Active Directory 权限委派操作指南

2013 年 6 月

目　　录

第 1 章　概述

1.1 实施概述

本文档依据 Exchange 2007 邮件系统升级项目实施准备条件要求，委派各分行管理员进行指定权限的 AD 管理，本文是根据该项目实施过程标准及规范形成该文档。

1.1.1 关于委派控制

委派范围：在 AD 中可以委派控制的范围是站点、域、和组织单位合称为：SDOU

从管理层面来看，不同的委派范围涉及不同的性质工作。例如：站点上最主要工作就是新建、删除站点、网站连接、子网络等项目。组织单位上最常见的工作，通常是新建、删除用户和计算机帐户、重设密码与应用组策略等。所以说，委派的范围有两重意义，第一，它界定了管辖权的范围，就是说被委派的对象只允许在此范围内行使管理权，第二，它提示了不同性质的工作属性，我们应当针对不同的范围委派的工作。

委派对象：在从多 AD 对象中只有用户、计算机和组可以作为委派控制的对象，此外，该对象不必和授权范围有任何隶属关系。例如：可以将 A 组织单位委派给 B 组织单位的成员管理，甚至可以委派给其它域的用户管理。

1.2 实施准备

准备客户端管理机及服务器远程管理工具安装包。客户端管理机须加域

1.3 实施目标

在当前分支机构，如北京、上海、福州等，部署了额外域控，。

1.4 实施思路

1) 准备一台管理操作主机，安装管理工具。
2) 设置管理员相应权限。
3) 派发管理 ou 的控制台文件。

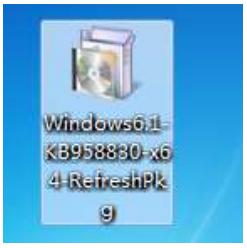
第 2 章　实施步骤

2.1 安装 AD 远程管理工具

[提示：为了避免活动目录域管理员登录后的 token 被窃取攻击的可能性，用户活动目录域 AD 远程管理的这台计算机一定要确保它的安全，这可能包括物理隔绝。]

2.1.1 安装 KB958830 补丁包

双击安装程序



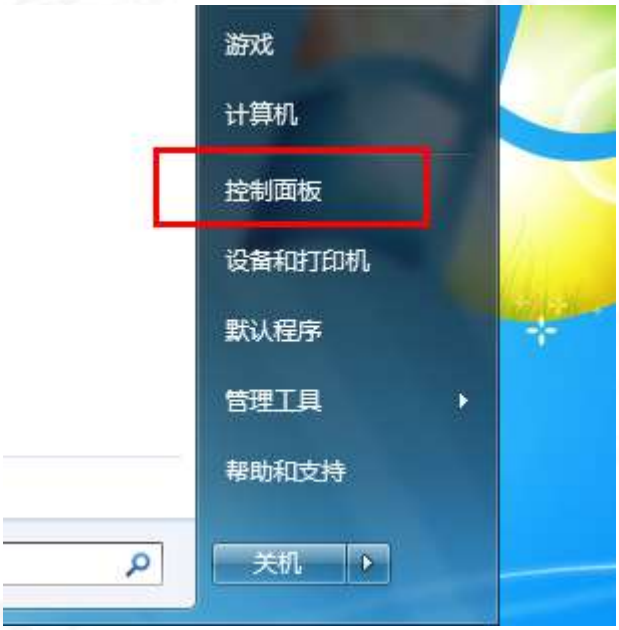
弹出提示是否安装 KB958830 补丁，选择“是”进行安装

选择“我接受”，进行更新安装

等待安装完成，点击“完成”退出。

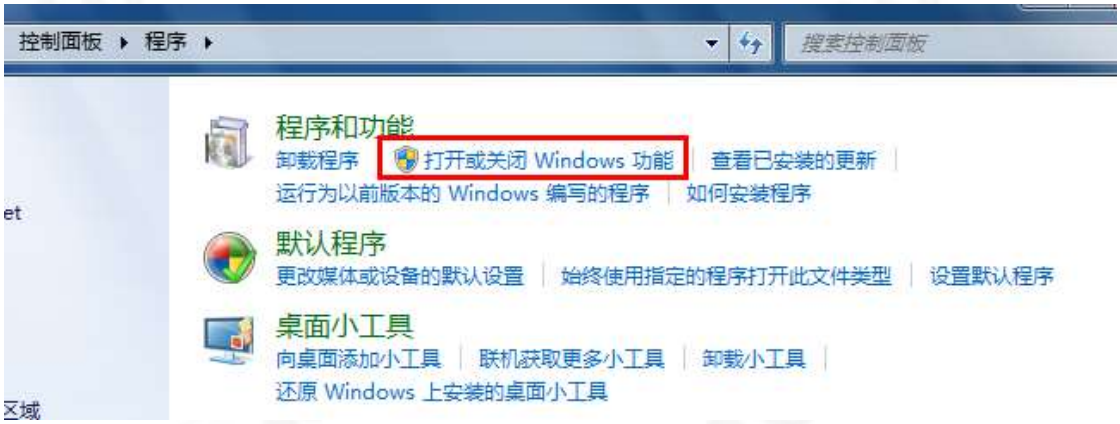
2.1.2 安装 AD 远程管理模块

（1） 安装完 KB958830 后，打开“控制面板”

