

子模块 7 组织单位与组策略

本章的主要任务是掌握组织单位的管理及组策略应用等技能。在较大规模的域网络中通过采用组织单位对网络中的用户和资源进行分层次组织和管理可以大大提高网络的管理效率，降低网络管理人员的劳动强度。同时，网络管理人员还希望利用某些手段对连接到网络上的用户和计算机的工作环境进行统一和灵活高效的控制，组策略正是完成该任务的理想工具。

7.1 技能一 组织单位的管理

组织单位是 Active Directory 中的容器管理单元，它不仅可以包括用户账号和组账号，还可以包括计算机、打印机、共享文件夹等活动目录上的对象。在实际工作当中一般用组织单位对应企业的各个职能部门。

7.1.1 任务一 创建组织单位

组织单位是活动目录上的一个容器，对它的管理需要使用“Active Directory 用户和计算机”工具。

(1) 打开“Active Directory 用户和计算机”窗口，在需要创建组织单位的域中右击，执行“新建”→“组织单位”命令，如图 7.1 所示。

(2) 在弹出的“新建对象—组织单位”对话框中输入新创建的组织单位的名称“运营部”，如图 7.2 所示。单击“确定”按钮完成组织单位的创建。

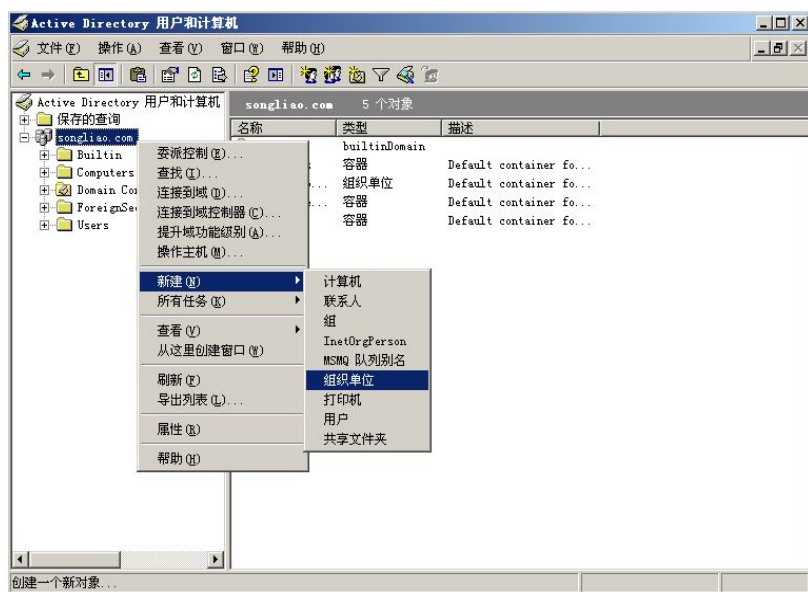


图 7.1 创建新的组织单位

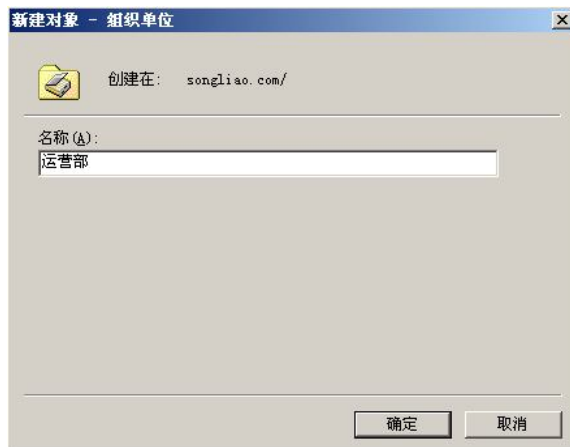


图 7.2 “新建对象—组织单位”对话框

☺ 相关链接：[组织单位](#)。

组织单位 (OU, Organization Unit) 又称组织单元, 是 Active Directory 中的一个特殊容器, 它可以把用户、组、计算机和打印机等对象组织在一起进行统一管理。OU 允许进行组策略设置, 这也是它被广泛应用于网络资源管理的主要原因。

在规划组织单位时, 一般原则是按管理对象的工作职能进行划分。假设是一家公司可按不同职能将各部门划分成管理部、技术部、财务部等组织单位。另外, 也可按照地域划分组织单位。

