

## 第4章 利用组策略管理用户工作环境

通过AD DS的**组策略**（group policy）功能，可以更容易管理用户工作环境与计算机环境、减轻网络管理负担、降低网络管理成本。

- 组策略概述
- 策略设置实例演练
- 首选项设置实例演练
- 组策略的处理规则
- 利用组策略来管理计算机与用户环境
- 利用组策略限制访问可移动存储设备
- WMI筛选器
- 组策略模型与组策略结果
- 组策略的委派管理
- 入门GPO的设置与使用



## 4.1 组策略概述

组策略是一个能够让系统管理员充分管理用户工作环境的功能，通过它来确保用户拥有符合要求的工作环境，也通过它来限制用户，如此不但可以让用户拥有适当的环境，也可以减轻系统管理员的管理负担。

### 4.1.1 组策略的功能

以下列举组策略所提供的主要功能：

- ✎ **账户策略的设置**：例如设置用户账户的密码长度、密码使用期限、账户锁定策略等。
- ✎ **本地策略的设置**：例如审核策略的设置、用户权限分配、安全配置等。
- ✎ **脚本的设置**：例如登录与注销、启动与关机脚本的设置。
- ✎ **用户工作环境的设置**：例如隐藏用户桌面上所有的图标、删除开始菜单中的运行/查找/关机等选项、在开始菜单中添加注销选项、删除浏览器的部分选项、强制通过指定的代理服务器上等等。
- ✎ **软件的安装与删除**：用户登录或计算机启动时，自动为用户安装应用软件、自动修复应用软件或自动删除应用软件。
- ✎ **限制软件的运行**：通过各种不同的软件限制规则来限制域用户只能运行特定的软件。
- ✎ **文件夹的重定向**：例如改变文件、开始菜单等文件夹的存储位置。
- ✎ **限制访问可移动存储设备**：例如限制将文件写入U盘，以免企业的机密文件轻易被带离公司。
- ✎ **其他众多的系统设置**：例如让所有的计算机都自动信任指定的CA（Certificate Authority）、限制安装设备驱动程序（device driver）等。

可以在AD DS中针对站点（site）、域（domain）与组织单位（OU）来设置组策略（如图4-1-1所示）。

组策略内包含**计算机配置**与**用户配置**两部分：

- ✎ **计算机配置**：当计算机启动时，系统会根据**计算机配置**的内容来设置计算机的环境。举例来说，如果针对域sayms.local设置了组策略，则此组策略内的**计算机配置**就会被应用到（apply）这个域内的所有计算机。
- ✎ **用户配置**：当用户登录时，系统会根据**用户配置**的内容来设置用户的工作环境。举例来说，如果针对组织单位**业务部**设置了组策略，则其中的**用户配置**就会被应用到这个组织单位内的所有用户。



图 4-1-1

除了可以针对站点、域与组织单位来设置组策略之外，还可以在每一台计算机上设置其本地计算机策略（local computer policy），这个计算机策略只会应用到本地计算机与在这台计算机上登录的所有用户。




### 4.1.2 组策略对象

组策略是通过组策略对象（Group Policy Object, GPO）来设置的，只要将GPO连接（link）到特定的站点、域或组织单位，此GPO内的设置值就会影响到该站点、域或组织单位内的所有用户与计算机。

#### 1. 内置的 GPO

AD DS域有两个内置的GPO，它们分别如下。

- **Default Domain Policy:** 此GPO默认已经被连接到域，因此其设置值会被应用到整个域内的所有用户与计算机。
- **Default Domain Controller Policy:** 此GPO默认已经被连接到组织单位Domain Controllers，因此其设置值会被应用到Domain Controllers内的所有用户与计算机（Domain Controllers内默认只有域控制器的计算机账户）。

可以通过【单击左下角开始图标Windows 管理工具组策略管理如图4-1-2所示】的方法验证Default Domain Policy与Default Domain Controller Policy GPO分别已经被连接到域

sayms.local与组织单位Domain Controllers。

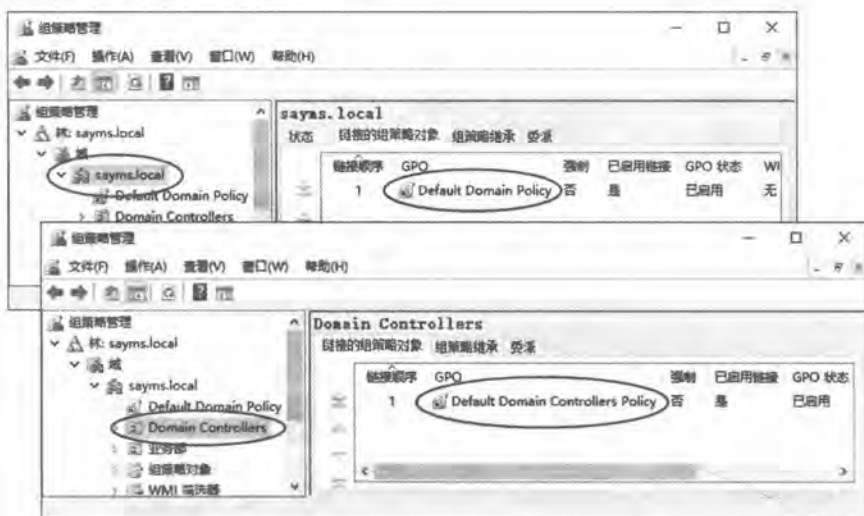


图 4-1-2







### 注意

在尚未彻底了解组策略以前，请暂时不要随意更改Default Domain Policy或Default Domain Controller Policy这两个GPO的设置值，以免影响系统运行。

## 2. GPO 的内容

GPO的内容被分为GPC与GPT两部分，它们分别被存储在不同的位置。

- **GPC (Group Policy Container) :** GPC是存储在AD DS数据库内，它记载着此GPO的属性与版本等数据。域成员计算机可通过属性来得知GPT的存储位置，而域控制器可利用版本来判断其所拥有的GPO是否为最新版本，以便作为是否需要从其他域控制器复制最新GPO设置的依据。

可以通过以下方法来查看GPC：【单击左下角开始图标  Windows 管理工具  Active Directory管理中心  选择树视图图标  单击域（例如sayms）  展开容器System  如图4-1-3所示单击Policies】，图中间圈起来的部分为Default Domain Policy与Default Domain Controller Policy这两个 GPO的GPC，图中的数字分别是这两个GPO的GUID（Global Unique Identifier）。

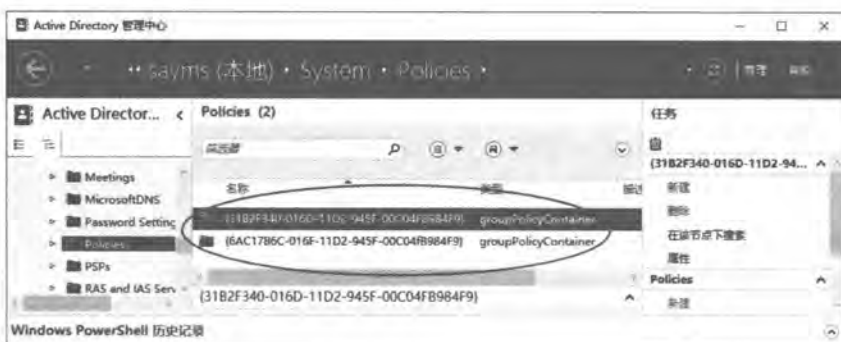


图 4-1-3

如果要查询GPO的GUID的话，例如要查询Default Domain Policy GPO的GUID，可以通过如图4-1-4所示【在组策略管理控制台中单击Default Domain Policy ➤ 单击详细信息选项卡 ➤ 唯一ID】的方法。



图 4-1-4

➤ **GPT (Group Policy Template)**：GPT是用来存储GPO设置值与相关文件，它是一个文件夹，而且是被建立在域控制器的`%systemroot%\SYSVOL\sysvol\域名\Policies`文件夹内。系统是利用GPO的GUID来当作GPT的文件夹名称，例如图4-1-5中两个GPT文件夹分别是Default Domain Policy与Default Domain Controller Policy GPO的GPT。



图 4-1-5



## 附注

每台计算机还有本地计算机策略，可以通过【按 **Win**+**R** 键⇨输入MMC后单击**确定**按钮⇨单击文件菜单⇨添加/删除管理单元⇨点选组策略对象编辑器⇨依序单击**添加**、**完成**、**确定**按钮】的方法建立管理本地计算机策略的工具(或直接按 **Win**+**R** 键⇨输入gpedit.msc后单击**确定**按钮)。本地计算机策略的设置数据是被存储在本地计算机的%systemroot%\System32\GroupPolicy文件夹内，它是隐藏文件夹。

### 4.1.3 策略设置与首选项设置

组策略的设置可分为策略设置与首选项设置两种：

- ✎ 只有域的组策略才有首选项设置功能，本地计算机策略并无此功能。
- ✎ 策略设置是强制性设置，客户端应用这些设置后就无法改编（有些设置虽然客户端可以自行更改设置值，不过下次应用策略时，仍然会被改为策略内的设置值）；然而首选项设置是非强制性的，客户端可自行更改设置值，因此首选项设置适合于用来当作默认值。
- ✎ 如果要筛选策略设置的话，必须针对整个GPO来筛选，例如某个GPO已经被应用到业务部，但是我们可以通过筛选设置来让其不要应用到业务部经理Mary，也就是整个GPO内的所有设置项目都不会被应用到Mary；然而首选项设置可以针对单一设置项目来筛选。
- ✎ 如果在策略设置与首选项设置内有相同的设置项目，而且都已做了定义，但是其设置值却不相同的话，则以策略设置优先。
- ✎ 要应用首选项设置的客户端需要安装支持首选项设置的Client-Side Extension（CSE）。Windows 7(含)之后的计算机已内不包含CSE，而Windows Vista SP1&SP2也可以通过安装Microsoft远程服务器管理工具（Remote Server Administration Tools, RSAT）来安装CSE。
- ✎ 要应用首选项的客户端还需要安装XMLLite。Windows XP SP3(含)之后的计算机已不包含XMLLite。

### 4.1.4 组策略的应用时机

当修改了站点、域或组织单位的GPO设置值后，这些设置值并不是立刻就对用户与计算机生效，而是必须等GPO设置值被应用到用户或计算机后才有效。GPO设置值内的计算机设置与用户设置的应用时机并不相同。

