Windows 7 && Windows *Server 2008* 网络 OPC 的 DCOM 配置

内部版本：

Ver0.1------ 2011-03-10 试用版本。

Ver0.2------ 2011-03-11 完善作为客户端的配置。

Ver0.3------ 2011-03-17 修改防火墙 DCOM 规则设置，“高级”属性允许域、公用、私有网络；“作用域”属性。

Ver0.4------2011-03-25 修改关于 32 位和 64 位运行库说明，实际上程序和动态库都是 32 位的，只是安装包将运行库复制的目标路径不同。

Ver0.5-----2013-12-23 增加 64 位下启动“组件服务”的方式。

适用 OS 系统：

Windows 7、Windows 7 with Service pack 1、

Windows Server 2008 R2、Windows Server 2008 R2 With Service pack 1

由于 OPC（OLE for Process Control）建立在 Microsoft 的 COM（COmponent Model）基础上，并且 OPC 的远程通讯依赖 Microsoft 的 DCOM（Distribute COM），安全方面则依赖 Microsof 的 Windows 安全设置。

通过网络相互通信，OPC Server（OPC 服务端）和 OPC Client（OPC 客户端）所在的操作系统，需要设置 DCOM 的安全属性，下面使用 Windows 7 系统介绍配置过程。

由于 OPC 通讯需要用到 OPC Foundation 提供的动态库，所以在开始配置前，首先安装 OPC Foundation 提供的运行分发包，安装时需要根据操作系统类型，32 位的系统选择 X86 运行库安装包；64 位系统选择 X64 运行库安装包。

需要注册的运行库的文件列表：

NO.	名称	版本	备注
1	*opc_aeps.dll*	*1.10.101.0*	
2	*opcbc_ps.dll*	*2.0.101.0*	
3	*opccomn_ps.dll*	*1.10.101.0*	
4	*opchda_ps.dll*	*1.20.101.0*	
5	*opcproxy.dll*	*3.0.101.0*	
6	*opcsec_ps.dll*	*1.0.101.0*	
7	*OpcEnum.exe*	*1.10.101.0*	

OPC Server（服务器）运行在 Windows 7 时的 DCOM 配置

一、 安装 OPC 运行库（如果安装力控的软件会自动安装）

OPC 服务器（OPC Server）和 OPC 客户端的正常运行需要依赖 OPC 运行库，如果两个组件运行在不同的计算机，那运行计算机上都需要安装运行库。如果 OPC 程序运行在 64 位平台，请安装对应版本的运行库安装包。

OPC Foundation 的网站（*www.**opc**foundation.org*）提供运行库分发包下载，链接如

下图：

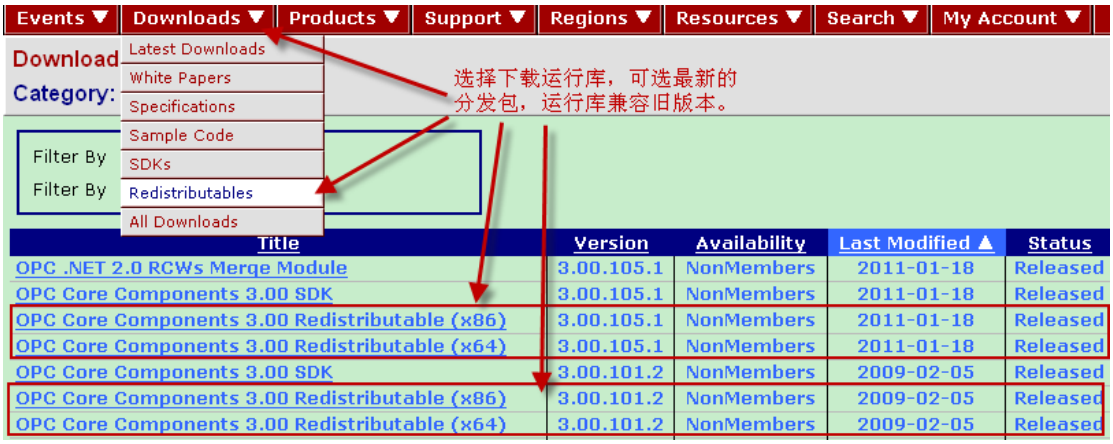

图 1 下载运行库分发包

选择下载适用版本的运行库分发包，然后在需要的计算机上运行分发包安装程序，安装程序会负责复制、注册运行库。运行库安装包依赖 Microsoft 的.Net Framewrok v1 运行库。

推荐：安装好 OPC 运行库，将计算机操作系统重新启动，然后再继续后面的配置工作。

二、 创建用户并赋予访问权限

1. 创建新用户

创建一个新用户，并赋予此用户运行和使用操作系统 DCOM 程序的权限。为了降低整个系统的安全风险，可以创建一个受限用户，而不是建立管理员级用户。为操作系统创建新用户需要管理员权限。

注意：

A、 需要在 OPC 服务器所在 OS 系统与 OPC 客户端所在 OS 系统，创建的用户的用户名和密码相同。

B、 由于 Windows 7 系列的 OS 系统 Guests 用户组的权限非常受限，所以新创建的用户需要是 Users 用户组级别权限，或比 Users 用户组级别更高的权限。推荐使用 Users 用户组。

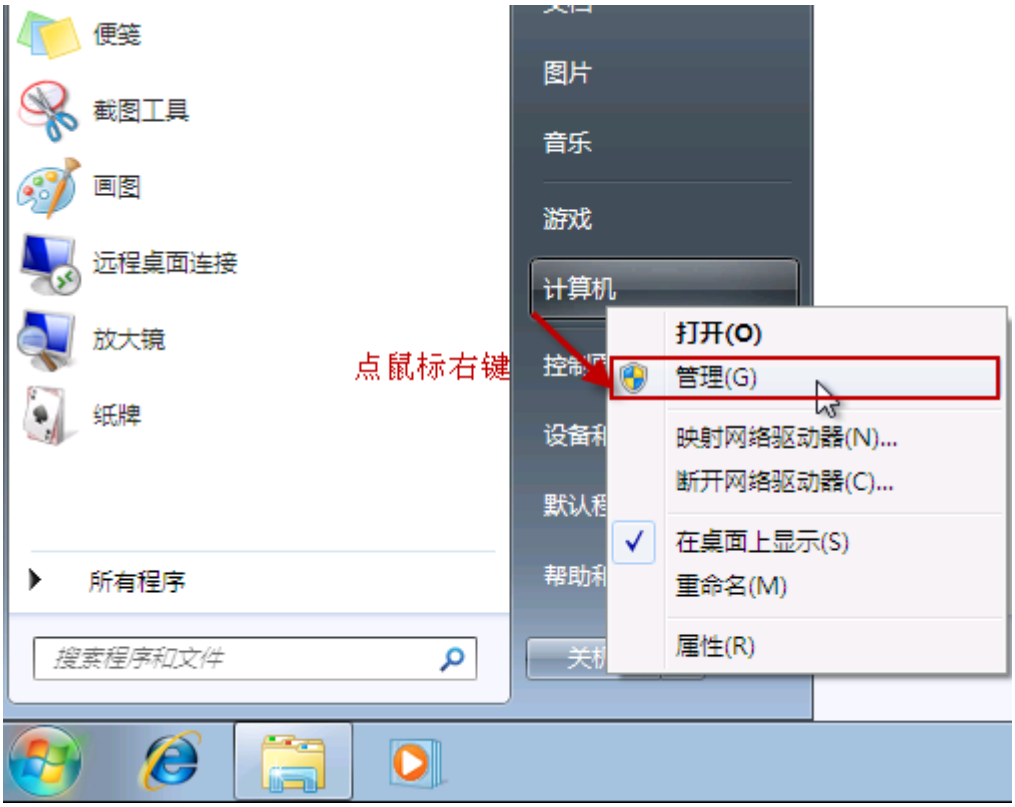

图 2 通过“管理”菜单或“控制面板”创建用户

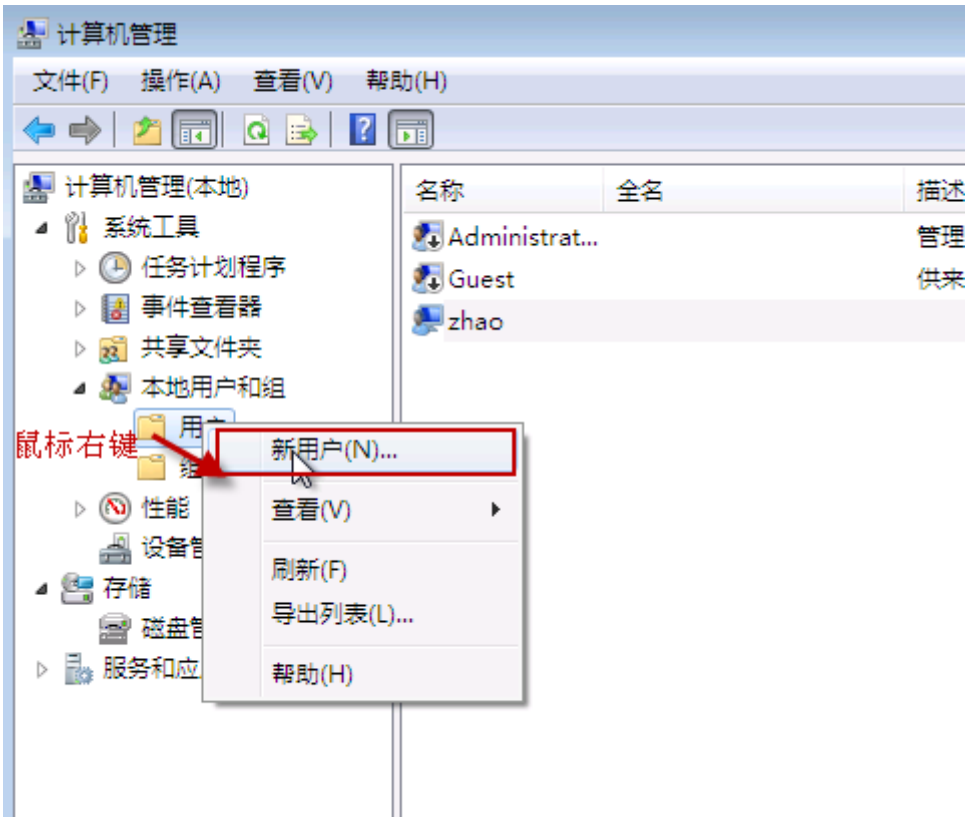

图 3 创建新用户

图 4 新用户属性

创建新用户，并设置用户属性。若是为了安全考量，请保持密码不为空。

2. 赋予用户访问 DCOM 的权限

要想使新创建的用户有使用 DCOM 的权限，需要将用户加入“Distribute COM Users”用户组。

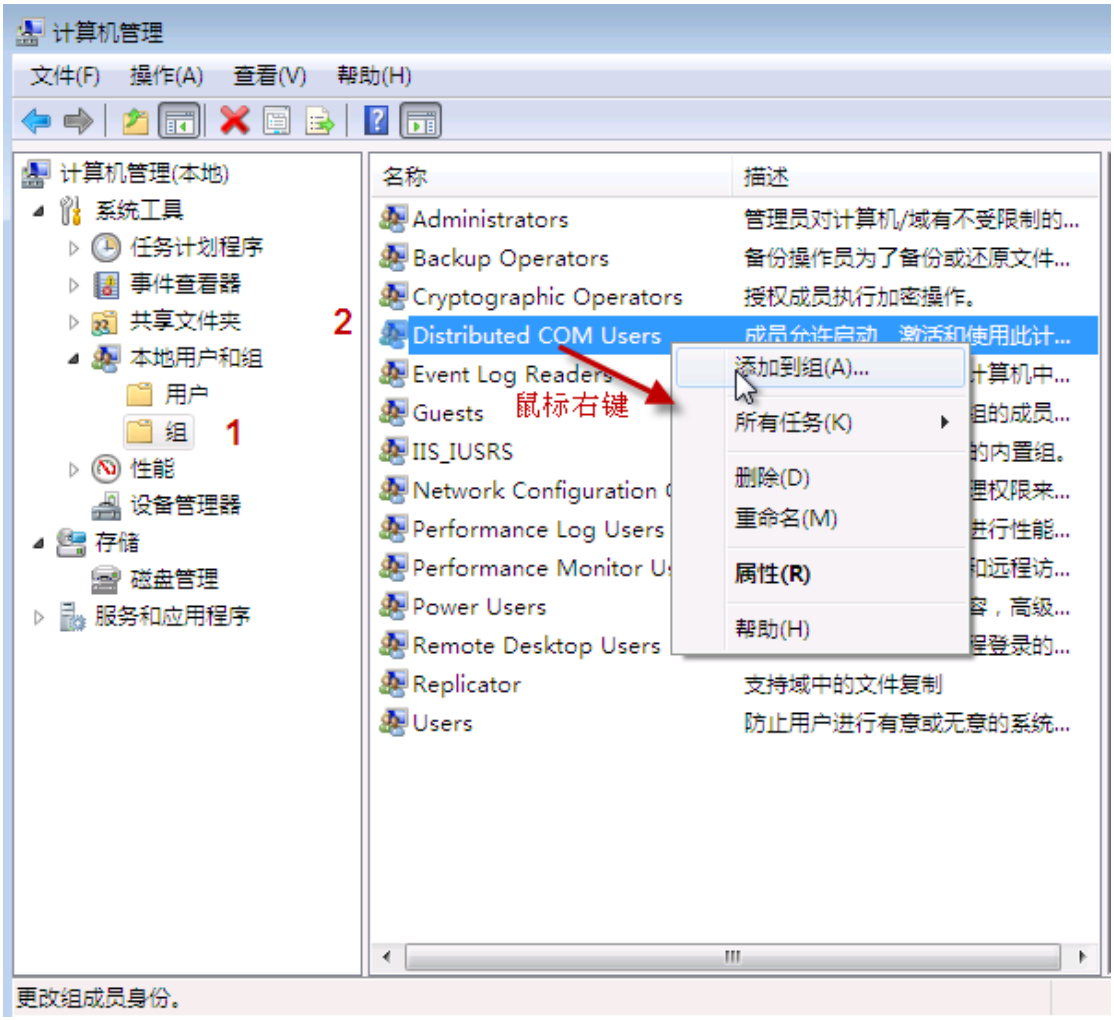
计算机管理
文件(F) 操作(A) 查看(V) 帮助(H)
计算机管理(本地)
系统工具
任务计划程序
事件查看器
共享文件夹
本地用户和组
用户
组
性能
设备管理器
存储
磁盘管理
服务和应用程序
2
1
名称
描述
Administrators
管理员对计算机/域有不受限制的...
Backup Operators
备份操作员为了备份或还原文件...
Cryptographic Operators
授权成员执行加密操作。
Distributed COM Users
Event Log Readers
Guests
IIS_IUSRS
Network Configuration
Performance Log Users
Performance Monitor U
Power Users
Remote Desktop Users
Replicator
支持域中的文件复制
Users
防止用户进行有意或无意的系统...
鼠标右键
添加到组(A)...
所有任务(K)
删除(D)
重命名(M)
属性(R)
帮助(H)
更改组成员身份。

