第3章

组策略的应用

【本章重点】

掌握组策略的功能、内容、管理与维护方法。掌握用组策略进行桌面设置、收藏夹和链接、文件夹重定向和硬件访问策略的设置方法与操作要点。掌握通过组策略进行程序的远程安装和禁止运行的技术和操作技巧。

组策略(Group Policy,GP)是系统管理员为计算机用户定义的用来控制应用程序,系统设置和管理模板的一种机制,也是一种用于管理网络内的用户设置和计算机设置的管理工具。所谓组策略,就是基于群体(组织单位、域、站点)的管理策略。它以 Windows 中的一个 MMC 管理单元的形式存在,可以帮助系统管理员针对整个计算机或是微软活动目录的逻辑要素自 Windows NT 4.0 开始便采用了组策略这一机制,经过 Windows 2000 发展到 Windows 2008 已相当完善。

3.1 组策略与组策略对象

组策略是介于控制面板和注册表之间的一种修改系统,是设置程序的工具。一些常用的系统、外观、网络设置等我们可通过控制面板修改,但大家对此肯定都有不满意的地方,因为通过控制面板能修改的东西太少;水平稍高点的用户进而通过修改注册表的方法来设置。我们知道注册表是 Windows 系统中保存系统、应用软件配置的数据库,随着 Windows 功能越来越丰富,注册表里的配置项目也越来越多。

很多配置都是可以自定义设置的,但这些配置分布在注册表的各个角落,如果是手工配置,可想而知是相当困难和繁杂的。而组策略则将系统重要的配置功能汇集成各种配置模块,供管理人员直接使用,从而达到方便管理计算机的目的。组策略使用自己的完善的管理组织方法,对各种对象中的设置进行管理,涉及的内容比控制面板中的多,安全性和控制面板一样非常高,而条理性、可操作性则比注册表强。

3.1.1 组策略的功能

组策略是活动目录的重要组成部分,也是活动目录里的重点内容。使用组策略可以

使工作变得简单化、条理化。利用组策略，用户可以设置多种配置，包括桌面配置和安全配置。例如，可以为特定用户或用户组定制可用的程序、桌面上的内容，以及“开始”菜单选项等，也可以在整个计算机范围内创建特殊的桌面配置。简而言之，组策略是Windows中的一套系统更改和配置管理工具的集合。

对于Windows 9X/NT用户来说，都知道“系统策略”的概念，其实组策略就是系统策略的高级扩展，它是自Windows 9X/NT的“系统策略”发展而来的，具有更多的管理模板、更灵活的设置对象及更多的功能，主要应用于Windows 2000/XP/2003/7/2008操作系统中。而系统策略只具有写入注册表项这一个功能，组策略可以完成更多的功能。

早期系统策略的运行机制是通过策略管理模板，定义特定的POL(通常是Config.pol)文件。当用户登录时，它会重写注册表中的设置值。当然，系统策略编辑器也支持对当前注册表的修改，另外也支持连接网络计算机并对其注册表进行设置。

而组策略及其工具，则是对当前注册表进行直接修改。显然，Windows 2000/XP/2003系统的网络功能是其最大的特色，所以其网络功能自然是不可少的，因此组策略工具还可以打开网络上的计算机进行配置，甚至可以打开某个Active Directory(活动目录)对象(即站点、域或组织单位)并对其进行设置。这是以前“系统策略编辑器”工具无法做到的。

当然，无论是“系统策略”还是“组策略”，它们的基本原理都是修改注册表中相应的配置项目，从而达到配置计算机的目的，只是它们的一些运行机制发生了变化和扩展而已。

3.1.2 组策略的内容

计算机组策略主要可进行两个方面的配置：计算机配置和用户配置。“计算机配置”是对整个计算机中的系统配置进行设置，它对当前计算机中所有用户的运行环境都起作用；“用户配置”则是对当前用户的系统配置进行设置，它仅对当前用户起作用。例如“计算机配置”和“用户配置”都提供了“停用自动播放”功能的设置，但效果是不同的；如果是在“计算机配置”中选择了该功能，那么所有用户的光盘自动运行功能都会失效；如果是在“用户配置”中选择了该功能，那么仅仅是该用户的光盘自动运行功能失效，其他用户则不受影响。