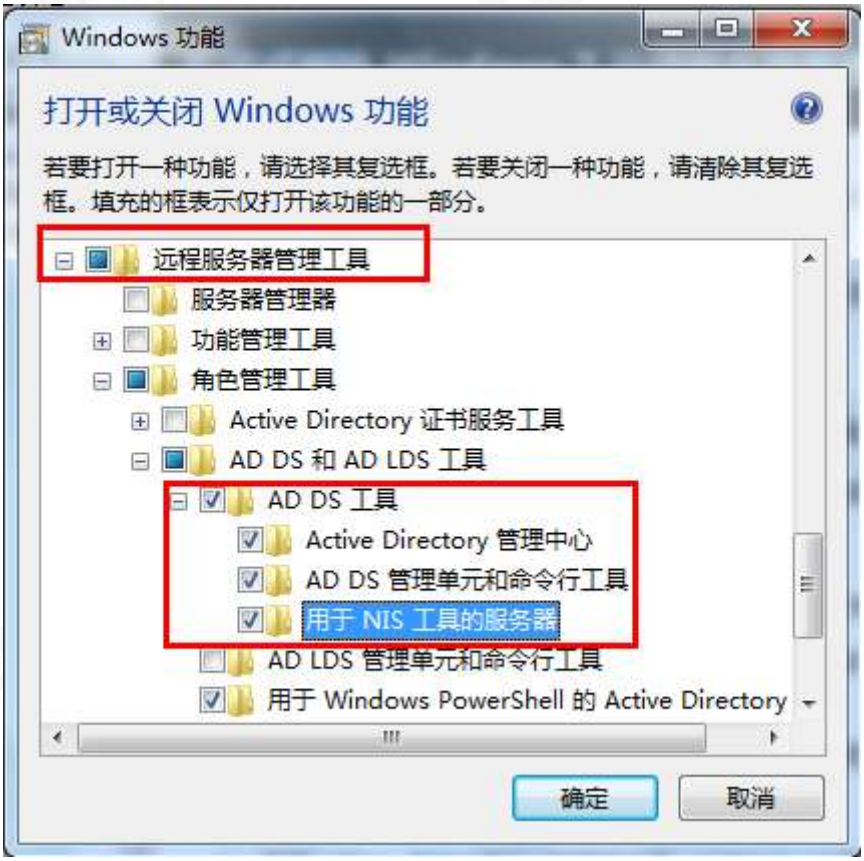


（2） 在“控制面板”里点击“程序”

（3） 选择“打开或关闭 windows 功能”