图 5 用户组

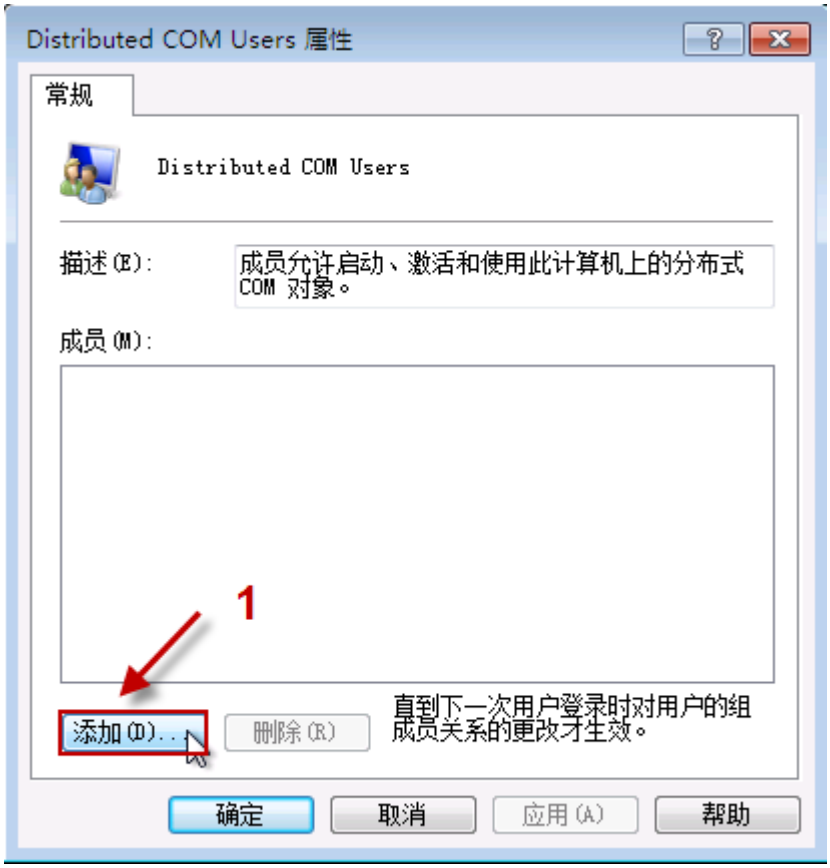

图 6 添加用户到用户组

图 7 选择要添加的用户

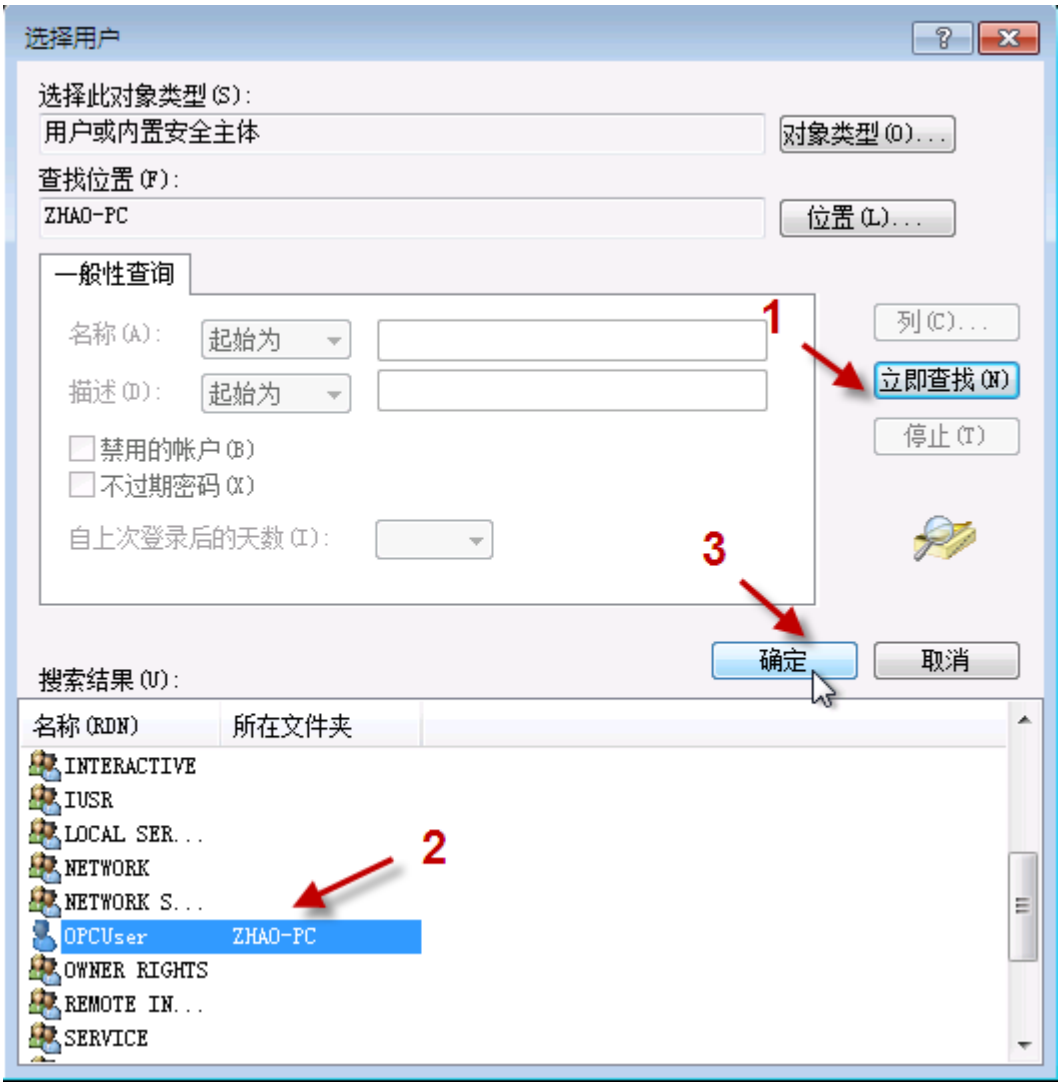

图 8 用户列表

图 9 选择添加的用户

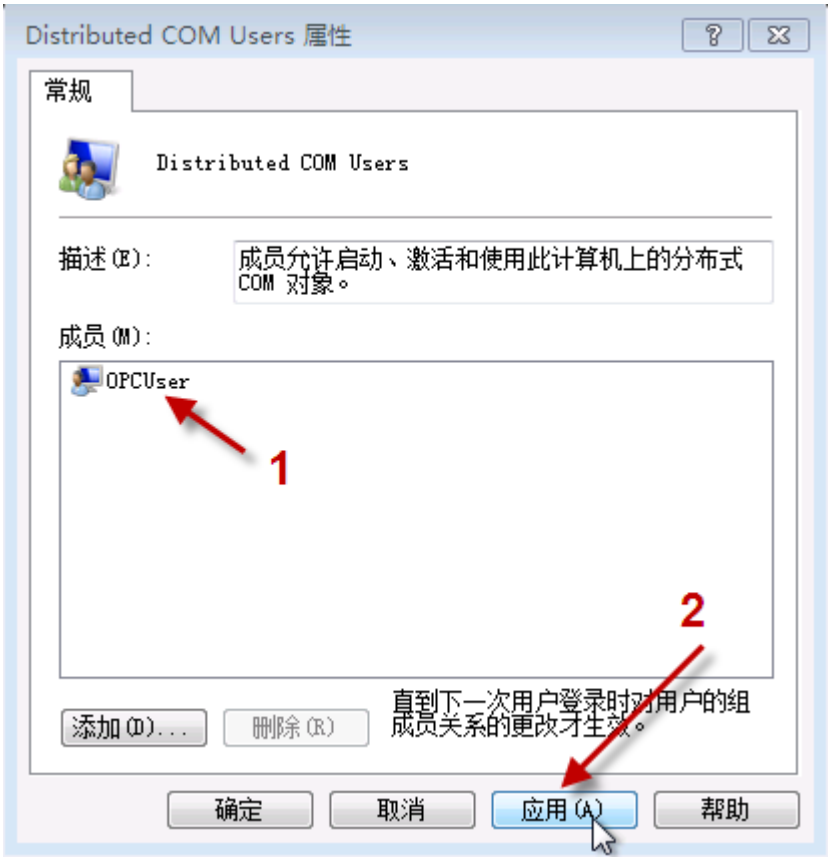

图 10 完成添加

可以添加多个用户到“Distribute COM Users”用户组，也可以添加现有用户到用户组。

三、 修改操作系统 Firewall（防火墙）关于 DCOM 和 OPC 的规则

由于 DCOM 使用操作系统的 135 端口，所以要想不同计算机上面的 OPC 服务器和 OPC 客户端通讯正常，要修改防火墙规则，允许 135 端口的连接。如果 OPC 服务器和 OPC 客户端安装在同一台计算机，不需要修改防火墙规则。下面用 Windows 7 的防火墙配置过程为示例。

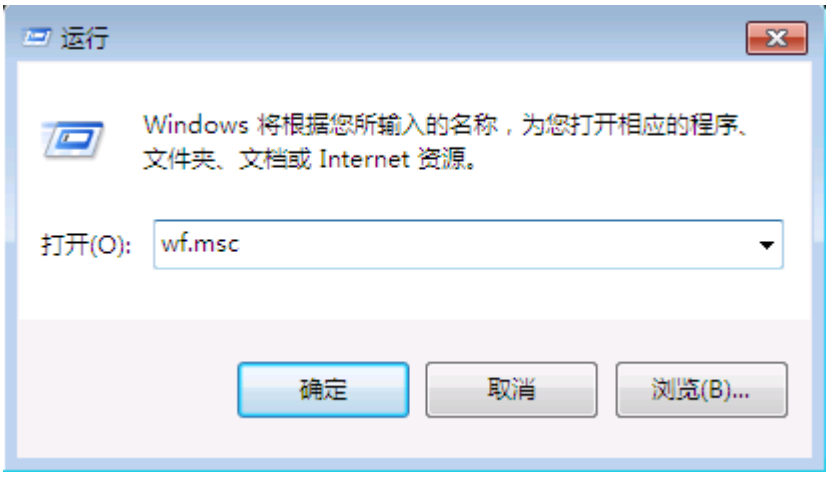

图 11 进入防火墙管理控制台

Windows 7 用户：要打开防火墙管理控制台，可以从“开始“->“控制面板”->“管理工具”->“Windows 防火墙”->“高级设置”，或在“运行”输入“wf.msc”命令。

