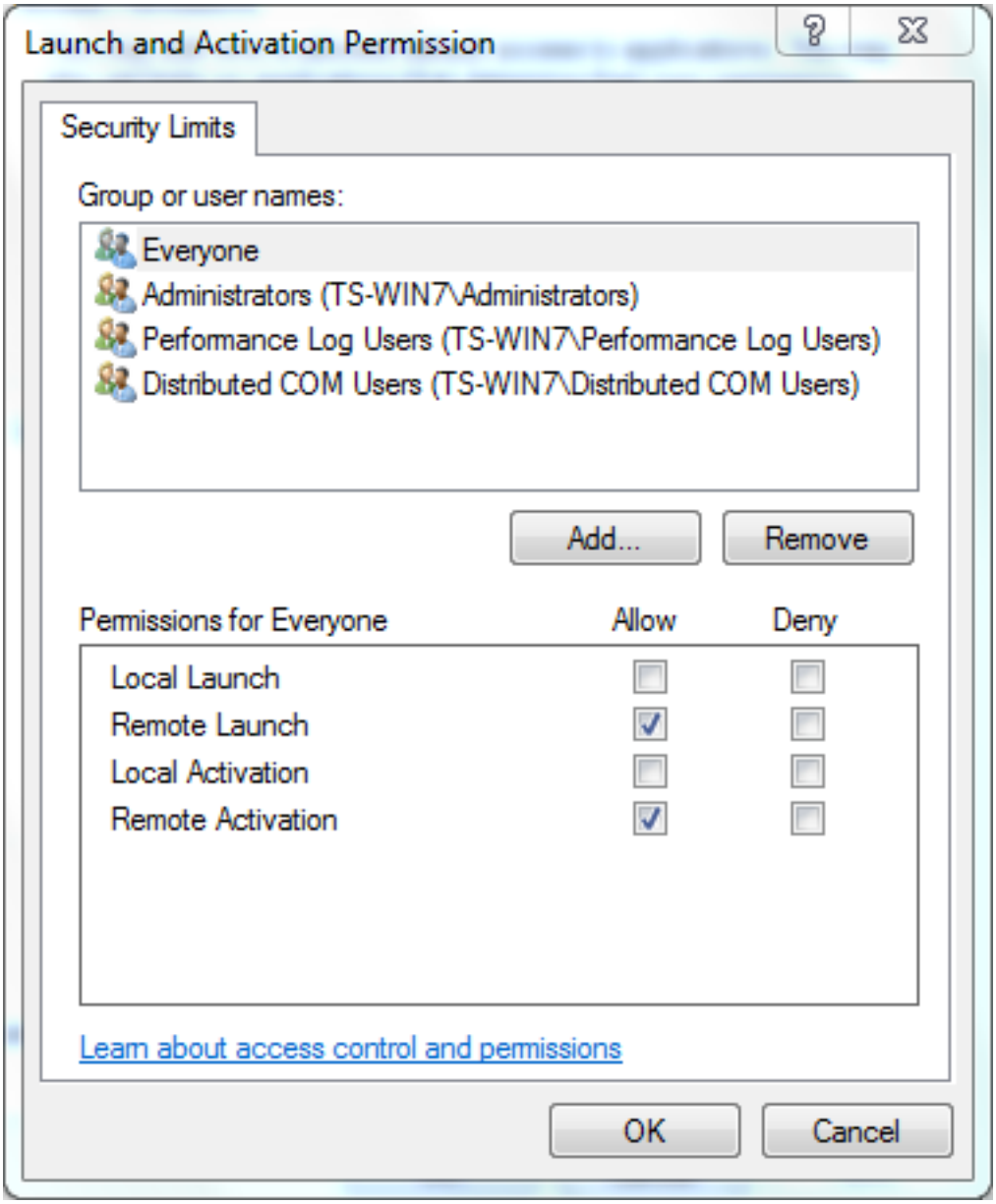
7. Na caixa de diálogo Iniciar e permissão de ativação, faça o seguinte caso seu nome ou seu grupo não apareça na lista Grupos ou nomes de usuário:

   Na caixa de diálogo Iniciar e permissão de ativação, clique em **Adicionar**.

   Na caixa de diálogo Selecionar usuários, computadores ou grupos, digite seu nome e o grupo no campo Inserir os nomes dos objetos a serem selecionados e clique em **OK**.

8. Na caixa de diálogo Iniciar e permissão de ativação, selecione seu usuário e grupo na seção

Grupo ou nomes de usuário.



9. Na coluna Allow (Permitir) em Permissions for User (Permissões para usuário), marque as caixas de seleção **Remote Launch (Inicialização remota**) e **Remote Ativation (Ativação remota)** e clique em **OK**.**Note**: Um nome de utilizador tem de ter direitos para consultar dados de início de sessão de utilizador num servidor AD. Para autenticar com um usuário via proxy, insira um nome de usuário totalmente qualificado. Por padrão, o domínio da conta que você usou para fazer logon no computador em que o agente instalou preenche automaticamente o campo Domínio. Se um usuário fornecido for membro de um domínio diferente, atualize o domínio para as credenciais de usuário fornecidas.
10. Se o problema persistir, no Controlador de Domínio tente adicionar o usuário na política Gerenciar auditoria e log de segurança. Para adicionar o usuário, faça o seguinte:

    Escolha o **Editor de Gerenciamento de Política de Grupo**.

    Escolha Configuração do computador > **Configurações do Windows** > **Configurações de segurança** > **Políticas locais** > **Atribuição de direitos de usuário**.

Escolha **Gerenciar auditoria e registro de segurança**.

Adicione o usuário.