#### 1. 计算机配置的应用时机

域成员计算机会在以下的情况下应用GPO的计算机配置值：



- ✎ 计算机开机时会自动应用。
- ✎ 如果计算机已经开机的话，则会每隔一段时间自动应用：
  - 域控制器：默认是每隔5分钟自动应用一次。
  - 非域控制器：默认是每隔90~120分钟之间自动应用一次。
  - 不论策略设置值是否有变化，都会每隔16小时自动应用一次安全策略。
- ✎ 手动应用：到域成员计算机上打开Windows PowerShell窗口（或命令提示符）、执行 `gpupdate /target:computer /force` 命令。

## 2. 用户配置的应用时机

域用户会在以下的情况下应用GPO的用户配置值：

- ✎ 用户登录时会自动应用。
- ✎ 如果用户已经登录的话，则默认会每隔90~120分钟之间自动应用一次。不论策略设置值是否发生变化，都会每隔16小时自动应用一次安全策略。
- ✎ 手动应用：到域成员计算机上打开Windows PowerShell窗口（或命令提示符）、执行 `gpupdate /target:user /force` 命令。

### 附注

1. 执行 `gpupdate /force` 会同时应用计算机配置与用户配置。
2. 部分策略设置可能需计算机重新启动或用户登录才生效，例如软件安装策略与文件夹重定向策略。

## 4.2 策略设置实例演练

在继续解释更高级的组策略功能之前，为了有一个比较清楚的概念，此处分别利用两个例子来练习GPO的计算机配置与用户配置中的策略设置。

### 4.2.1 策略设置实例演练一：计算机配置

系统默认是只有某些组（例如administrators）内的用户，才有权限在扮演域控制器角色的计算机上登录，而普通用户在域控制器上登录时，屏幕上会出现如图4-2-1所示的无法登录的警告消息，除非他们被赋予允许本地登录的权限。





图 4-2-1

以下假设要开放让域SAYMS内Domain Users组内的用户可以在域控制器上登录。我们将通过默认的Default Domain Controllers Policy GPO来设置，也就是要让这些用户在域控制器上拥有允许本地登录的权限。

**注意**

- 1. 一般来说，域控制器等重要的服务器不应该开放普通用户登录。
- 2. 如果要在成员服务器、Windows 10等非域控制器的客户端计算机上练习的话，则以下步骤可省略，因为Domain Users默认已经在这些计算机上拥有允许本地登录的权限。

- STEP 1 请到域控制器上利用系统管理员身份登录。
- STEP 2 单击左下角开始图标➡Windows 管理工具➡组策略管理。
- STEP 3 如图4-2-2所示【展开到组织单位Domain Controllers ➡选中右侧的Default Domain Controllers Policy并右击➡编辑】。



图 4-2-2

- STEP 4 如图4-2-3所示【展开计算机配置➡策略➡Windows设置➡安全设置➡本地策略➡用户权限分配➡双击右侧的允许本地登录】。





图 4-2-3

**STEP 5** 如图4-2-4所示【单击**添加用户或组**按钮输入或选择域SAYMS内的Domain Users组单击两次**确定**按钮】。由此图中可看出默认只有Account Operators、Administrators等组才拥有允许本地登录的权限。



图 4-2-4

完成后，必须等这个策略应用到组织单位Domain Controllers内的域控制器后才有效（见前一小节的说明）。等应用完成后，就可以利用任何一个域用户账户在域控制器上登录，以测试**允许本地登录**功能是否正常。

## 附注

如果域控制器是利用Hyper-V搭建的虚拟机，并且在查看处勾选了增强会话，由于此时是采用远程桌面连接来连接虚拟机的，因此请先利用Active Directory管理中心（或Active Directory用户和计算机）将Domain Users组加入Remote Desktop Users组，并执行gpedit.msc开放让Remote Desktop Users组具备允许通过远程桌面服务登录的权限（计算机配置→安全设置→本地策略→用户权限分配→……），否则域用户无法登录。

另外如果域内有多台域控制器的话，由于策略设置默认会先被存储到扮演PDC模拟器操作主机角色的域控制器（默认是域中的第1台域控制器），因此需要等待这些策略设置被复制到其他域控制器，然后再等这些策略设置值应用到这些域控制器。

## 附注

可以利用【单击左下角开始图标→Windows 管理工具→Active Directory用户和计算机→选中域名并右击→操作主机→PDC选项卡】来查看扮演PDC模拟器操作主机的域控制器。

系统可以利用以下两种方式来将PDC模拟器操作主机内的组策略设置复制到其他域控制器：

- **自动复制：**PDC模拟器操作主机默认是15秒后会自动将其复制出去，因此其他的域控制器可能需要等15秒或更久时间才会接收到此设置值。
- **手动复制：**假设PDC模拟器操作主机是DC1，而我们要将组策略设置手动复制到域控制器DC2。请在域控制器上【单击左下角开始图标→Windows 管理工具→Active Directory站点和服务→Sites→Default-First-Site-Name→Servers→展开目标域控制器（DC2）→NTDS Settings→选中PDC模拟器操作主机（DC1）并右击→立即复制】。

## 4.2.2 策略设置实例演练二：用户配置

假设域sayms.local内有一个组织单位**业务部**，而且已经限制他们需要通过企业内部的代理服务器上网（代理服务器proxy server的设置留待后面说明），而为了避免用户私自更改这些设置值，因此以下要将其**Internet选项**中**连接**选项卡内更改Proxy的功能禁用。

由于当前并没有任何GPO被连接到组织单位**业务部**，因此我们将先建立一个连接到**业务部**的GPO，然后通过修改此GPO设置值的方式来达到目的。

**STEP 1** 请到域控制器上利用系统管理员身份登录。

**STEP 2** 单击左下角开始图标→Windows 管理工具→组策略管理。

**STEP 3** 如图4-2-5所示【展开到组织单位**业务部**→选中**业务部**并右击→在这个域中创建GPO并在此处链接】。

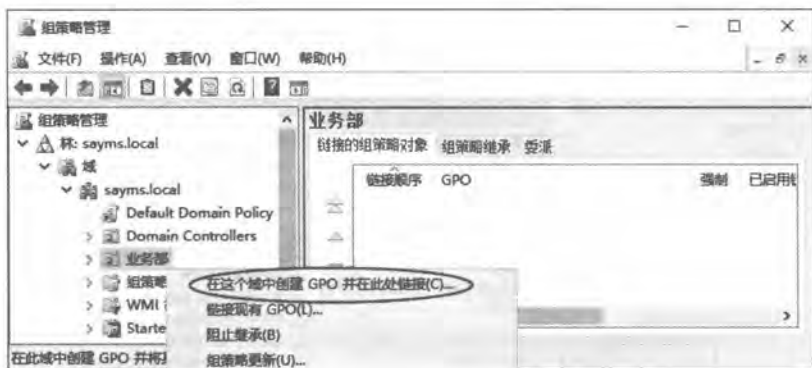


图 4-2-5

也可以先通过【选中组策略对象并右击➡新建】的方法来建立新GPO，然后再通过【选中组织单位业务部并右击➡链接现有GPO】的方法来将上述GPO连接到组织单位业务部。

## 附注

若要备份或还原GPO的话：【选中组策略对象并右击➡备份或从备份还原】。

**STEP 4** 在图4-2-6中为此GPO命名（例如测试用的GPO）后单击**确定**按钮。

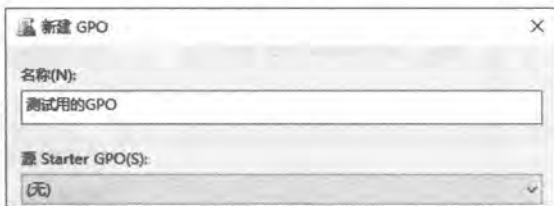


图 4-2-6

**STEP 5** 如图4-2-7所示选中这个新建的GPO并右击➡编辑。



图 4-2-7

**STEP 6** 如图4-2-8所示【展开用户配置➡策略➡管理模板➡Windows组件➡Internet Explorer➡将右侧阻止更改代理设置改为已启用】。



图 4-2-8

**STEP 7** 请利用**业务部**内的任何一位用户账户到任何一台域成员计算机上登录。

**STEP 8** 按 **Win+R** 键  $\Rightarrow$  输入 **control** 后按 **Enter** 键  $\Rightarrow$  **网络和 Internet**  $\Rightarrow$  **Internet 选项**  $\Rightarrow$  如图 4-2-9 所示单击**连接**选项卡下的**局域网设置**按钮，从前景图可知无法更改这些设置。Windows 10 也可以通过【单击左下角**开始**图标  $\Rightarrow$  单击**设置**图标  $\Rightarrow$  **网络和 Internet**  $\Rightarrow$  **代理**】的方法来看，如图 4-2-10 所示。



图 4-2-9



图 4-2-10

## 4.3 首选项设置实例演练

首选项设置并非强制性的，客户端可自行更改设置值，因此它适合用来当作默认值。

### 4.3.1 首选项设置实例演练一

我们要让位于组织单位**业务部**内的用户 Peter 登录时，其驱动器号 Z 会自动连接到 \\dc1\tools 共享文件夹，不过同样是位于**业务部**内的其他用户登录时不会有 Z 磁盘。我们要利用前面所建立的**测试用的 GPO**来练习。

- STEP 1 请到域控制器 dc1 上利用系统管理员身份登录。
- STEP 2 打开**文件资源管理器**、建立文件夹 tools，并将其设置为共享文件夹，然后为 Everyone 开放**读取/写入**的共享权限。
- STEP 3 单击左下角开始图标 **Windows 管理工具** **组策略管理**。
- STEP 4 在图 4-3-1 中选中组织单位**业务部**之下的**测试用的 GPO**并右击 **编辑**。



图 4-3-1

**STEP 5** 如图4-3-2所示展开用户配置→首选项→Windows设置→选中驱动器映射扩展项并单击→新建→映射驱动器。



图 4-3-2

### 附注

在Windows设置之下的应用程序、驱动器映射、环境等被称为扩展（extension）。

**STEP 6** 在图4-3-3中的操作处选择更新、位置处输入共享文件夹路径\\dc1\ tools，使用Z磁盘来连接此共享文件夹，勾选重新连接以便客户端每次登录时都会自动利用Z磁盘来连接。其中的操作可以有以下的选择：

- **创建**：会在客户端计算机建立用来连接此共享文件夹的Z磁盘。
- **替换**：客户端如果已存在网络驱动器Z，则将其删除后改以此处的设置取代原来的Z：磁盘。如果客户端不存在Z磁盘的话，则新建。
- **更新**：修改客户端的Z磁盘设置，例如修改客户端连接共享文件夹时所使用的用户账户与密码。如果客户端不存在Z磁盘的话，则新建。此处我们选择默认的更新。
- **删除**：删除客户端的Z磁盘。