Windows Server 2008 R2 用户：要打开防火墙管理控制台，可以在“服务器管理工具”，或在“运行”输入“wf.msc”命令。

1、 开放 DCOM 访问

在默认状态，Windows 防火墙是阻止另一台计算机连接的。如果要允许 OPC 客户端与 OPC 服务器正常访问，需要放开这个访问规则。

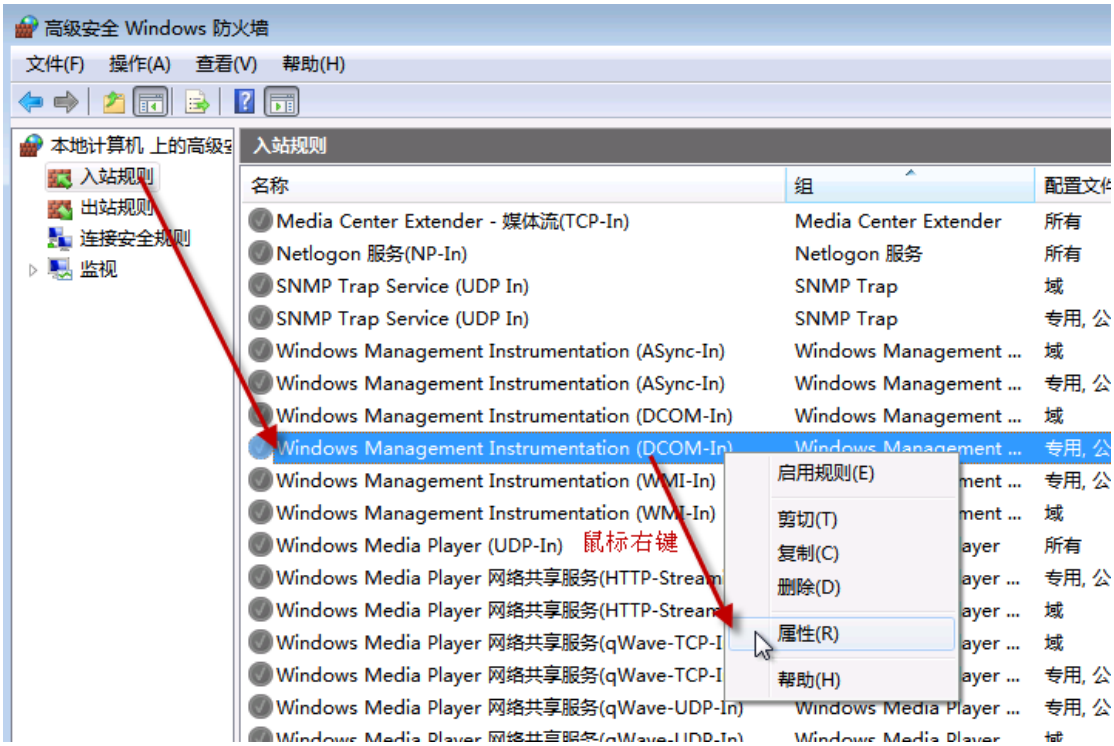

图 12 防火墙规则

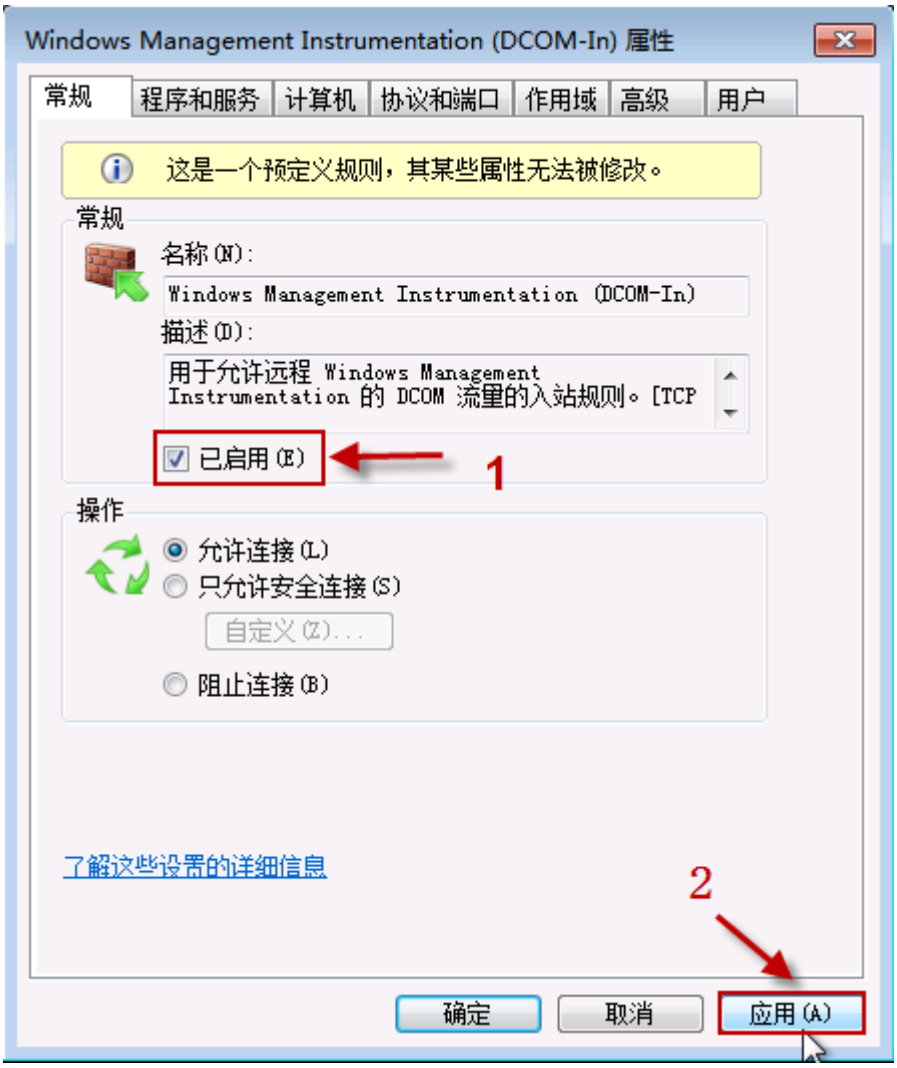

图 13 允许 DCOM 连接

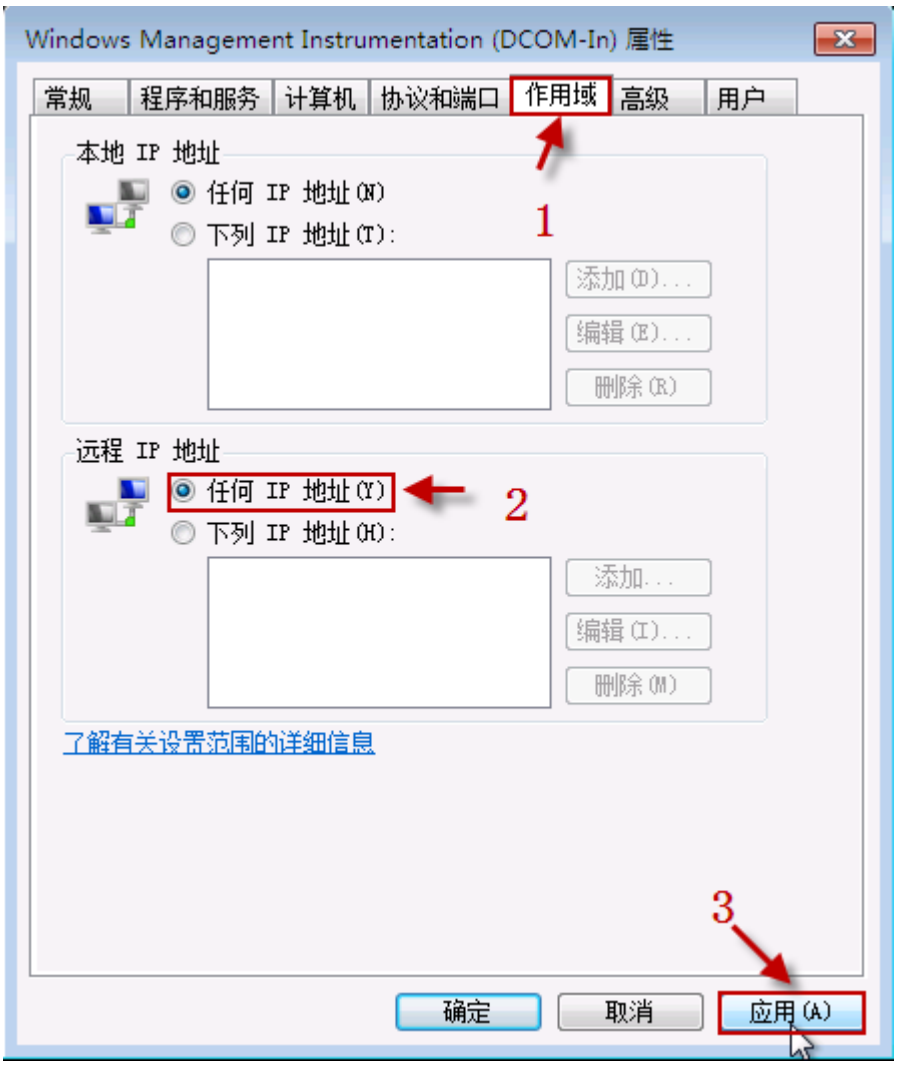

图 14 防火墙 DCOM 规则作用域设置

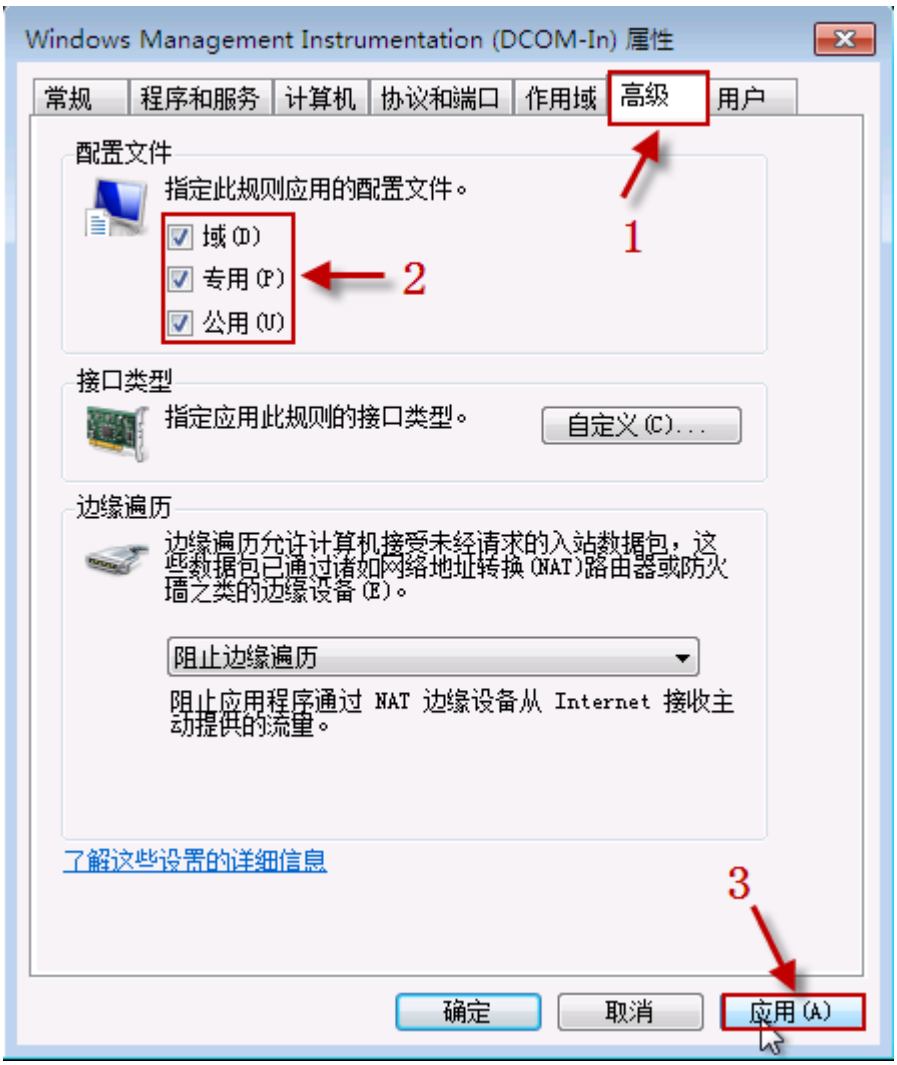

图 15 防火墙 DCOM 规则高级属性配置

Windows 7 用户：如果“COM+ Network access”或“DCOM”规则不在防火墙的预定义规则列表中，可自己手动添加两个“PORT”（端口）规则：

- TCP 135
- UDP 135

2、 创建 OPC 程序规则

需要手动添加 OPC 服务器程序的规则。同样也需要添加 OPCEnum 系统服务程序规则，因为远程的 OPC 客户端计算机就是通过它获得这台计算机上面的 OPC 服务器名称列表的。

下面我们通过创建 OPCEnum 应用的规则，演示如何创建应用的防火墙规则。可用同样步骤创建 OPC 服务器的防火墙规则。

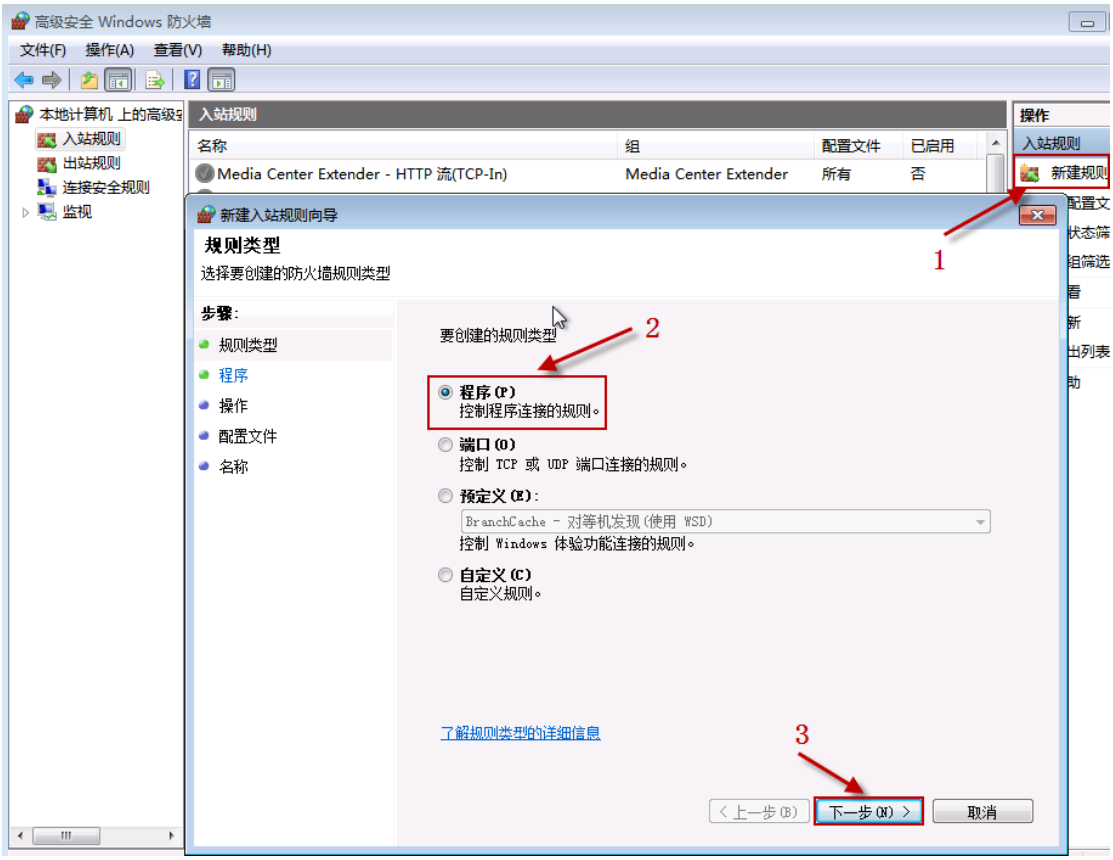

图 16 创建应用规则

*选择“新建规则”;

