第 10 章　组策略

Windows 2000 引入了组策略（Group Policy），这是一种重要的更新和配置管理技术。组策略为所管理的计算机和用户定义了桌面配置。组策略非常灵活，其中包括了策略设置、安全性设置、应用程序管理、计算机脚本以及文件夹重定向等选项。组策略使得管理员能够通过活动目录把组策略管理单元创建的组策略对象（GPO）应用于大量的计算机和用户，能够创建并不链接到活动目录容器的组策略对象，并以本地安全策略的形式把策略应用到本地机器；能够把安全配置模板导入组策略以进一步定制组策略的应用，并帮助部署跨企业的组策略；还能够使用安全配置工具集来编辑和应用这些模板（第 11 章将详细介绍安全模板和安全配置工具集）。

10.1　组策略概述

组策略是用户和计算机配置设置的集合。可以将这些设置链接到计算机、站点（Site）、域（Domain）和组织单元（OU），以指定用户的桌面配置状况。

组策略对象（Group Policy Object, GPO）则是大量组策略设置的一个集合，即可以为一组计算机或用户指定特定的桌面设置。

Microsoft 管理控制台 MMC 中集成了一个管理单元（或者叫插件，Snap-In）：组策略对象管理单元。通过这个管理单元，可以创建计算机和用户的配置。它是管理员为单位中的用户和计算机定义并控制程序、网络资源及操作系统行为的主要工具。

组策略可以为计算机和用户的桌面配置定义表 10-1 中所列出的组策略选项。

表 10-1　组策略选项

组件	说明
管理模板	设置基于注册表的策略
安全设置	为域、计算机和用户配置安全性
软件安装	向应该得到的用户分配或发布程序
脚本	指定用户登录/注销以及计算机启动/关闭的脚本
文件夹重定向	将特殊文件夹（如“My　Documents”）放在网络上

默认情况下，组策略能够从站点、域和最后到的组织单元继承而来。应用组策略对象（把组策略对象链接到它们的目标上）的顺序和级别决定了用户或计算机实际能收到的组策略设置。另外，组策略能够在站点、域、组织单元这些级别上被阻塞；组策略还能够基于组策略对象强制实施。这可以通过将组策略对象链接到它们的目标上，然后将链接设置为非覆盖方式来实现。

默认情况下，组策略影响站点、域、或组织单元中所有用户和计算机，而不影响站点、域、或组织单元中的其他对象。但特别要指出的是，组策略不影响安全组。

10.1.1　组策略的基础结构

1. 组策略对象和组策略管理单元

可以把组策略对象想象为关联组策略管理单元的文档。这就好比.doc 文档与 Microsoft Word 关联，. txt 文件与记事本关联一样。

可以将组策略管理单元作为独立工具或者活动目录管理单元的扩展来使用，从而创建组策略对象。但不能以只读的方式打开组策略对象。

2. 组策略对象的链接

可以将组策略对象链接到指定的站点、域或组织单元，从而尽量发挥活动目录的作用。组策略对象中的数据由受影响的客户来评估，由客户来展开活动目录的层次结构并最终决定当组策略设置有冲突时谁优先。

3. 组策略管理单元的访问

可以通过使用组策略管理单元来创建一个非本地的组策略对象，或者作为活动目录管理单元的扩展，或者作为一个单独的 MMC 控制台。

最常见的组策略管理单元的使用方法来自于“ Active Directory 用户和计算机 ”。它允许用户将组策略对象链接到一个域或者组织单元，也可以通过活动目录站点与服务来访问组策略。从两个活动目录的控制台上，可以通过上下文菜单来访问组策略。右击站点、域或组织单元，选择“ 属性 ”命令，然后打开“ 组策略 ”选项卡，在其中将组策略链接到站点。

4. 通过安全组成员筛选

通过在安全组中使用成员关系和设置任意访问控制表（DACL）权限，就可以达到在计算机和用户上筛选组策略的效果。这种实施方式保证了更快地处理组策略对象。更进一步，通过使用安全组，可以在企业中限制谁能创建链接到组策略对象的活动目录，以及谁能访问到创建和修改了的组策略对象。

10.1.2 使用组策略的管理要求

为了给一个选定的活动目录站点、域或组织单元设置组策略，必须让该活动目录能够访问到 Windows 2000 的域控制器，还必须有访问域控制器（即%SYSTEMROOT%\Sysvol 目录）的读/写权限，而且还必须有修改权限以选择目录站点、域或组织单元。当用户安装一个 Windows 2000 域控制器或将某个服务器提升成域控制器时，就默认创建了 Sysvol 目录。

默认情况下，组策略对象影响活动目录中组策略对象链接到的站点、域或组织单元。然而，可以基于 Windows 2000 安全组中的用户或计算机成员关系来筛选组策略的影响。为了筛选组策略，用户可以在组策略对象的“ 属性 ”对话框中使用“ 安全 ”选项卡，也可以使用权限来授权对组策略管理单元的使用。