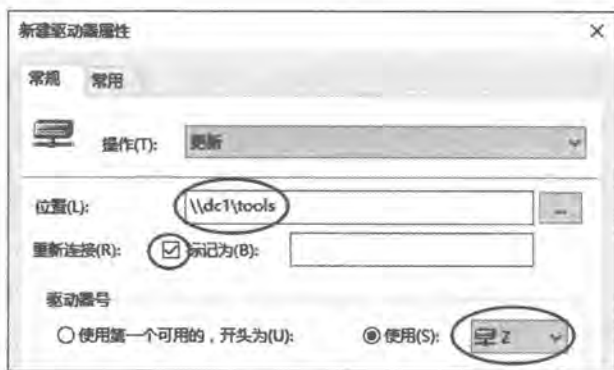


图 4-3-3

**STEP 7** 单击图4-3-4中常用选项卡、如图所示进行勾选：

- ❏ 如果发生错误，则停止处理该扩展中的项目：如果在驱动器映射扩展内有多个设置项目的话，则默认是当系统在处理本项目时，如果发生错误，它仍然会继续处理下一个项目，但如果勾选此选项的话，它就会停止，不再继续处理下一个项目。
- ❏ 在登录用户的安全上下文中运行（用户策略选项）：客户端CSE默认是利用本地系统账户身份来处理首选项设置的项目，这使得CSE只能访问可供本地计算机访问的环境变量与系统资源，而此选项可让CSE改用用户的登录身份来处理首选项的项目，如此CSE就可以访问本地计算机无权访问的资源或用户环境变量，例如此处利用网络驱动器Z来连接网络共享文件夹\\dc1\tools，就需要勾选此选项。
- ❏ 当不再应用项目时删除此项目：当GPO被删除后，客户端计算机内与该GPO内策略设置有关的设置都会被删除，然而与首选项有关的设置仍然会被保留，例如此处的网络驱动器Z仍然会被保留。如果勾选此选项的话，则与此首选项有关的设置会被删除。
- ❏ 应用一次且不重新应用：客户端计算机默认会每隔90分钟重新应用GPO内的首选项设置，因此如果用户自行更改设置的话，则重新应用后又会恢复为首选项内的设置值，如果希望用户能够保留自定义的设置值的话，请勾选此选项，此时它只会应用一次。



图 4-3-4



- ▮ **项目级别目标**：它让你针对每一个**首选项**项目来决定此项目的应用目标，例如可以选择将其只应用到特定用户或特定Windows系统。本示例只是要将设置应用到组织单位**业务部**内的单一用户Peter，故需勾选此选项。

**STEP 8** 单击前面图4-3-4中**常用选项卡**下的**目标**按钮，以便将此项目的应用对象指定到用户Peter，换句话说，此项目的**目标**为用户Peter。

**STEP 9** 在图4-3-5中【单击左上角的**新建项目**⇨选择**使用用户**⇨在**用户**处浏览或选择将此项目应用到域SAYMS的使用者Peter后，单击**确定**按钮】。



图 4-3-5

**STEP 10** 回到**新建驱动器属性**界面时单击**确定**按钮。

**STEP 11** 图4-3-6右侧为刚才建立、利用Z磁盘来连接\\dc1\Tools共享文件夹的设置，这样的一个设置被称为一个**项目（item）**。



图 4-3-6



**STEP 12** 到任何一台域成员计算机上利用组织单位**业务部**内的用户账户**Peter**登录、打开**文件资源管理器**，之后将如图4-3-7所示看到其Z磁盘已经自动连接到我们指定的共享文件夹。但是如果利用组织单位**业务部**内的其他用户账户登录的话，就不会有Z磁盘。



图 4-3-7

### 4.3.2 首选项设置实例演练二

以下假设要让组织单位**业务部**内的所有用户，必须通过企业内部的代理服务器（proxy server）上网。假设代理服务器的网址为proxy.sayms.local、端口号为8080、客户端所使用的浏览器为Internet Explorer 11或10。我们要利用前面所建立的**测试用的GPO**来练习。

**STEP 1** 请到域控制器dc1上利用系统管理员身份登录。

**STEP 2** 单击左下角开始图标☞**Windows 管理工具**☞**组策略管理**。

**STEP 3** 在图4-3-8中选中组织单位**业务部**之下的**测试用的GPO**并右击☞**编辑**。



图 4-3-8

**STEP 4** 如图4-3-9所示展开【**用户配置**☞**首选项**☞**控制面板设置**】，然后【选中**Internet**设置右击☞**新建**☞**Internet Explorer 10**】（也适用于Internet Explorer 11、Microsoft Edge客户端）。



图 4-3-9

**STEP 5** 如图4-3-10所示单击**连接**选项卡下的**局域网设置**按钮。

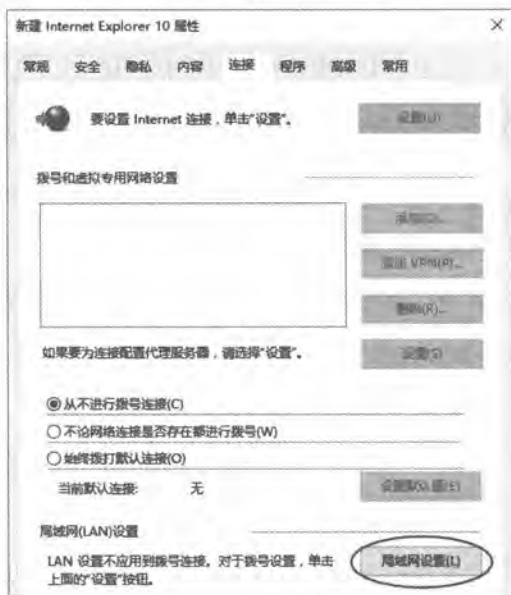


图 4-3-10

**STEP 6** 如图4-3-11所示勾选后【输入代理服务器的网址proxy.sayms.local、端口号码8080↵按**F5**键↵单击两次**确定**按钮结束设置】。

### 注意

需要按**F5**键来启用此选项卡下的所有设置（设置项目下代表禁用的红色底线会变成绿色）；按**F8**键可停用此选项卡下的所有设置；如果要启用当前所在的项目的话，请按**F6**键、禁用请按**F7**键。



图 4-3-11

STEP 7 请利用业务部内任何一位用户账户到任何一台域成员计算机登录。

STEP 8 按 **Win+R** 键 **⇨** 输入 control 后按 **Enter** 键 **⇨** 网络和 Internet **⇨** Internet 选项 **⇨** 如图 4-3-12 所示单击 **连接** 选项卡下的 **局域网设置** 按钮，从前景图可知其 Proxy 服务器被指定到我们所设置的 proxy.sayms.local、端口为 8080，而且无法更改这些设置（这是之前练习的策略设置的结果。Windows 10 的系统也可以通过【单击左下角开始图标 **Win** **⇨** 单击设置图标 **⚙** **⇨** 网络和 Internet **⇨** Proxy】的方法来查看，如图 4-3-13 所示。

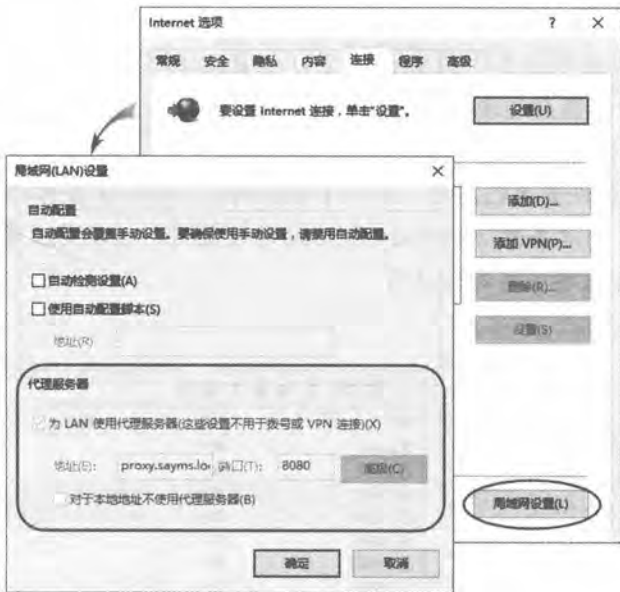


图 4-3-12



图 4-3-13

## 4.4 组策略的处理规则

域成员计算机在处理（应用）组策略时有一定的程序与规则，系统管理员必须了解它们，才能够通过组策略来充分地掌控用户与计算机的环境。

### 4.4.1 一般的继承与处理规则

组策略设置是有继承性的，也有一定的处理规则：

- 如果在高层父容器的某个策略被设置，但是在其下低层子容器并未设置此策略的话，则低层子容器会继承高层父容器的这个策略设置值。

以图4-4-1为例，如果位于高层的域sayms.local的GPO内，其从[开始]菜单中删除[运行]菜单策略被设置为已启用，但位于低层的组织单位业务部的这个策略被设置为没有定义的话，则业务部会继承sayms.local的设置值，也就是业务部的从[开始]菜单中删除[运行]菜单策略是已启用。

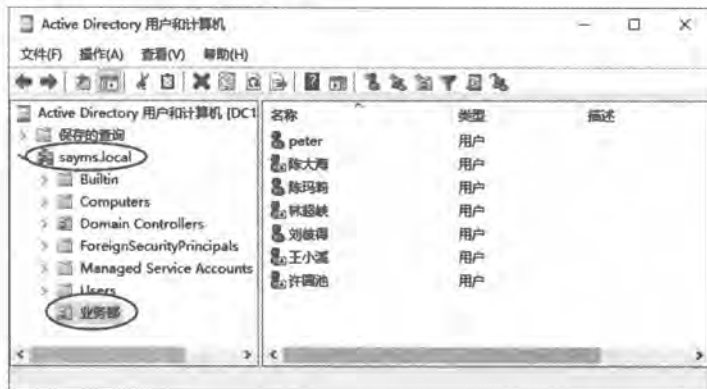


图 4-4-1



如果组织单位**业务部**之下还有其他子容器，并且它们的这些策略也被设置为**未配置**的话，则它们也会继承这个设置值。

- 如果在低层子容器内的某个策略被设置的话，则此设置值默认会覆盖由其高层父容器所继承下来的设置值。

以图4-4-1为例，如果位于高层的域sayms.local的GPO内，其从**[开始] 菜单中删除 [运行] 菜单策略**被设置为已启用，但是位于低层的组织单位**业务部**的这个策略被设置为已禁用，则**业务部**会覆盖sayms.local的设置值，也就是对组织单位**业务部**来说，其从**[开始] 菜单中删除 [运行] 菜单策略**是已禁用。

- 组策略设置是有累加性的，例如如果在组织单位**业务部**内建立了GPO，同时在站点、域内也都有GPO，则站点、域与组织单位内的所有GPO设置值都会被累加起来作为组织单位**业务部**的最后有效设置值。