当计算机配置与用户配置发生矛盾时，计算机配置优先。其下所有设置项的配置都将保存到注册表的相关项目中。计算机配置保存到注册表的HKEY_LOCAL_MACHINE子树中，用户配置保存到HKEY_CURRENT_USER。在Windows 2008以及Windows 2003中，组策略一般放在“系统安装:\windows\system32\GroupPolicy”文件夹中，文件名为gpedit.msc。

如图3-1所示，组策略分为两大部分：计算机配置和用户配置。每一个部分都有自己的独立性，因为它们配置的对象类型不同。计算机账户部分控制计算机账户，同样用户配置部分控制用户账户。其中有部分配置在计算机部分拥有且在用户部分也有同样的配置，它们是不会跨越执行的。假设某个配置选项你希望计算机账户启用、用户账户也启用，那么就必须在计算机配置和用户配置部分都进行设置。总之计算机配置下的设置仅对计算机对象生效，用户配置下的设置仅对用户对象生效。

分别展开“计算机配置”和“用户配置”会发现还有以下三个项目，如图 3-1 所示。

图 3-1　组策略对象界面

- 软件设置：用于对已经安装好的软件进行管理和维护。
- Windows 设置：用于系统或用户的开关机脚本，系统安全等内容的设置。
- 管理模块：主要用于对系统、网络、Windows 组件等内容进行设置，还可以添加或者删除管理模块。

组策略是 Windows 2008 中提供的一种重要的更新和配置管理技术。它与域或组织单位结合，就能控制和管理网络中的域用户和计算机的工作环境。它有几千项配置，主要包括以下功能：用户工作环境的设置，安全设置，软件的安装与删除，脚本的设置，文件夹重定向。

在域环境内可以有成百上千个组策略能够创建和存在于活动目录中，并且能够通过活动目录这个集中控制技术，实现对整个计算机、用户和网络的基于组策略的控制管理。在活动目录中我们可以为站点、域、OU 创建不同管理要求的组策略，而且允许每一个站点、域、OU 能同时设置多套组策略。

3.1.3　创建和链接组策略对象

组策略设置存储在组策略对象(GPO)中，即组策略是由具体的组策略对象来实现的。根据组策略对象的作用范围，可分为以下两种。

本地组策略对象：它只存在一台计算机上，只对本地用户及该计算机起作用。

Active Dirctory 组策略对象：存储在控制器上，只能在活动目录环境下使用，适用于组策略所作用的站点、域、组织机构中的用户和计算机。

当多个组策略在一起时，执行的顺序是本地组策略、活动目录的站点策略、活动目录的域策略、活动目录的组织单位策略。这些策略不一致时，后应用的策略覆盖前一个策略。在活动目录层次结构的每一级组织单位中，可以链接一个、多个或不链接组策略对象，如果一个组织对象链接了多个组策略，则按管理员制定的顺序处理，较前位置的组策略具有较高的优先权。

下面我们就说明如何建立组策略和连接组策略。

（1）在 Windows Server 2008 上，以管理员身份登录，依次选择“开始”→“管理工具”→“组策略管理”，如图 3-2 所示。

图 3-2　启动组策略管理

（2）进入组策略管理界面，依次选择“组策略管理”→“林：thw. com”→“域”→thw. com→xuesheng，右击 xueshengOU（组织单元），在弹出的菜单中选择“在这个域中创建 GPO 并在此处链接”选项，如图 3-3 所示。