10.1.3 Windows 2000 与 Windows NT 策略的比较

Windows NT 4.0 引入了系统策略编辑器（Poledit.exe），它是一个允许指定存储在 Windows NT 注册表中的用户和计算机设置的工具。通过使用系统策略编辑器，可以控制用户的网络环境，并为运行 Windows NT 4.0 系统的所有计算机强制系统配置设置。系统策略设置为注册表设置，用来定义桌面环境中不同组件的行为。

而在 Windows 2000 中，则引入了组策略基础结构和组策略管理单元，扩展了系统策略编辑器的功能，并可以通过使用组策略管理单元来为一组特定的用户和计算机组创建特殊的桌面配置。对于 Windows 2000 客户，组策略管理单元几乎能完全代替系统策略编辑器。它允许为大型的、可以嵌套的、甚至交叠的计算机组和用户组管理桌面配置。非本地的组策略对象通过链接一定数量的目标来发挥作用，这些目标可以为活动目录中的站点、域或者组织单元。

两者之间所提供的基础结构与功能之间还存在着一些显著的差别。Windows NT 4.0、Windows 95 和 Windows 98 中使用系统策略编辑器指定的系统策略设置具有下列特点：

- 被应用到域

- 能够在安全组中被用户成员进一步控制
- 不安全，用户能够通过注册表编辑器（Regedit.exe）进行改动
- 在用户配置文件中保持不变。当用策略编辑器进行注册表设置后，该设置将保留直到指定设置被更改或者用户编辑注册表
- 被限制基于注册表设置来强制管理桌面的行为，即有效地限制到桌面锁定

而 Windows 2000 的组策略管理单元为基于注册表的策略、安全设置、软件安装、脚本和文件夹重定向提供内置的特征。用户创建的组策略设置包含在组策略对象中，也可以从属于任何非本地（即基于活动目录）的组策略对象。使用组策略指定的策略设置是 Windows 2000 中启用中心化的更新和配置管理的首选方式。组策略设置能够：

- 与站点、域、组织单元相关联
- 在站点、域、组织单元中影响用户和计算机
- 被安全组中的用户或计算机成员进一步控制
- 是安全的，只有系统管理员才能更改设置
- 默认的策略设置并不是一成不变的
- 用于很好地调整桌面控制，增强用户的计算环境

10.2 组策略的存储

组策略对象有两种：本地组策略对象和非本地组策略对象。本地组策略对象存储在每台基于 Windows 2000 的计算机中，而非本地组策略对象是基于活动目录的，用全局惟一标识符确定。如果两者发生冲突，那么本地组策略对象的设置可以被非本地组策略对象所覆盖。

本地组策略保存在每台 Windows 2000 系统的%SYSTEMROOT%\system32\GroupPolicy 目录中。而非本地组策略对象在两个位置存储组策略信息：组策略容器和组策略模板。它们以全局惟一标识的方式命名，使得它们之间保持同步。组策略容器含有细小的或不经常发生变化的信息，而较大的或经常发生变化的信息则都保存在组策略模板中。在组策略用户界面上这种数据的分离对用户来说是透明的。

10.2.1 本地组策略对象的存储

本地组策略对象存在于每一台计算机上，并且默认情况下仅位于安全设置下面的节点被配置。位于本地组策略对象中的名字空间的其他部分的设置被开启或关闭。本地组策略对象被存储在%SYSTEMROOT%\System32\GroupPolicy 中，并且有下列的权限设置。

- Administrators 组：完全控制。
- SYSTEM：完全控制。
- 用户：读取。

如果从本地 Administrators 组收回读取权限，则组策略不被应用。这是一种把本地管理员从一组策略对象中排除的简易方法，即使他们的组策略应用权限设置为“ 允许 ”。

1. Gpt.ini 文件

本地组策略对象 Gpt.ini 文件包含下面的信息。

- GPCUserExtensionNames：包括一个 GUID 的列表，告诉客户端的引擎哪些客户端的扩展在组策略对象中有用户数据。
- GPCMachineExtensionNames：包括一个 GUID 的列表，它告诉客户端的引擎哪些客户端的扩展在组策略对象中有计算机数据。
- 选项：指向组策略对象选项，如用户部分关闭或计算机部分关闭。

- Version：为创建组策略对象的组策略扩展工具的版本号。

2. 组策略模板子目录

组策略模板目录包含一个子目录树，在树中呈现的子目录数目取决于组策略对象。但默认至少有两个子目录：Machine 和 User。

- Machine：包括一个 Registry.pol 文件，该文件包含应用到计算机的注册表设置。计算机初始化时，Registry.pol 文件被下载并应用到注册表的 HKEY_LOCAL_MACHINE 部分。
- User：包括一个 Registry.pol 文件，该文件中包含应用到用户的注册表设置。当用户登录到计算机时，Registry.pol 文件被下载并应用到注册表的 HKEY_CURRENT_USER 部分。