7.1.2 任务二 成员管理

对于已创建的组织单位, 可向其中添加、移动、删除用户、计算机和其他组织单位等成员。

(1) 在指定的组织单位上, 通过新建方式添加成员。打开“Active Directory 用户和计算机”窗口, 选中组织单位“运营部”右击, 执行“新建”→“用户”命令来添加新的用户成员, 如图 7.3 至图 7.5 所示。还可用同样的方法创建“计算机”和下层“组织单位”等成员, 结果如图 7.6 所示。



图 7.3 创建用户

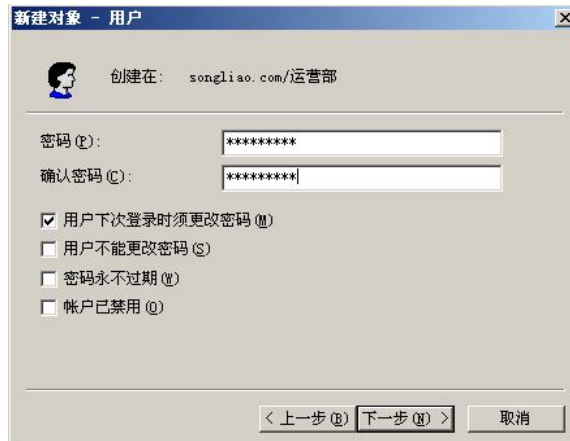


图 7.4 设置用户密码



图 7.5 用户创建完毕

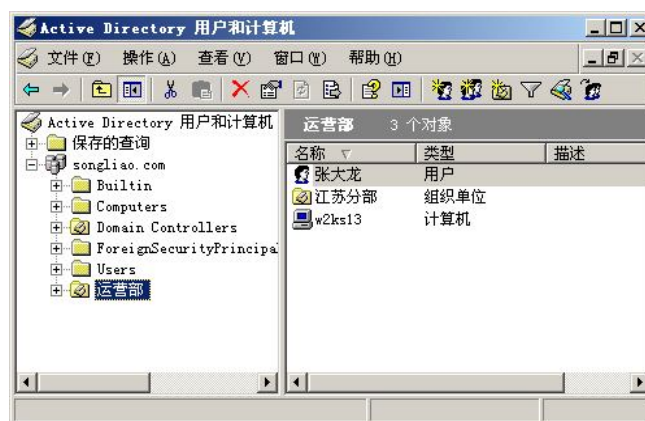


图 7.6 组织单位中的成员

(2) 选择其他组织单位的成员对象，通过移动方式添加到指定组织单位中。在“Active Directory 用户和计算机”窗口中选择相应组织单位中的指定对象，右击，执行“移动”命令，

如图 7.7 所示，然后在弹出的对话框中选择想要移动到的组织单位名称，如图 7.8 所示。单击“确定”按钮，完成对象的移动。

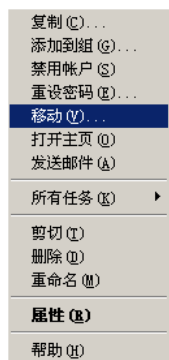


图 7.7 移动对象



图 7.8 “移动”对话框

(3) 在指定的组织单位上删除成员。打开“Active Directory 用户和计算机”窗口，选中组织单位“运营部”，在要删除的成员上右击，执行“删除”命令，如图 7.9 所示。在弹出的确定对话框中确认后即可删除组织单位中的成员对象，如图 7.10 所示。

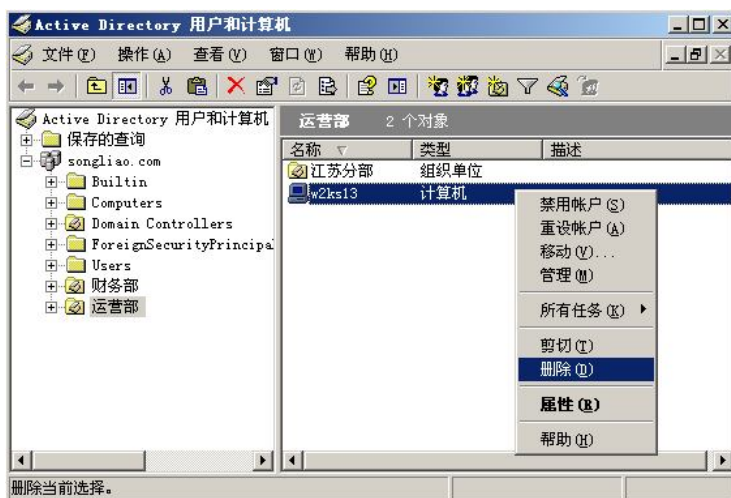


图 7.9 删除组织单位中的成员

7.1.3 任务三 组织单位属性的查看和设置

可以通过组织单位的属性来查看和指定组织单位的常规信息、管理者以及组策略的应用等。

(1) 打开“Active Directory 用户和计算机”窗口，选中组织单位“运营部”右击，执行“属性”命令，弹出“运营部属性”对话框，查看和设置相应属性，如图 7.11 所示。