但如果站点、域与组织单位**业务部**之间的GPO设置发生冲突时，则优先级为：**组织单位的GPO**最优先、**域的GPO**次之、**站点的GPO**优先权最低。

- 如果组策略内的**计算机配置**与**用户配置**发生冲突的话，则以**计算机配置**优先。
- 如果将多个GPO连接到同一处，则所有这些GPO的设置会被累加起来作为最后的有效设置值，但如果这些GPO的设置相互冲突时，则以**连接顺序**在前面的GPO设置优先，例如图4-4-2中的**测试用的GPO**的设置优先于**防病毒软件策略**。



图 4-4-2

#### 附注

本地计算机策略的优先级最低，也就是说如果本地计算机策略内的设置值与站点、域或组织单位的设置冲突时，则以站点、域或组织单位的设置优先。

### 4.4.2 例外的继承设置

除了一般的继承与处理规则外，还可以设置以下的例外规则。

#### 1. 阻止继承策略

可以设置让子容器不要继承父容器的设置，例如若不要让组织单位**业务部**继承域



sayms.local的策略设置的话：请【如图4-4-3所示选中**业务部**并右击**阻止继承**】，此时组织单位**业务部**将直接以自己的GPO设置为其设置值，若其GPO内的设置为**未配置**的话，则采用默认值。

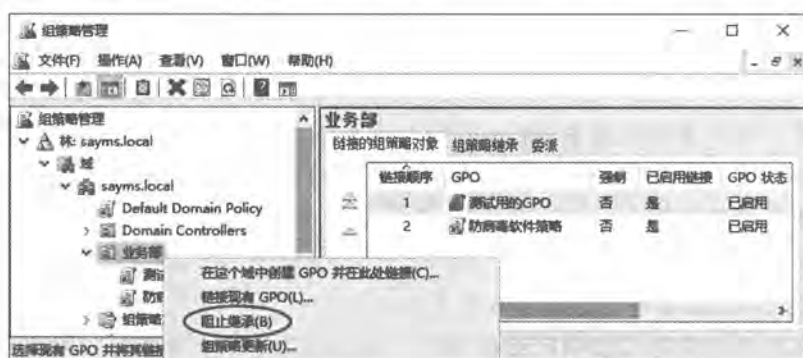


图 4-4-3

## 2. 强制继承策略

可以通过父容器来强制其下子容器必须继承父容器的GPO设置，不论子容器是否选用了**阻止继承**。例如若我们在图4-4-4中域sayms.local之下建立了一个GPO（**企业安全防护策略**），以便通过它来设置域内所有计算机的安全措施：【选中此策略并右击**强制**】来强制其下的所有组织单位都必须继承此策略。



图 4-4-4

## 3. 筛选组策略设置

以组织单位**业务部**为例，当针对此组织单位建立GPO后，此GPO的设置会被应用到这个组织单位内的所有用户与计算机，如图4-4-5所示默认是被应用到Authenticated Users组（身份经过确认的用户）。





图 4-4-5

不过也可以让此GPO不要应用到特定的用户或计算机，例如此GPO对所有业务部人员的工作环境做了某些限制，但是却不想将此限制加在业务部经理上。位于组织单位内的用户与计算机，默认对该组织单位的GPO都具有**读取与应用组策略**权限，可以【如图4-4-6所示单击GPO（例如**测试用的GPO**）→单击**委派**选项卡→单击**高级**按钮→选择**Authenticated Users**】进行查看。



图 4-4-6

如果不想将此GPO的设置应用到组织单位**业务部**内的用户Peter的话：【请单击图4-4-6中的**添加**按钮→选择用户Peter→如图4-4-7所示将Peter的**应用组策略**权限设置为**拒绝**即可】。

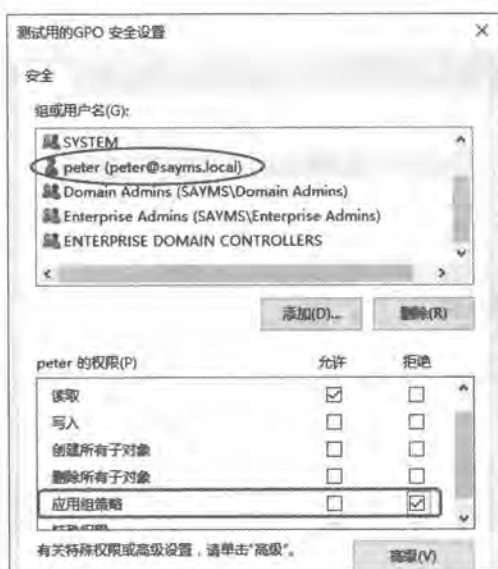


图 4-4-7

### 4.4.3 特殊的处理设置

这些特殊处理设置包含强制处理 GPO、慢速连接的 GPO 处理、回送处理模式与禁用 GPO 等。

#### 1. 强制处理 GPO

客户端计算机在处理组策略的设置时，会将不同类型的策略交给不同的 DLL（Dynamic-Link Libraries）来负责处理与应用，这些 DLL 被称为 Client-Side Extension（CSE）。不过 CSE 在处理其所负责的策略时，只会处理上次处理过后的最新改动策略，这种做法虽然可以提高处理策略的效率，但有时候却无法达到所期望的目标，例如在 GPO 内对用户做了某项限制，在用户因为这个策略而受到限制之后，如果用户自行将此限制删除，则当下一次用户计算机在应用策略时，客户端的 CSE 会因为 GPO 内的策略设置值并没有变动而不处理此策略，因而无法自动将用户自行更改的设置改回来。

解决方法是强制要求客户端 CSE 一定要处理指定的策略，不论该策略设置值是否发生变化。可以针对不同策略来个别设置。举例来说，假设要强制组织单位**业务部**内所有计算机必须处理（应用）**软件安装策略**的话：在**测试用的 GPO**的设置界面中选用【**计算机配置**➤**策略**➤**管理模板**➤**系统**➤如图 4-4-8 所示双击**组策略**右侧的**配置软件安装策略处理**➤选择**已启用**➤勾选**即使尚未更改组策略对象也进行处理**➤单击**确定**按钮】。



## 附注

只要策略名称最后两个字是处理（processing）的策略设置都可以做类似的更改。

如果要手动让计算机来强制处理（应用）所有计算机策略设置的话，可以在计算机上执行 `gpupdate /target:computer /force` 命令；如果是用户策略设置的话，可以执行 `gpupdate /target:user /force` 命令；或利用 `gpupdate /force` 命令来同时强制处理计算机与用户设置。



图 4-4-8

## 2. 慢速连接的 GPO 处理

可以让域成员计算机自动检测其与域控制器之间的连接速度是否太慢，如果是的话，就不要应用位于域控制器内指定的组策略设置。除了图4-4-9中配置注册表策略处理与配置安全策略处理这两个策略之外（无论是否慢速连接都会应用），其他策略都可以设置为慢速连接不应用。



图 4-4-9

假设要求组织单位**业务部**内的每一台计算机都要自动检测是否为慢速连接：请在**测试用的GPO**的计算机配置界面中，如图4-4-10所示【双击**组策略**右侧的**配置组策略慢速链接检测**→选择**已启用**→在**连接速度**处输入慢速连接的定义值→单击**确定**按钮】，图中我们设置只要连接速度低于500 Kbps，就视为慢速。如果禁用或未配置此策略的话，则默认也是将低于500 Kbps视为慢速连接。



图 4-4-10

接下来假设组织单位**业务部**内的每一台计算机与域控制器之间即使是慢速连接，也需要应用**软件安装策略处理策略**，其设置方法与图4-4-8相同，不过此时需在前景图中勾选**允许通过慢速网络连接进行处理**。

### 3. 环回处理模式

一般来说，系统会根据用户或计算机账户在AD DS内的位置，来决定如何将GPO设置值应用到用户或计算机。例如如果服务器SERVER1的计算机账户位于组织单位**服务器**内，此组织单位有一个名称为**服务器GPO**的GPO，而用户Jackie的用户账户位于组织单位**业务部**内，此组织单位有一个名称为**测试用的GPO**的GPO，则当用户Jackie在SERVER1上登录域时，在正常的情况下，他的用户环境是由**测试用的GPO**的用户配置来决定的，不过他的计算机环境是由**服务器GPO**的计算机配置来确定的。

然而如果在**测试用的GPO**的用户配置内，设置让组织单位**业务部**内的用户登录时，就自动为他们安装某个应用程序的话，则这些用户到任何一台域成员计算机上（包含SERVER1）登录时，系统将为他们在这台计算机内安装此应用程序，但是却不想为们在这台重要的服务器SERVER1内安装应用程序，此时要如何来解决这个问题呢？可以启用**环回处理模式**（loopback processing mode）。

如果在**服务器GPO**启用了**环回处理模式**，则不论用户账户是位于何处，只要用户是利用



组织单位服务器内的计算机（包含服务器SERVER1）登录，则用户的工作环境可改由服务器GPO的用户配置来确定，这样Jackie到服务器SERVER1登录时，系统就不会替他安装应用程序。环回处理模式分为两种模式：

- **替换模式**：直接改由服务器GPO的用户配置来确定用户的环境，而忽略测试用的GPO的用户配置。
- **合并模式**：先处理测试用的GPO的用户配置，再处理服务器GPO的用户配置，如果两者发生冲突，则以服务器GPO的用户配置优先。

假设我们要在服务器GPO内启用环回处理模式：请在服务器GPO的计算机配置界面中【如图4-4-11所示双击组策略右侧的配置用户组策略环回处理模式☞选择已启用☞在模式处选择替换或合并】。