*选择“程序”类型规则

*点击“下一步”按钮

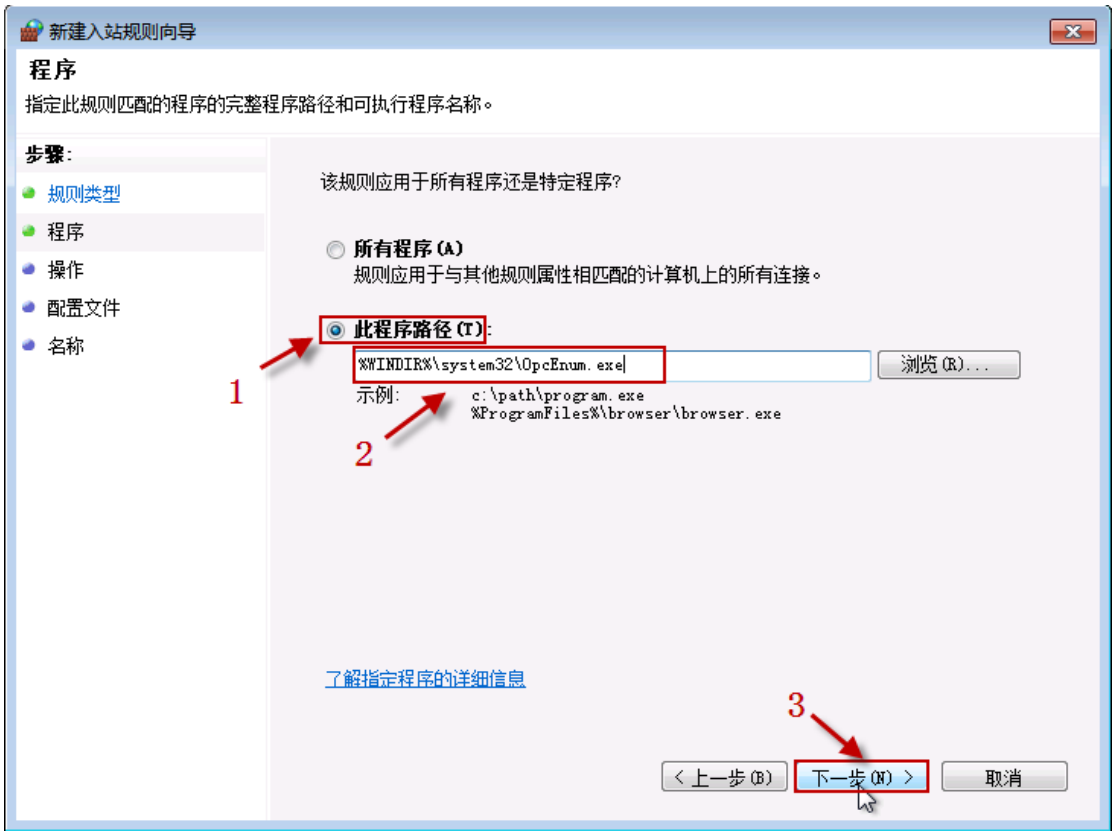

图 17 选择应用程序文件

*选择“此程序路径”项目；

*填写程序的完整路径和应用程序名称；

*也可使用“浏览”按钮，在弹出的文件选择对话框里查找磁盘上应用程序的文件名；

*点击“下一步”按钮；

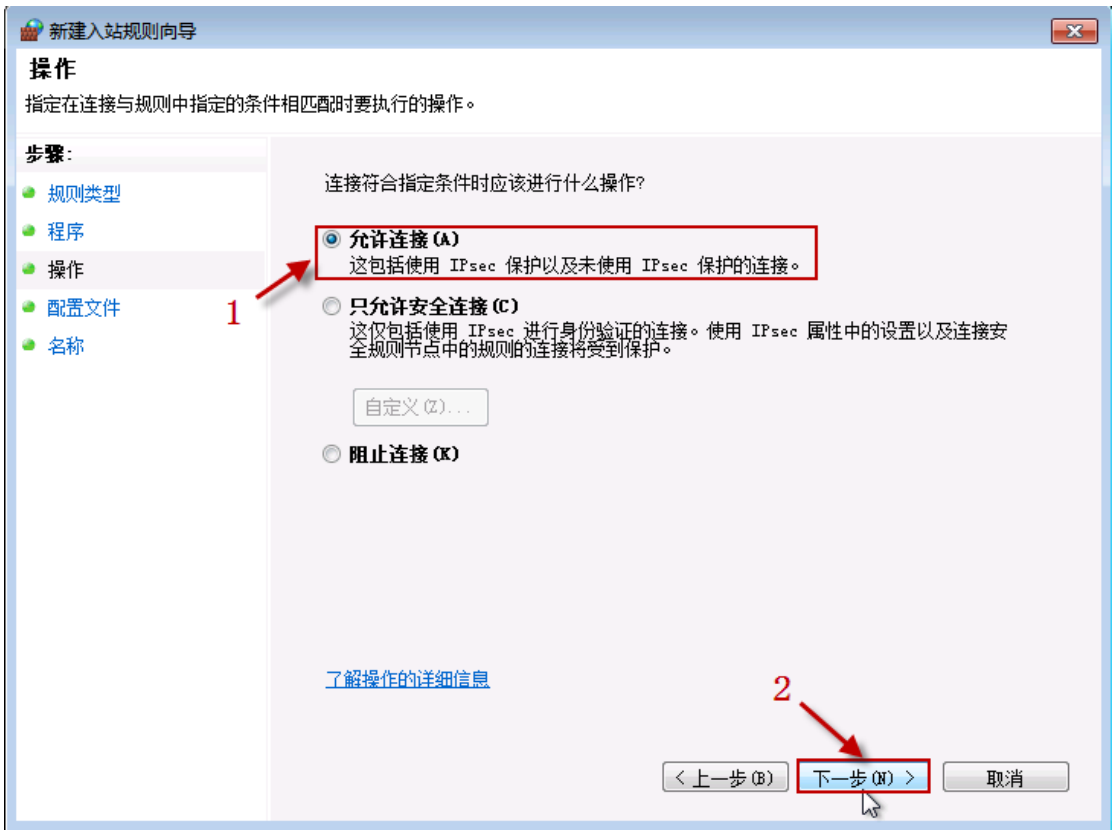

图 18 规则属性

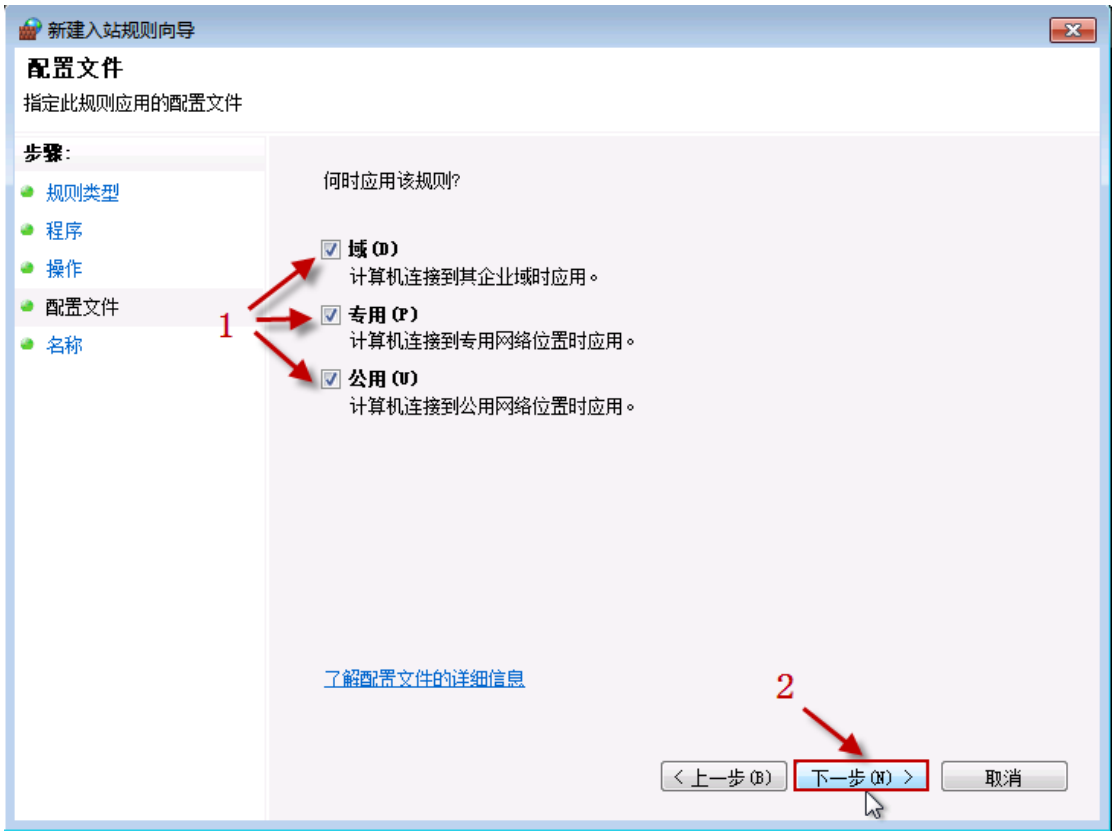

图 19 规则适用条件

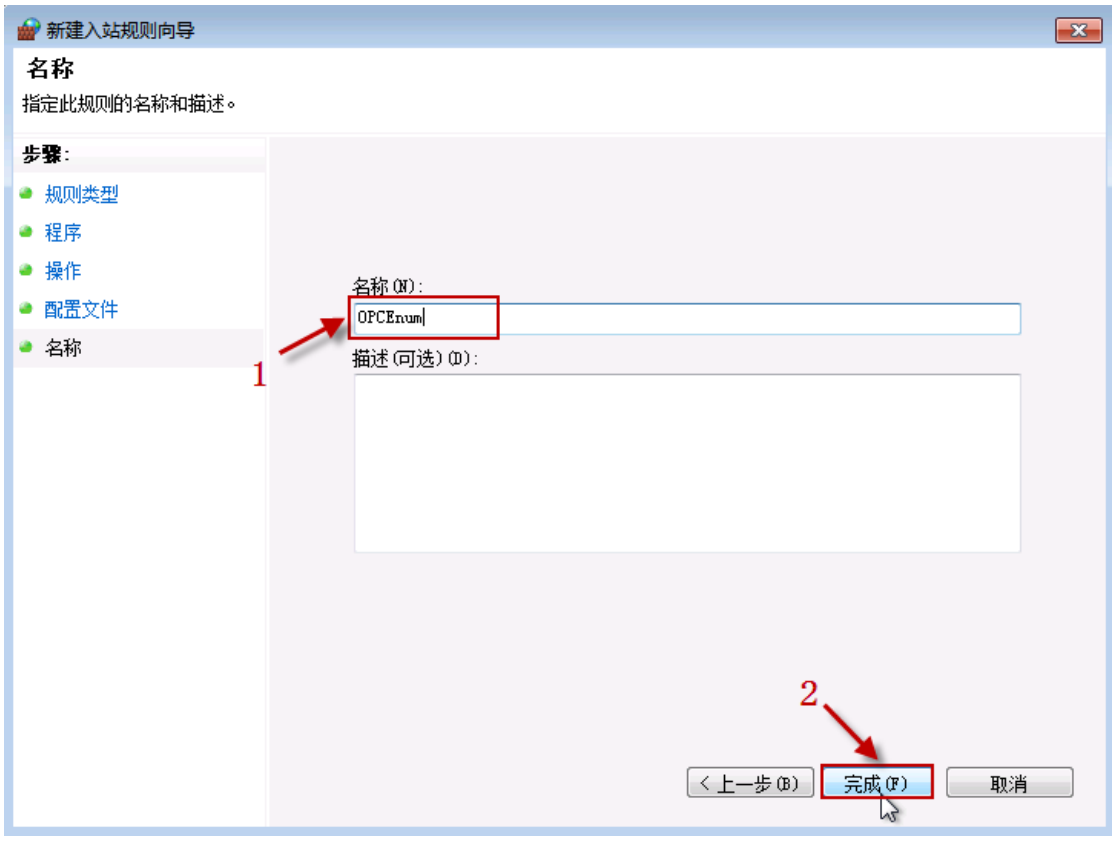

图 20 规则命名

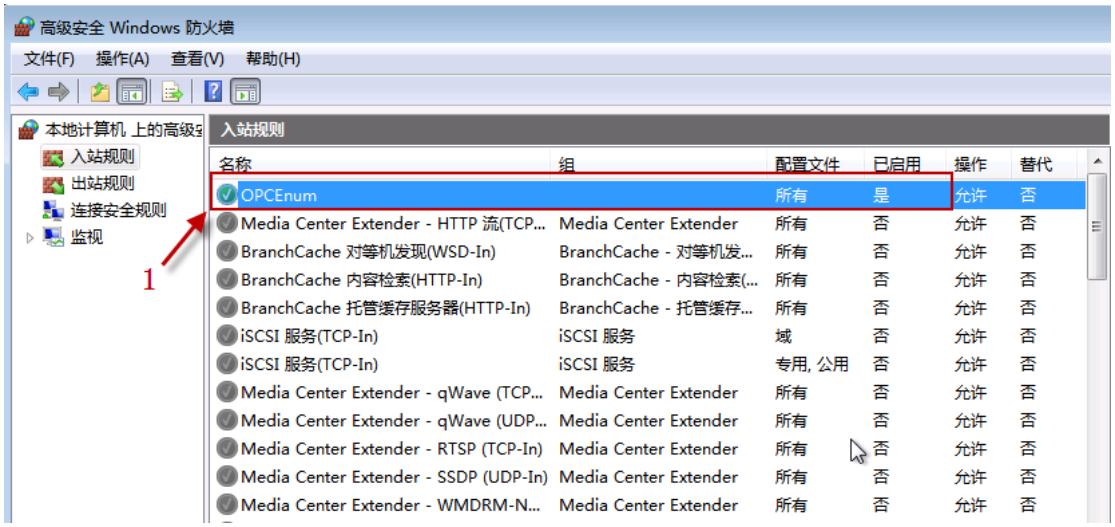

图 21 规则处于活跃状态

同样步骤，创建 OPC 服务器应用程序的防火墙访问规则。

四、 配置 DCOM 安全

为通过网络正常访问 OPC 服务器，需要配置 DCOM 的访问和激活安全属性。

1. 启动“组件服务”,32 位操作系统和 64 位操作系统不同，如下：

32 位操作系统下在菜单“开始\运行”，输入：mmc comexp.msc ，点击“确定”按钮，进入“组件服务管理器”。

如图：

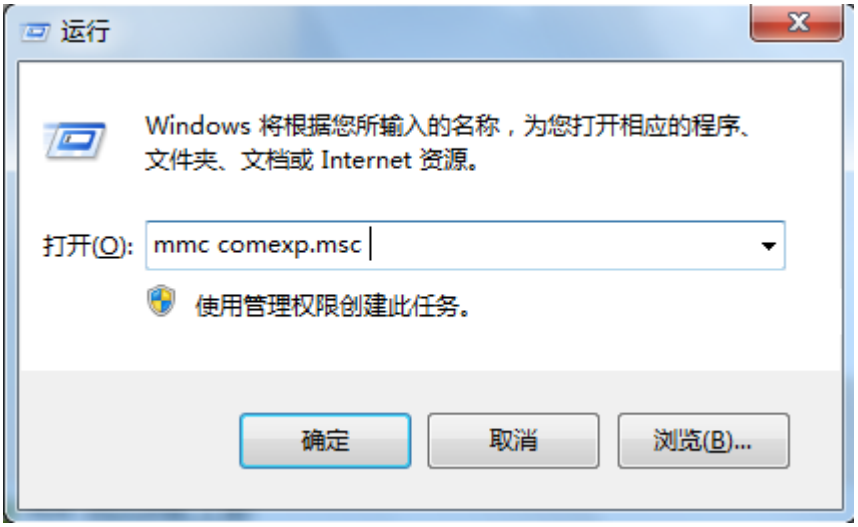

图 22 运行组件服务

64 位操作系统下在菜单“开始\运行”，输入：mmc comexp.msc /32，点击“确定”按钮，进入“组件服务管理器”。

如图：

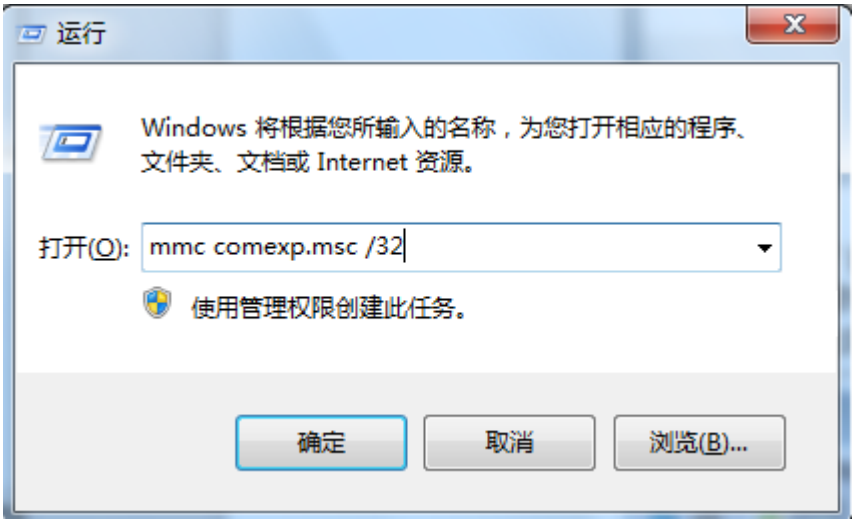

图 23 运行组件服务

2. 配置“我的电脑”的安全设置

在“组件服务”管理器的左侧树形菜单，选择“组件服务\计算机\我的电脑”，在鼠标右键的弹出菜单，选择“属性”项目，如图：

