向Sourcefire用户代理使用的Active Directory用户帐户授予最低权限

目录

简介

本文档介绍如何向Active Directory(AD)用户提供查询AD域控制器所需的最小权限。Sourcefire用户代理使用AD用户来查询AD域控制器。要执行查询，AD用户不需要任何附加权限。

先决条件

要求

思科要求您在Microsoft Windows系统上安装Sourcefire用户代理，并提供对AD域控制器的访问。

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

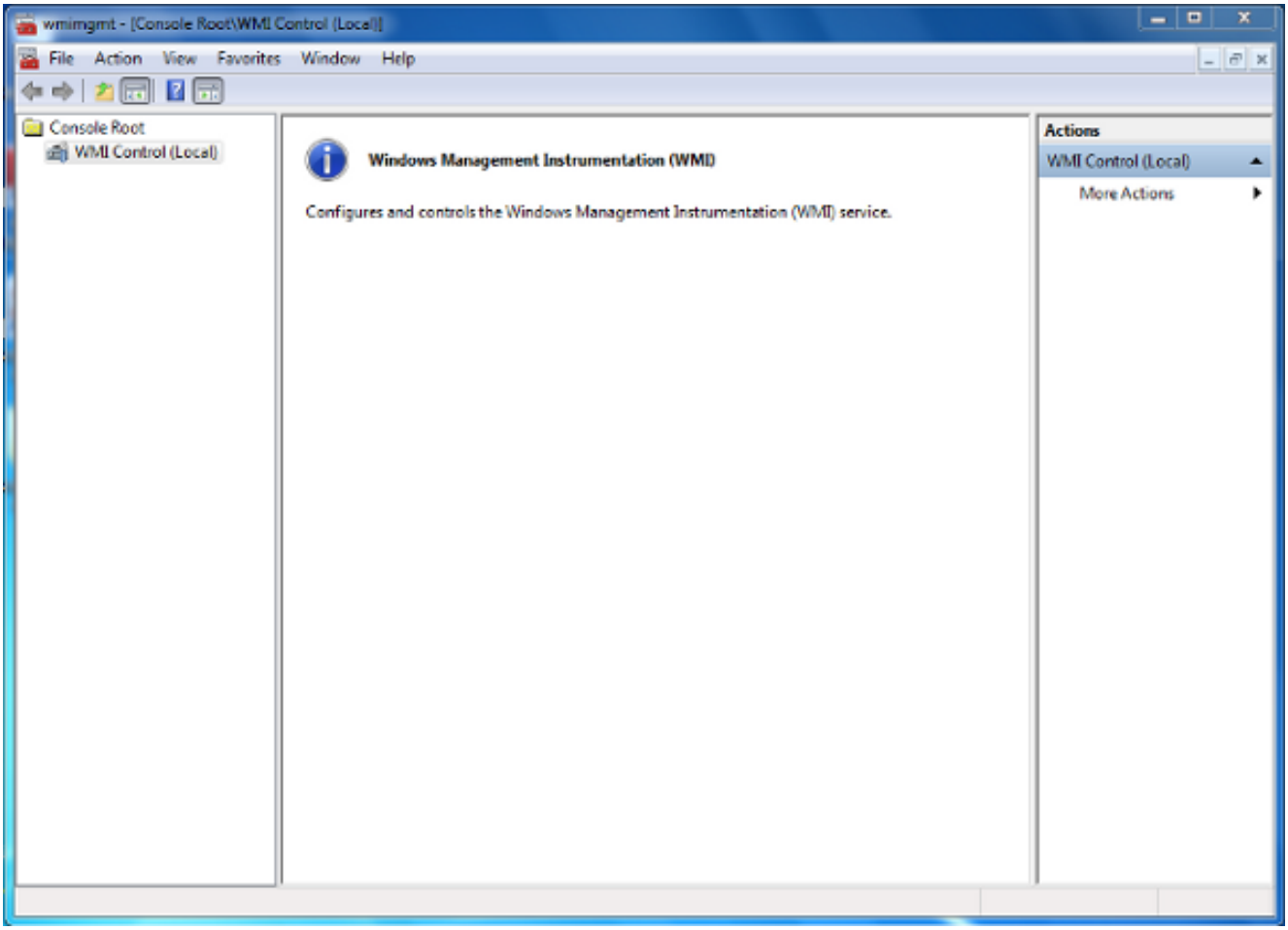
首先，管理员必须专门为用户代理访问创建新的AD用户。如果此新用户不是域管理员组的成员（而且不应是），则可能必须明确授予该用户访问Windows Management Instrumentation(WMI)安全日志的权限。要授予权限，请完成以下步骤：