组策略模板文件夹还包含下面的子目录。

- Adm：包含组策略对象的所有. adm 文件。
- Machine\Scripts\ShutDown：包含计算机关闭时运行的脚本。
- Machine\Scripts\Startup：包含计算机启动时运行的脚本。
- Machine\Applications：它的内容取决于在给定的组策略对象前提下，有哪些应用程序被计算机指定。
- Machine\Microsoft\Windows NT\Secedit：包含 GptTmpl.inf 文件，它是 Windows 2000 域控制器的默认安全配置设置。
- User\Applications：包含 Windows Installer 所使用的广告文件（.aas 文件）。
- User\Document&Settings：包含 Fdeploy.ini，它包含有关当前用户所指文件夹的文件夹重定向的状态信息。
- User\Microsoft\RemoteInstall：包含 OSCfilter.ini，它包含通过远程安装服务的关于操作系统安装的用户的选择。
- User\Microsoft\IEAK：包含 Internet Explorer Maintenance Snap-in 的设置。
- User\Scripts\Logoff：包含当用户注销计算机时所运行的脚本。
- User\Scripts\Logon：包含当用户登录到计算机时所运行的脚本。

其中，User 目录和 Machine 目录在安装时被创建，其他的目录则在策略设置需要时才会被创建。

3. Registry. pol 文件

组策略的管理模板扩展在组策略模板中存储信息，名称为 Registry.pol 的文本文件。这些文件包含了定制的注册表设置，这些设置应用到注册表中的 Machine 或 User 部分，而注册表由用户使用组策略管理单元来指定。Windows 2000 的 Registry.pol 文件类似于 Windows 95，Windows 98 及 Windows NT 4.0 的 Config.pol 文件。两个 Registry.pol 文件在组策略模板中创建和存储，一个用于计算机配置，它存储于\ Machine 子目录中，而另一个用于用户配置，它存储于\User 子目录中。

10.2.2 非本地组策略对象的存储

1. 组策略容器

组策略容器是一个关于组策略对象的活动目录存储区域，它包括计算机和用户组策略信息。组策略容器具有如下属性。

- 版本信息：用来保证信息与组策略模板信息同步。

- 状态信息：用来指明组策略对象是处于开启状态还是关闭状态。
- 组件（扩展）的列表：它在组策略对象中设置。
- 被扩展插件所定义的策略设置。

例如，组策略容器存储的被软件安装插件所使用的信息描述了可以安装的软件状态的信息。

2. 组策略模板

组策略对象也在一个被称为组策略模板的目录结构中存储组策略的信息。该组策略模板位于域控制器的系统卷中的一个子目录（%SYSTEMROOT%\Sysvol\Policies）中。组策略模板是这样一个容器：它包含基于管理模板的策略设置、安全设置、软件安装可用的应用、脚本文件等。

当修改一组策略对象时，给予组策略模板的目录名为将要修改的组策略对象的 GUID。例如，一个组策略模板目录可能命名为：

%systemroot%sysvol\SYSVOL\www.SjtuInfosec.net\Policies\{47636445-af79-11d0-91fe-080036644603}

组策略模板目录中含有的文件和子目录可参见“ 本地组策略对象的存储 ”一节。

10.3 组策略的配置

组策略管理单元的根节点是以组策略对象和它所存储在的域名称来显示的。格式为：

<组策略对象名称> [<域名称>]策略

例如：Default Domain Policy [SjtuInfosec.net] Policy

下一级的名字空间有两个结点：计算机配置和用户配置，它们是用来配置指定的桌面环境及分别在计算机和用户组上强制使用组策略的父文件夹。如图 10-1 所示：

图 10-1 组策略配置

- 计算机配置：计算机配置包括所有与计算机相关的策略设置，它们用来指定操作系统行为、桌面行为、安全设置、计算机开机与关机脚本、指定的计算机应用选项以及应用设置。当操作系统被初始化时，在固定的刷新周期内，与计算机相关的组策略被实施。一般情况下，计算机策略比与之冲突的用户策略具有更高的优先级。
- 用户配置：用户配置包括所有与用户相关的策略设置，它们用来指定操作系统行为、桌面设置、安全设置、指定和发布的应用选项、应用设置、文件夹重定向选项、用户登录与注销脚本等。当用户登录到计算机时，在固定的刷新周期内，与用户相关的组策略被实施。

在计算机配置和用户配置父节点下包括以下一些子节点。

- 软件设置：它为独立软件开发商（ISV）进行扩充提供了位置。如果没有节点被 ISV 添加，那么软件设置仅仅包含软件安装这个扩展，包括 Windows 2000。