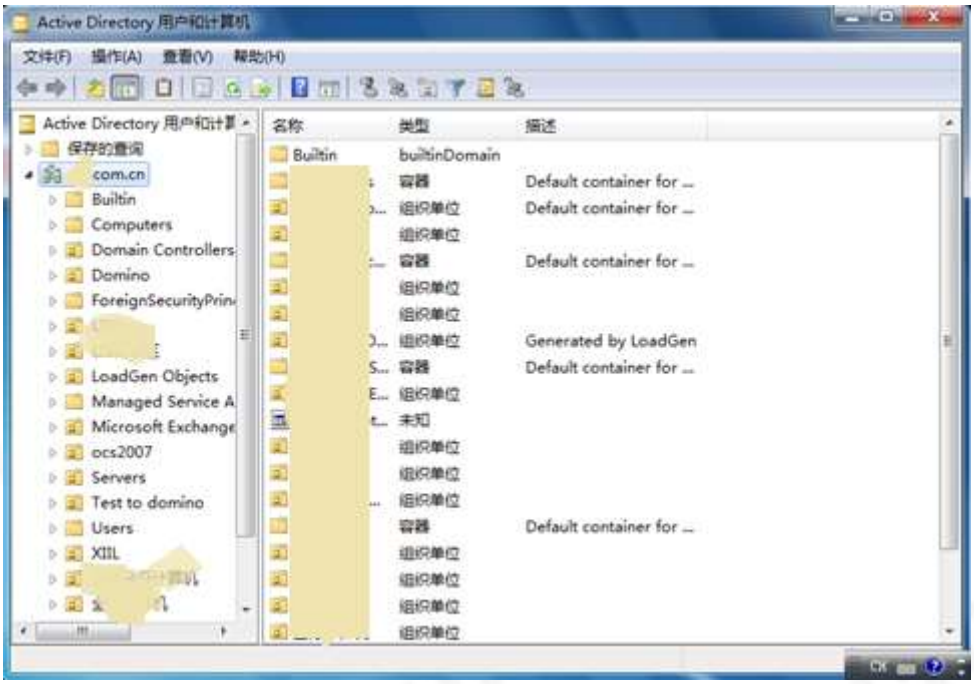
（4） 在“远程管理工具”中添加需要的服务，在这里我们添加“AD 管理工具”。



（5） 点击确定后，进行工具安装。

（6） 选中之后确定添加，添加完毕后，再点击开始，在管理工具中就可以看到 AD 的相关管理工具了

（7） 打开“Active Directory 用户和计算机”，即可浏览到域控信息。



2.2 委派控制

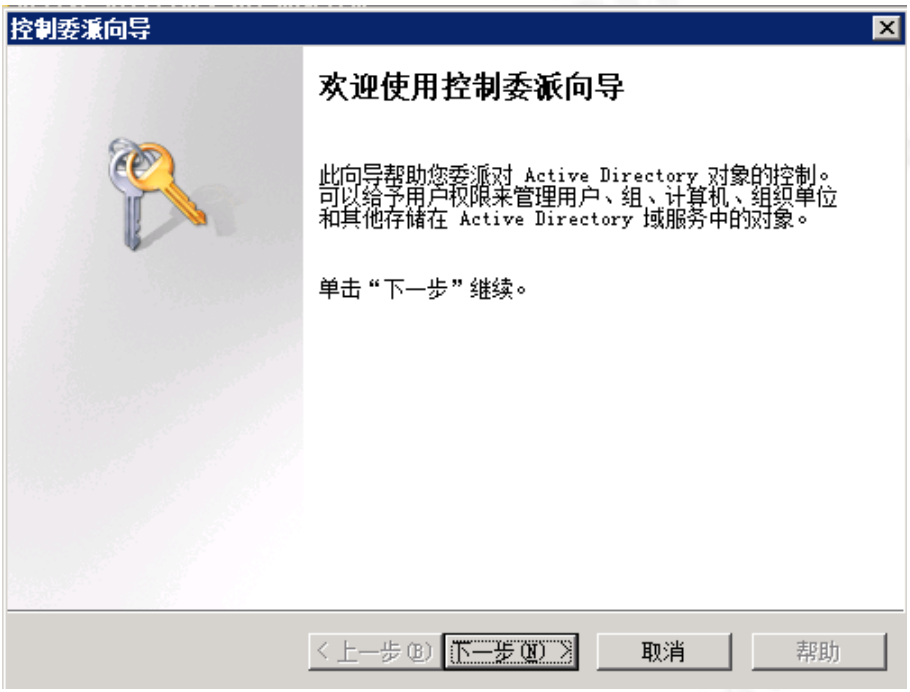
2.2.1 委派步骤

这里以 BJDAG 帐号对北京分行的组织单元进行管理员权限委派为例。

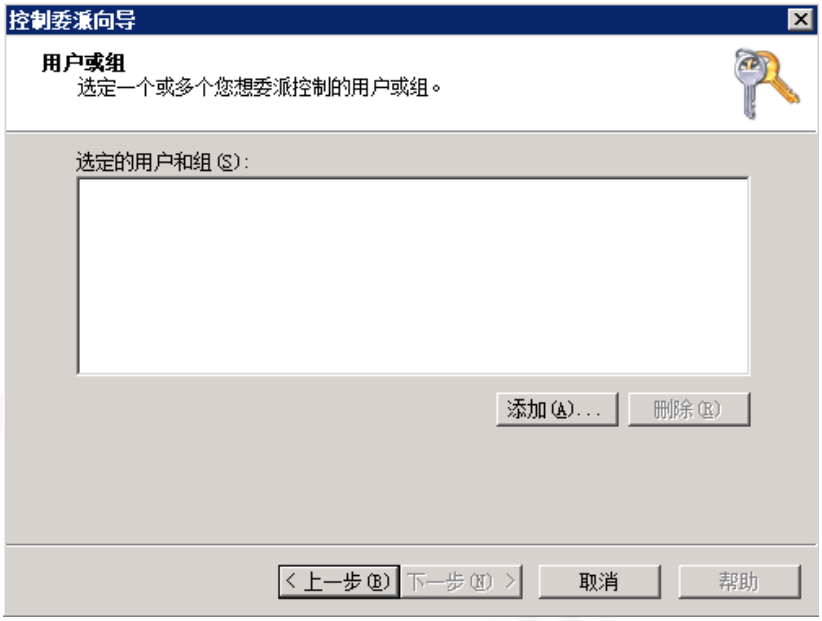
（1）启动“Active Directory 用户和计算机”（ADUC），找到需要委派的 OU：北京分行

（2）右击“北京分行”OU，选择菜单：委派控制

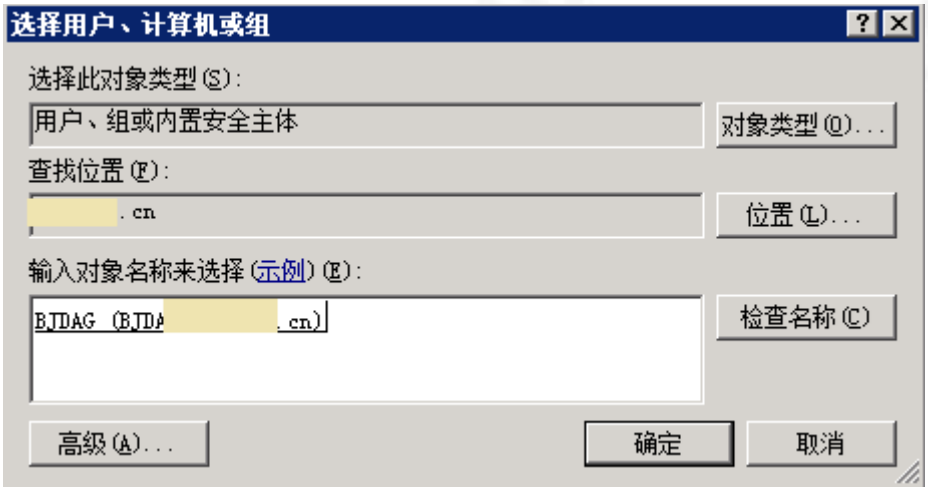
（3）进入委派控制的配置向导



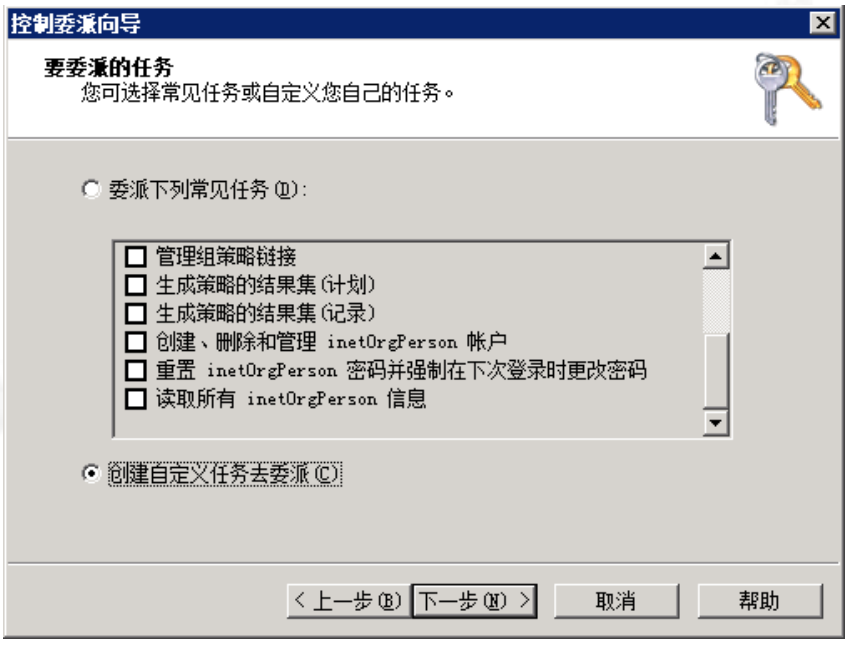
（4）点击“下一步”