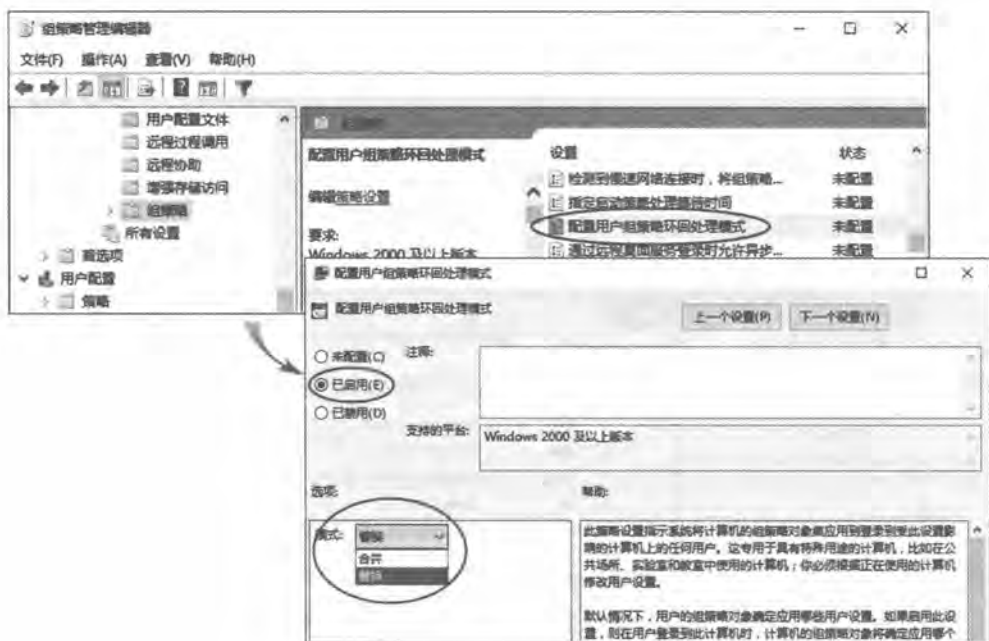


图 4-4-11

#### 4. 禁用 GPO

若有需要的话，可以将整个GPO禁用，或单独将GPO的计算机配置或用户配置禁用。以测试用的GPO为例说明：

- 如果要将整个GPO禁用的话，请如图4-4-12所示选中测试用的GPO并右击，然后取消勾选已启用链接。



图 4-4-12

- 如果要将在GPO的计算机配置或用户配置单独禁用的话：先进入测试用的GPO的编辑界面，如图4-4-13所示单击测试用的GPO，单击上方属性图标，勾选禁用计算机配置设置或禁用用户配置设置。



图 4-4-13

#### 4.4.4 更改管理GPO的域控制器

当新增、修改或删除组策略设置时，这些改动默认先被存储到扮演PDC模拟器操作主机角色的域控制器，然后再由它将其复制到其他域控制器，域成员计算机再通过域控制器来应用这些策略。

但如果系统管理员在上海，可是PDC模拟器操作主机却在远程的北京，此时上海的系统



管理员会希望其针对上海员工所设置的组策略，能够直接存储到位于上海的域控制器，以便上海的用户与计算机能够通过这台域控制器来快速应用这些策略。

可以通过**DC选项**与策略设置两种方式将管理GPO的域控制器从**PDC模拟器操作主机**更改为其他域控制器：

- ❏ **利用DC选项**：假设供上海分公司使用的GPO为**上海分公司专用GPO**，则请进入编辑此GPO的界面（**组策略对象编辑器**界面），然后如图4-4-14所示【单击**上海分公司专用GPO**点选**查看菜单**→**DC选项**→在前景图中选择要用来管理组策略的域控制器】。图中选择域控制器的选项有以下三种：

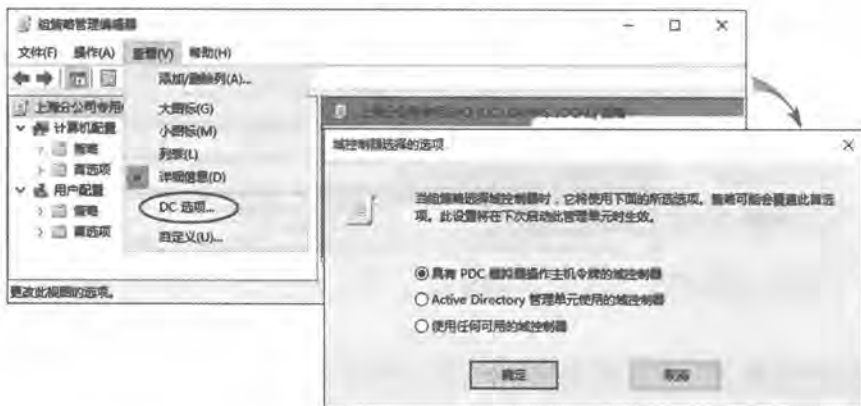


图 4-4-14

- **具有PDC 模拟器操作主机令牌的域控制器**：也就是使用**PDC模拟器操作主机**，这是默认值，也是建议值。
- **Active Directory管理单元使用的域控制器**：当系统管理员执行**组策略对象编辑器**时，此**组策略对象编辑器**所连接的域控制器就是我们要选用的域控制器。
- **使用任何可用的域控制器**：此选项让**组策略对象编辑器**可以任意挑选一台域控制器。
- ❏ **利用策略设置**：假设要针对上海系统管理员来设置。我们需要针对其用户账户所在的组织单位来设置：如图4-4-15所示进入编辑此组织单位的GPO界面（**组策略对象编辑器**界面）后，双击右侧的**配置组策略域控制器选择**，然后如图所示来选择域控制器，图中的选项说明同上，其中**主域控制器**就是**PDC模拟器操作主机**。





图 4-4-15

#### 4.4.5 更改组策略的应用间隔时间

前面已经介绍过域成员计算机与域控制器何时会应用组策略的设置。可以更改这些设置值，不过建议不要将更新组策略的间隔时间设置得太短，以免增加网络负担。

##### 1. 更改计算机配置的应用间隔时间

例如要更改组织单位**业务部**内所有计算机的应用**计算机配置**的间隔时间的话：请在**测试用的GPO**的**计算机配置**界面中，如图4-4-16所示【双击**组策略**右侧的**设置计算机的组策略刷新间隔**选择**已启用**通过前景图来设置单击**确定**按钮】，图中设置为每隔90分钟加上0到30分钟的随机值，也就是每隔90~120分钟之间应用一次。如果禁用或未配置此策略的话，则默认就是每隔90~120分钟之间应用一次。如果应用间隔设置为0分钟的话，则会每隔7秒钟应用一次。

如果要更改域控制器的应用**计算机配置**的间隔时间的话，请针对组织单位**Domain Controllers**内的GPO来设置（例如**Default Domain Controllers GPO**），其策略名称是**设置域控制器的组策略刷新间隔**（参见图4-4-16中背景图），在双击此策略后，如图4-4-17所示可知其默认是每隔5分钟应用组策略一次。如果禁用或未配置此策略的话，则默认就是每隔5分钟应用一次。如果将应用间隔时间设置为0分钟的话，则会每隔7秒钟应用一次。



图 4-4-16



图 4-4-17

## 2. 更改用户配置的应用间隔时间

例如要更改组织单位**业务部**内所有用户的应用**用户配置**的间隔时间的话，请在**测试用的 GPO 的用户配置**界面中，通过图 4-4-18 中**组策略**右侧的**设置用户的组策略刷新间隔**来设置，其默认也是每隔 90 分钟加上 0~30 分钟的随机值，也就是每隔 90~120 分钟之间应用一次。如果

停用或未设置此策略的话，则默认就是每隔90~120分钟之间应用一次。如果将间隔时间设置为0分钟的话，则会每隔7秒钟应用一次。



图 4-4-18

## 4.5 利用组策略来管理计算机与用户环境

我们将通过以下几个设置来说明如何管理计算机与用户的工作环境：计算机配置的管理模板策略、用户配置的管理模板策略、账户策略、用户权限分配策略、安全选项策略、登录/注销/启动/关机脚本与文件夹重定向等。

### 4.5.1 计算机配置的管理模板策略

我们在策略设置实例演练一：计算机配置中已练习过管理模板策略，此处仅说明两个常用设置，它们是在【计算机配置➡策略➡管理模板】内：

- **显示“关闭事件跟踪程序”**：如果禁用此策略的话，则用户将计算机关机时，系统就不会再要求用户提供关机的理由。其设置方法为【系统➡双击右侧的显示“关闭事件追踪程序”】。默认会将关闭事件追踪器显示在服务器计算机上（例如Windows Server 2016，如图4-5-1所示），而工作站计算机（例如Windows 10）不会显示。可以针对服务器、工作站或两者来设置。



图 4-5-1



- ✎ **显示用户上次交互登录的信息：**用户登录时屏幕上会显示用户上次成功、失败登录的日期与时间；自从上次登录成功后，登录失败的次数等信息（如图4-5-2所示）。其设置途径为【Windows组件☞Windows登录选项☞双击右侧的在用户登录期间显示有关以前登录的信息】。客户端计算机必须是Windows Vista以上。



图 4-5-2

### 注意

除了会应用到客户端计算机的GPO需要启用此功能之外，还需要在会应用到域控制器的GPO（例如Default Domain Controller Policy或Default Domain Policy）来启用此功能，否则用户登录时将无法获取登录信息，也无法登录（见图4-5-3）。



图 4-5-3

可以通过【打开Active Directory管理中心☞双击用户账户☞单击扩展节☞单击属性编辑器】的方法来查看该用户的这些属性值（例如msDS-LastSuccessfulInteractiveLogonTime、msDS-LastFailedInteractiveLogonTime、msDS-FailedInteractiveLogonCountAtLastSuccessfulLogon等）。

也可以使用【打开Active Directory用户和计算机☞单击查看菜单☞高级功能☞选中



用户账户并右击**属性**，单击**属性编辑器**选项卡，从**属性**列表中的来查看这些属性值】。

### 注意

如果在客户端计算机上通过**本地组策略**来启用此策略，但是此计算机并未加入域功能级别为Windows Server 2008（含）以上的域的话，则用户在这台计算机登录时将无法获取登录信息，也无法登录。

## 4.5.2 用户配置的管理模板策略

我们在**策略配置实例演练二：用户配置**中已经练习过**管理模板策略**，此处仅说明几个常用配置，它们是在**【用户配置>策略>管理模板】**中：

- 限制用户只能或不能运行指定的Windows应用程序：其设置方法为**【系统>双击右侧的只运行指定的Windows应用程序或不运行指定的Windows应用程序】**。在添加程序时，请输入该应用程序的可执行文件名称，例如eMule.exe。



如果用户利用**文件资源管理器**更改此程序的文件名的话，是否这个策略就无法发挥作用？



是的，不过可以利用第6章的**软件限制策略**来达到限制用户执行此程序的目的，即使其文件名被改名。

- 隐藏或只显示控制面板内指定的项目：用户在控制面板内将看不到被隐藏起来的项目或只看得到被指定要显示的项目：**【控制面板>双击右侧的隐藏指定的“控制面板”项或只显示指定的“控制面板”项】**。在添加项目时，请输入项目名称，例如鼠标、用户账户等。
- 禁用按**Ctrl + Alt + Del**键后所出现的界面中的选项：用户按这3个键后，将无法使用界面中被禁用的按钮，例如**更改密码**按钮、**任务管理器**按钮、**注销**按钮等。其设置方法为：**【系统>Ctrl+Alt+Del选项】**。
- 隐藏和禁用桌面上的所有项目：其设置方法为**【桌面>隐藏和禁用桌面上的所有项目】**。用户登录后，传统桌面上所有项目都会被隐藏、选中桌面按鼠标右键也无作用。
- 删除Internet选项中的部分选项卡：用户**【按**Win+R**键>输入control后按**Enter**键>网络和Internet>Internet选项】**，无法选用被删除的选项卡，例如**安全**、**连接**、**高级**等选项卡。其设置方法为**【Windows组件>Internet Explorer>双击右侧的Internet控制面板】**。
- 删除开始菜单中的关机、重启、睡眠和休眠命令：其设置方法为**【[开始]菜单和任务栏>双击右侧删除并禁止访问“关机”、“重新启动”、“睡眠”和“休眠”命**