- Windows 设置：它包括由 Microsoft 所提供的扩展，包括脚本（启动/关机、登录/注销）、安全设置、Internet Explorer 维护、目录重定向和远程安装服务等节点。
  - 脚本　含有计算机特殊脚本的信息。启动和关闭脚本存在于计算机配置节点中，指定了当计算机启动或关闭时作为本地系统运行的脚本；登录和注销脚本存在于用户配置节点中，在用户模式而非特权模式中运行。
  - 安全设置　含有登录到计算机的所有用户的安全设置，可以在本地、计算机、域和网络一级定义安全设置。该节点下面具有账户策略、本地策略、公钥策略和 IP 安全策略等子节点。
  - 目录重定向　可以使用目录重定向来重定向 Windows 2000 所指定的文件夹到网络上一个可选的位置，在这里用户能够中心化地管理它们。Windows 2000 可以重定向 My Documents、应用数据、桌面及开始菜单等文件夹。
  - Internet Explorer 维护　可以在基于 Windows 2000 的计算机上使用 Intenet Explorer 维护来管理和定制 Microsoft 的 Internet Explorer。
  - 远程安装服务　可以使用远程安装服务（RIS）来控制远程操作系统安装显示到客户计算机的行为特征。
- 管理模板：管理模板是供组策略用来生成用户界面设置的文件，可由管理员进行配置。这些文件由分层的目录和子目录所组成，目录定义了哪些选项将显示在组策略中，以及可以显示哪些可由组策略进行修改的注册表设置。这些设置包括基于注册表的可以控制有关桌面行为和外观（以及操作系统组件和应用程序）的注册表设置的组策略配置，它们被写入到注册表数据库中的 HKEY_CURRENT_USER 以及 HKEY_LOCAL_MACHINE 部分。管理模板的名字空间是由.adm 文件或者组策略扩展来创建的。在第一次使用管理模板节点时，就会自动安装一些.adm 文件。在这些管理模板下显示的用户界面就是用这些.adm 文件填充的。Windows 2000 包含以下一些管理模板：
  - System.adm：为 Windows 2000 客户默认安装在组策略中。
  - Inetres.adm：也为 Windows 2000 客户默认安装在组策略中，用来配置 Internet Explorer 策略。
  - Winnt.adm：控制在 Windows NT 4.0 中使用系统编辑器时的特殊用户界面。
  - Windows.adm：控制在 Windows 95/98 中使用系统编辑器时的特殊用户界面。
  - Common.adm：控制在 Windows 95/98 和 Windows NT 4.0 中使用系统编辑器时的特殊用户界面。

图 10-2 显示了当前系统所应用的组策略模板，也可以实现对当前的策略模板进行添加和删除的功能。

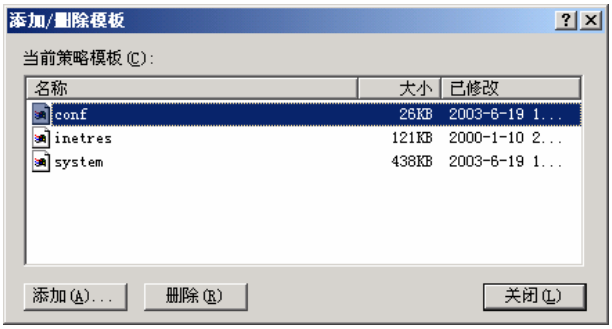


图 10-2　组策略模板的查看、添加和删除界面

10.4 组策略的应用

现在已经知道，组策略是由计算机策略和用户策略组成的，它们分别保存在组策略的计算机配置节点和用户配置节点下。计算机策略是在计算机引导的时候加载，而用户策略则是在用户登录的时候加载。

计算机和用户是仅有的接收组策略的活动目录对象类型，安全组不需要应用策略。

组策略对象是按照特定的顺序应用的，并且当组策略对象配置不能协调一致时还会把以前所应用的策略覆盖掉。但是当不同策略中的设置相互排斥时，它们仍能够组合形成一个有效的策略。

10.4.1 组策略的应用顺序

1. 默认的组策略应用顺序

组策略配置的默认应用顺序如下。

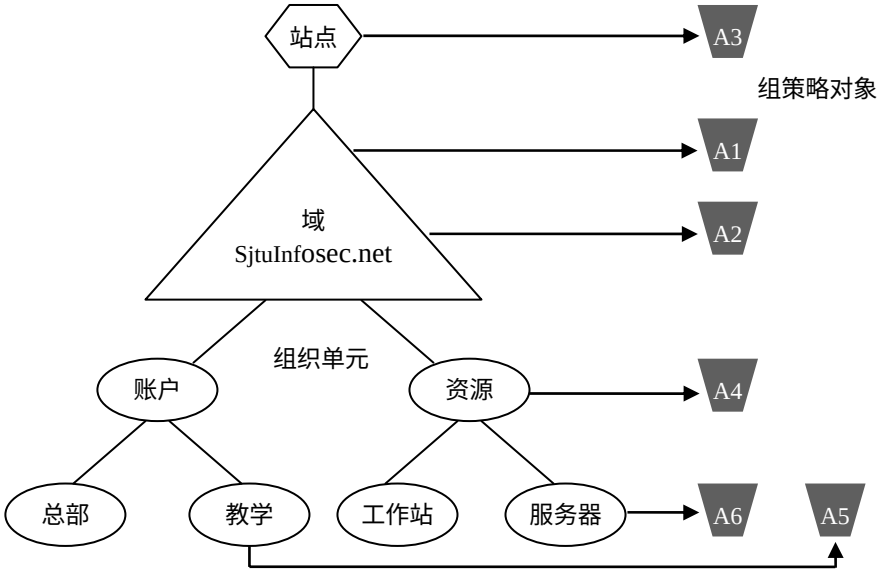
① 本地组策略对象（Local GPO）：每台运行 Windows 2000 的计算机都只存储有一个本地的组策略对象。