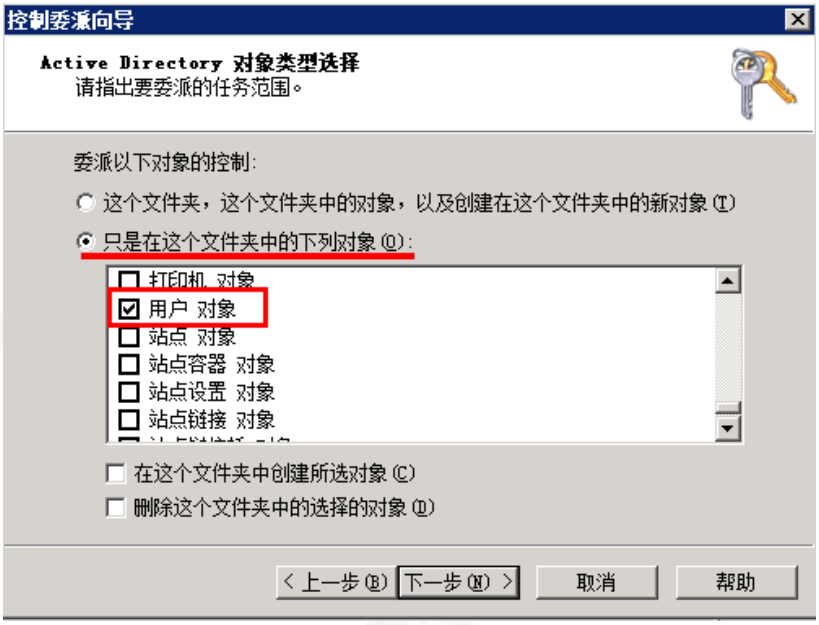
（5）点击“添加（A）”按钮，选择需要指派的用户：

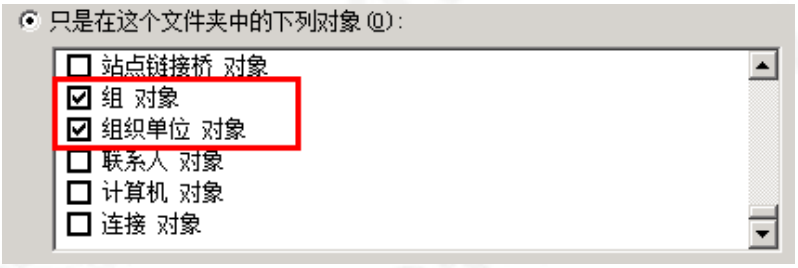


（6）点击“确定”，并进入下一步，在此我们选择创建自定义任务去委派：

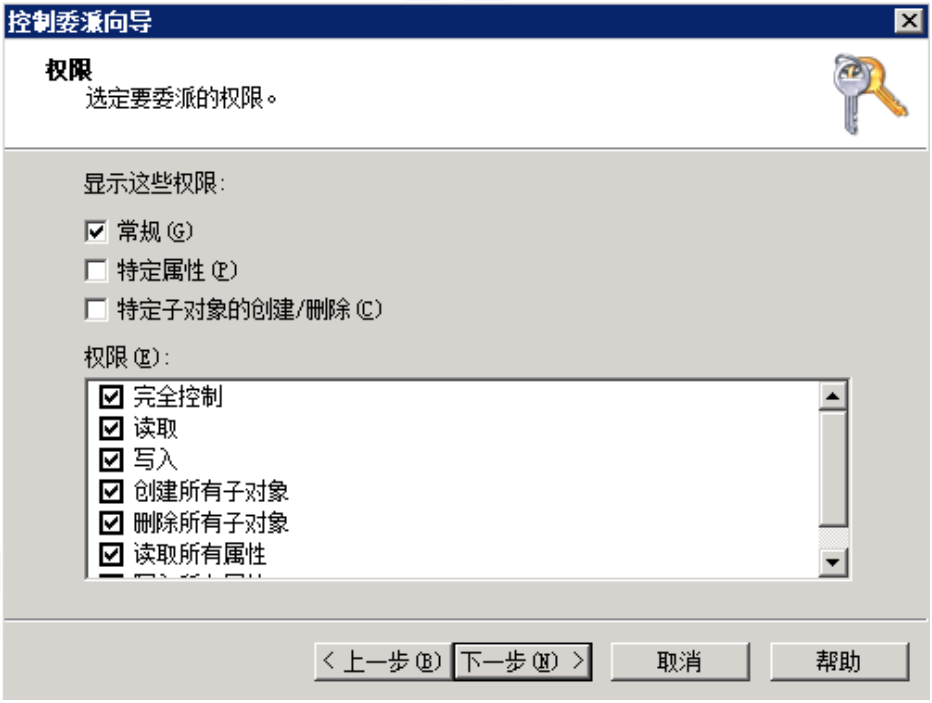


（7）在出现 ad 对象类型选择，选择只是在这个文件夹中的下列对象用户、组、组织单元三项，并点击“下一步”





（8）点击下一步，将权限设为完全控制



（9）点击“下一步”完成控制委派向导：

2.2.2 委派控制的本质

AD 委派控制本质就是修改 AD 对象中的 ACL，使委派的对象具有相符的权限。

查看委派：启动 ADUC 的高级功能，选择“查看”-“高级功能”

右击委派的 OU，选择“属性”