(2) 在“管理者”选项卡中，执行“更改”命令为组织单位设置管理者，如图 7.12 所示。

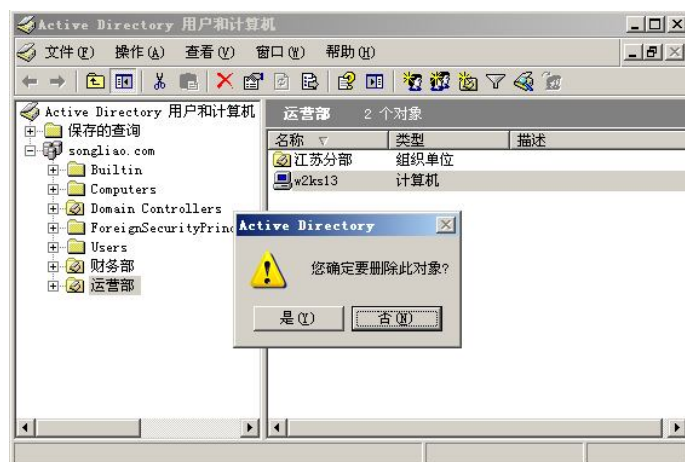


图 7.10 确认删除组织单位成员对话框



图 7.11 “运营部属性”对话框



图 7.12 “管理者”选项卡

😊 相关链接：组策略。

组策略是 Windows Server 2003 提供的一项功能强大的配置用户和计算机工作环境的工具。由于组策略可以应用于组织单位，所以组织单位中的各类对象就能够被统一进行策略管理，实施组策略是管理大中型网络的一项重要工作，能够显著地减轻网络管理人员的工作强度和负担。

组策略的设置比较复杂，我们在 7.2 节进行详细讲解。

7.2 技能二 组策略应用

组策略设置和定义了网络管理人员对用户桌面环境的各项控制。包括用户桌面上“开始”菜单中的选项以及自动安装软件等环境配置。组策略不仅可以应用于用户和客户端计算机，还应用于成员服务器、域控制器以及管理范围中的其他计算机。一般情况下，应用于域的组策略

会影响到域中的所有计算机和用户。

组策略包含“计算机配置”和“用户配置”两个部分。“计算机配置”的作用是：当网络中的计算机启动时，系统会按照其配置要求自动初始化该计算机的工作环境；而“用户配置”的作用是：当网络中的用户登录时，系统会按照其配置要求自动初始化该用户的工作环境。

7.2.1 任务一 组策略对象管理

(1) 打开“Active Directory 用户和计算机”窗口，选中组织单位“运营部”右击，执行“属性”命令，弹出“运营部属性”对话框，单击“组策略”选项卡，如图 7.13 所示。

(2) 执行“新建”命令创建一个新的名称为“运营部成员”的组策略对象，此时的组策略并没有实际内容，如图 7.14 所示。在后面的“编辑和应用组策略”任务中讲解具体的组策略内容设置。



