

对Sourcefire用户代理使用的活动目录用户帐户的格兰特最低的权限

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[验证](#)

[故障排除](#)

简介

本文描述如何提供激活目录(AD)用户必要的最小权限查询AD域控制器。 Sourcefire用户代理使用一个AD用户为了查询AD域控制器。为了执行查询，AD用户不需要任何另外的权限。

先决条件

要求

思科要求您安装在Microsoft Windows系统的Sourcefire用户代理并且提供存取对于AD域控制器。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始(默认)配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

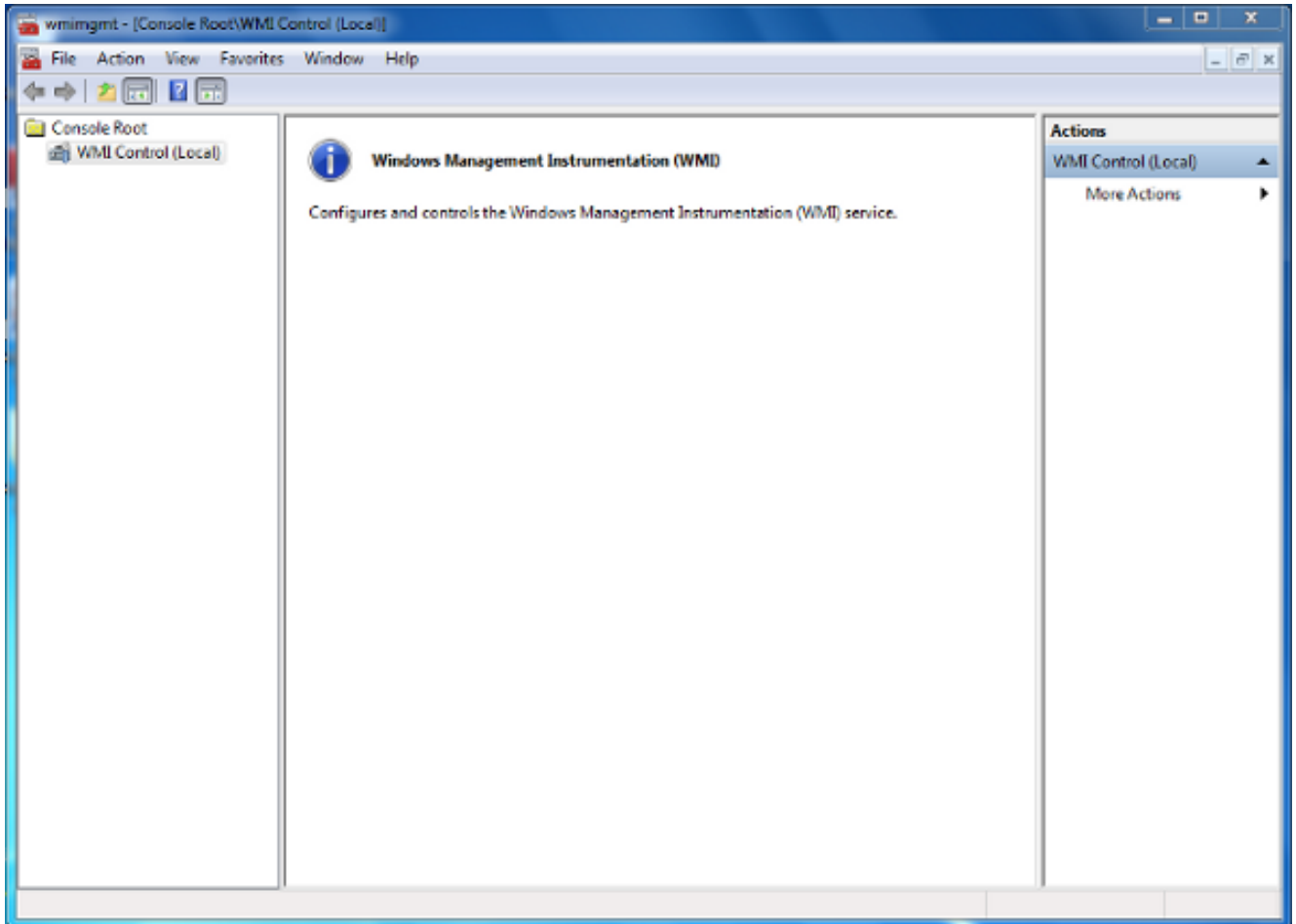
首先，管理员必须特别地创建一个新的AD用户用户代理访问的。如果此新用户不是域管理员组的成员(和他们不应该是)，用户也许必须明确地授权权限访问Windows管理设备(WMI)安全日志。为了同意权限，请完成这些步骤：