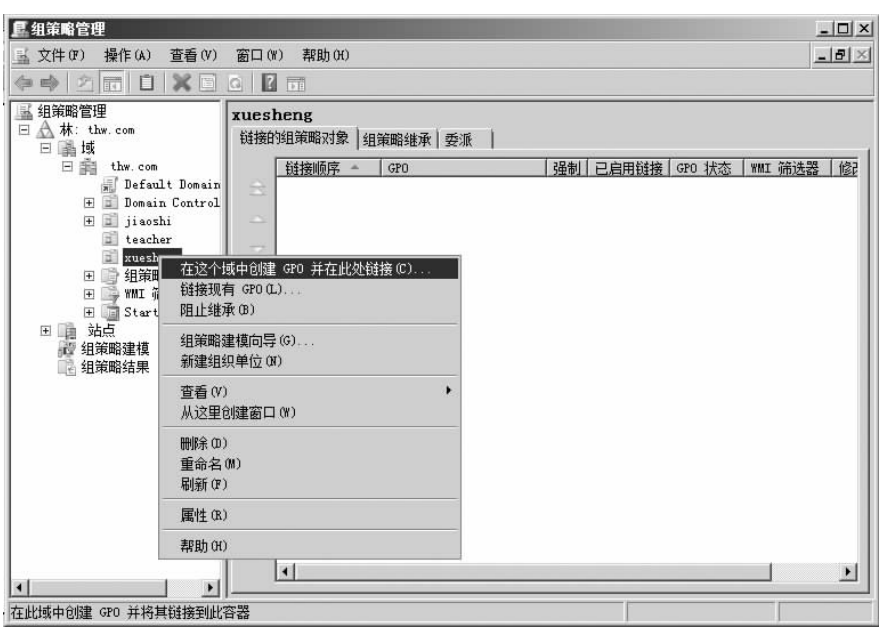

图 3-3　在这个域中创建 GPO 并在此处链接

（3）在弹出的对话框中为新建立的 GPO 起个名字，例如：software OU，如图 3-4 所示。

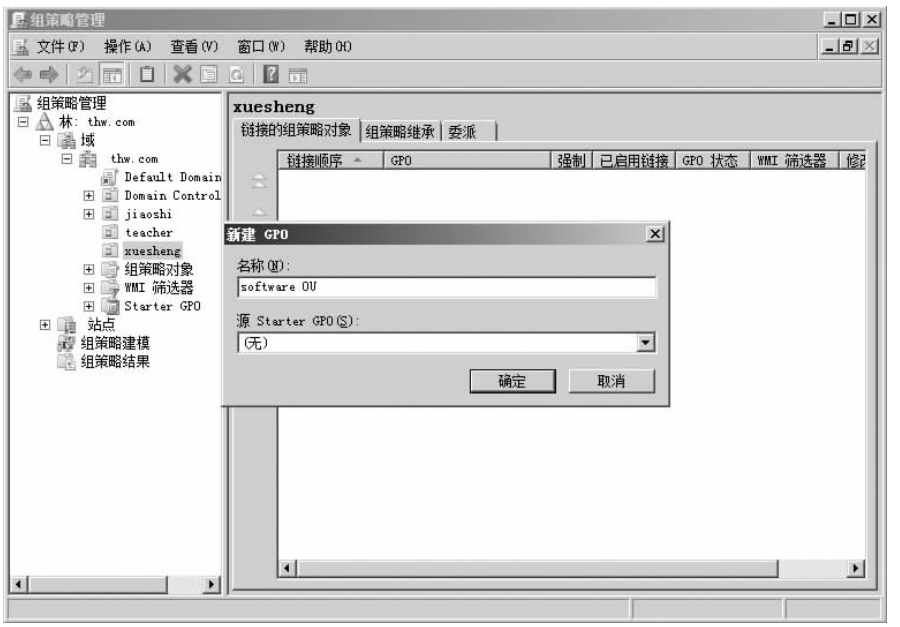

图 3-4　新建组策略

（4）右击新建立的 software OU，在弹出菜单中选择“编辑”，如图 3-5 所示对话框；然后进入组策略管理编辑器，图 3-6 所示。

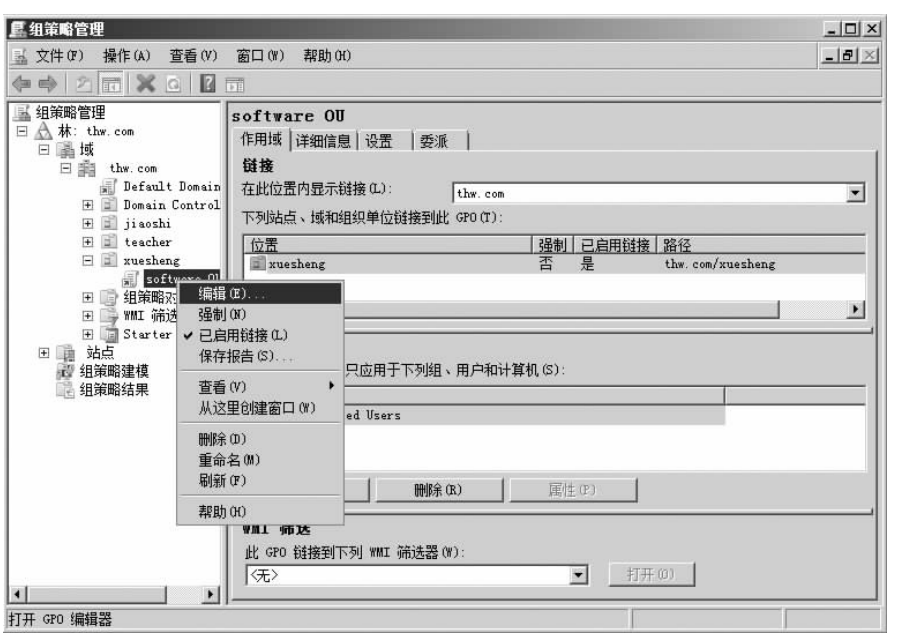

图 3-5　启动组策略管理编辑器

图 3-6　组策略管理编辑器

3.2　通过组策略定制工作环境

3.2.1　修改登录用户的桌面

桌面是打开计算机并登录到 Windows 之后看到的主屏幕区域。就像实际的桌面一样，它是用户工作的平面。打开程序或文件夹时，它们便会出现在桌面上。还可以将一些项目（如文件和文件夹）放在桌面上，并且随意排列它们。有时桌面定义更为广泛，包括任务栏和 Windows 边栏。任务栏位于屏幕的底部，显示正在运行的程序，并可以在它们之间进行切换。它还包含“开始”按钮 ，使用该按钮可以访问程序、文件夹和计算机设置。边栏位于屏幕的一侧，包含称为小工具的小程序。

下面的操作说明如何设置统一的桌面壁纸。

（1）打开组策略编辑器，在左侧的目录树中依次选择“用户配置”→“策略”→“管理模板：从本地计算机检索到的策略定义（AIMX 文件）”→“桌面”→“桌面”，在右边的显示视图中会出现可以对桌面进行的配置，如图 3-7 所示。