在弹出的属性选项中，选择“安全”选项卡：

选取安全选项卡中的“高级”属性来验证委派的 ACL，我们可以查看到 BJDAG 配置了关于“组”/“组织单位”/“用户”三个权限项目

选中对应的权限项目，点击“编辑”按钮，显示委派工作的内容。

2.2.3　删除管理员

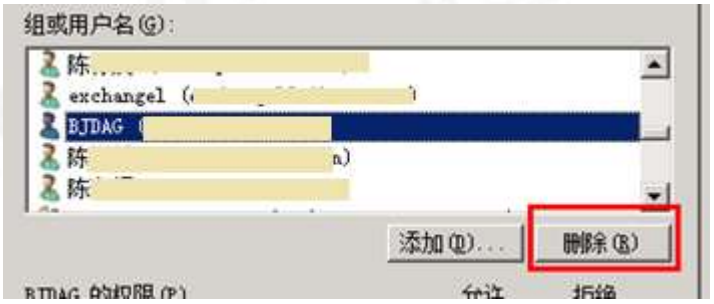
委派控制向导有一个缺点：只能够用来建立委派工作，但是无法删除或更改委派工作，如果要取消或更改授权的人选或者工作属性，则必须直接修改该对象的 ACL。

删除方法：右击对应的 OU 打开其属性，切换到“安全”选项卡，再按编辑就可以修改委派的权限，或者点击删除按钮

（1）　右键单击选中需要删除管理员的组织单元，选择属性

（2） 在弹出的属性选项中，选择“安全”选项卡

（3） 选中要删除的管理员，点击删除即可。最终点击确定。



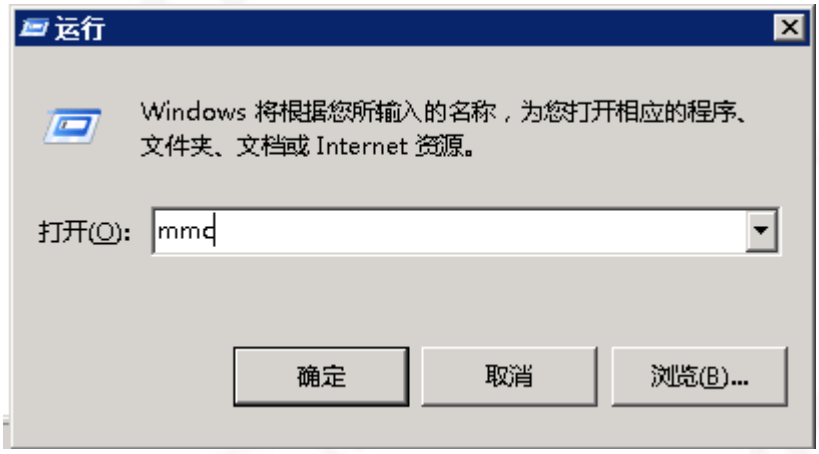
2.3 委派用户管理方式

使用服务器远程管理工具登录

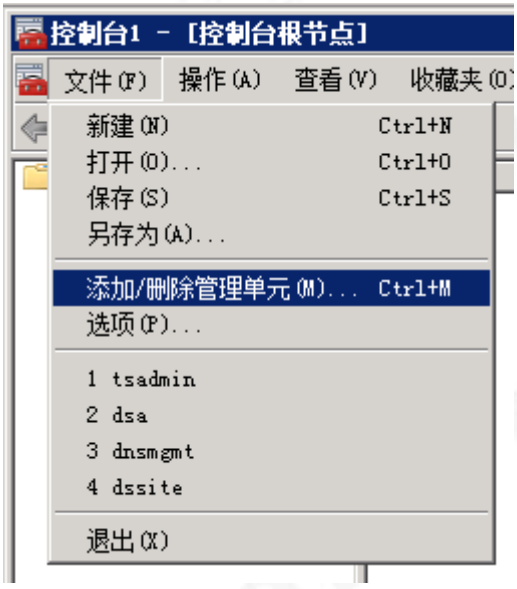
自定义 MMC 限定 OU 访问控制

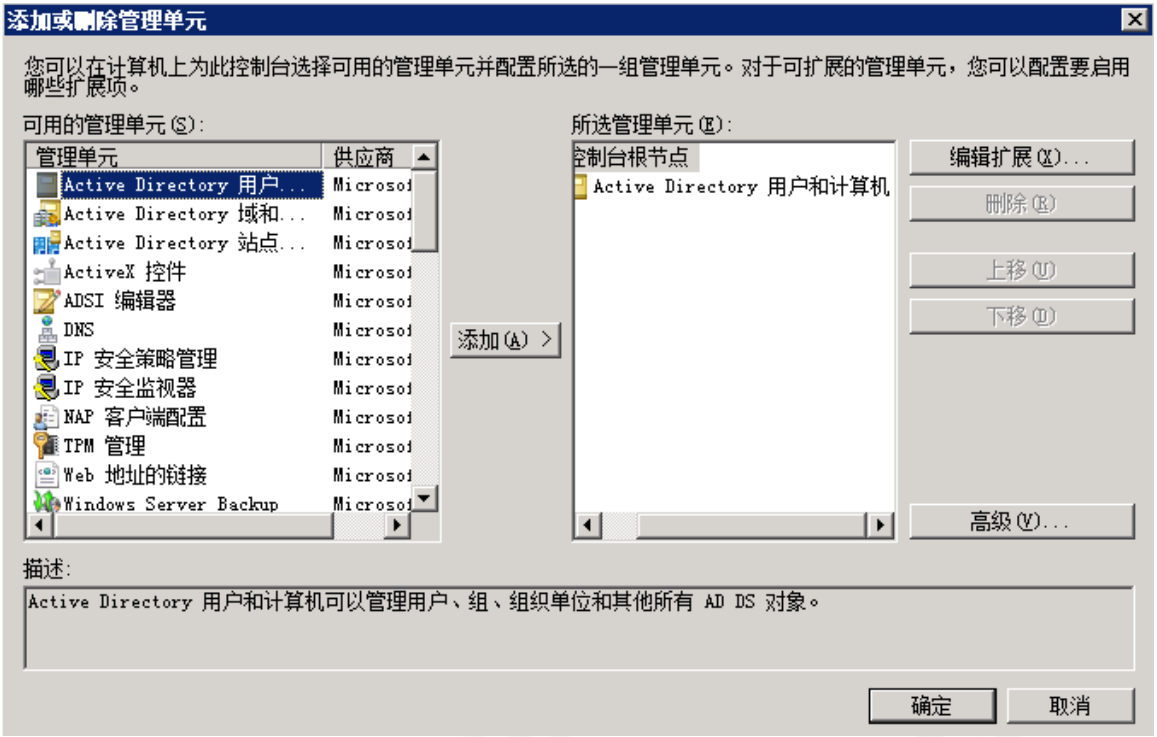
方法：将 Active Directory 用户和计算机（ADUC）的 mmc 进行自定义，只把委派用户管理的 OU 列出，保存后发送给此用户，然后将 ADUC 所需的文件拷贝的客户端，此用户就可以管理特定 OU 而无法浏览到其他 OU。