② 站点组策略对象（Site GPO）：处理链接到计算机所在站点的所有组策略对象。处理是同步进行的，管理员指定要链接到站点的组策略对象顺序。

③ 域组策略对象（Domain GPO）：处理链接到计算机所在域的所有组策略对象。如果多个组策略对象链接到一个域，那么计算机就按照管理员指定的顺序同步处理它们。

④ 组织单元组策略对象（OU GPO）：首先处理链接到活动目录层次结构最高级 OU 的组策略对象，然后按照从父 OU 到子 OU 的顺序，以及按照在每个 OU 的级别上管理员指定的顺序依次进行，最后处理的组策略对象是链接到含有计算机和用户的 OU 的那些对象。

这个应用顺序意味着本地组策略对象最先处理，链接到计算机或用户是其直接成员的 OU 的组策略对象最后处理，并覆盖早先处理的组策略对象。图 10-3 说明了组策略在活动目录环境中的应用顺序。



教学 OU 的组策略应用顺序：A3, A1, A2, A5

服务器 OU 的组策略应用顺序：A3, A1, A2, A4, A6

图 10-3 组策略的应用顺序

2. 组策略继承关系

一般来说，组策略在活动目录服务中是从父容器遗传到子容器的。如果将一个单独的组策略分配给父容器，那么该组策略将应用于父容器下方的所有容器，包括父容器中的用户和计算机对象。不过，若为子容器指定了一个组策略设置，子容器的组策略设置将优先于从父容器继承的设置。

- 如果父组织单元（OU）中的策略设置未配置，那么子 OU 将不继承这些设置。被禁用的策略设置继承后仍为禁用状态。
- 如果配置了父 OU 的一个策略，而子 OU 的相同策略未配置，那么子 OU 将继承父 OU 的策略设置。
- 如果一个父策略和子策略兼容，子策略将继承父策略，而且子策略的设置也适用。只要策略兼容，策略就会被继承。例如，如果父策略将某个目录放到桌面上，而子策略设置调用了另外一个目录，那么用户将会看到两个目录。
- 如果为父 OU 配置的策略与为子 OU 配置的相同策略不兼容，那么子 OU 将不会从父 OU 中继承该策略设置，也就是子 OU 中的设置将被应用。

3. 特殊的应用顺序和继承

在处理组策略的应用顺序时，除了上述的默认应用顺序和继承关系之外，还必须考虑以下一些特殊情况。

- 工作组成员：作为工作组成员的计算机只处理本地组策略对象。
- “禁止替代”（No override）选项：链接到站点、域或组织单元（不包括本地）的任何一个组策略对象都可以使用“禁止替代”选项，来防止随后处理的组策略对象覆盖该组策略对象中的所有策略设置。如果有多个组策略对象设置为“禁止替代”时，那么就会优先采用在活动目录层次结构中处于更高层的那一个。如果最高层的那一级有多个 OU，那么就采用被指定为具有最高优先权的那个 OU。
- “锁定策略继承”（Block Policy Inheritance）：在任何一个站点、域或组织单元上，组策略继承都可以被选择性的标记为“锁定策略继承”，来禁止从父目录容器继承组策略。但是，设置为“禁止替代”的组策略对象链接将始终都会被采用，且不能阻止。“锁定策略继承”设置直接应用于站点、域或组织单元，而不应用于组策略对象，也不应用于组策略对象链接。所以，“锁定策略继承”将使来自上级可以到达站点、域或组织单元的所有组策略设置产生偏差，而不管这些设置来自哪些组策略对象。
- “反向”（Loopback）：在获取其配置会影响用户的组策略对象顺序列表时，“反向”提供了与默认方法不同的备用方法。这是一个高级的组策略设置，在某些封闭的管理环境（如实验室、机房和教室等）中的计算机上非常有用。默认情况下，用户设置来自于组策略对象的顺序列表，该列表取决于用户在活动目录服务中的位置所决定的继承关系，从链接到站点的组策略对象到链接到域的组策略对象再到链接到组织单元的组策略对象。各级管理员还可以指定系统在遍历活动目录层次结构时的顺序。“反向”可以被设置为“未配置”（Not Configured）、“启用”（Enabled）或“禁用”（Disabled）。其中在“启用”状态下，“反向”可设置为“合并”（Merge）模式还是“替换”（Replace）模式。
  - 替换　若选中该设置，用户的组策略对象列表可被系统启动时已经被计算机获得的组策略对象列表完全替代。计算机组策略对象替换用户组策略对象通常只应用于用户。
  - 合并　若选中该设置，组策略对象列表将会连结在一起。系统启动时为计算机