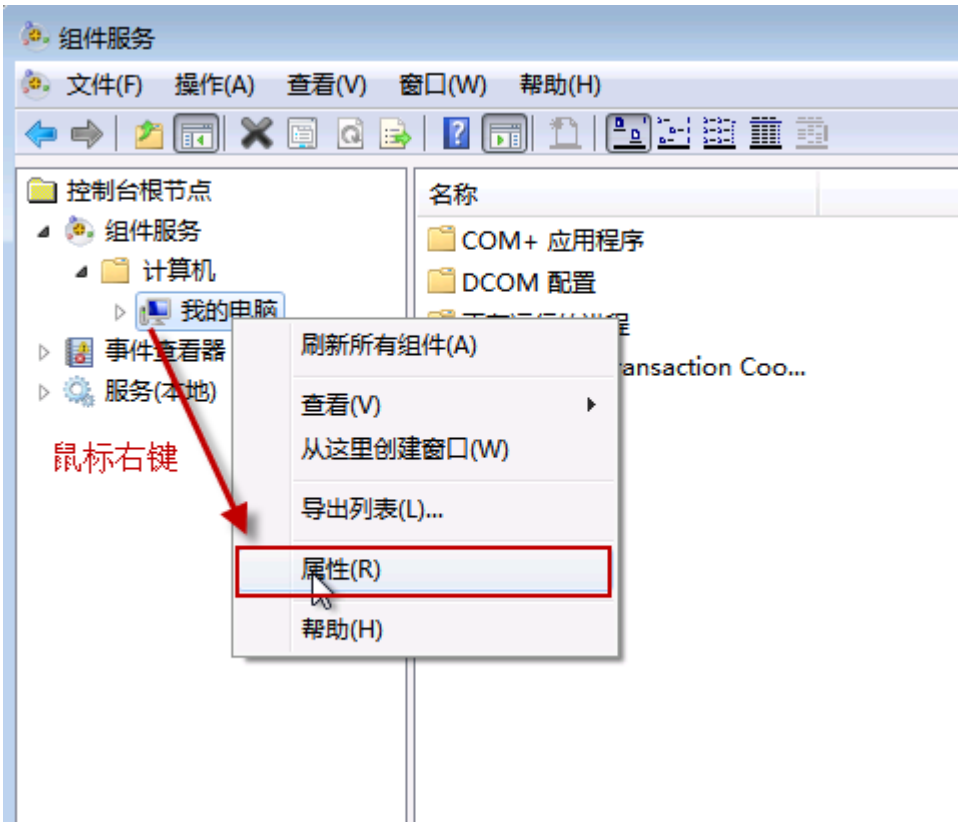

图 24 属性

在弹出的“我的电脑属性”，选择“默认属性”标签页，如下图：

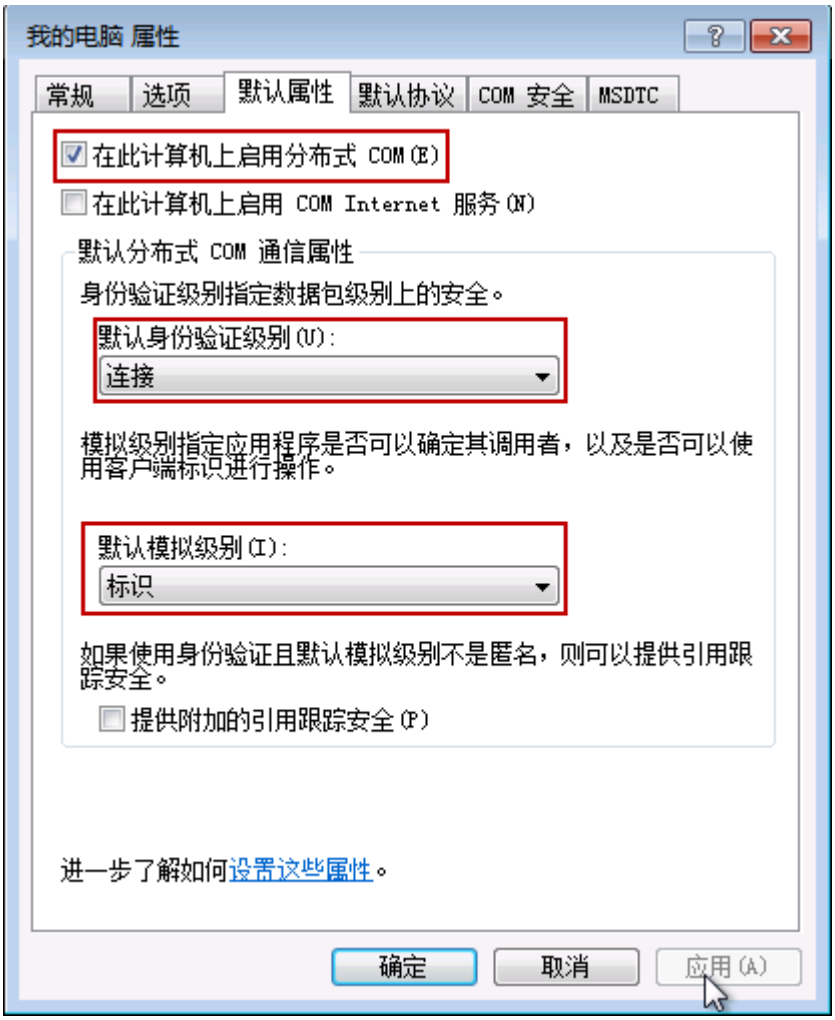

图 25 属性

请确认几个属性的设置内容或状态：

在此计算机上启用分布式 COM，此属性处于“选中”状态；

默认分布式 COM 通信属性栏目下，“默认身份验证级别”，选择的项目是：“连接”，“默认模拟级别”，选择的项目是：“标识”。

选择“我的电脑属性”属性页面的“默认协议”标签页，如下图：

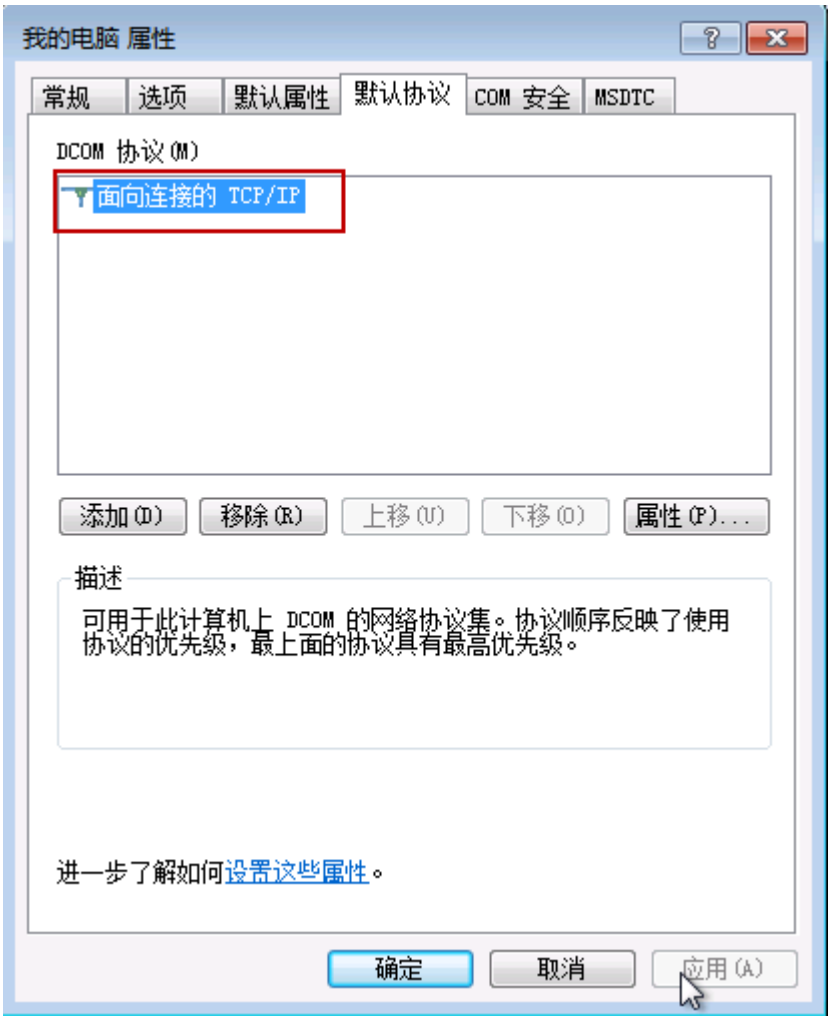

图 26 属性

确认 DCOM 协议属性内容是：面向连接的 TCP/IP。

选择“我的电脑属性”属性页面的“COM 安全”标签页，如下图：

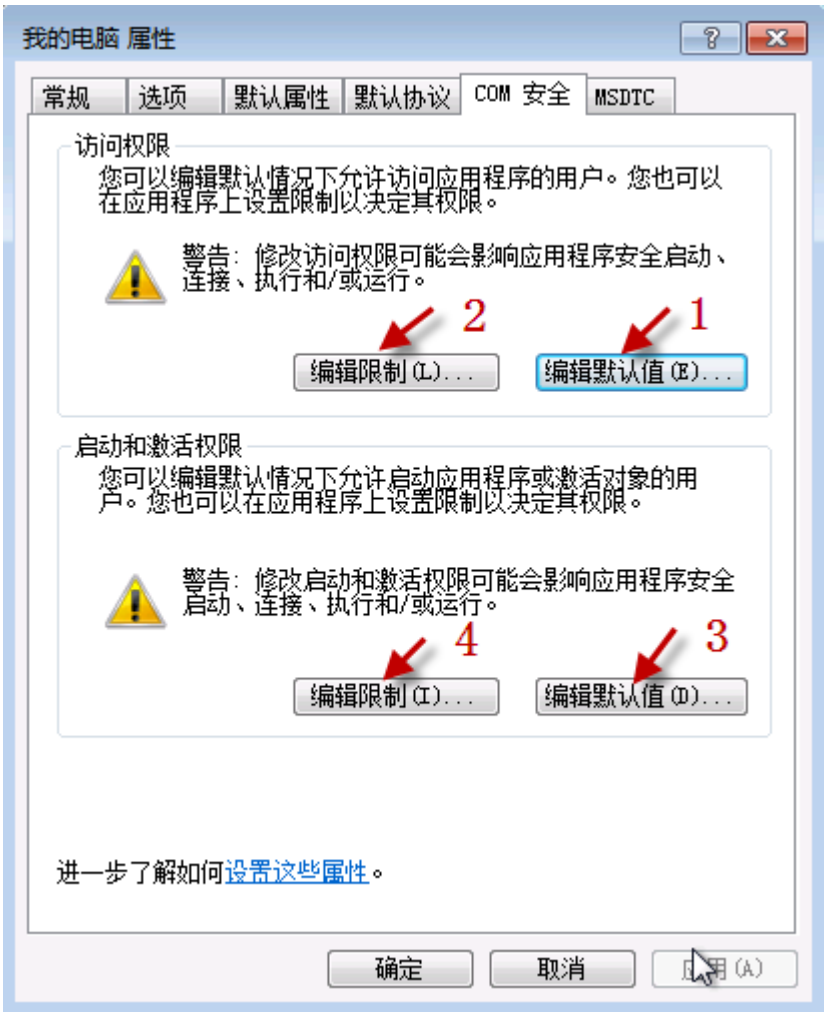

图 27 COM 安全

选择“COM 安全”标签页面的“访问权限”栏目的“编辑默认值…”按钮（图 27 中按钮 1），弹出“访问权限”设置对话框，如下图：

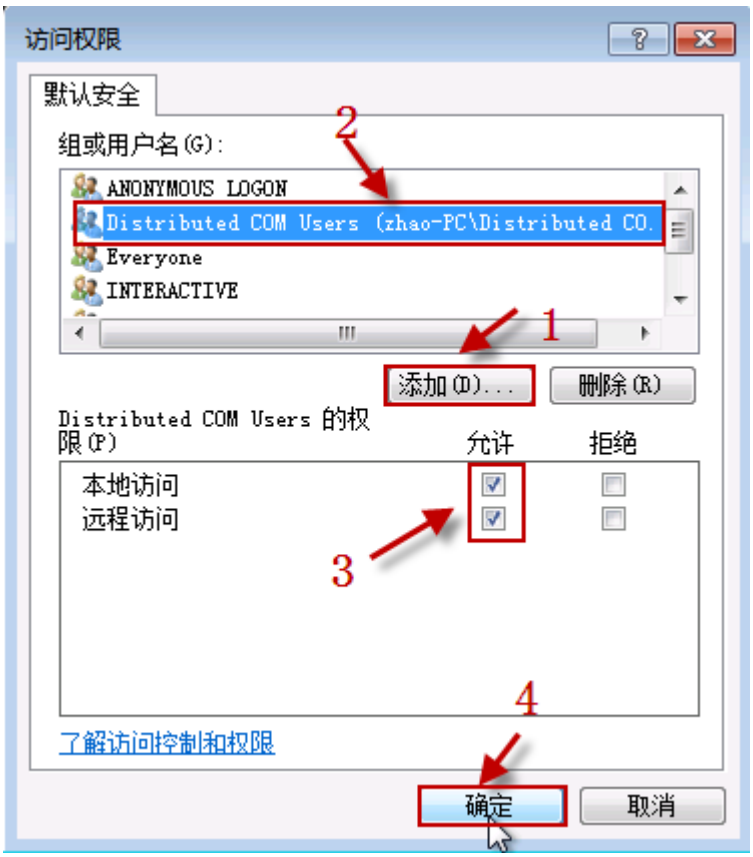

图 28 配置访问权限

点击此对话框上的“添加”按钮，添加下边列表的用户，并设置用户的访问权限，核实后，点击“确定”按钮保存。

NO.	组或用户名	本地访问	远程访问	属性
1	Distribute COM Users	允许	允许	系统内置用户组
2	Anonymous logon	允许	允许	系统内置帐户
3	everyone	允许	允许	系统内置帐户
4	Interactive	允许	允许	系统内置帐户
5	SYSTEM	允许	允许	系统内置帐户
6	SELF	允许	允许	系统内置帐户