令】。用户的开始菜单中，这些功能的图标会被删除或无法选择、按 **Ctrl** + **Alt** + **Del** 键后也无法使用它们。

### 4.5.3 账户策略

我们可以通过账户策略来设置密码的使用标准与账户锁定方式。在设置账户策略时请特别注意以下说明：

- ✎ 针对域用户所设置的账户策略需要通过**域级别的GPO**来设置才有效，例如通过域的 Default Domain Policy GPO来设置，此策略会被应用到域内所有用户。通过站点或组织单位的GPO所设置的账户策略，对域用户没有作用。  
账户策略不但会被应用到所有的域用户账户，也会应用到所有域成员计算机内的本地用户账户。
- ✎ 如果针对某个组织单位（如图4-5-4中的**金融部**）来设置账户策略，则这个账户策略只会被应用到位于此组织单位的计算机（例如图中的Win10PC101、Win10PC102、Win10PC103）的本地用户账户而已，但是对位于此组织单位内的域用户账户（例如图中的王大杰等）却没有影响。



图 4-5-4

#### 附注

1. 如果域与组织单位都设置了用户账户策略，并且设置发生冲突时，则此组织单位内的成员计算机的本地用户账户会采用域的设置。
2. 域成员计算机也有自己的本地账户策略，不过如果其设置与域/组织单位的设置发生冲突的话，则采用域/组织单位的设置。

要设置域账户策略的话：【选中**Default Domain Policy GPO**（或其他域级别的GPO）并右击**编辑**如图4-5-5所示展开**计算机配置**→**策略**→**Windows设置**→**安全设置**→**账户策略**】的方法。

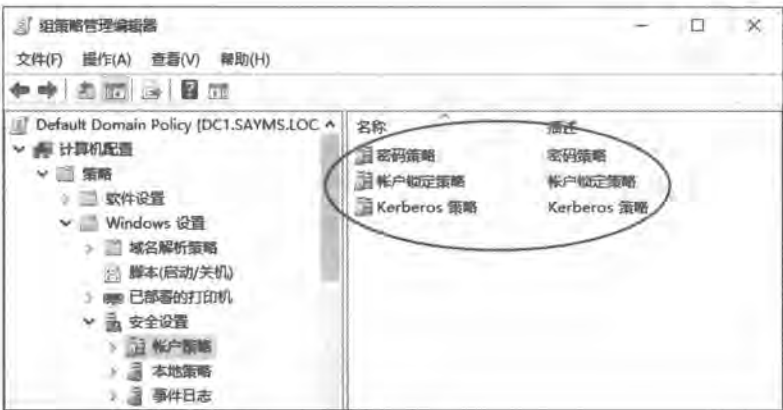


图 4-5-5

### 1. 密码策略

如图4-5-6所示单击**密码策略**后就可以设置以下策略：

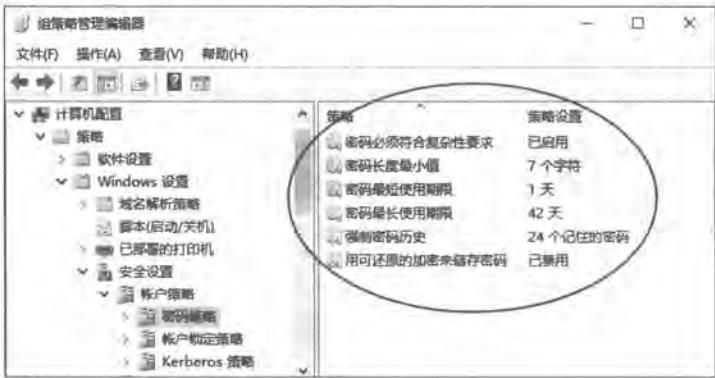


图 4-5-6

- **用可还原的加密来存储密码：**如果有应用程序需要读取用户的密码，以便验证用户身份的话，可以启用此功能，不过它相当于用户密码没有加密，因此不安全。默认为禁用。
- **密码必须符合复杂性要求：**如果启用此功能的话，则用户的密码需要同时满足以下条件：
  - 不能包含用户账户名称（指用户 **SamAccountName**）或全名。
  - 长度至少要6个字符。
  - 至少需要包含A~Z、a~z、0~9、非字母数字（例如!、\$、#、%）等4组字符中的3组。

因此123ABCdef是有效的密码，而87654321是无效的，因它只使用数字这一种字符。又如用户账户名称为mary，则123ABCmary是无效密码，因为包含用户账户名称。AD DS域与独立服务器默认是启用此策略的。





- ✎ **密码最长使用期限**：用来设置密码最长的使用期限（可为0~999天）。用户在登录时，如果密码使用期限已到的话，系统会要求用户更改密码。若此处为0，则表示密码没有使用期限。AD DS域与独立服务器默认值都是42天。
- ✎ **密码最短使用期限**：用来设置用户密码的最短使用期限（可为0~998天），在期限未到前，用户不能更改密码。如果此处为0表示用户可以随时更改密码。AD DS域的默认值为1，独立服务器的默认值为0。
- ✎ **强制密码历史**：用来设置是否要记录用户曾经使用过的旧密码，以便决定用户在更改密码时，是否可以重复使用旧密码。此处可被设置为：
  - 1~24：表示要保存密码历史记录。例如设置为5，则用户的新密码不能与前5次所使用过的旧密码相同。
  - 0：表示不保存密码历史记录，因此密码可以重复使用，也就是用户更改密码时，可以将其设置为以前曾经使用过的任何一个旧密码。
 AD DS域的默认值为24，独立服务器的默认值为0。
- ✎ **密码长度最小值**：用来设置用户账户的密码最少需几个字符。此处可为0~14，若为0，表示用户账户可以没有密码。AD DS域的默认值为7，独立服务器的默认值为0。

## 2. 账户锁定策略（account lockout policy）

可以通过图4-5-7中的**账户锁定策略**来设置锁定用户账户的方式。

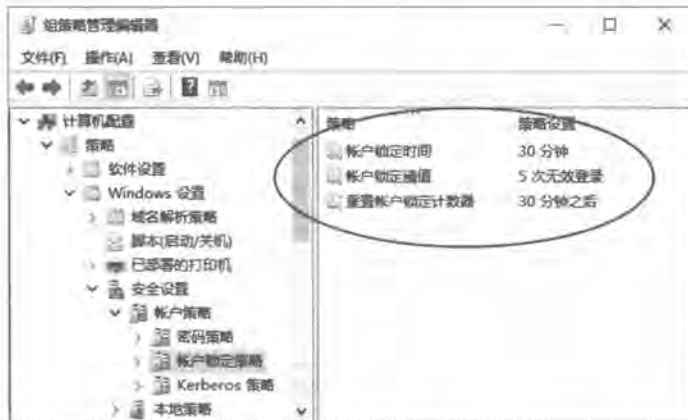


图 4-5-7

- ✎ **账户锁定阈值**：可以让用户在登录多次失败后（密码错误），就将该用户账户锁定，在未被解除锁定之前，用户无法再利用此账户来登录。此处用来设置登录失败次数，其值可为0~999。默认为0，表示账户永远不会被锁定。
- ✎ **账户锁定时间**：用来设置锁定账户的期限，期限过后会自动解除锁定。此处可为0~99999分钟，如果为0分钟表示永久锁定，不会自动被解除锁定，此时需由系统管理员手动解除锁定，也就是如图4-5-8所示单击用户账户属性的**账户**节处的**解锁账户**（账户被锁定后才会有此选项）。



图 4-5-8

- ❏ **重设账户锁定计数器：**“锁定计数器”是用来记录用户登录失败的次数，其起始值为0，用户如果登录失败，则锁定计数的值就会加1，如果登录成功，则锁定计数器的值就会归零。如果锁定计数器的值等于**账户锁定阈值**，该账户就会被锁定。如果用户最近一次登录失败后，到现在为止已经超过此处的时间的话，则锁定计数器值便会自动归零。以前面的图4-5-7来说，如果用户连续3次登录失败的话，其账户就会被锁定。但在尚未连续3次登录失败之前，如果最近一次登录失败后，到现在为止已超过30分钟的话，则锁定计数器值就会归零。

## 4.5.4 用户权限分配策略

可以通过图4-5-9中的**用户权限分配**来将执行特殊工作的权限分配给用户或组（此图是以 Default Domain Controller Policy GPO为例）。



图 4-5-9



如果要为用户分配图4-5-9右侧任何一个权限时：【双击该权限 ➤ 在如图4-5-10所示中单击**添加用户或组**按钮 ➤ 选择用户或组】。



图 4-5-10

以下列举几个常用的权限策略说明：

- **允许本地登录：**允许用户直接在本地计算机上登录（例如按 **Ctrl** + **Alt** + **Del** 键）。
- **拒绝本地登录：**与前一个权限刚好相反。此权限优先于前一个权限。
- **将工作站添加到域：**允许用户将计算机加入到域。

#### 附注

每一位域用户默认有10次将计算机加入域的机会，不过一旦拥有**将工作站添加到域**的权限后，其次数就没有限制，

- **关闭系统：**允许用户将此计算机关机。
- **从网络访问此计算机：**允许用户通过网络上其他计算机来连接、访问这台计算机。
- **拒绝从网络访问这台计算机：**与前一个权限刚好相反。此权限优先于前一个权限。
- **从远程系统强制关机：**允许用户利用远程计算机来将此台计算机关机。
- **备份文件和目录：**允许用户备份硬盘内的文件与文件夹。
- **还原文件和目录：**允许用户还原所备份的文件与文件夹。
- **管理审核和安全日志：**允许用户指定要审核的事件，也允许用户查询与清除安全日志。
- **更改系统时间：**允许用户更改计算机的系统日期与时间。
- **加载和卸载设备驱动程序：**允许用户加载与卸载设备的驱动程序。