1. 打开WMI控制架：

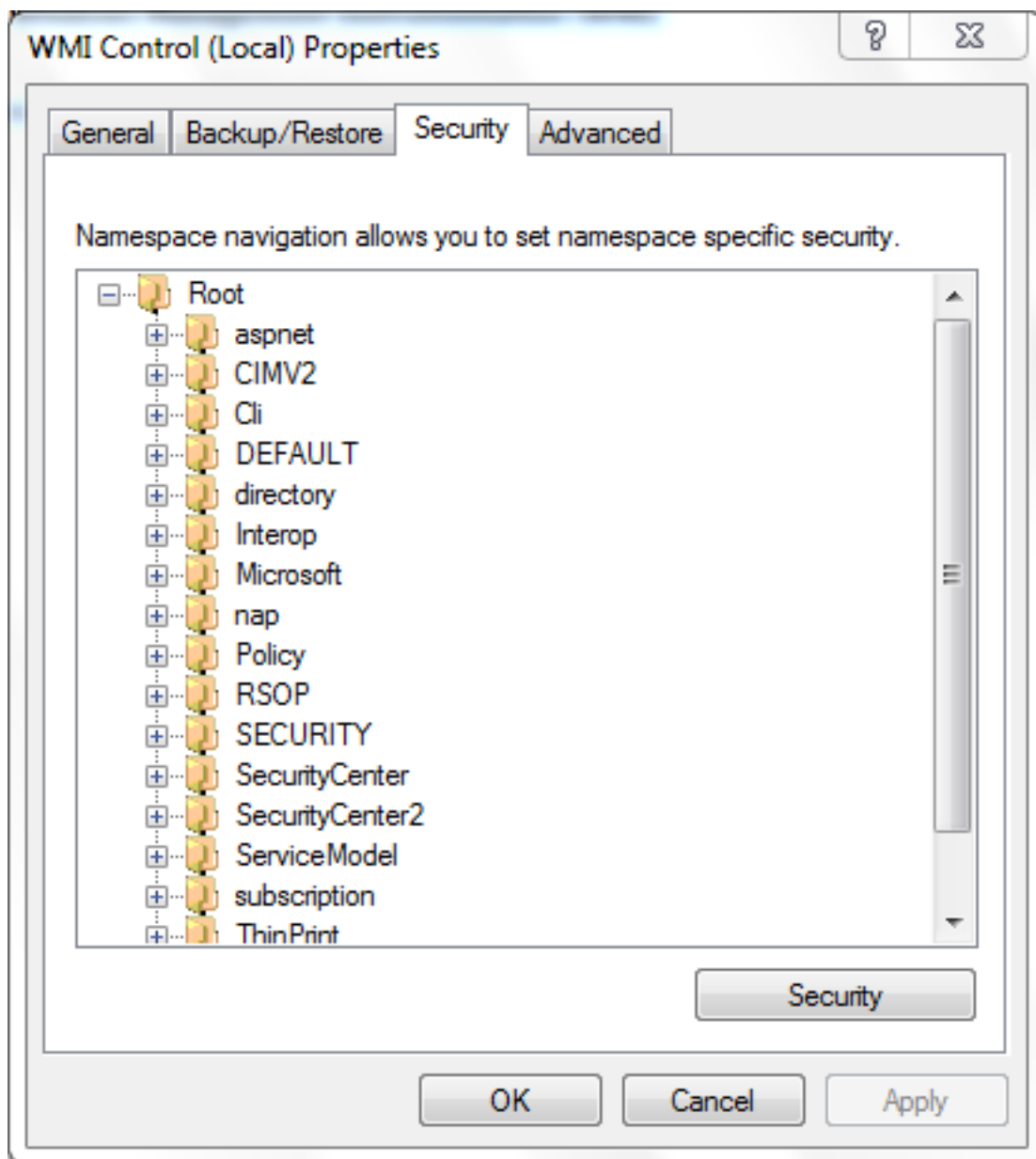
在AD服务器上，请选择**开始菜单**。

点击**运行**并且输入**wmimgmt.msc**。

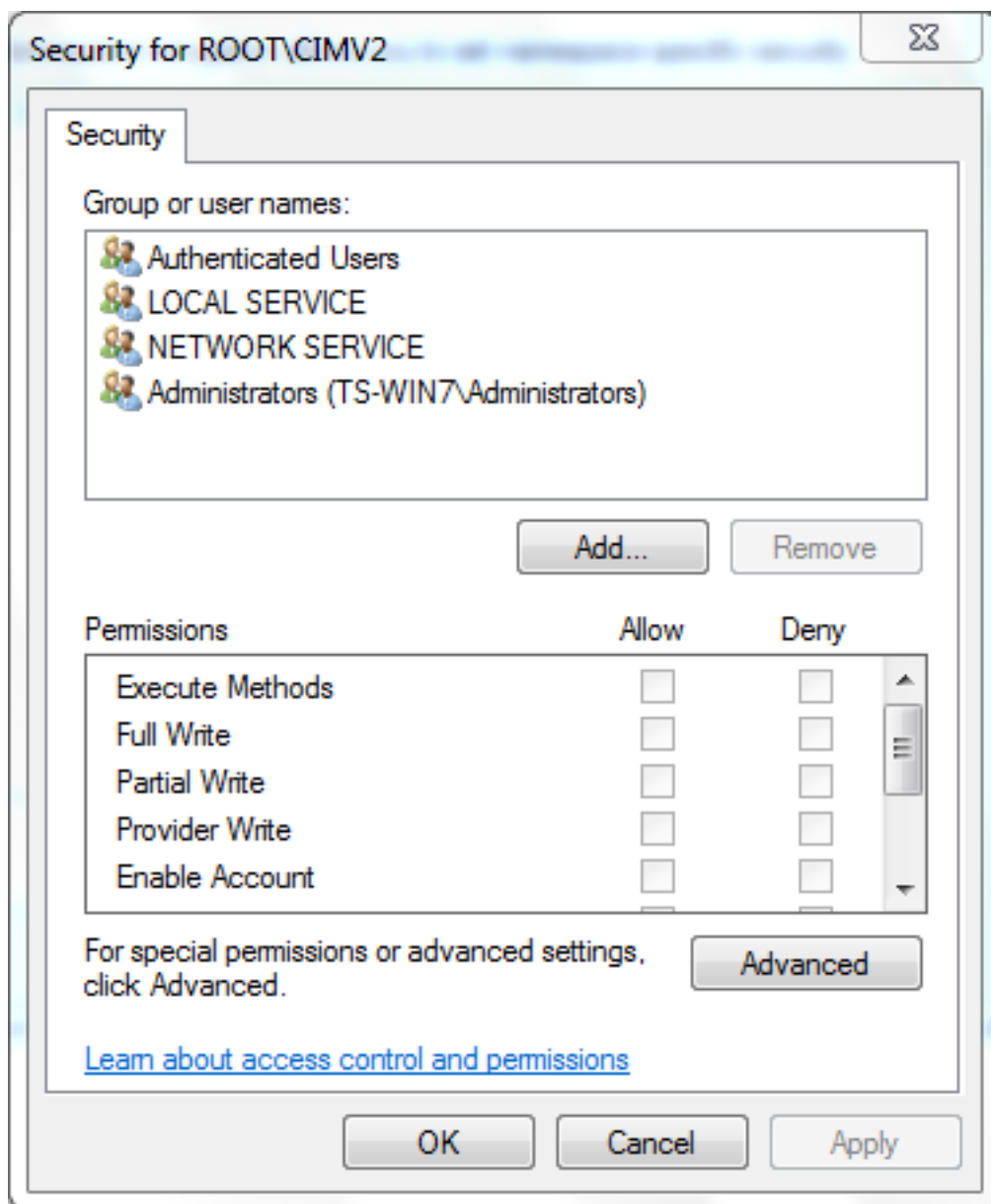
单击 **Ok**。WMI控制架出现。



2. 在WMI控制台结构树上，右键单击**WMI控制**然后单击**属性**。
3. 单击 **Security** 选项卡。
4. 选择您要提供用户或组访问的namespace (`Root\CIMV2`)，然后单击**安全**。



5. 在安全对话框中，请单击**添加**。



6. 在Select Users , Computers , 或Groups对话框 , 请输入对象的名称(用户或组)您想要添加。点击**检查名称**为了验证您的条目然后点击OK键。您也许必须更改位置或单击**先进**为了查询对象。请参阅上下文相关的帮助()以获得详情。
7. 在安全对话框中 , 在Permissions部分 , 请选择**准许**或**拒绝**为了同意权限对新用户或组(最容易给所有权限)。必须给用户至少**远程Enable (event)**权限。
8. 单击**应用**为了保存更改。关闭窗口。