图 3-7　组策略的桌面配置

（2）选择启动 Active Desktop，如图 3-8 所示。

（3）设置统一桌面墙纸，如图 3-9 所示（已提前将墙纸存入共享文件夹中）。

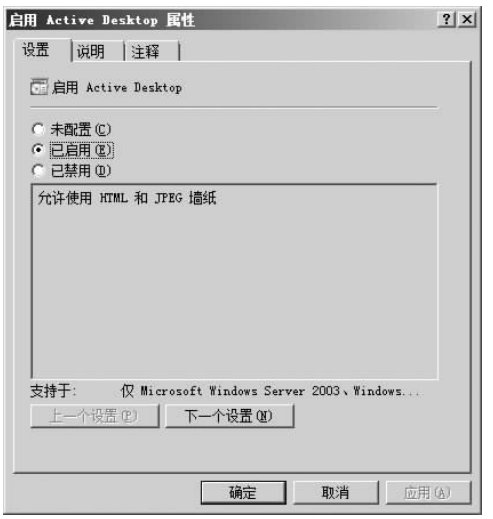

图 3-8　设置启动 Active Desktop

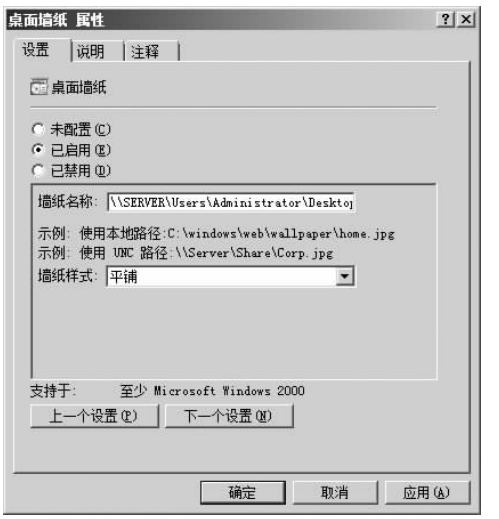

图 3-9　桌面墙纸的设置

（4）设定用户不能自行修改桌面，如图 3-10 所示。

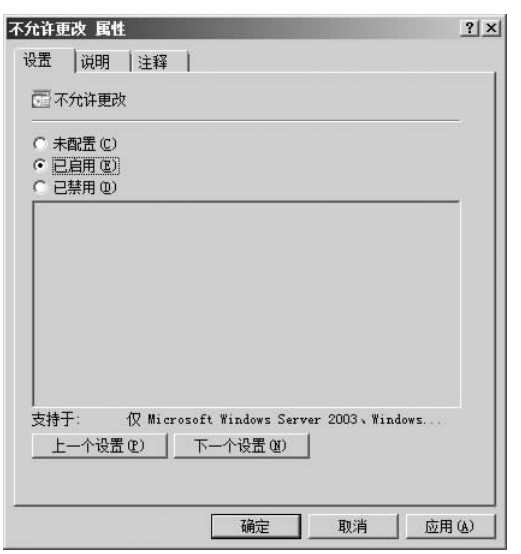

图 3-10　不允许更改设置

（5）以组策略所管辖的用户身份登录客户机，就可看到统一设置的桌面墙纸，如图 3-11 所示。

3.2.2　配置用户的收藏夹和链接

利用组策略可以对用户上网时使用的 IE 浏览器进行有效的管理，如可以禁用导入/

图 3-11　组策略统一设置桌面墙纸

导出收藏夹，禁用更改高级选项卡，禁用邮件快捷菜单，自定义 IE 标题栏等。这里以配置用户的收藏夹和链接为例来说明。

（1）找到“用户配置”→“策略”→“Windows 设置”→“Internet Explorer 维护”选项，如图 3-12 所示。