（1） 在 DC 上，点击开始-运行，输入 mmc，确定。

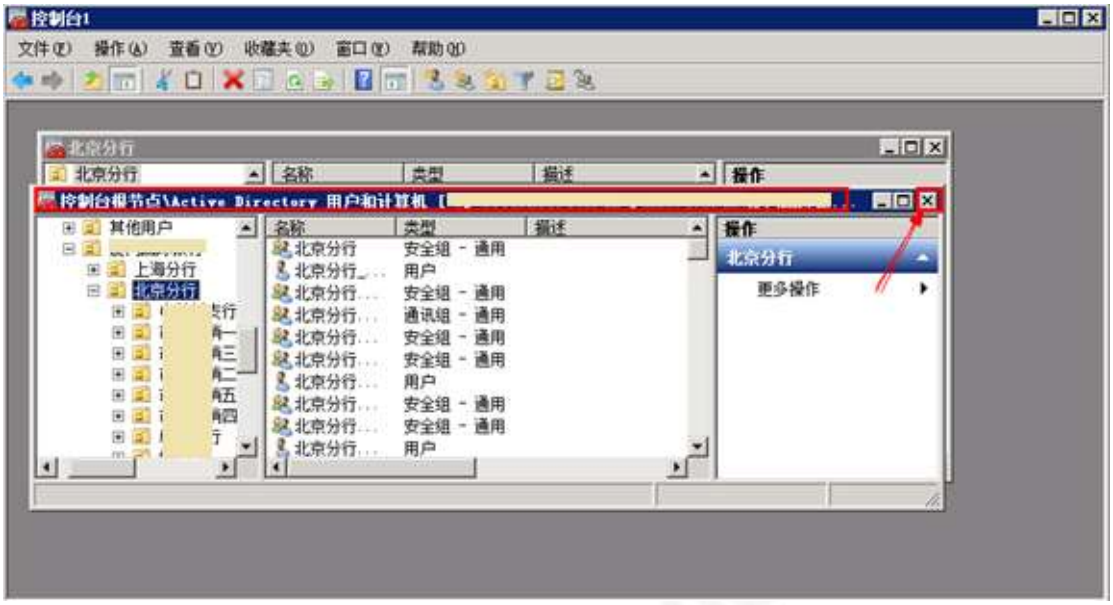


添加 ADUC 管理单元。

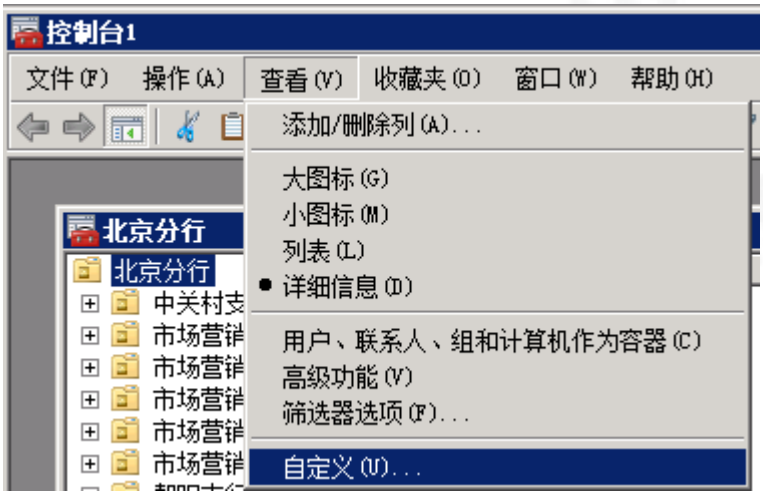


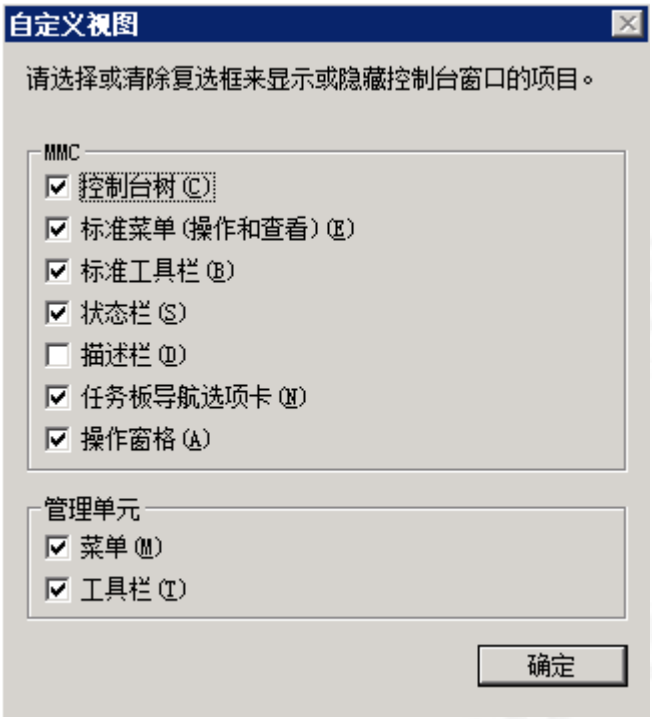


找到将委派给用户的 OU，右键单击选择 从这里创建窗口。将显示整个域的窗口关闭，只留下特定 OU 的窗口。