1. 打开WMI控制台：

在AD服务器上，选择“开始”菜单。

单击**Run**,**然后输**入wmimgmt.**msc**。

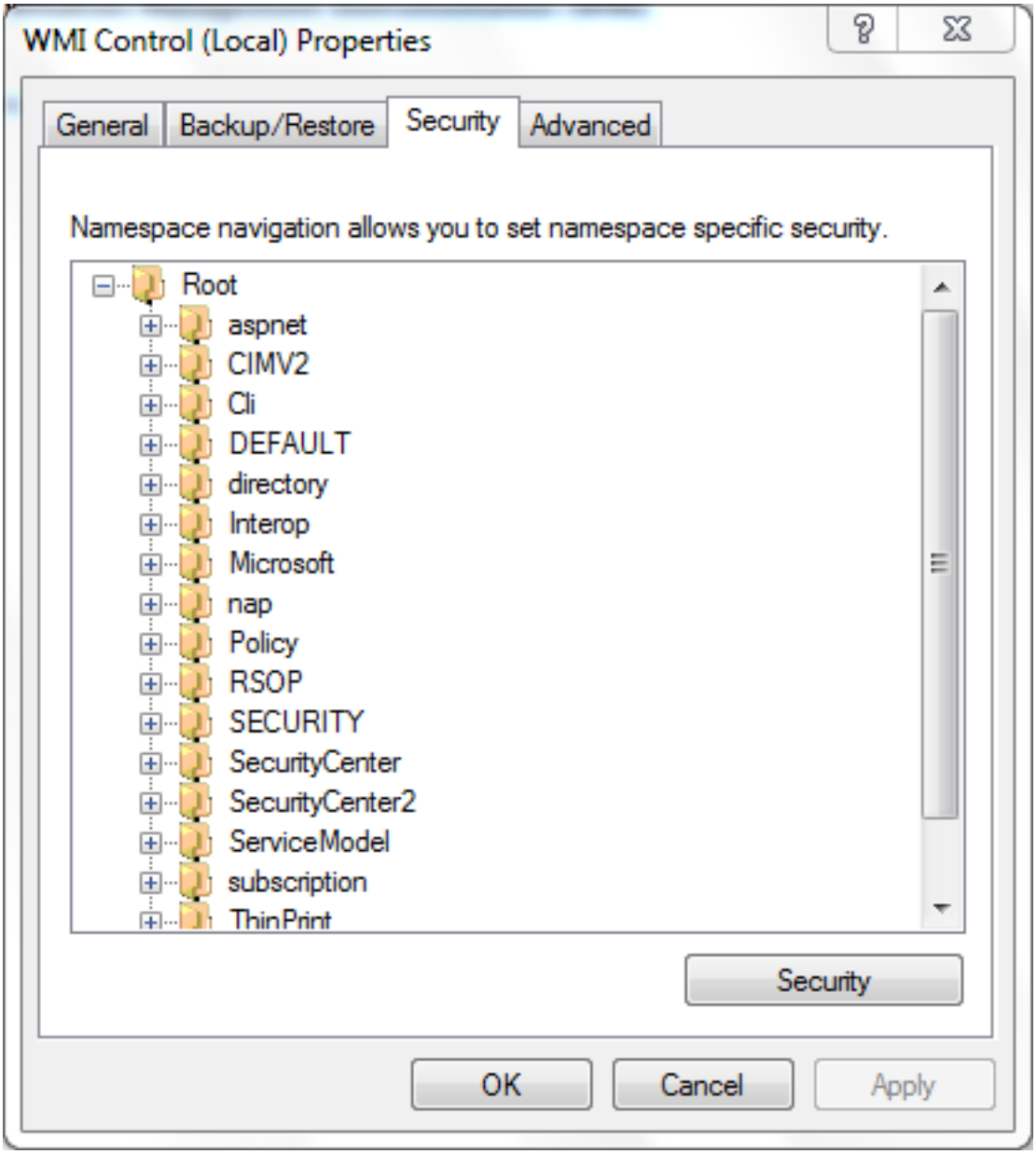
Click **OK**.系统将显示WMI控制台。



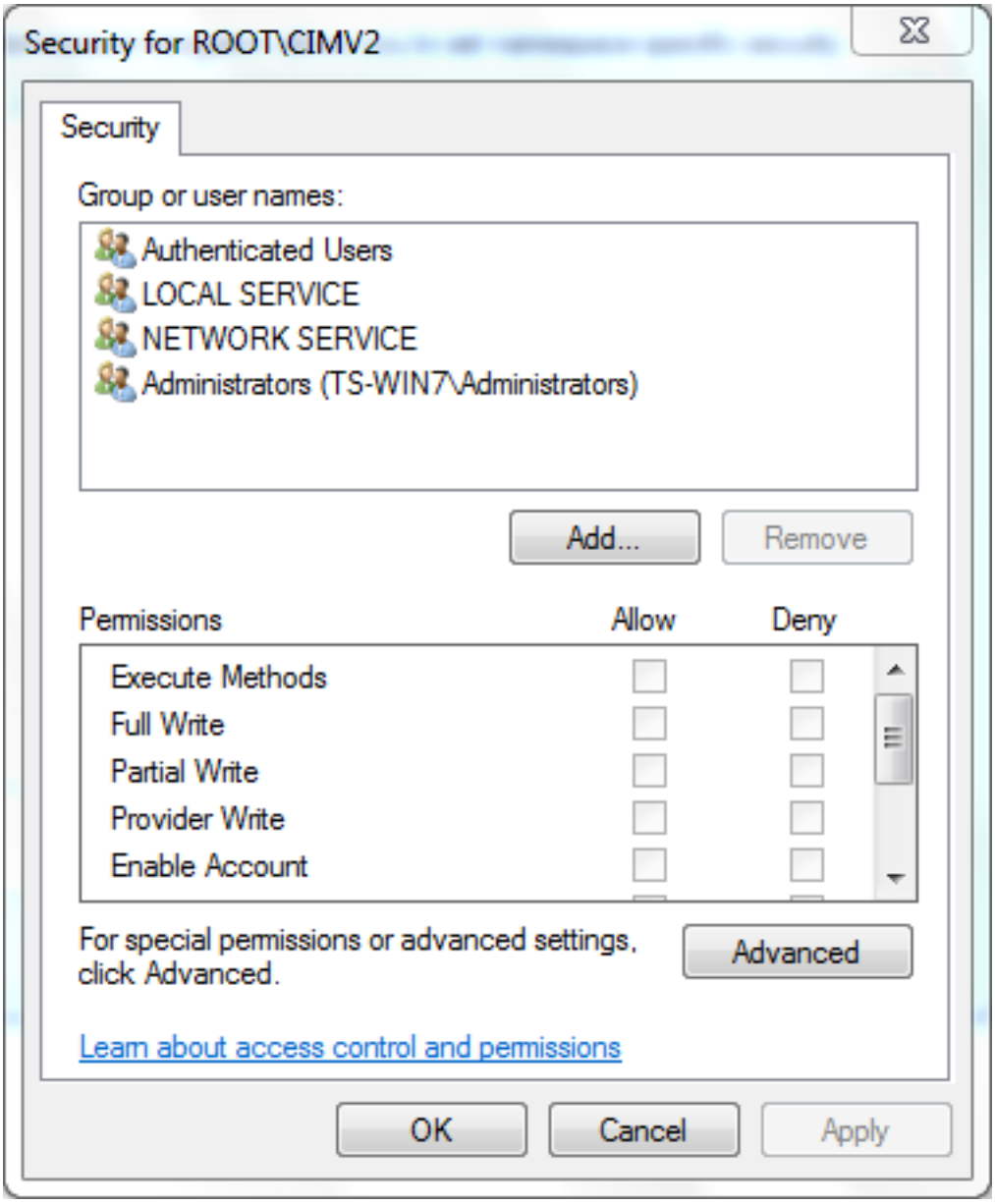
2. 在WMI控制台树上，右键单击WMI控**件，然**后单击**属性**。

3. 单击“Security”选项卡。

4. 选择要为其授予用户或组访问权限的命名空(**Root\CIMV2**)，然后单击**Security**。



5. 在“安全”对话框中，单击“**添加**”。



6. 在选择用户、计算机或组对话框中，输入要添加的对象（用户或组）的名称。单击**Check Names(检**查名称)以验证您的条目，然后单击**OK（确定）**。您可能必须更改位置或单击“高**级**”以查询对象。有关详细信息，请参**阅上下文**相关帮助(?)。

7. 在“安全”对话框的“权限”部分，选择**允许**或**拒绝**，以便向新用户或组授予权限（最容易授予所有权限）。 必须至少为用户授予“远程启**用**”权限。