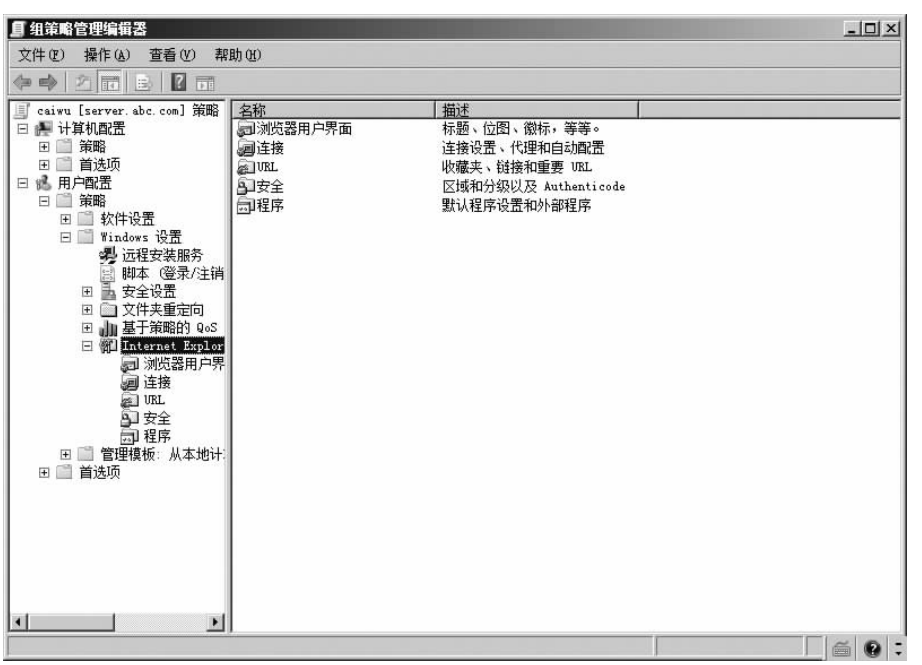

图 3-12　Internet Explorer 维护

（2）选择 URL，在右边的显示视图中会出现可以对 URL 配置两个选项，我们双击收藏夹和链接，这时会弹出“收藏夹和链接”对话框，如图 3-13 所示。

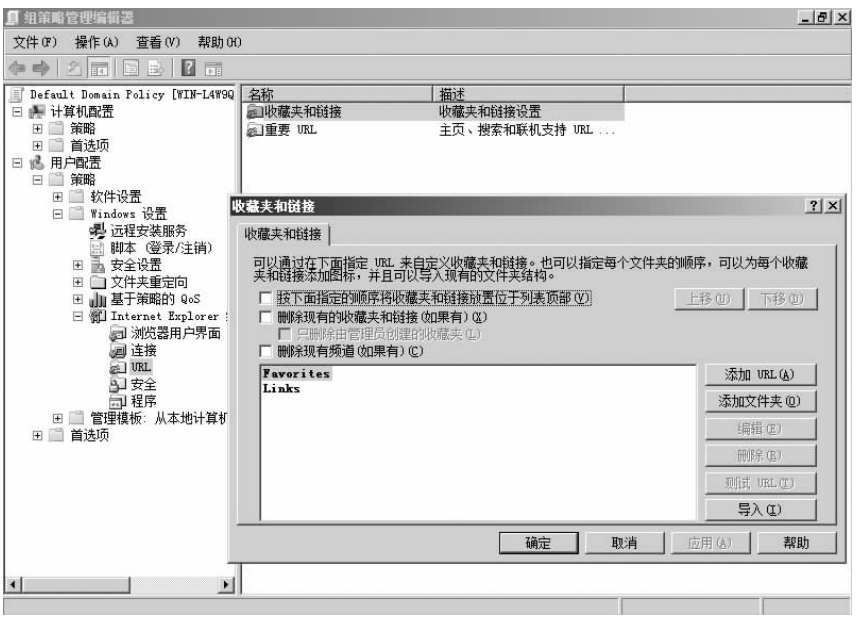

图 3-13　收藏夹和链接

（3）选中 Favorites，单击“添加 URL”，弹出“详细信息”界面，这时我们可以输入要加入的网址名称和 URL 地址。这里我们以“百度”为例，如图 3-14 所示。

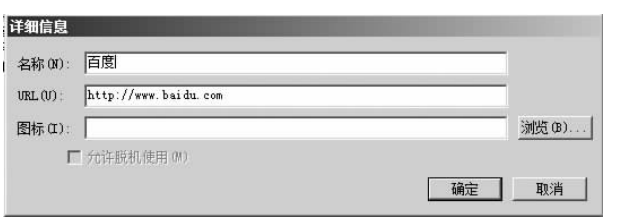

图 3-14　添加收藏夹链接

这样百度就会在用户的收藏夹中出现，进而实现了收藏夹的统一配置。

3.2.3　取消密码复杂性的要求

在 Windows Server 2008 系统中，对密码的复杂性要求较高，越是复杂的密码其安全系数就越高。但是也存在弊端，越复杂的密码越难记忆，因此很多普通用户会抱怨密码太长，很容易把密码忘记。因此在这里我们讲解管理员如何通过修改域控制器的安全策略，来取消系统中密码的负载性要求。在保证安全的前提下可以使用简单的密码，其具体操作如下。