选择“COM 安全”标签页面的“访问权限”栏目的“编辑限制…”按钮（图 27 中按钮 2），弹出“访问权限”设置对话框，如下图：

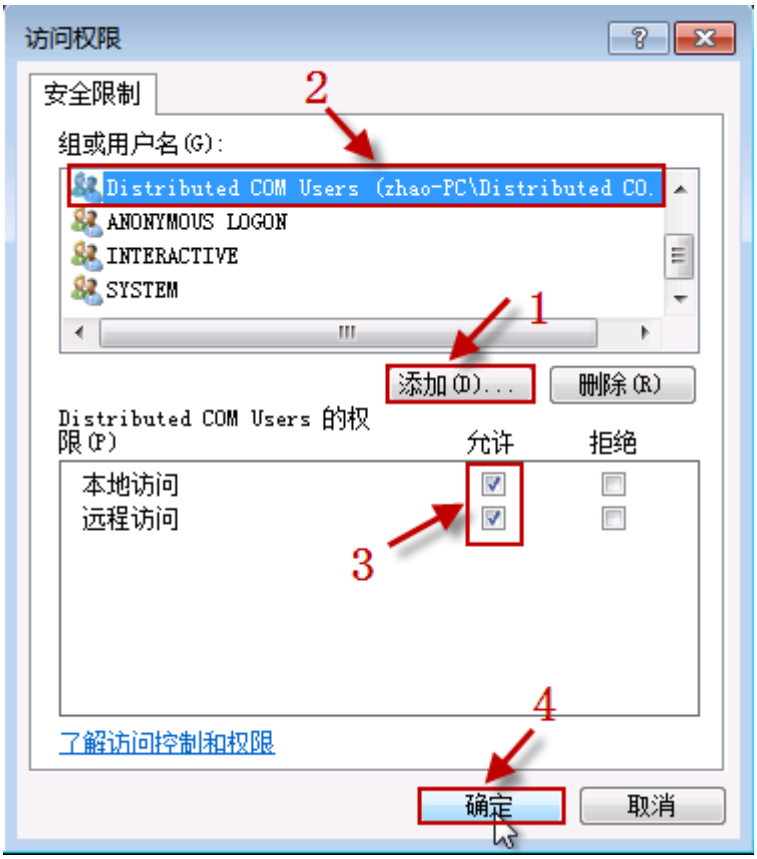

图 29 配置访问权限

点击此对话框上的“添加”按钮，添加下边列表的用户，并设置用户的访问权限，核实后，点击“确定”按钮保存。

NO.	组或用户名	本地访问	远程访问	属性
1	Distribute COM Users	允许	允许	系统内置用户组
2	Anonymous logon	允许	允许	系统内置帐户
3	everyone	允许	允许	系统内置帐户
4	Interactive	允许	允许	系统内置帐户
5	SYSTEM	允许	允许	系统内置帐户

选择“COM 安全”标签页面的“启动和激活权限”栏目的“编辑默认值…”按钮（图 27 中按钮 3），弹出“启动和激活权限”设置对话框，如下图：

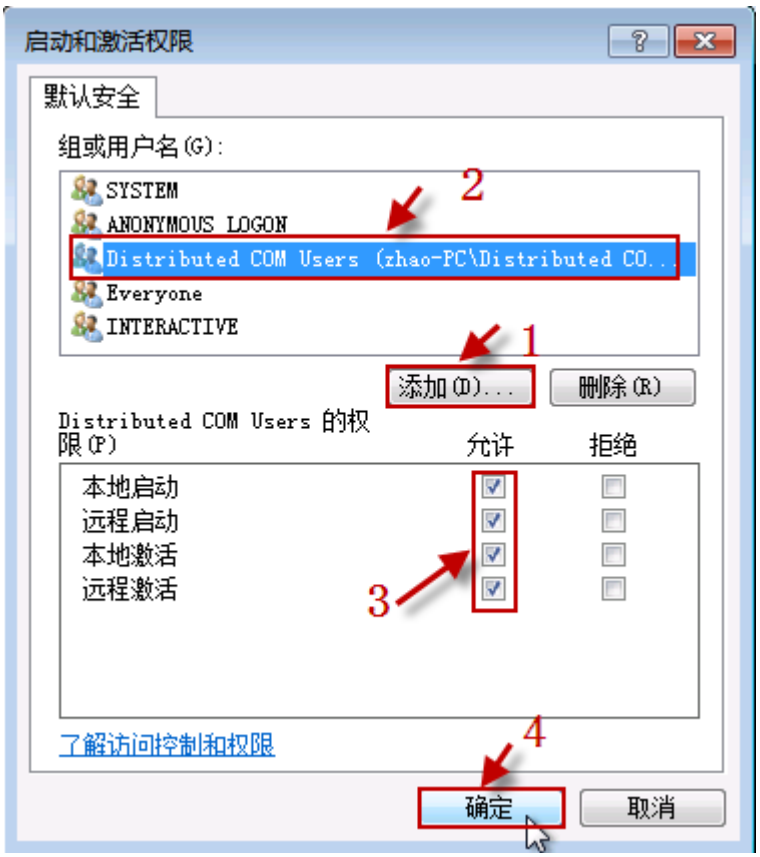

图 30 配置启动激活权限

点击此对话框上的“添加”按钮，添加下边列表的用户，并设置用户的访问权限，核实后，点击“确定”按钮保存。

NO.	用户名	本地启动	远程启动	本地激活	远程激活	属性
1	Distribute COM Users	允许	允许	允许	允许	系统内置用户组
2	ANONYMOUS LOGON	允许	允许	允许	允许	系统内置帐户
3	Everyone	允许	允许	允许	允许	系统内置帐户
4	INTERACTIVE	允许	允许	允许	允许	系统内置帐户
5	SYSTEM	允许	允许	允许	允许	系统内置帐户

选择“COM 安全”标签页面的“启动和激活权限”栏目的“编辑限制…”按钮（图 27 中按钮 4），弹出“启动和激活权限”设置对话框，如下图：

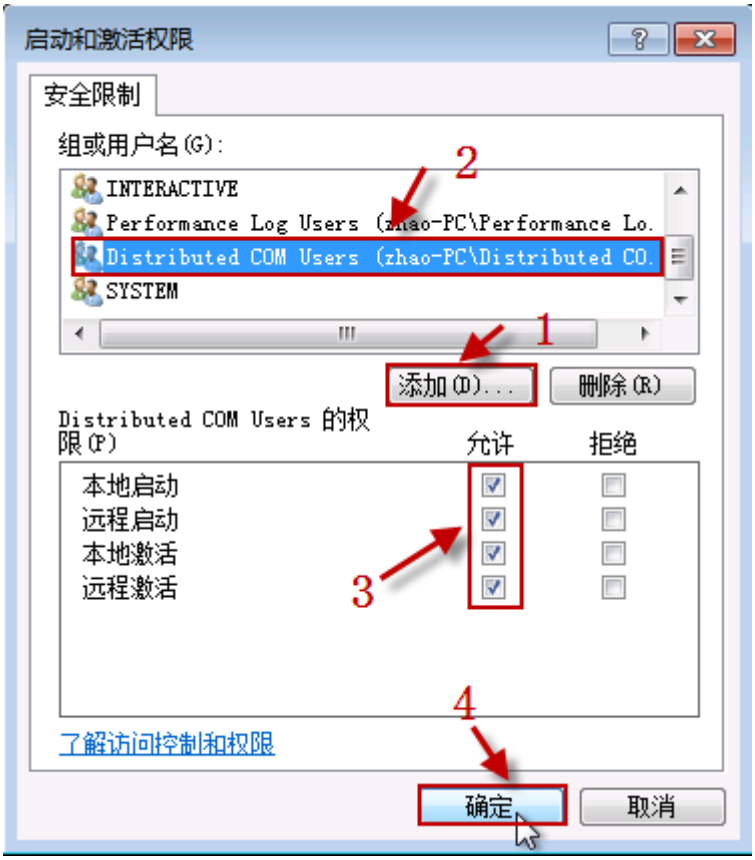

图 31 配置启动激活权限

点击此对话框上的“添加”按钮，添加下边列表的用户，并设置用户的访问权限，核实后，点击“确定”按钮保存。

NO.	用户名	本地启动	远程启动	本地激活	远程激活	属性
1	Distribute COM Users	允许	允许	允许	允许	系统内置用户组
2	ANONYMOUS LOGON	允许	允许	允许	允许	系统内置帐户
3	Everyone	允许	允许	允许	允许	系统内置帐户
4	INTERACTIVE	允许	允许	允许	允许	系统内置帐户
5	SYSTEM	允许	允许	允许	允许	系统内置帐户

配置完成后，点击“我的电脑属性”属性页面的“确定”按钮，由于涉及到系统安全属性的修改，此时操作系统弹出警告消息，如图：

图 32 警告消息

由于是我们手动修改的安全设置，并确认修改，点击“是”按钮，保存刚才做出的所有修改，退出“我的电脑属性”属性页面。

3. 配置 OPCENUM 的安全设置

在“组件服务”左侧树形菜单，选择“组件服务\计算机\我的电脑\DCOM 配置”，在列表中选择 opcenum 项目，在鼠标右键弹出的菜单，选择“属性”项目，如下图：