获得的组策略对象列表将被附在登录时为用户获得的组策略对象列表之后。而在默认情况下，为计算机获得的组策略对象将比为用户获得的组策略对象更具有优先权。

10.4.2 使用安全组筛选组策略

在 Windows 2000 系统中可以通过使用安全组设置相应的权限来筛选组策略，即决定哪些用户和计算机组受一特定组策略对象的限制。

具体的实现方法为：在组策略对象（GPO）的“ 属性 ”对话框中的“ 安全 ”选项卡对特定的安全组设置是允许还是拒绝组策略，如图 10-4 所示。

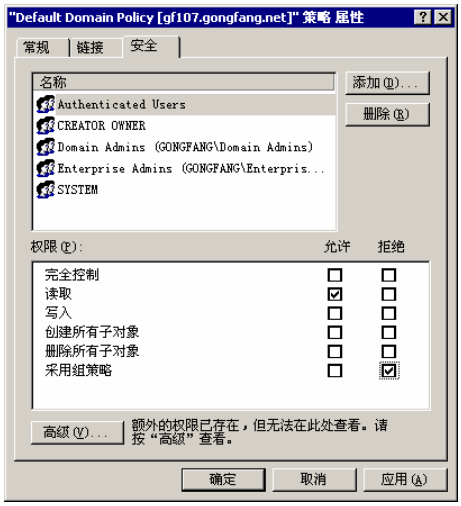


图 10-4 筛选组策略

筛选在总体上影响组策略的设置，即不能使用安全组来在组策略对象上的部分设置上起作用（或者是阻止起作用）。然而，文件夹重定向和软件安装这两种情况下可以例外，这二者在组策略对象这一层上有进一步的 ACL 设置以进一步调整基于安全组成员的行为。

10.4.3 组策略对启动和登录的影响

在计算机启动和用户登录的时候，组策略（包括计算机配置和用户配置）将按照以下列举的顺序来设置和应用。

（1）网络启动。网络首先启动，然后依次是“ 远程过程调用系统服务 ”（Remote Procedure Call System Service, RPCSS）和“ 多用途通用命名规则提供程序 ”（Multiple Universal Naming Convention Provider, MUP）服务启动。

（2）计算机获得一个组策略对象顺序列表。该顺序列表取决于：

- 计算机是否是 Windows 2000 域的一部分，因而通过活动目录取决于组策略
- 是否启用了“ 反向 ”选项及反向策略设置的状态
- 计算机对象在活动目录中的位置

（3）应用计算机策略的配置。该项任务默认按照以下顺序同步进行：本地 GPO、站点 GPO、域 GPO、组织单元 GPO、子组织单元 GPO …。直到所有计算机策略都加载完毕后才会显示用户界面。

（4）运行启动（Startup）脚本。该进程默认为隐藏和同步。每个脚本必须在下一个脚本开始之前完成或超时退出（默认的超时时间为 600 秒，可以使用若干个组策略配置来进行更改）。

（5）用户按下 SAS 热键（默认为 Ctrl+Alt+Del 组合键）登录。

（6）用户通过身份验证之后，就会在当前策略设置的控制下加载用户配置文件。

（7）计算机获得用户的一个组策略对象顺序列表。该顺序列表取决于：

- 该用户是否是 Windows 2000 域的一部分，因而通过活动目录取决于组策略
- 是否启用了“ 反向 ”选项及反向策略设置的状态
- 用户在活动目录中的位置

如果要应用的顺序组策略列表没有被改变，那么也就不会进行任何处理。

（8）应用用户策略的配置。该项任务默认按照以下顺序同步进行 :本地 GPO、站点 GPO、域 GPO、组织单元 GPO、子组织单元 GPO …。计算机在处理用户策略的同时，用户界面不会给出任何提示。

（9）运行登录（Login）脚本。与 Windows NT 4.0 不同的是，基于组策略的登录脚本在运行的时候是隐藏的。用户对象脚本最后运行。

(10) 组策略指定的操作系统用户界面出现。

10.5 组策略的实现

组策略工具集由组策略管理单元、对“ Active Directory 用户和计算机 ”控制台的扩展和对“ Active Directory 站点和服务 ”控制台的扩展所组成。可以使用这些工具来配置计算机安全性的不同方面，最简单的方法就是用所加载的相应管理单元创建一个自定义的 Microsoft 管理控制台。

10.5.1 访问组策略管理单元

访问组策略管理单元有两种基本的方法 :第一种是在 MMC 中选择作为独立管理单元的组策略，指定对象或计算机以访问其策略；第二种则是在一个 Active Directory 管理控制台（既包括用户和计算机控制台，也包括站点和服务控制台）中选择对象，并将组策略作为扩展管理单元来访问。

组策略管理单元的各个单项，如安全设置、管理模板等自身都是 MMC 管理单元扩展程序，而且提供这些项的管理单元扩展程序自身都可扩展。比如说安全设置管理单元，它自身包括若干个管理单元扩展程序。默认情况下，当启动组策略管理单元时，所有可用的扩展程序都将加载。

1. 打开本地组策略管理单元

本地组策略指的是存储在每台运行 Windows 2000 计算机上的那些组策略。

具体的打开方法为：在 MMC 控制台中，选择“ 添加/删除管理单元 ”功能，然后选择添加“ 组策略 ”，并在如图 10-5 所示的“ 选择组策略对象 ”对话框中选择“ 本地计算机 ”。