（1）打开“组织策略管理器”对话框，依次选择“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“账户策略”→“密码策略”，密码必须符合复杂性要求策略，如图 3-15 所示。

（2）双击“密码必须符合复杂性要求”，选择“已禁用”，如图 3-16 所示。

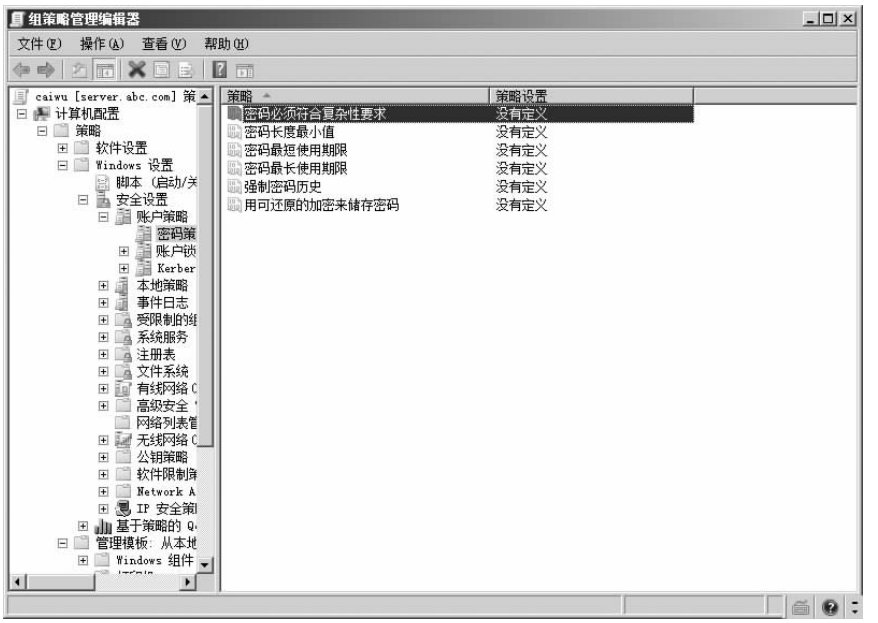

图 3-15　设置密码复杂度策略

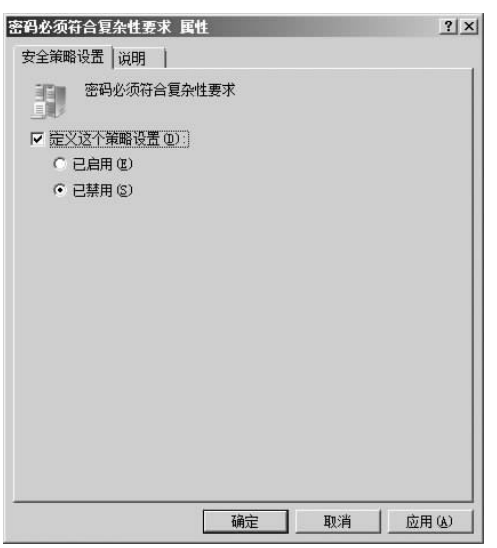

图 3-16　禁用密码复杂性要求

3.2.4　设置硬件访问控制策略

1. 可移动存储访问策略

随着移动存储设备越来越普及，移动设备的存储空间也越来越大，病毒的传播很多也可以通过移动存储进行，因此对移动设备的管理难度更是越来越复杂，伴随着出现了管理 CD 和 DVD 带来的新问题，Windows Server 2008 通过组策略可以控制对移动设备的访问和对硬件设备的安装。