8. 单击**Apply**以保存更改。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

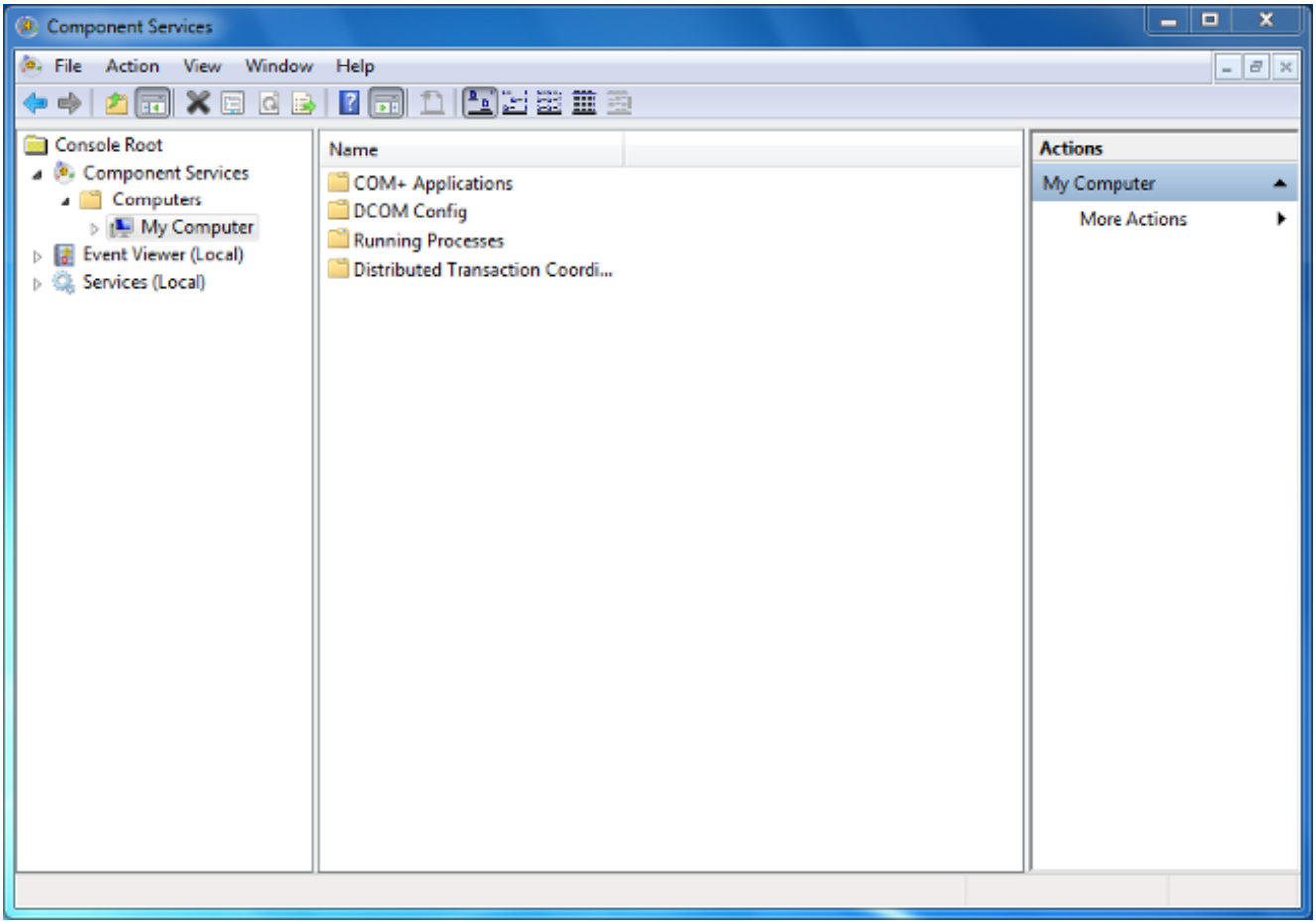
本部分提供的信息可用于对配置进行故障排除。

如果配置更改后问题仍然存在，请更新分布式组件对象模型(DCOM)设置以允许远程访问：

1. 选择“开**始**”菜单。

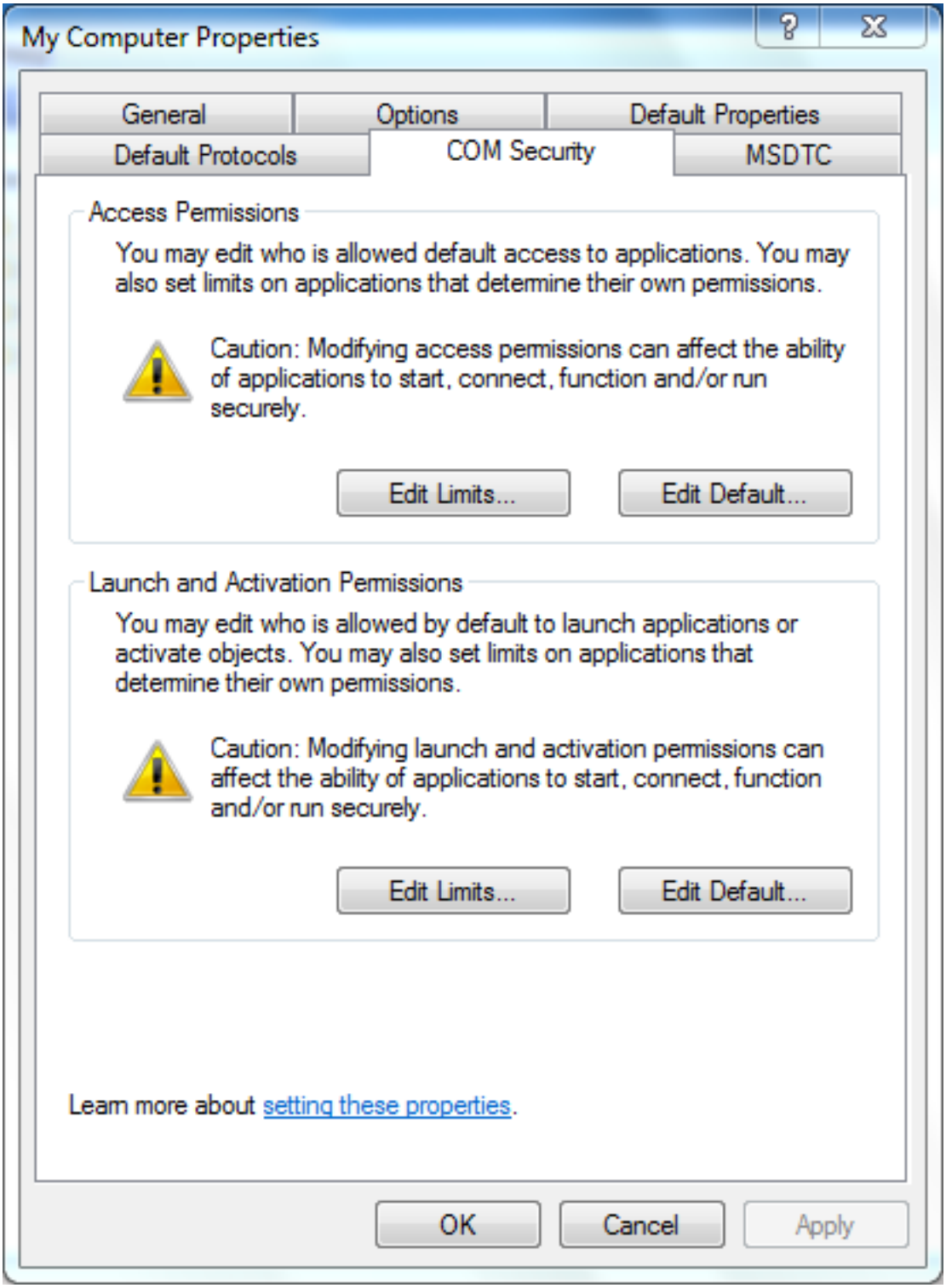
2. 单击Run并**输入**DCOMCNFG。

3. Click **OK**.系统将显示“组件服务”对话框。



4. 在“组件服务”对话框中，展开**组件服务**，展开**计算机**，然后右键单击**我的计算机**并选择**属性**。

5. 在“我的计算机属性”对话框中，单击“COM安**全**”**选**项卡。



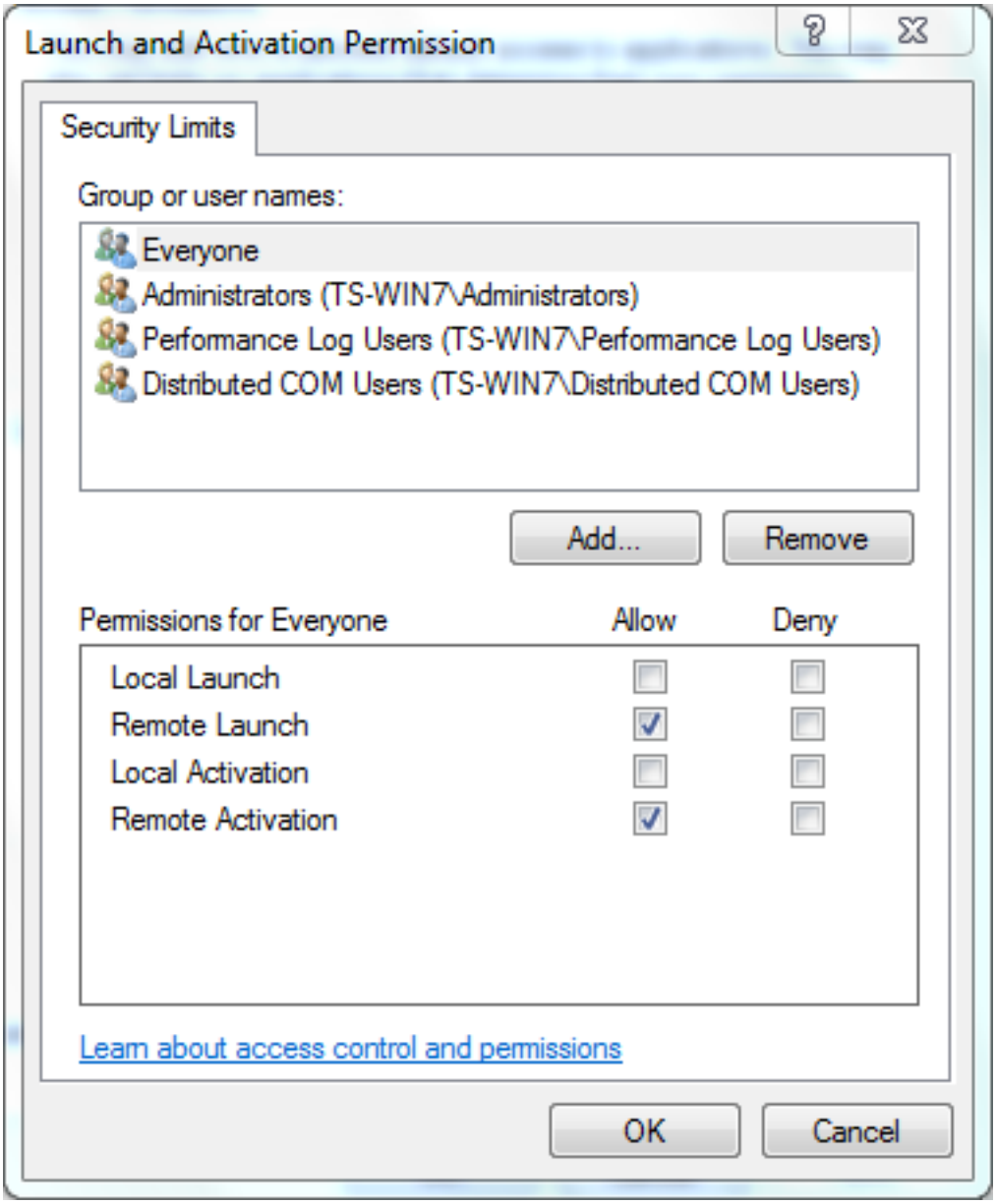