图 10-5 选择组策略对象

2. 打开远程主机的组策略管理单元

只要拥有远程主机的管理权限，也可以打开该计算机的本地组策略对象。具体方法也是在 MMC 中选择添加“ 组策略 ”管理单元，只不过需在图 10-5 中单击“ 浏览 ”按钮，然后切换到“ 计算机 ”选项卡输入远程计算机的名称，如图 10-6 所示。

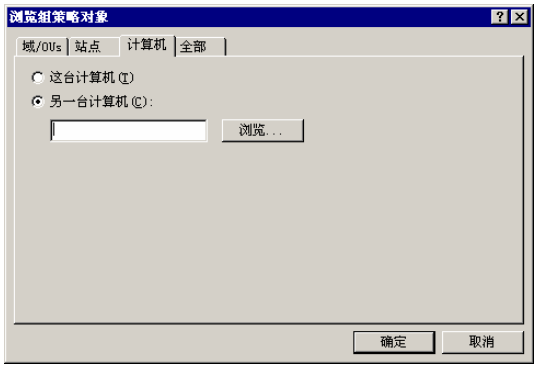


图 10-6 浏览远程计算机上的组策略对象

3. 从 Active Directory 用户和计算机控制台打开组策略管理单元

除了与特定计算机相关的组策略对象外，也可以为 Active Directory 对象（如站点、组织单元和站点）创建组策略。

若要通过 Active Directory 用户和计算机控制台访问组策略单元，就需要在控制台树中右击需要设置组策略的域或组织单元，并从弹出的菜单中选择“ 属性 ”，然后切换到“ 组策略 ”选项卡。现在就可以在“ 组策略对象链接 ”列表中选择一个现有的组策略项，然后单击“ 编辑 ”按钮，就可以打开链接到所选域或组织单元的组策略管理单元（也可以选择“ 新建 ”按钮来创建一个组策略，然后再进行编辑）。如图 10-7 所示。

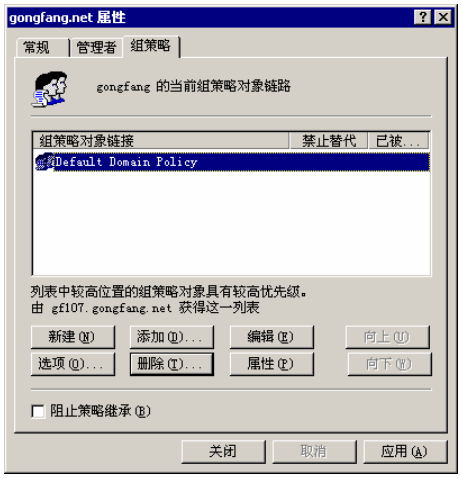


图 10-7 通过 Active Diretory 控制台打开组策略管理单元

4. 从 Active Directory 站点和服务控制台打开组策略管理单元

这与上述通过 Active Directory 用户和计算机控制台访问组策略单元基本相同，只不过是在 Active Directory 站点和服务控制台中进行，并且访问的是链接到站点的组策略管理单元。

10.5.2 设置组策略

打开组策略管理单元，然后管理单元的控制台树中展开需要设置的特定策略项，然后在详细信息窗格中双击该策略项，就可以对该策略的设置进行指定。

10.5.3 禁用未使用的组策略设置

如果创建或修改组策略的过程以计算机配置或用户配置文件夹中未配置的策略结束，那么就可以通过禁用文件夹来防止客户端主机耗用资源处理策略，来加速受组策略影响的计算机的启动和登录进程。

若要禁用组策略的计算机配置或用户配置，可参照以下步骤：

（1）打开组策略管理单元。

（2）右击控制台的根目录节点，从弹出的菜单中选择“ 属性 ”命令。

（3）在“ 属性 ”对话框中的“ 常规 ”选项卡中，选中“ 禁用计算机配置设置 ”或者“ 禁用用户配置设置 ”复选框。如图 10-8 所示。

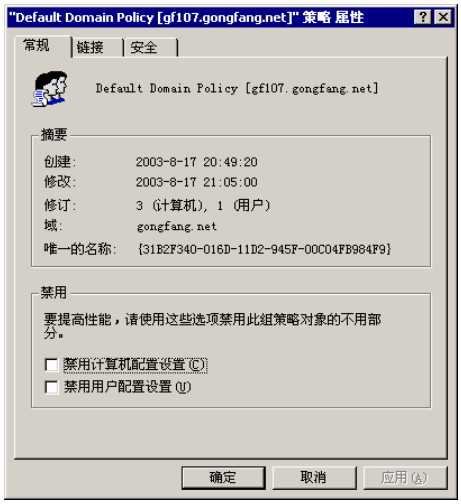


图 10-8 禁用未使用的组策略设置

10.5.4 指定组策略对象的特殊应用顺序和继承

1. 修改组策略应用顺序

通过“ Active Directory 用户和计算机 ”的扩展打开组策略管理单元来设置域或组织单元的组策略应用顺序，或者通过“ Active Directory 站点 ”的扩展打开组策略管理单元来设置站点的组策略应用顺序。