图 7.13 设置组织单位组策略属性

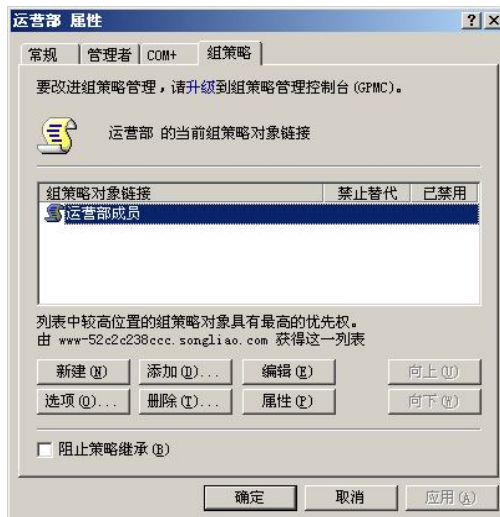


图 7.14 创建组策略

(3) 执行“添加”命令将组策略与站点、域或组织单位进行链接，以便将策略应用于各类对象，如图 7.15 所示。

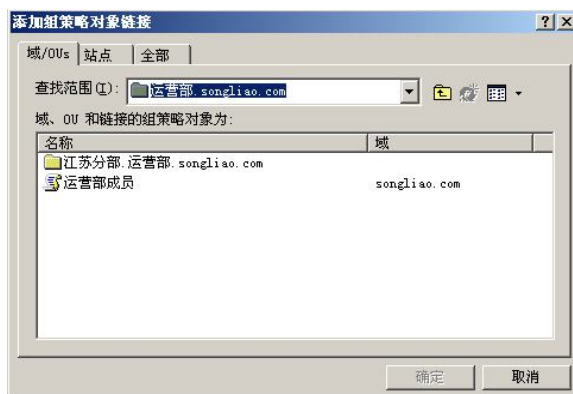


图 7.15 “添加组策略对象链接”对话框

(4) 执行“删除”命令将指定的组策略删除，如图 7.16 所示。

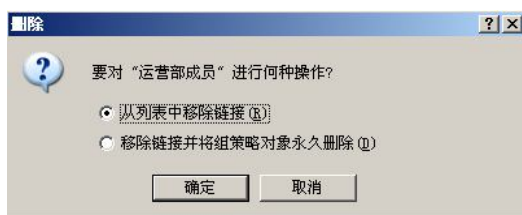


图 7.16 确认删除组策略对话框

☺ **相关知识链接：**组策略的应用顺序与规则。

在本地计算机、站点、域与组织单位内部都可以设置组策略，那么这些处于不同地方的组策略的应用顺序和规则又是怎样的呢？

组策略的应用顺序如下：

- (1) 本地组策略。
- (2) 站点的组策略。
- (3) 域的组策略。
- (4) 组织单位的组策略。

默认情况下，后面应用的组策略会覆盖前面应用的组策略。比如，如果在域的组策略和组织单位的组策略发生冲突时，系统以应用顺序在后面的组织单位的组策略为准。具体的应用规则如下：

(1) 如果在高层容器中建立了组策略，但未在其低层容器中建立组策略，则低层容器会继承高层容器内所建立的组策略。

(2) 如果在低层容器中建立了组策略，则此组策略的默认设置会代替其高层父容器所传递下来的组策略。

(3) 如果在父容器的组策略内的某个策略被设置为“未被配置”，则子容器并不会继承这个策略。

(4) 如果在父容器的组策略内的某个策略被设置为“启用”或“禁用”，但是子容器内的组策略并未设置此策略，则子容器会继承这个设置。

7.2.2 任务二 组策略属性设置

(1) 打开“Active Directory 用户和计算机”窗口，选中组织单位“运营部”右击，执行“属性”命令，弹出“运营部属性”对话框。展开“组策略”选项卡，选择“运营部成员”组策略，并执行“属性”命令查看组策略的常规信息，如图 7.17 所示。

(2) 查看组策略被应用到哪些域、组织单位或站点上，可以选择“链接”选项卡，如图 7.18 所示。

(3) 在“安全”选项卡中可以设置用户对组策略对象具有的权限，如图 7.19 所示。

(4) 在“WMI 筛选器”选项卡中可以为组策略设置 WMI 筛选器，以筛选组策略对象的应用，如图 7.20 所示。WMI 筛选器使用 WQL 查询语言编写，适用于 Windows XP、Professional 和 Windows Server 2003 作为操作系统的客户端计算机。