6. 在“启动和激活权限”下，单击**编辑限制**。

7. 在“启动和激活权限”对话框中，如果您的姓名或组未出现在“组”或“用户名”列表中，请完成以下步骤：

   在启动和激活权限对话框中，单击**添加**。

   在“选择用户、计算机或组”对话框中，在“输入要选择的对象名称”字段中输入您的名称和组，然后单击“**确定**”。

8. 在“启动和激活权限”对话框中，在“组”或“用户名”部**分中选择您的用户**和组。



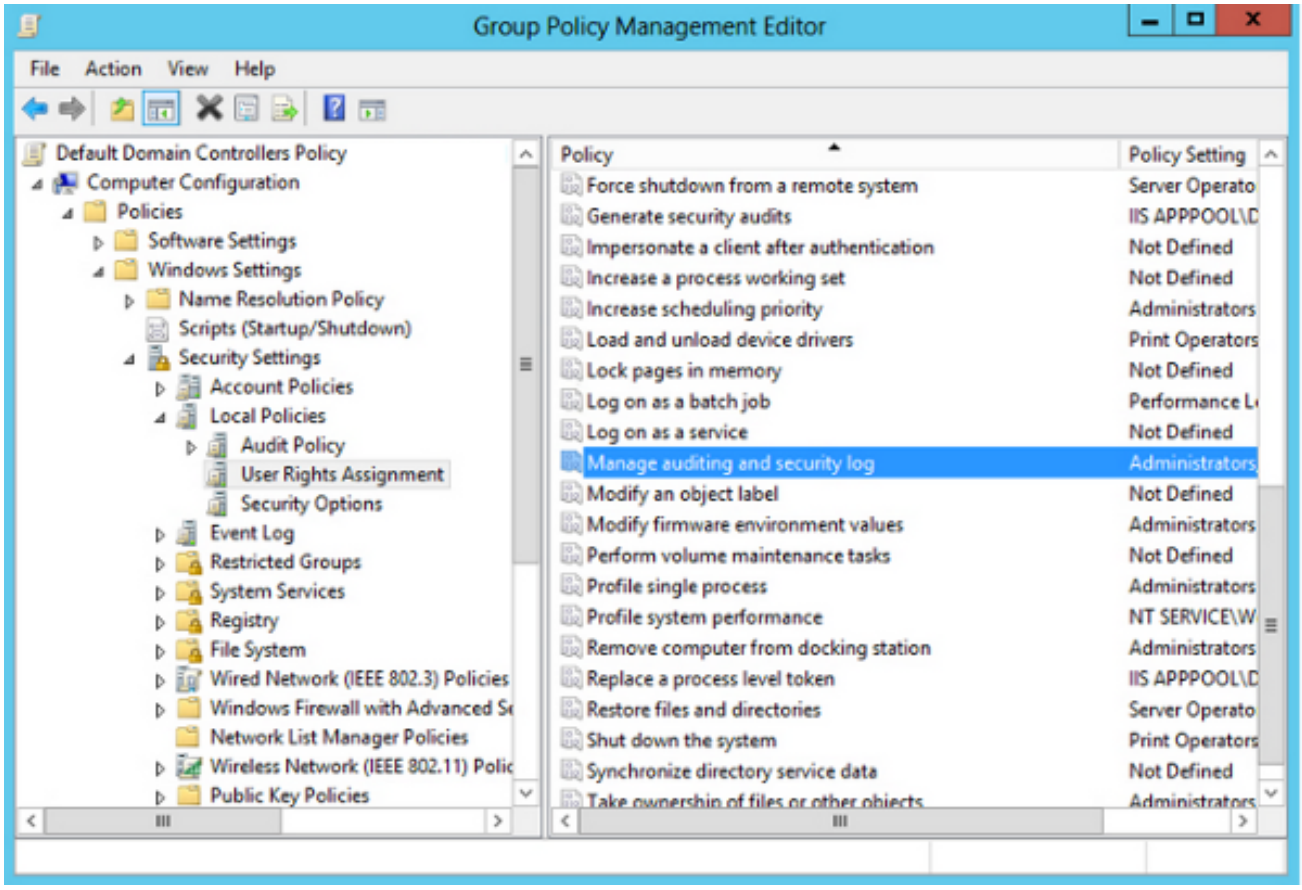
9. 在“用户权限”下的“允许”列中，选中“远程启**动”和**“远程**激活”**复选框，然后单击**确定。注意：**用户名必须具有在AD服务器上查询用户登录数据的权限。要通过代理向用户进行身份验证，请输入完全限定的用户名。默认情况下，用于登录安装代理的计算机的帐户的域会自动填充“域”字段。如果您提供的用户是不同域的成员，请更新提供的用户凭据的域。