验证

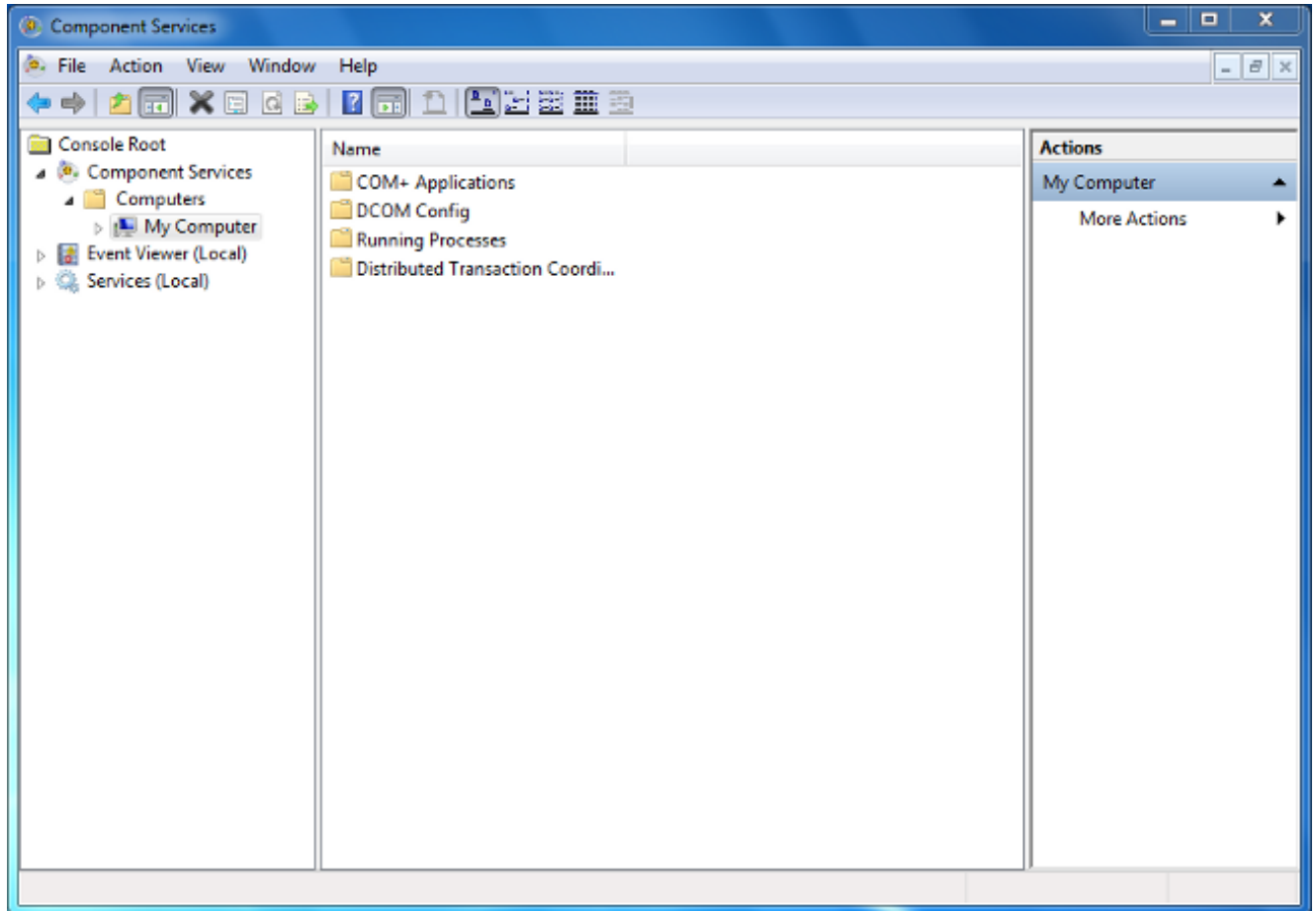
当前没有可用于此配置的验证过程。

故障排除

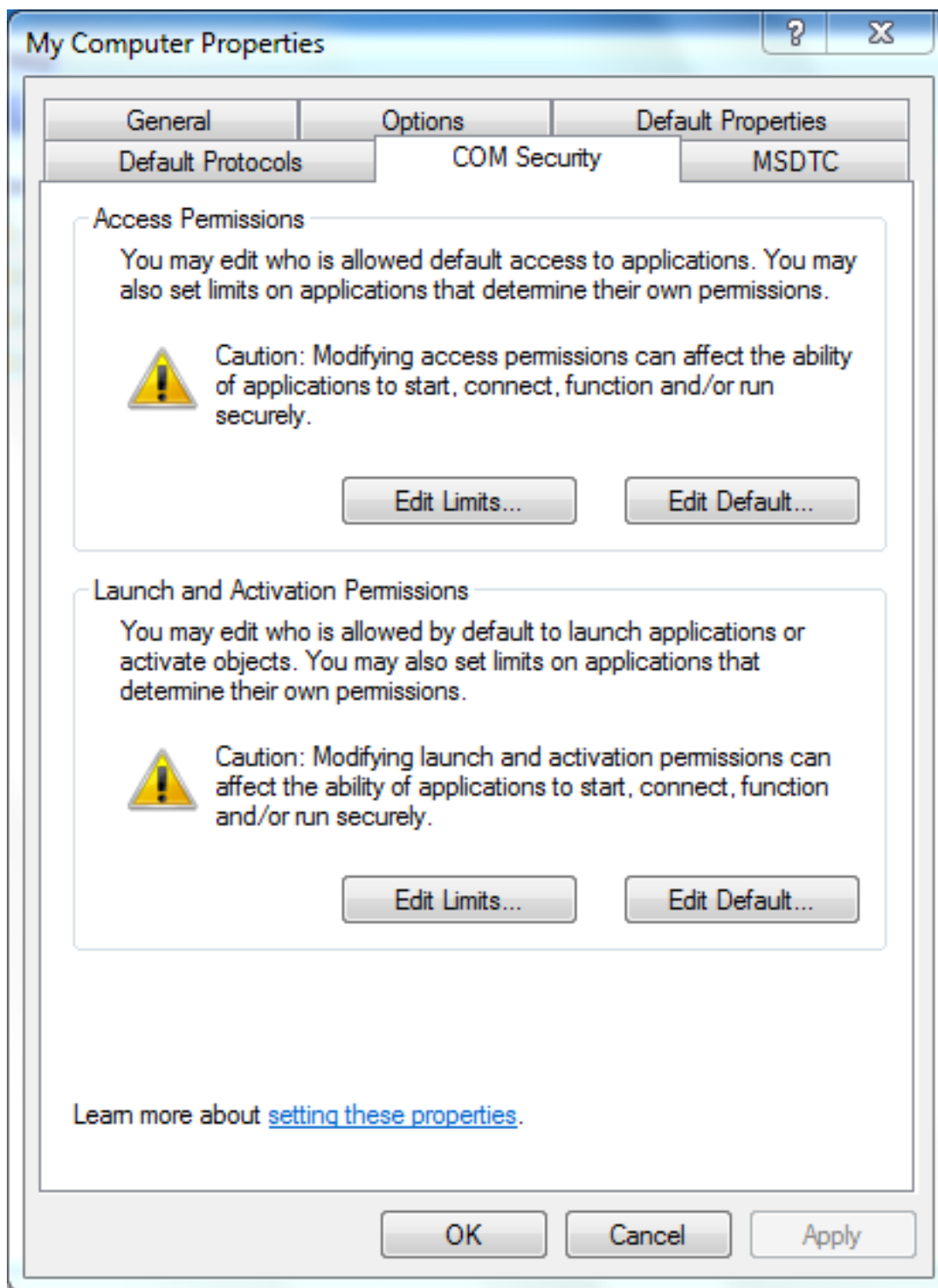
本部分提供的信息可用于对配置进行故障排除。

如果问题在配置更改以后仍然存在，请更新分布式组件对象模型(DCOM)设置为了允许远程访问：

1. 选择**开始菜单**。
2. 点击**运行**并且输入**DCOMCNFG**。
3. 单击 **Ok**。组件服务对话框出现。



4. 在组件服务对话框中，请扩展**组件服务**，展开**计算机**，然后用鼠标右键单击**我的计算机**并且选择**属性**。
5. 在我的计算机Properties对话框中，请点击**COM安全**选项卡。