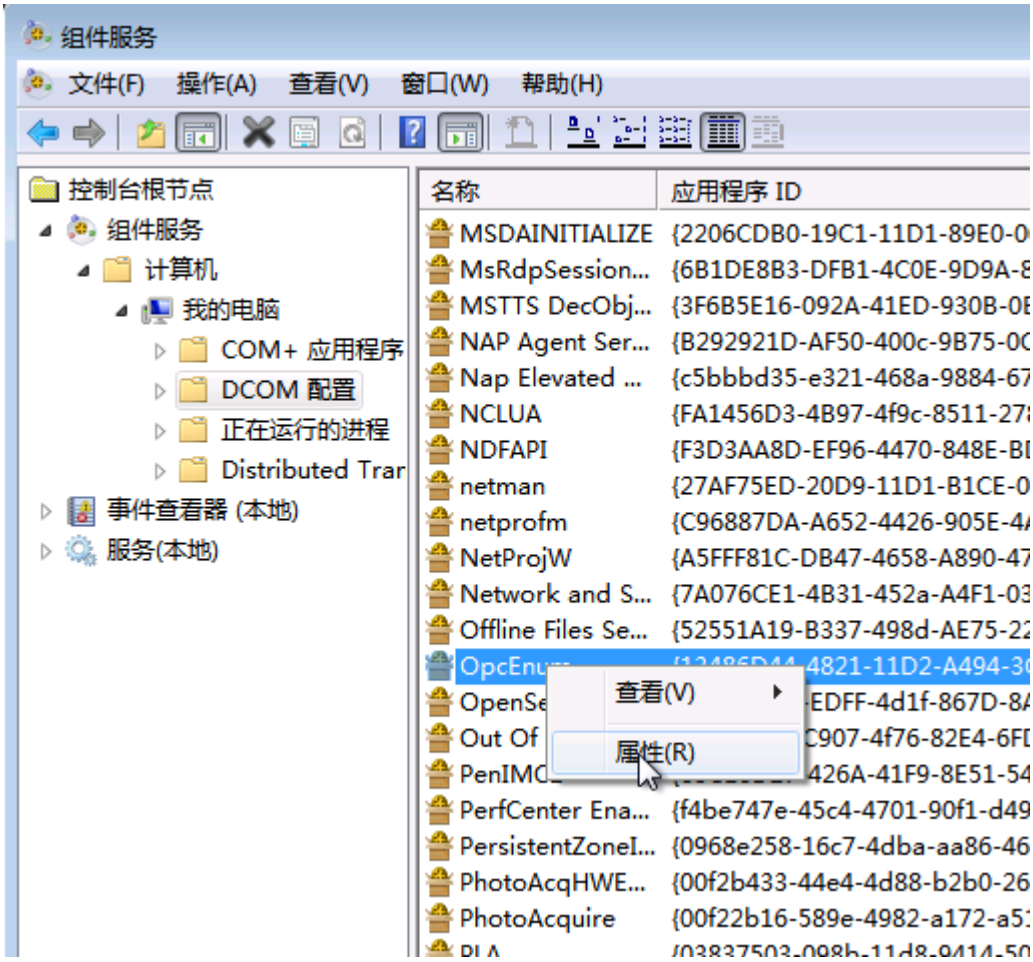

图 33

在弹出的“OPCENUM 属性”属性框的“常规”标签页，确认“身份验证级别”属性，设置项目是：无，如下图：

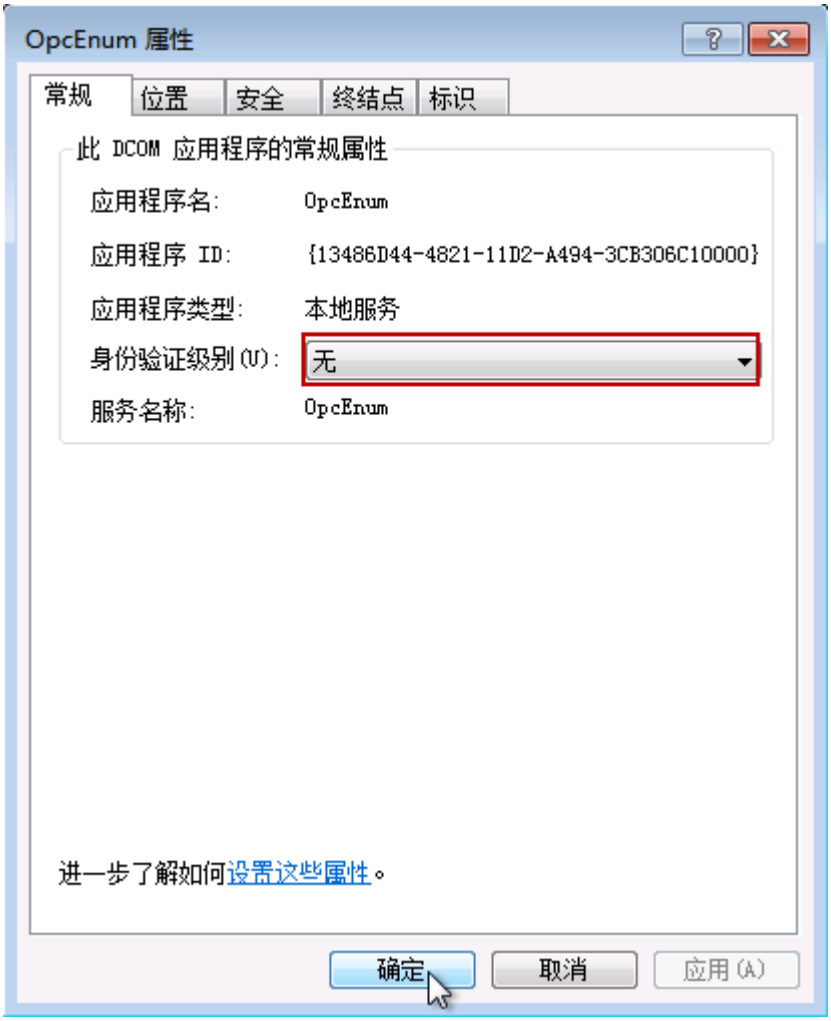

图 34

在“OPCENUM 属性”框，选择“安全”标签页，如下图：

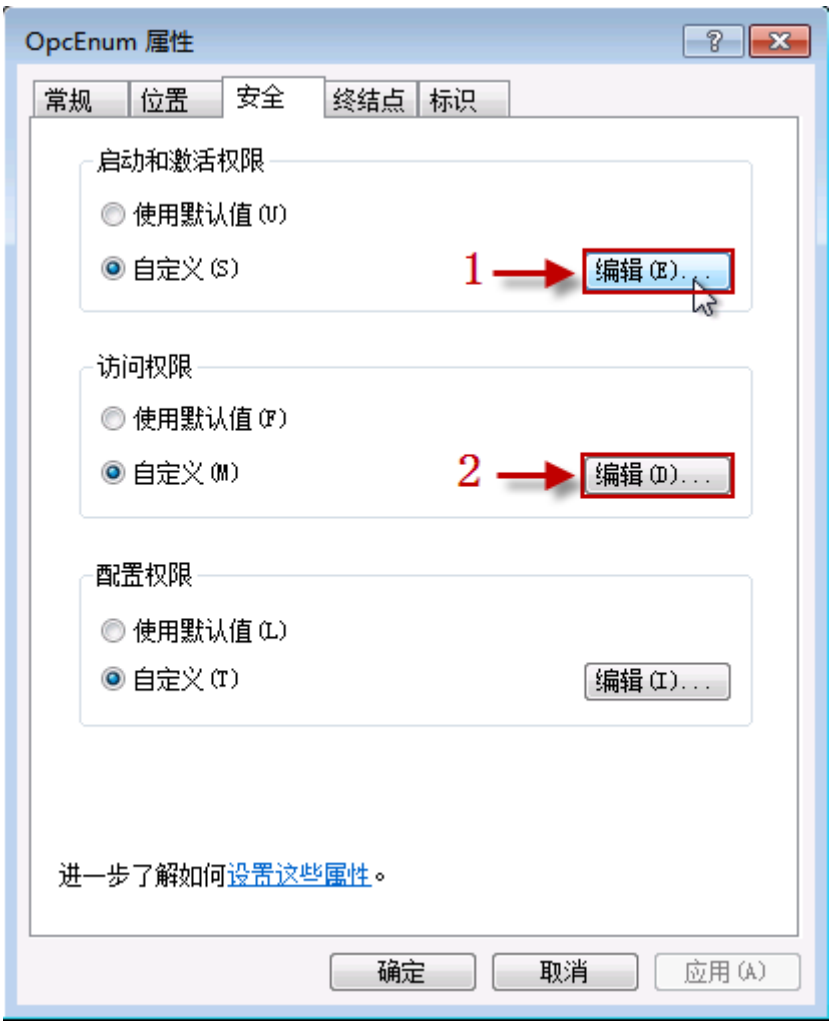

图 35

在“安全”标签页，选择“启动和激活权限”栏目，选择“自定义”选项，并点击“编辑…”按钮，如下图：

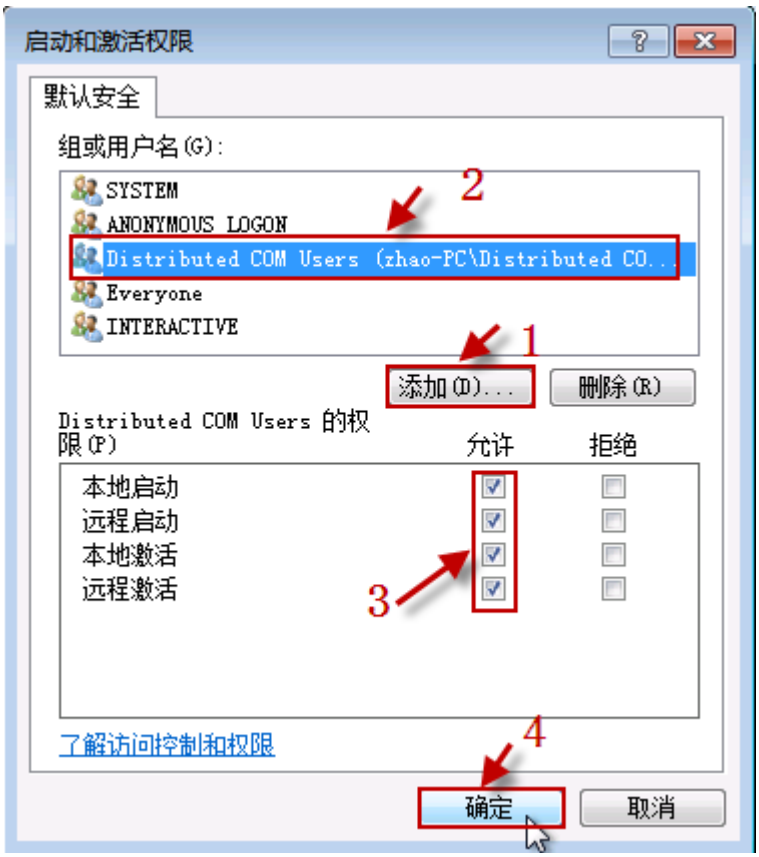

图 36

在弹出的“启动和激活权限”属性设置对话框，使用“添加”按钮，添加下表的组或用户，核实并确认后，点击“确定”按钮保存。

NO.	用户名	本地启动	远程启动	本地激活	远程激活	属性
1	Distribute COM Users	允许	允许	允许	允许	系统内置用户组
2	ANONYMOUS LOGON	允许	允许	允许	允许	系统内置帐户
3	Everyone	允许	允许	允许	允许	系统内置帐户
4	INTERACTIVE	允许	允许	允许	允许	系统内置帐户
5	SYSTEM	允许	允许	允许	允许	系统内置帐户

在“安全”标签页，选择“访问权限”栏目，选择“自定义”选项，并点击“编辑…”按钮，如下图：

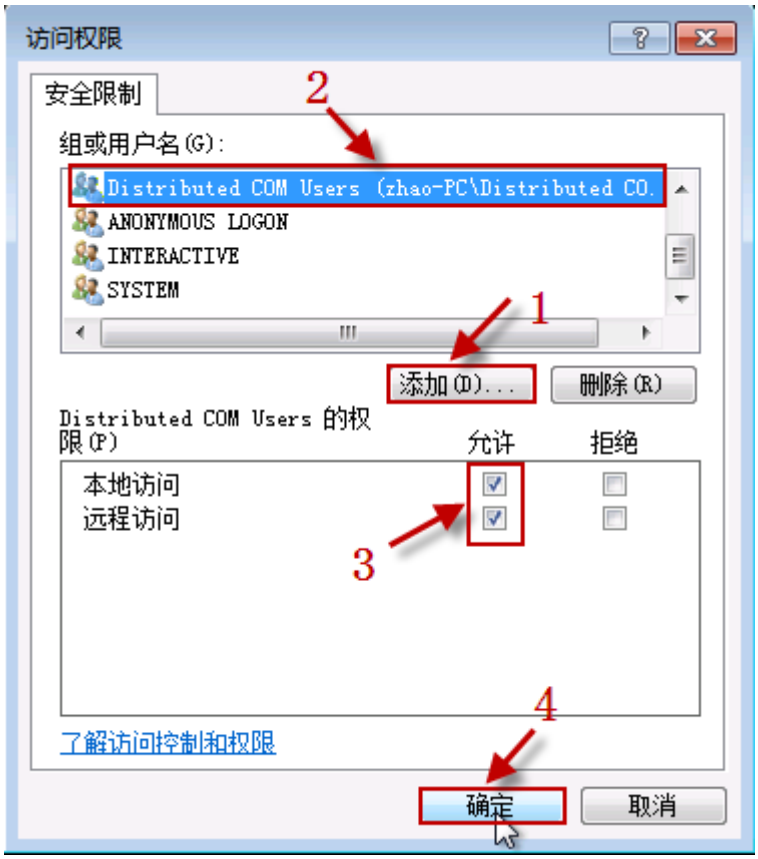

图 37

在弹出的“访问权限”属性设置对话框，使用“添加”按钮，添加下表的组或用户，核实并确认后，点击“确定”按钮保存。

NO.	组或用户名	本地访问	远程访问	属性
1	Distribute COM Users	允许	允许	系统内置用户组
2	Anonymous logon	允许	允许	系统内置帐户
3	everyone	允许	允许	系统内置帐户
4	Interactive	允许	允许	系统内置帐户
5	SELF	允许	允许	系统内置帐户
6	SYSTEM	允许	允许	系统内置帐户