10. 如果问题仍然存在，请在域控制器上尝试在管理审核和安全日志策略中添加用户。要添加用户，请完成以下步骤：

    选择组策**略管理编辑器**。

    选择“计算机配置”**>“**Windows设置”>“**安全设置”>**“本地**策略”>“用户权**限分配”。

    选择Manage auditing and security log。

    添加用户。


Group Policy Management Editor
File Action View Help
Default Domain Controllers Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Se
Network List Manager Policies
Wireless Network (IEEE 802.11) Polic
Public Key Policies
Policy
Policy Setting
Force shutdown from a remote system
Server Operato
Generate security audits
IIS APPPOOL\D
Impersonate a client after authentication
Not Defined
Increase a process working set
Not Defined
Increase scheduling priority
Administrators
Load and unload device drivers
Print Operators
Lock pages in memory
Not Defined
Log on as a batch job
Performance L
Log on as a service
Not Defined
Manage auditing and security log
Administrators
Modify an object label
Not Defined
Modify firmware environment values
Administrators
Perform volume maintenance tasks
Not Defined
Profile single process
Administrators
Profile system performance
NT SERVICE\W
Remove computer from docking station
Administrators
Replace a process level token
IIS APPPOOL\D
Restore files and directories
Server Operato
Shut down the system
Print Operators
Synchronize directory service data
Not Defined
Take ownership of files or other objects
Administrators