图 7.17 组策略属性

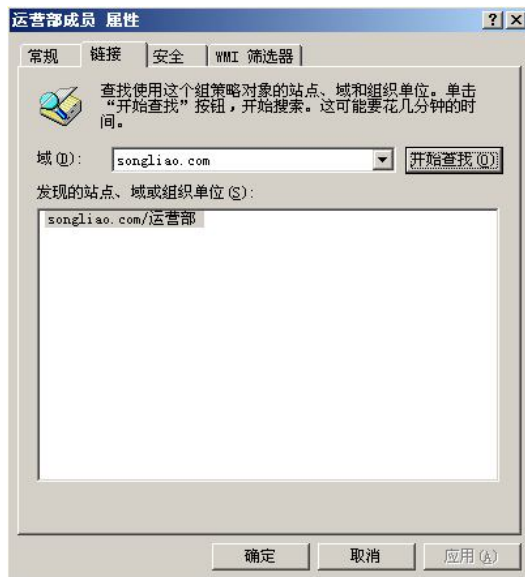


图 7.18 “链接”选项卡

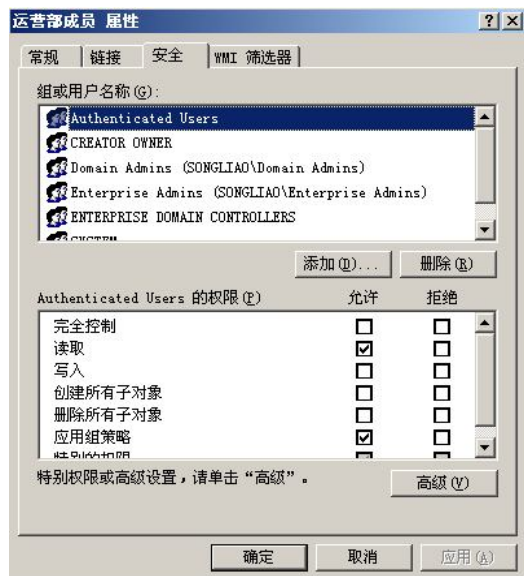


图 7.19 “安全”选项卡

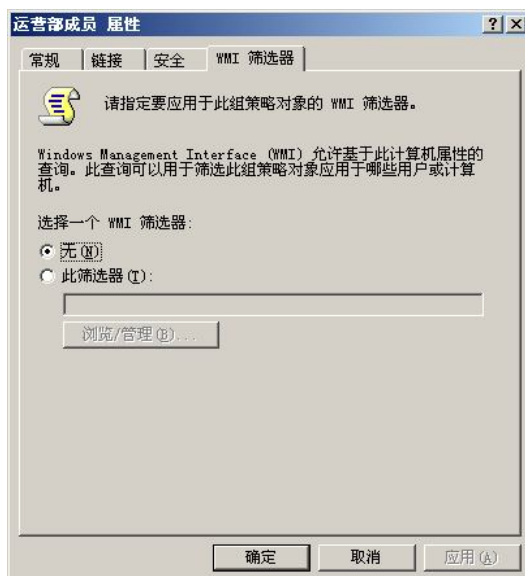


图 7.20 “WMI 筛选器”选项卡

7.2.3 任务三 编辑和应用组策略

在组策略编辑器中针对“计算机配置”和“用户配置”都有“软件设置”、“Windows 设置”及“管理模板”三项对应，每一项中又有若干具体设置项目。以下采用案例方式讲解组策略的编辑和应用。

1. 软件设置

下面介绍使用组策略为用户发布软件包的步骤。

(1) 打开“Active Directory 用户和计算机”窗口，选中组织单位“运营部”右击，执行“属性”命令，弹出“运营部属性”对话框。展开“组策略”选项卡，选择“运营部成员”组策略，并执行“编辑”命令，如图 7.21 所示。