具体的操作如下：

（1）打开组策略管理单元。

（2）在需要修改组策略应用顺序的站点、域或组织单元对象上右击。

（3）从弹出的“ 属性 ”对话框中选择“ 组策略 ”选项卡。

（4）在“ 组策略对象链接 ”列表中选择一个组策略对象，并通过单击“ 向上 ”或者“ 向下 ”按钮来更改其在应用顺序列表中的位置，如图 10-9 所示。

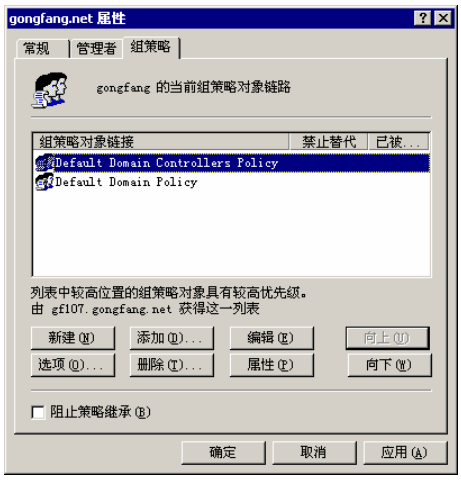


图 10-9 修改组策略的应用顺序

在该列表中位置较高的组策略对象具有较高的优先权。所以，Windows 2000 系统是按照从下往上的顺序来处理列表中的组策略对象的。这样，优先权最高的组策略的策略设置将最后应用，覆盖级别较低的组策略的策略设置。

2. 使用“禁止替代”选项

可通过“Active Directory 用户和计算机”的扩展打开组策略管理单元来设置域或组织单元的“禁止替代”选项，或者通过“Active Directory 站点”的扩展打开组策略管理单元来设置站点的“禁止替代”选项。

具体的操作如下：

（1）打开组策略管理单元。

（2）在需要修改组策略应用顺序的站点、域或组织单元对象上右击。

（3）从弹出的“属性”对话框中选择“组策略”选项卡。

（4）在“组策略对象链接”列表中选择需要修改的组策略对象，单击“选项”按钮。

（5）选中“禁止替代”复选框，以防止其他组策略对象覆盖此组策略对象中的策略设置，如图 10-10 所示。

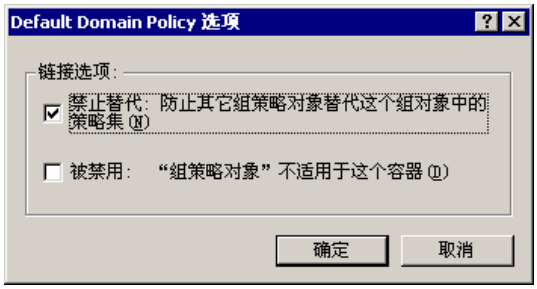


图 10-10 设置“禁止替代”选项

3. 阻止策略继承

若要阻止 Active Directory 对象继承组策略中的策略设置，可以参照如下操作步骤：

（1）打开组策略管理单元。

（2）在需要修改组策略应用顺序的站点、域或组织单元对象上右击。

（3）从弹出的“属性”对话框中选择“组策略”选项卡。

（4）选中“阻止策略继承”复选框，以指定已经链接到父站点、父域或父组织单元的所有组策略域的本站点、本域或本组织单元的链接都将被阻止。但是不能阻止启用了“禁止替

代 ” 选项的组策略。

图 10-11　阻止策略继承

4. 启用 “ 反向 ” 设置

若要启用 “ 反向 ” 设置，可参照如下步骤：

（1）打开组策略管理单元。

（2）在控制台树中，展开 “ 计算机配置 ” → “ 管理模板 ” → “ 系统 ” → “ 组策略 ”。

（3）在详细信息窗格中，双击 “ 用户组策略反向对应处理方式 ”，显示 “ 属性 ” 对话框，如图 10-12 所示。

（4）选择 “ 启用 ”，然后在 “ 方式 ” 列表中选择下列模式之一。

- 合并 :用计算机启动时已获得的组策略列表附在登录时获得的用户组策略列表上。
- 替换：用计算机启动时已获得的组策略列表替换用户组策略列表。

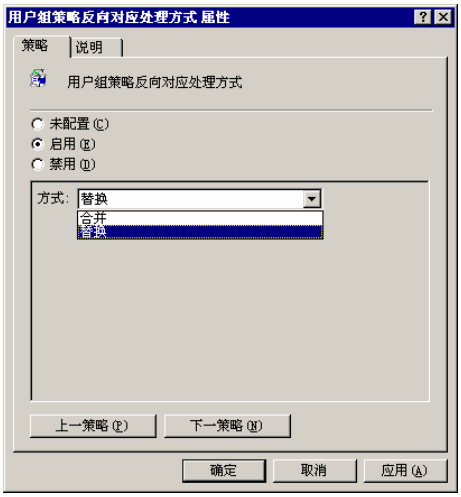


图 10-12 启用 “ 用户组策略反向对应处理方式 ”