在“OPCENUM 属性”框，选择“标识”标签页，确认“选择运行此应用程序的用户账户”属性，设置项目是：系统账户（仅用于服务），如下图：

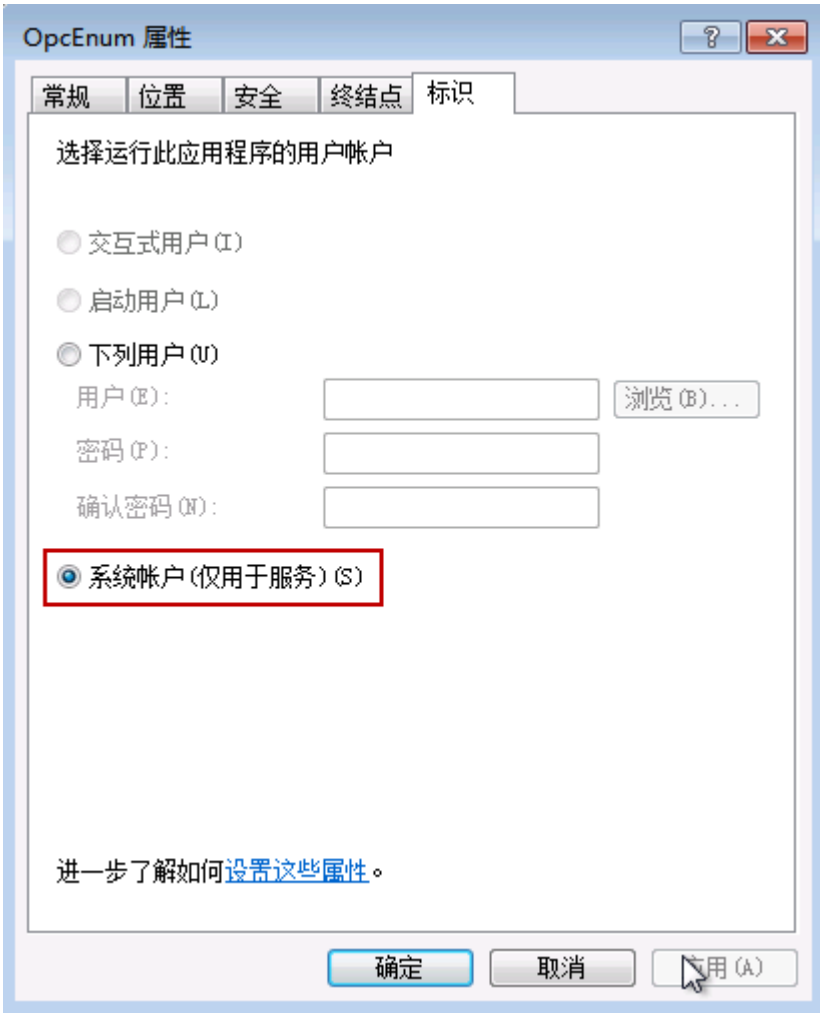

图 38

确认后点击“确定”按钮保存所作的修改。

4. OPC 服务器的安全设置

OPC 服务器的安全设置可参照 OPCEnum 的设置过程，只是在“标识”属性页面不同，设置如下图：

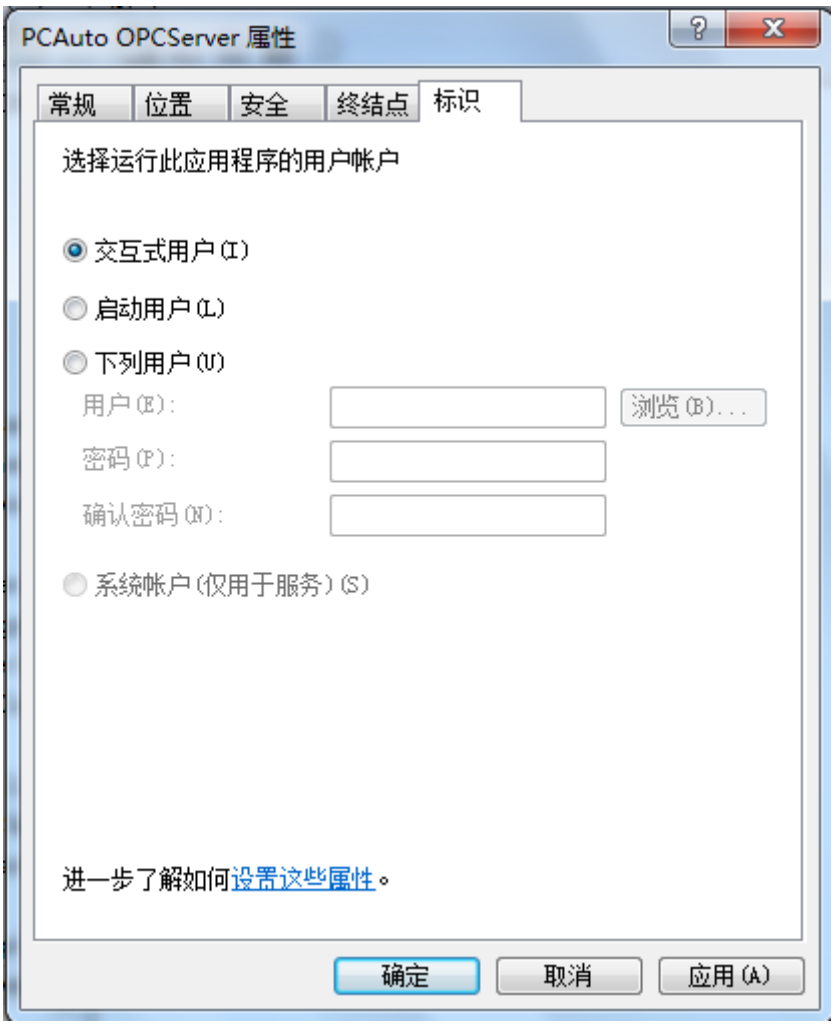

图 39

五、配置本地安全策略

1、 启动“本地安全策略”管理器

在“开始\运行”输入：secpol.msc，点击“确定”按钮，启动“本地安全策略”管理器，如下图：

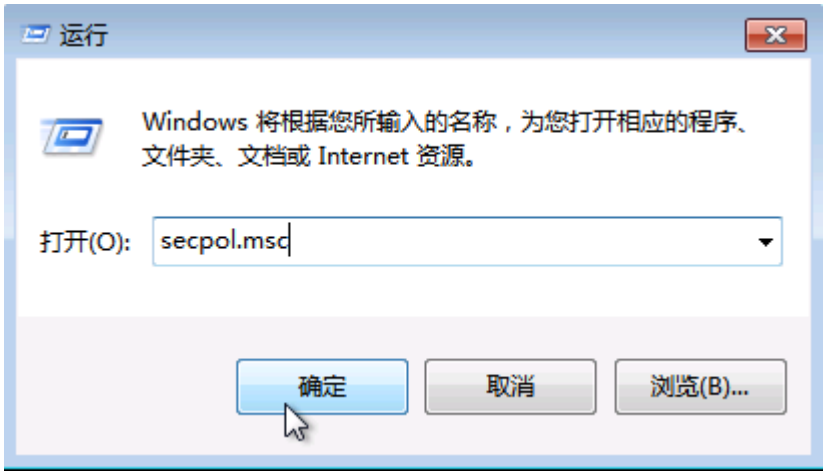

图 40

2、用户权限分配设置

拒绝从网络上访问这台计算机选项中删除 guest 用户如下图

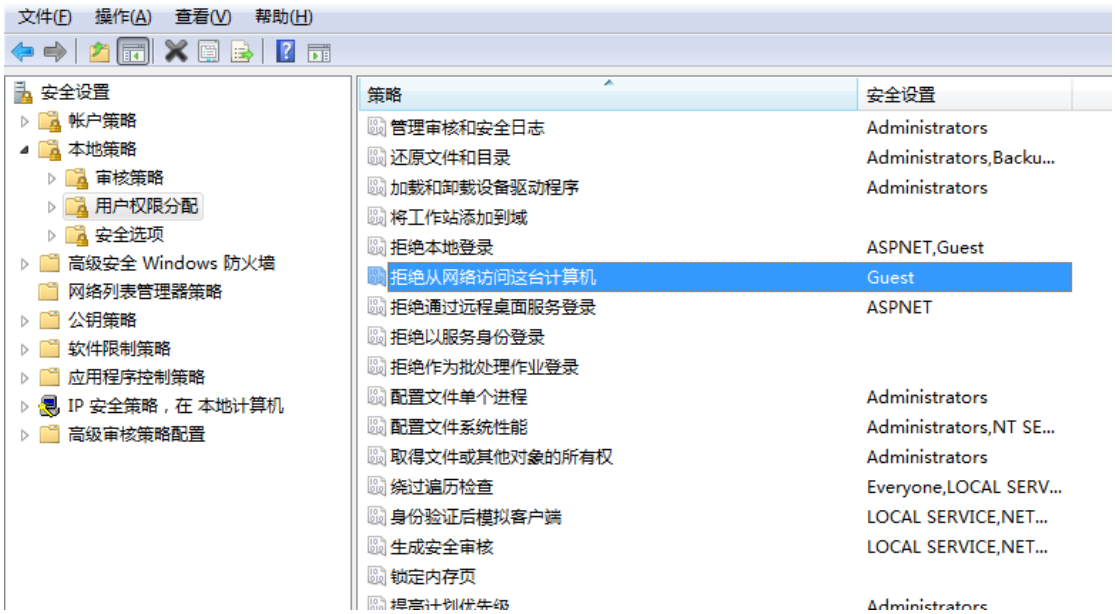

图 41

3、安全选项设置

修改“网络访问：将 Everyone 权限应用于匿名访问匿名用户”设置

修改“安全设置\本地策略\安全选项”下的“网络访问：将 Everyone 权限应用于匿名访问匿名用户”设置，将规则启用，如下图：

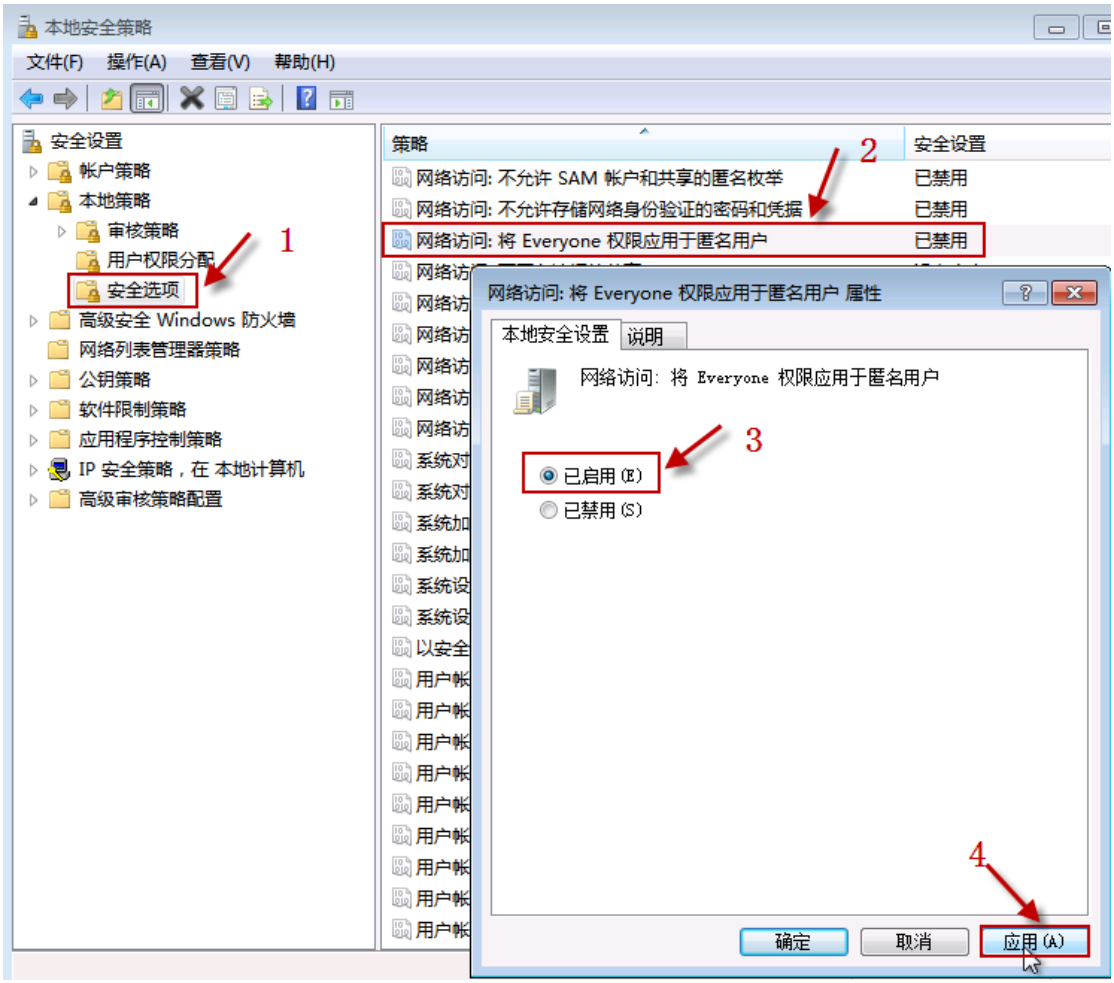

图 42

修改网络访问：本地账户的共享和安全模型为经典模式

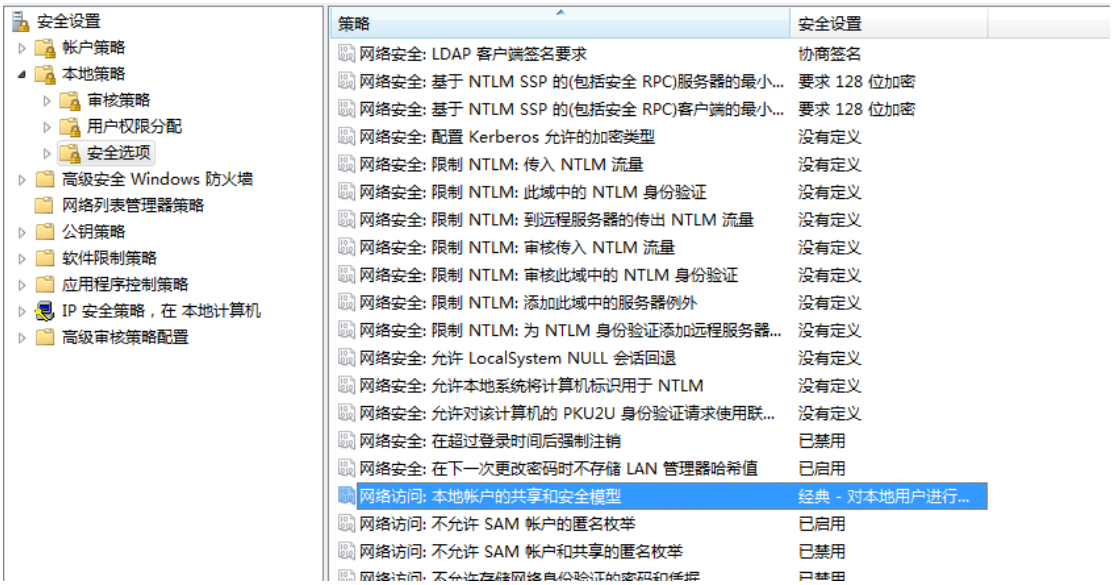

图 43

修改账户：来宾帐户启用

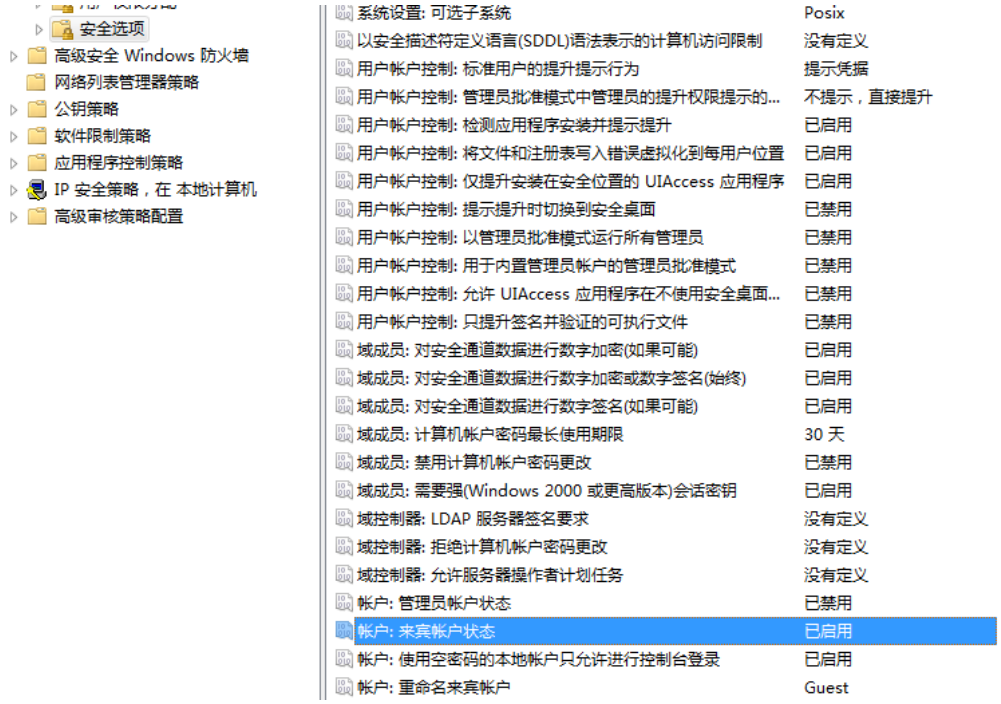

图 44

六、客户端配置

客户端配置除 DCOM 不需要配置 opcserver 之外，其他的可以按照服务器的配置进行配置。

七、其他

1. 防火墙运行状态下，可能 OPC 客户端会出现拒绝访问，可能是防火墙阻止程序访问网络，可以试着修改防火墙设置。调试或测试时，可先将防火墙禁用，排除干扰；

2. 其它防火墙软件配置，可参考 Windows 系统防火墙配置。

3. RPC 服务器不可用

这个错误意味着没能建立与 RPC 服务之间的网络连接。

*如果错误发生在尝试读取远程计算机上边的 OPC 服务器列表时，请检查 OPC 服务器计算机与 OPC 客户端计算机的防火墙配置，看 OPCEnum 应用是否已经加入例外规则列表。

*DCOM 所使用的 135 端口，是否已加入防火墙规则。

*如果错误发生在连接 OPC 服务器时，请检查 OPC 服务器计算机的防火墙配置，看 OPC 服务器应用程序是否已加入防火墙的例外规则列表。

4. 拒绝访问

请检查 DCOM 的安全配置，包括 OPC 服务器所在计算机与 OPC 客户端所在计算机。

5. “IOPCServerList Interface Not Found”错误

请在安装 OPC 运行库分发包或注册 OPC 运行库后，重新启动计算机系统。