图 7.21 编辑组策略

(2) 选中“用户配置”栏中的“软件设置—软件安装”项右击，执行“新建”→“程序包”命令，如图 7.22 所示。

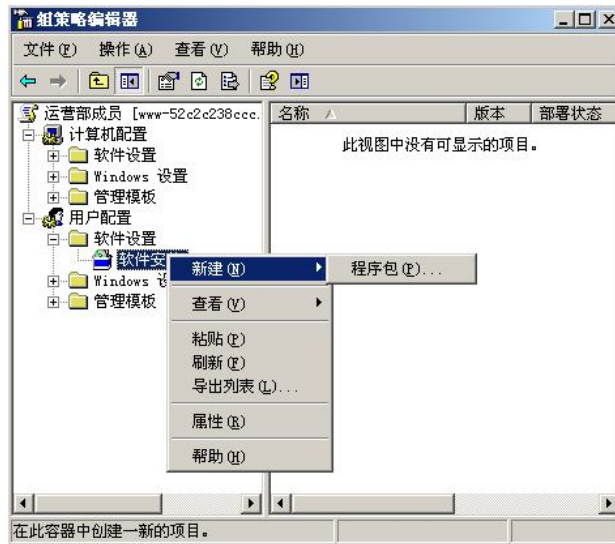


图 7.22 创建软件程序包

(3) 在创建“程序包”对话框中选择指定的程序包文件，如图 7.23 所示。

(4) 在“部署软件”对话框中选择部署方法，并单击“确定”按钮，如图 7.24 所示。

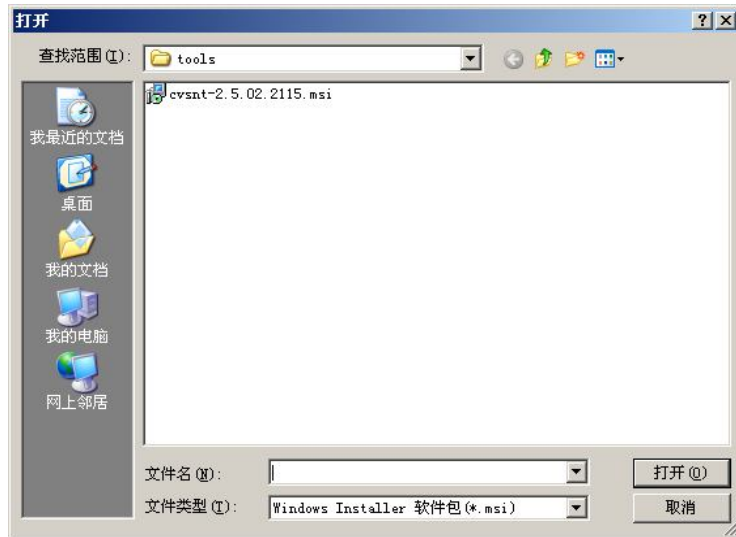


图 7.23 选择程序包对话框

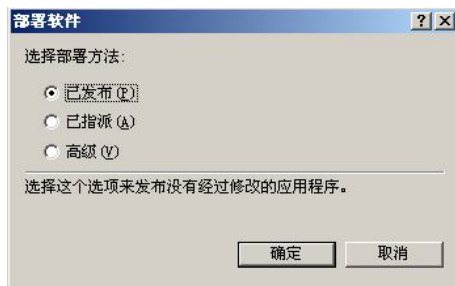


图 7.24 选择软件部署方法

2. Windows 设置

下面介绍设置用户登录运行脚本的步骤。

(1) 利用记事本编写文件名为 start.vbs 的脚本文件，如图 7.25 所示。



图 7.25 登录脚本文件

(2) 在“运营部成员”组策略编辑器中选择“用户配置”栏中的“Windows 设置—脚本”项，如图 7.26 所示。

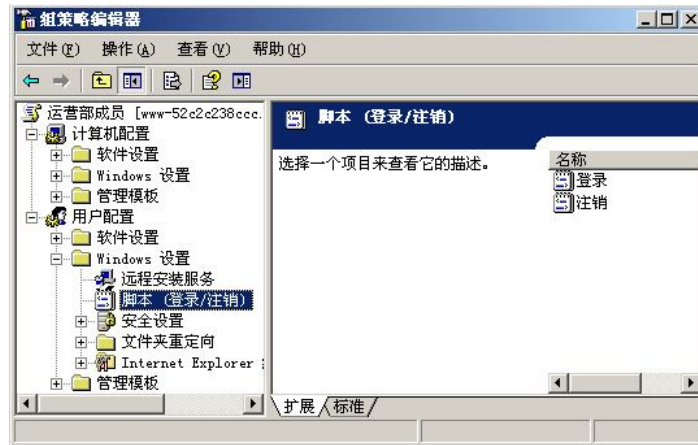


图 7.26 Windows 设置—脚本对话框

(3) 双击“登录”图标，弹出“登录属性”设置对话框，如图 7.27 所示。



图 7.27 “登录属性”设置对话框

(4) 在“登录属性”对话框中执行“添加”命令并在弹出的“添加脚本”设置对话框中通过执行“浏览”命令指定相应的脚本文件，如图 7.28 所示。



图 7.28 “添加脚本”文件对话框

3. 管理模板

下面介绍从“开始”菜单中删除“运行”命令项的步骤。

(1) 打开“Active Directory 用户和计算机”窗口，选中组织单位“运营部”右击，执行“属性”命令，弹出“运营部属性”对话框。编辑“运营部成员”组策略，选中“用户配置”栏中的“管理模板—任务栏和「开始」菜单”，如图 7.29 所示。