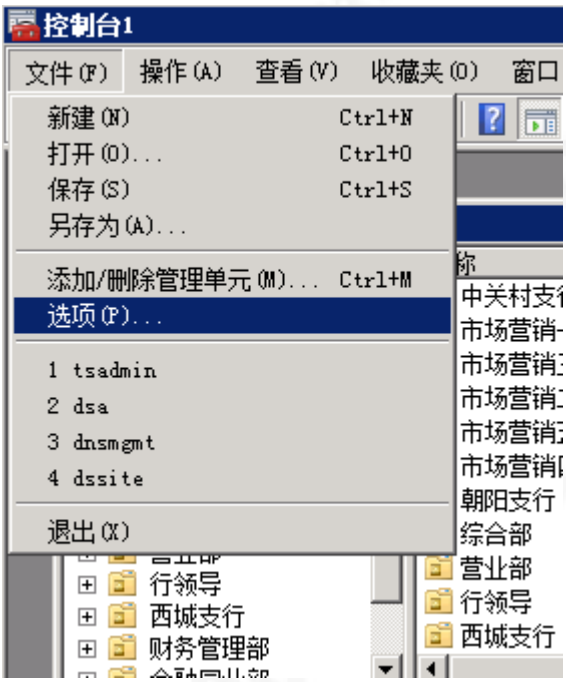


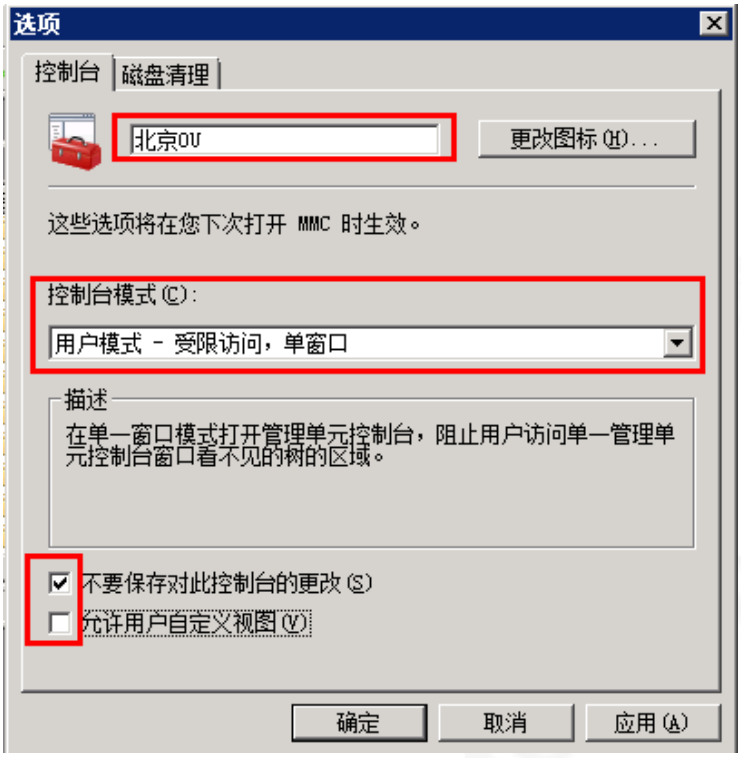
在查看-自定义中可以选择用户可以在 UI 上进行的操作，选择好后确定。





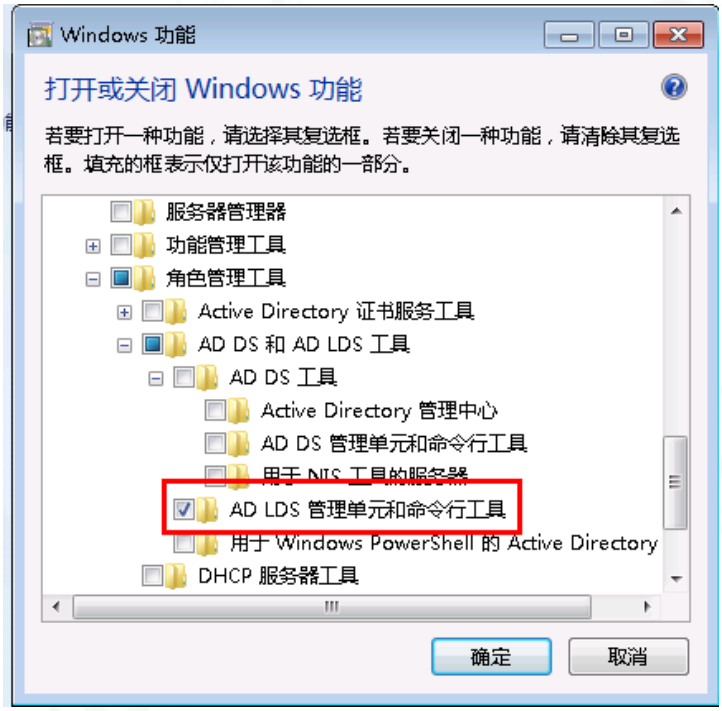
在文件-选项中，将控制台改名（可选），模式改为“用户模式-受限访问，单窗口”。勾选“不要保存对此控制台的更改”， 不勾选“允许用户自定义视图”。