- 取得文件或其他对象的所有权：允许取得其他用户所拥有的文件、文件夹或其他对象的所有权。

#### 附注

此处的“用户权限分配”原文为User Rights Assignment，应被翻译为“用户权利分配”。在Windows Server 2016内将permission（权限）与rights（权利）都翻译为“权限”。

## 4.5.5 安全选项策略

可以通过如图4-5-11的安全选项策略来启用计算机的一些安全设置。图中以测试用的GPO为例，并列举以下几个安全选项策略：

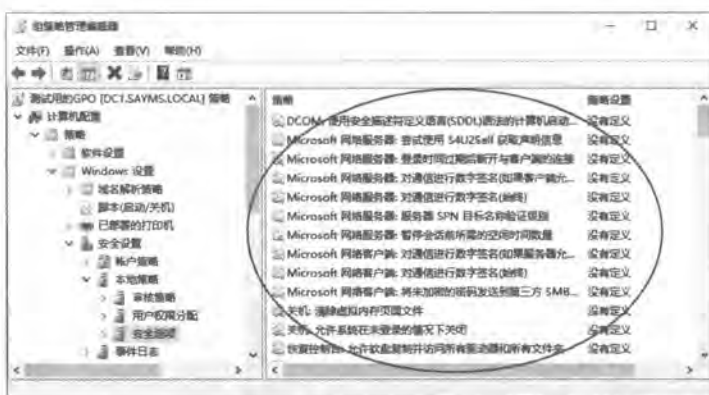


图 4-5-11

- 交互式登录：无须按`Ctrl` + `Alt` + `Del`键。登录界面不会再显示类似按`Ctrl` + `Alt` + `Del`登录的消息（这是Windows 10等客户端的默认值）。
- 交互式登录：不显示最后用户名。  
客户端登录界面上不显示上一次登录的用户名。
- 交互式登录：提示用户在过期之前更改密码。用来设置在用户的密码过期前几天，提示用户更改密码。
- 交互式登录：之前登录到缓存的次数（域控制器不可用时）。域用户登录成功后，其账户信息会被存储到用户计算机的缓存区，如果之后此计算机因故无法与域控制器连接的话，该用户仍然可以通过缓存区的账户数据来验证身份与登录。可以通过此策略来设置缓存区内账户数据的数量，默认为记录10个登录用户的账户数据（Windows Server 2008为25个）。
- 交互式登录：试图登录的用户的消息标题、试图登录的用户的消息本文。如果用户在登录时按`Ctrl` + `Alt` + `Del`键后，界面上能够显示希望用户看到的消息的话，可以通过这两个选项来设置，其中一个用来设置消息的标题文字，一个用来设置消息内容。



- ❏ 关机：允许系统在未登录的情况下关闭。让登录界面的右下角能够显示关机图标，以便在未登录的情况下就可直接通过此图标将计算机关机（这是Windows 10等客户端的默认值）。

## 4.5.6 登录/注销、启动/关机脚本

可以让域用户在登录时，其系统就自动执行**登录脚本**（script），而当用户注销时，就自动执行**注销脚本**；另外也可以让计算机在开机启动时自动执行**启动脚本**，而关机时自动执行**关机脚本**。

### 1. 登录脚本的设置

以下利用文件名为**logon.bat**的批处理文件来练习登录脚本。请利用**记事本**（notepad）来建立此文件，其中只有一行如下所示的命令，它会在C:\之下新建文件夹TestDir：

```
mkdir c:\TestDir
```

下面我们利用组织单位**业务部**的**测试用的GPO**来说明。

- STEP 1** 单击左下角开始图标田 Windows 管理工具 Windows 组策略管理 展开到组织单位业务部 选中测试用的GPO并右击 编辑。
- STEP 2** 如图4-5-12所示【展开用户配置 策略 Windows设置 脚本（登录/注销） 双击右侧的登录 单击显示文件按钮】。



图 4-5-12

- STEP 3** 出现图4-5-13的界面时，请将登录脚本文件logon.bat粘贴到界面中的文件夹内，此文件夹是位于域控制器的SYSVOL文件夹内，其完整路径为（其中的GUID是测试用的GPO的GUID）：

%systemroot%\SYSVOL\sysvol\域名\Policies\{GUID}\User\Scripts\Logon



图 4-5-13

- STEP 4** 请关闭图4-5-13窗口，回到前面图4-5-12的前景图中单击**添加**按钮。
- STEP 5** 在图4-5-14中通过**浏览**按钮从前面图4-5-13的文件夹内选择登录脚本文件logon.bat。完成后单击**确定**按钮。

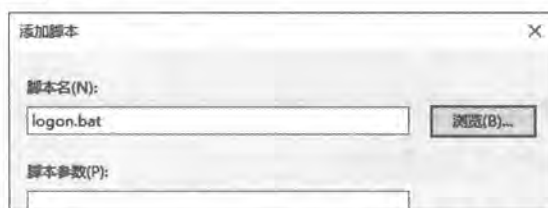


图 4-5-14

- STEP 6** 回到图4-5-15的界面时单击**确定**按钮。



图 4-5-15

- STEP 7** 完成设置后，组织单位**业务部**内的所有用户登录时，系统就会自动执行登录脚本logon.bat，它会在C:\之下建立文件夹TestDir，请自行利用文件资源管理器来检查（如图4-5-16所示）。

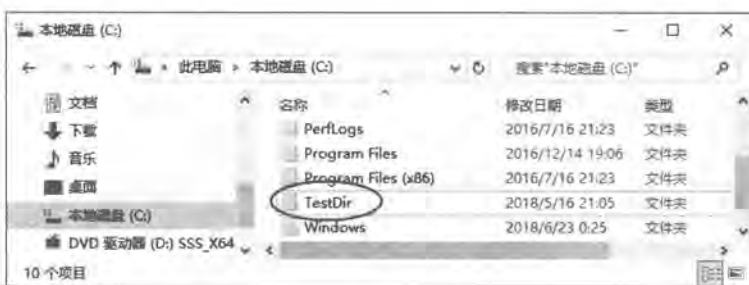


图 4-5-16

### 注意

若客户端是Windows 8.1、Windows 8的话，可能需等待3、5分钟才看得到上述登录脚本的执行结果。

## 2. 注销脚本的设置

以下利用文件名为**logoff.bat**的批处理文件来练习注销脚本。请利用**记事本**（notepad）来建立此文件，其中只有一行如下所示的命令，它会将C:\TestDir文件夹删除：

```
rmdir c:\TestDir
```

以下利用组织单位**业务部的测试用的GPO**来说明。

- STEP 1** 请先将前一个登录脚本设置删除，也就是单击前面图4-5-15中的logon.bat后单击**删除**按钮，以免干扰验证本实验的结果。
- STEP 2** 以下演练的步骤与前一个登录脚本的设置类似，不再重复，不过在图4-5-12中背景图改选**注销**、文件名改为**logoff.bat**。
- STEP 3** 在客户端计算机【按**Win+R**键→执行gpupdate命令】以便立即应用上述策略设置、在客户端计算机上利用注销、再重新登录的方式来应用上述策略设置。
- STEP 4** 再注销，这时候就会执行注销脚本**logoff.bat**来删除C:\TestDir，请再登录后利用**文件资源管理器**来确认C:\TestDir已被删除（请先确认logon.bat已经删除，否则它又会建立此文件夹）。

## 3. 启动/关机脚本的设置

我们可以利用图4-5-17中组织单位**业务部的测试用的GPO**为例来说明，而且以图中计算机名称为Win10PC1的计算机来练习启动/关机脚本。如果您要练习的计算机不是位于组织单位**业务部**内，而是位于容器Computers内，则请通过域级别的GPO来练习（例如DefaultDomain Policy），或将计算机账户移动到组织单位**业务部**。



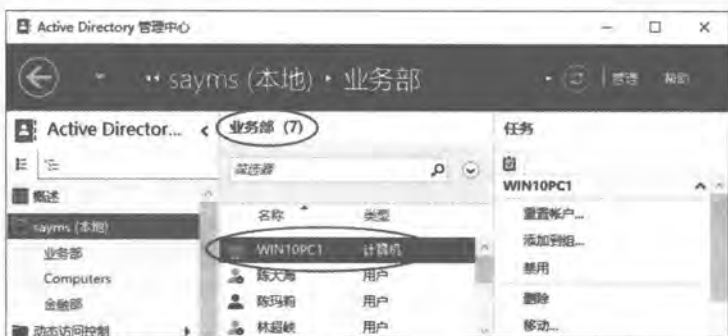


图 4-5-17

由于启动/关机脚本的设置步骤与前一个登录/注销脚本的设置类似，故此处不再重复，不过在图4-5-18中改为通过计算机配置。可以直接利用前面的登录/注销脚本的示例文件来练习。



图 4-5-18

## 4.5.7 文件夹重定向

可以利用组策略来将用户的某些文件夹的存储位置，重定向到网络共享文件夹内，这些文件夹包含文件、图片、音乐等，如图4-5-19所示。

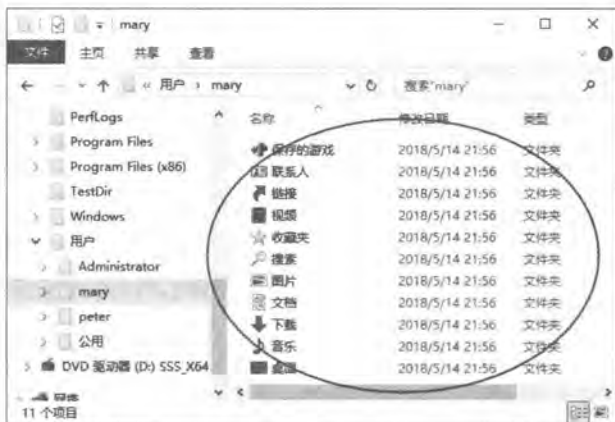


图 4-5-19



这些文件夹平常是存储在本地用户配置文件内，也就是`%SystemDrive%\用户\用户名`（或`%SystemDrive%\Users\用户名`）文件夹内，例如图4-5-19为用户mary的本地用户配置文件文件夹，因此用户换到另外一台计算机登录的话，就无法访问到这些文件夹，而如果能够将其存储位置改为（重定向到）网络共享文件夹的话，则用户到任何一台域成员计算机上登录时，都可通过此共享文件夹来访问这些文件夹内的文件。