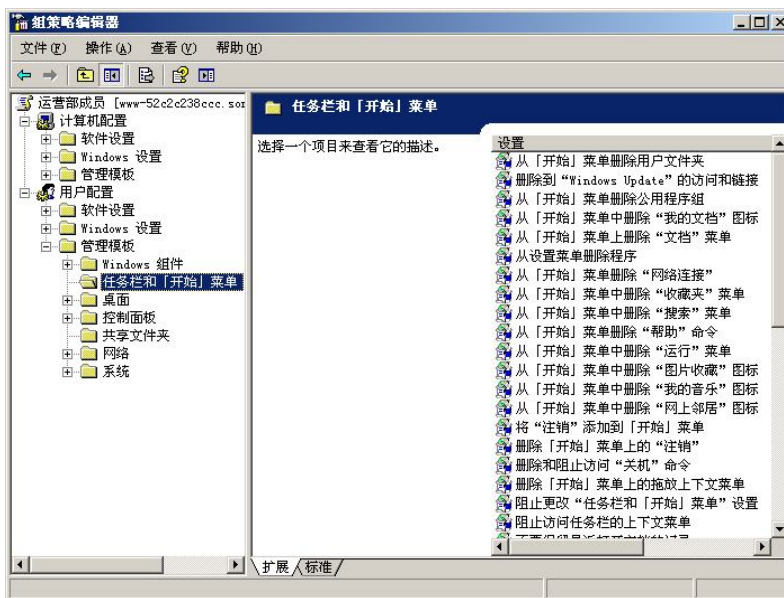


图 7.29 管理模板—任务栏和「开始」菜单设置

(2) 在右侧内容栏中双击“从「开始」菜单中删除‘运行’菜单”项，并在弹出的属性设置对话框中设置为“已启用”，如图 7.30 所示。

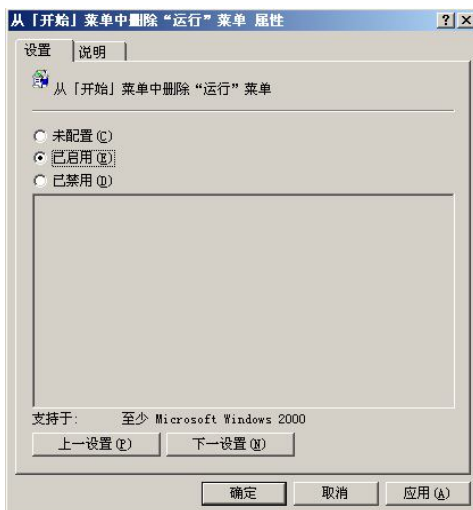


图 7.30 管理模板属性对话框

☺ 相关知识链接：组策略的设置类型。

组策略的类型很丰富，涉及系统管理的各个方面，主要包含：

(1) 管理模板：基于注册表的设置策略，用来设置用户的工作环境。可以用来设置任务

栏和「开始」菜单、桌面、控制面板、打印机等对象的策略应用。

(2) 脚本：设置用户开机/关机、登录/注销时执行的脚本。

(3) 文件夹重定向：在网络服务器上设置相应的存储位置来对应用户常用的文件夹，如我的文档、桌面等。

(4) 安全设置：设置本地计算机、域及网络安全的设置，包括账户策略、本地策略、系统服务等。

(5) 软件安装：对各计算机的软件安装进行集中式的管理。

7.3 子模块小结

本模块介绍了在 Windows Server 2003 网络操作系统中创建组织单位以及管理组织单位成员的方法。同时，结合组策略的相关知识的讲解可以使读者掌握以组策略的方式管理网络资源的技能。组织单位是 Active Directory 和企业的实际网络工作环境相联系的纽带和桥梁，而组策略又是管理网络资源的高效率工具。因此，掌握组织单位与组策略的使用是网络管理人员必备的重要技能。

7.4 拓展技能实训 7

| | |
|------|--|
| 实训名称 | 在组织单位中实施组策略 |
| 实训要求 | <ol style="list-style-type: none">1. 创建一个组织单位2. 在组织单位中添加、移动、删除成员3. 对组织单位编辑和应用组策略 |
| 要点提示 | <ol style="list-style-type: none">1. “计算机配置”和“用户配置”的区别2. 组策略的应用顺序和规则 |
| 操作步骤 | |
| 小结 | |