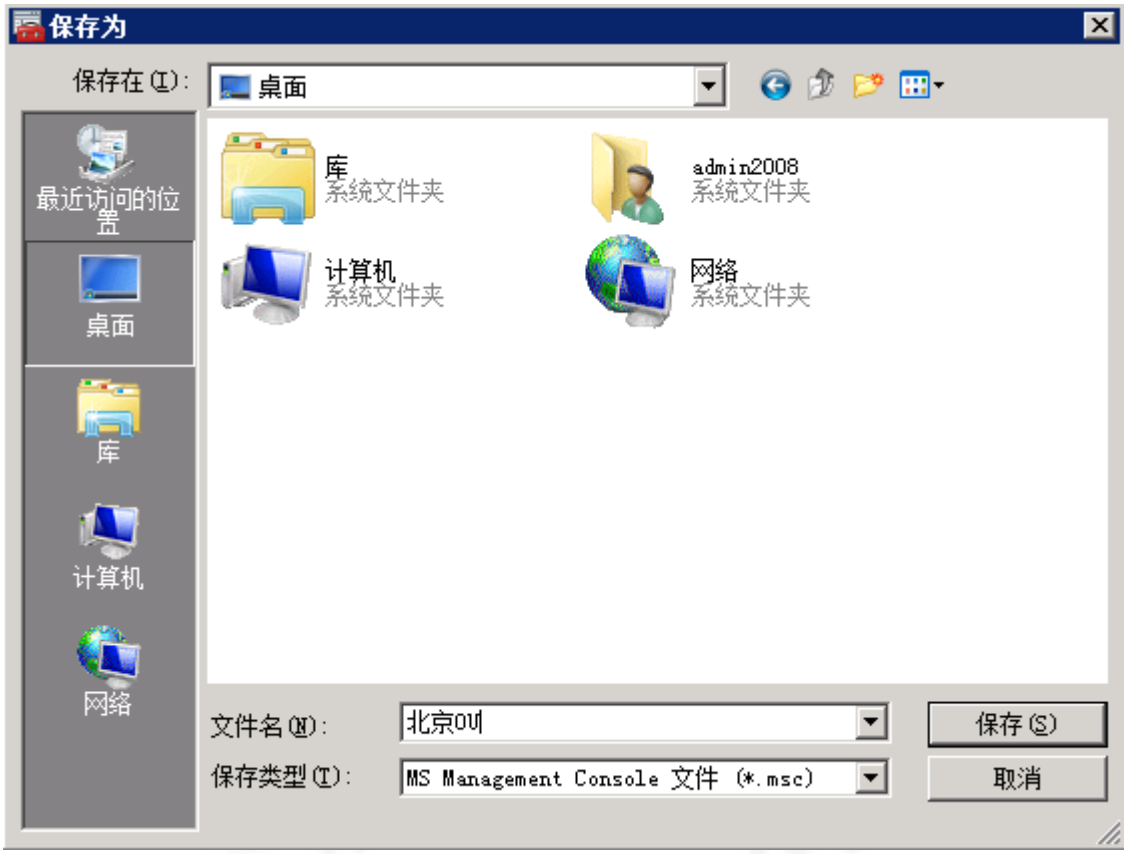
将自定义好的 mmc 保存后发给用户。并将 DC 上 system32 文件夹下的 adprop.dll、dsadmin.dll 和 dsprop.dll 拷贝到客户端的 system32 文件夹，然后在客户端运行 regsvr32 adprop.dll、regsvr32 dsadmin.dll 和 regsvr32 dsprop.dll 注册这些文件。

然后在客户端上安装：

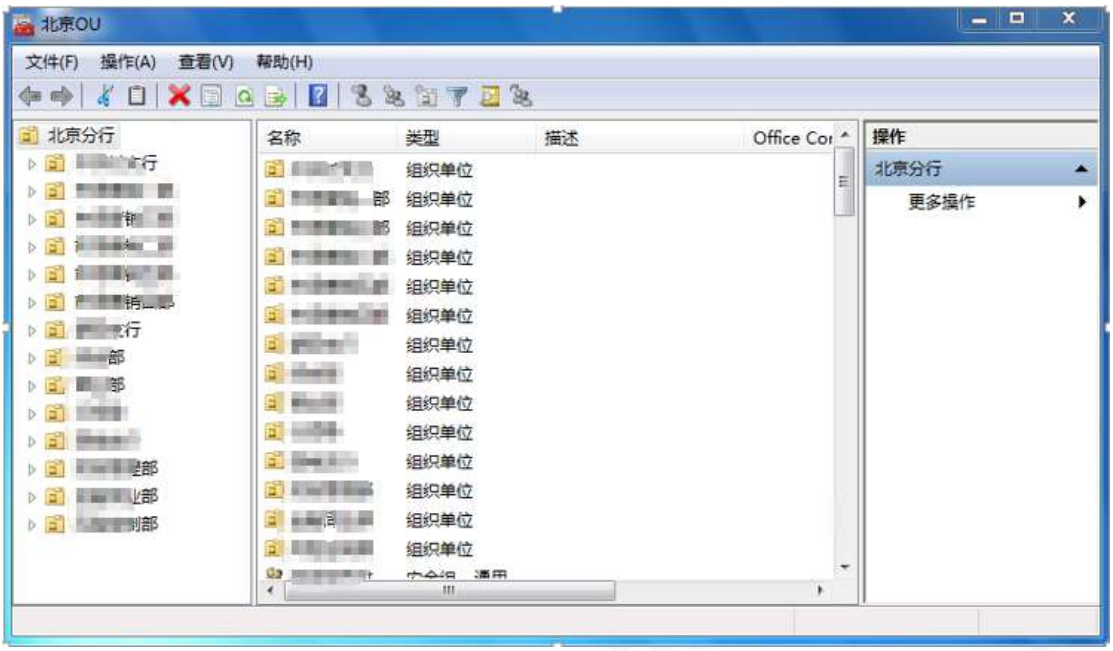


这样客户端就可以管理特定 OU 而无法看到其它 OU 了。

注意：从 DC 上拷贝文件要和客户端对应，2008 R2 要拷到 Windows 7，且 32 位、64 位要对应。



使用 BJDAG 登录 bj-dc01 后，将配置文档复制到域控上


北京OU
文件(F)
操作(A)
查看(V)
帮助(H)
北京分行
名称
类型
描述
Office Cor
组织单位
操作
北京分行
更多操作

第 3 章　QA

3.1 暂无