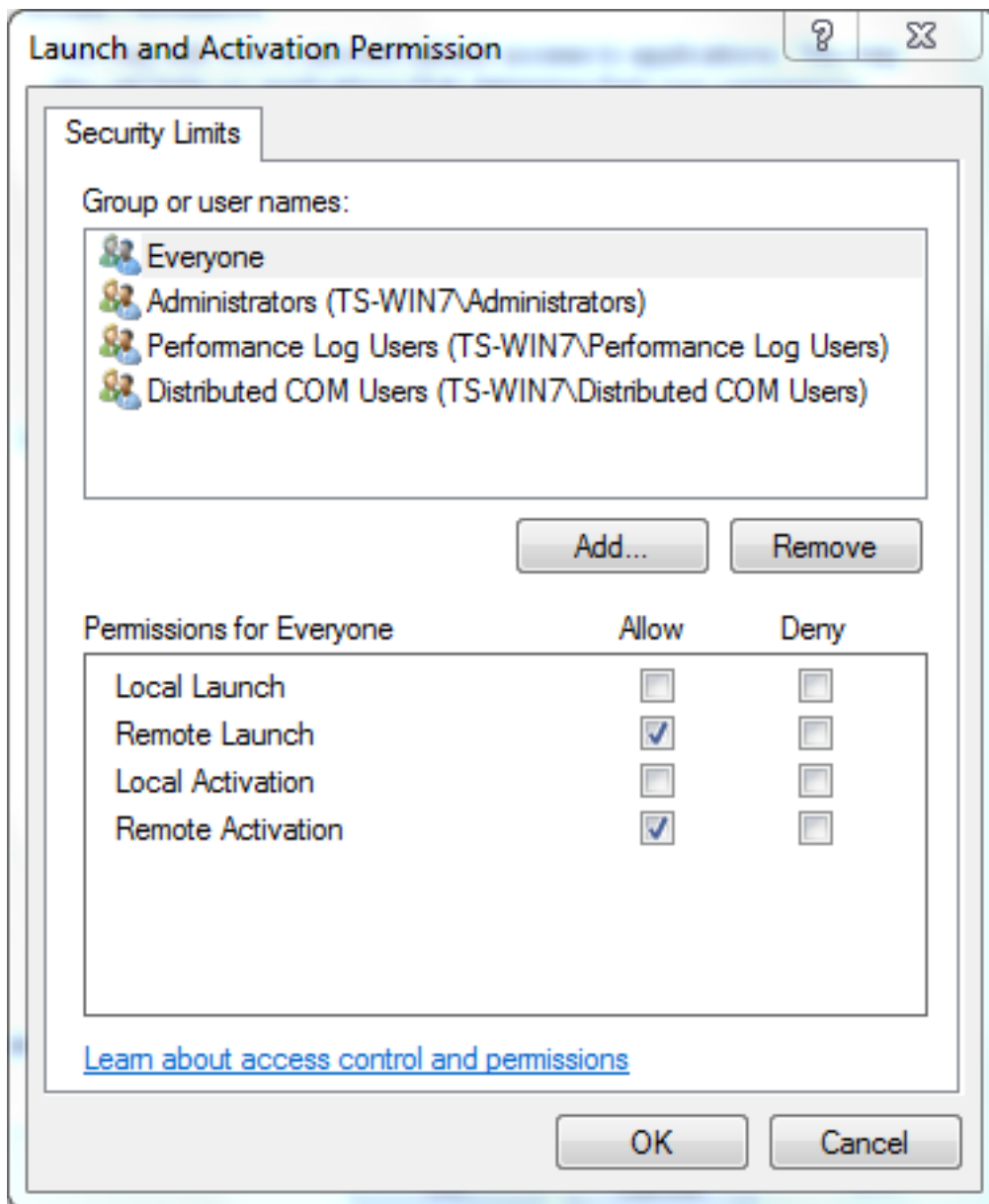
6. 在启动和激活权限下，请单击**编辑限额**。

7. 在启动和激活权限对话框中，如果您的名称或您的组在组或用户名名单，没出现请完成这些步骤：

在启动和激活权限对话框中，请单击**添加**。

在Select Users，Computers，或Groups对话框，请输入您的名称和组回车到对象名到Select字段，然后点击OK键。

8. 在启动和激活权限对话框中，请选择您的用户和组**组或用户名**部分的。



9. 在权限下的允许列用户的，请检查**远程启动**和**远程激活**复选框，然后点击OK键。**Note:**用户名必须有权利查询在AD服务器的用户登录数据。为了验证与用户通过代理，请输入一个完全合格的用户名。默认情况下，您曾经登录计算机您安装代理程序自动填充Domain字段的帐户的域。如果您供应的用户是一个不同的域的成员，更新由供应的用户凭证的域。
10. 如果问题持续，在域控制器尝试添加管理审计和安全日志策略的用户。为了添加用户，请完成这些步骤：

选择**组策略管理编辑器**。

选择**Computer Configuration > Windows Settings > Security Settings > 本地策略 > 用户权限分配**。

选择**管理审计和安全日志**。

添加用户。