## 1. 将“文档”文件夹重定向

我们利用将组织单位**业务部**内所有用户（包含mary）的文件文件夹快捷方式，来说明如何将此文件夹重定向到另外一台计算机上的共享文件夹。

**STEP 1** 到任何一台域成员计算机上建立一个文件夹，例如我们在服务器dc1上建立文件夹C:\DocStore，然后将组织单位**业务部**内所有用户的文件文件夹重定向到此位置。

**STEP 2** 将此文件夹设置为**共享文件夹**、将共享权限**读取/写入**赋予Everyone（系统会同时将完全控制的共享权限与NTFS权限赋予Everyone）。

### 附注

其共享名默认为文件夹名称DocStore，建议将共享文件夹隐藏起来，也就是将共享名最后一个字符设置为\$符号，例如DocStore\$。

**STEP 3** 到域控制器上【单击左下角开始图标 $\Rightarrow$ Windows 管理工具 $\Rightarrow$ 组策略管理 $\Rightarrow$ 展开到组织单位**业务部** $\Rightarrow$ 选中测试用的GPO右击 $\Rightarrow$ 编辑】。

**STEP 4** 如图4-5-20所示【展开**用户配置** $\Rightarrow$ 策略 $\Rightarrow$ Windows设置 $\Rightarrow$ 文件夹重定向 $\Rightarrow$ 选中文件夹重定向并右击 $\Rightarrow$ 属性】。



图 4-5-20

**STEP 5** 参照图4-5-21来设置，完成后单击**确定**按钮。图中的**根路径**指向我们所建立的共享文件夹\\dc1\DocStore，系统会在此文件夹之下自动为每一位登录的用户分别建立一个专用文件夹，例如账户名称为mary的用户登录后，系统会自动在\\dc1\DocStore之下，建立一个名称为mary的文件夹。图中在**设置**处共有以下几种选择：

- ✎ **基本 - 将每个人的文件夹重定向到同一个位置：**它会将组织单位业务部内所有用户的文件夹都重定向。
- ✎ **高级 - 为不同的用户组指定位置：**它会将组织单位业务部内隶属于特定组的用户的文件夹重定向。
- ✎ **未配置：**也就是不进行重定向。

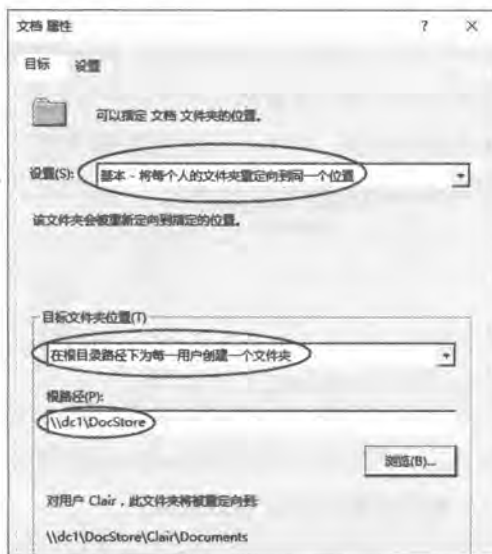


图 4-5-21

另外，图中的**目标文件夹位置**共有以下的选择：

- ✎ **重定向到用户的主目录：**如果用户账户中有指定主目录的话，则此选择可将文件夹重定向到其主目录。
- ✎ **在根目录路径下为每一用户创建一个文件夹：**如前面所述，它让每一个用户各自有一个专用的文件夹。
- ✎ **重定向到下列位置：**将所有用户的文件夹重定向到同一个文件夹。
- ✎ **重定向到本地用户配置文件位置：**重定向回原来的位置。

**STEP 6** 出现图4-5-22的界面是在提醒我们需另外设置，才能够将策略应用到旧版



图 4-5-22



Windows系统，请直接单击是(Y)按钮继续（后面再介绍如何设置）。

**STEP 7** 请利用组织单位**业务部**内的任何一个用户账户到域成员计算机（以Windows 10为例）登录，以用户mary为例，mary的文件将被重定向到\\dc1\DocStore\mary\documents 文件夹（也就是\\dc1\DocStore\mary\文件文件夹）。Mary可以【打开文件资源管理器⇨如图4-5-23所示选中快速访问或本地之下的文件并右击⇨属性】来得知其文件文件夹是位于重定向后的新位置\\dc1\DocStore\mary。



图 4-5-23

### 注意

用户可能需要登录两次后，文件夹才会成功地被重定向：用户登录时，系统默认并不会等待网络启动完成后再通过域控制器来验证用户，而是直接读取本地缓存区的账户数据来验证用户，以便提高用户登录的效率。之后等网络启动完成，系统就会自动在后台应用策略。不过因为**文件夹重定向策略**与**软件安装策略**需要在登录时才起作用，因此本实验可能需要登录两次才有作用。

如果用户账户内有被指定使用漫游用户策略文件、主目录或登录脚本的话，则该用户登录时，系统会等网络启动完成后才让用户登录。

如果用户第一次在此计算机登录的话，因缓存区内没有该用户的账户数据，故必须等网络启动完成，此时就可以取得最新的组策略设置值。

通过组策略来更改客户端此默认值的方法为：【计算机配置⇨策略⇨管理模板⇨系统⇨登录⇨计算机启动和登录时总是等待网络】。

由于用户的**文档**文件夹已经被重定向，因此用户原本位于本地用户配置文件文件夹内的

文档文件夹将被删除，例如图4-5-24中为用户mary的本地用户配置文件文件夹的内容，其内已经看不到文档文件夹。



图 4-5-24

可以到共享文件夹所在的服务器dc1上来检查此共享文件夹之下，是否已经自动建立用户mary专用的文件夹，如图4-5-25所示的C:\DocStore\Mary \Documents文件夹就是mary的文档的新存储位置。



图 4-5-25

## 2. 文件夹重定向的好处

将用户的文档文件夹（或其他文件夹）重定向到网络共享文件夹后，便可以享有以下好处与特色。

- ❑ 用户到网络上任何一台计算机登录域时，都可以访问到此文件夹。
- ❑ 使用漫游用户配置文件的用户的文档文件夹被重定向后，在漫游用户策略文件文件夹内就不会存储文档，故用户登录、读取漫游用户策略文件时，或注销、保存漫游用户策略文件时，因不需加载、存储文档，因此登录、注销的效率。
- ❑ 文档文件夹被重定向到网络服务器的共享文件夹后，其中的文件可通过信息部门的



服务器定期备份工作，使得用户的文件多了一份保障。

- ❏ 文档文件夹被导向到服务器的网络共享文件夹后，系统管理员可通过**磁盘配额**设置，来限制用户的文档在服务器内可使用的磁盘空间。
- ❏ 文档文件夹默认是与操作系统在同一个磁盘内的，在将其重定向到其他磁盘后，即使操作系统磁盘被格式化、重新安装，也不会影响到文档内的文件。

### 3. 文件夹重定向的其他设置值

可以通过图4-5-26中的**设置**选项卡来设置以下选项（以**文件**文件夹为例）。

- ❏ 授予用户对文档的独占权限

只有用户自己与系统对重定向后的新文件夹具备完全控制的权限，其他用户无任何权限，系统管理员也没有权限。如果未勾选此选项，则会继承其父文件夹的权限。

- ❏ 将文档的内容移到新位置

它会将原文件夹内的文件移动到重定向后的新文件夹内。如果未勾选此选项，则文件夹虽然会被重定向，但是原文件夹内的文件仍然会被留在原地。



图 4-5-26

- ❏ 也将重定向策略应用到 Windows 2000、Windows 200 Server、Windows XP 及 Windows Server 2003 操作系统  
重定向策略默认只会被应用到新版的 Windows 系统，但勾选此选项后，便可以应用到 Windows 2000 等旧系统。
- ❏ 策略删除  
用来设置当组策略被删除后（例如 GPO 被删除或禁用），是否要将文件夹重定向回原来的位置，默认是不会，也就是仍然留在新文件夹。

## 4.6 利用组策略限制访问可移动存储设备

系统管理员可以利用组策略来限制用户访问可移动存储设备（removable storage device，例如U盘），以免企业内部员工轻易地通过这些存储设备将重要数据带离公司。

以组织单位为例，如果是针对**计算机配置**来设置这些策略的话，则任何域用户只要在这个组织单位内的计算机登录，就会受到限制；如果是针对**用户配置**来设置这些策略的话，则所有位于此组织单位内的用户到任何一台域成员计算机上登录时，就会受到限制。

### 注意

这些策略设置仅对Windows Vista(含)等新版的Windows客户端有效。

系统总共提供了如图4-6-1右侧所示的策略设置（图中以**用户配置**为例）：

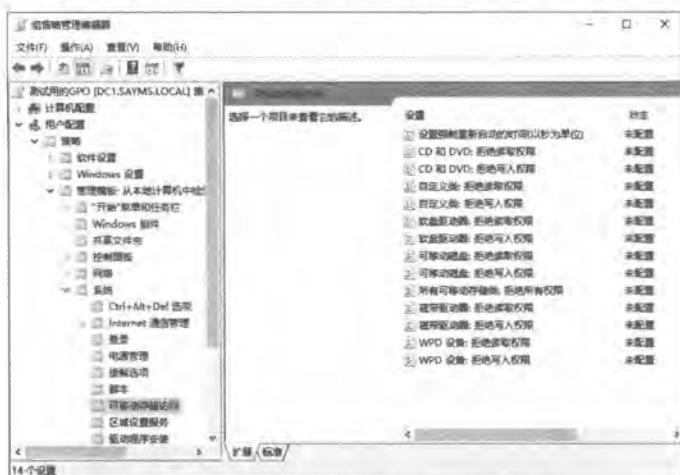


图 4-6-1

### 设置强制重新启动的时间（以秒为单位）

有些策略设置必须重新启动计算机才会应用，而如果如图4-6-2所示启用这个策略的话，则系统就会在图中指定的时间到达时自动重新启动计算机。



图 4-6-2





## ❏ CD和DVD：拒绝读取权限、拒绝写入权限

拒绝用户读取或写入属于CD与DVD类的设备（包含通过USB连接的设备）。

## ❏ 自定义类：拒绝读取权限、拒绝写入权限

属于同一类型的设备会拥有相同的**设备类型**（device setup class），例如所有的光驱都是隶属于**CD ROM设备类型**，它们都是采用相同的安装与设置方式。**设备类型**代码是采用32个字符的GUID格式（也就是xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx），可以通过**设备类型**来拒绝用户读取或写入到拥有此GUID的存储设备。

可以通过**设备管理器**来查询设备的GUID，以Windows 10中的光驱为例：【打开**计算机管理**→**设备管理器**→如图4-6-3所示展开右侧的**DVD/CD-ROM光驱**→双击光驱设备→单击前景图中的**详细信息**选项卡→在属性列表中选择**类GUID**→从**值**字段可得知其GUID】。



图 4-6-3

接下来利用组策略来拒绝用户读取或写入到拥有此GUID的设备，假设要拒绝用户写入此存储设备：【双击前面图4-6-1右侧的**自定义类：拒绝写入权限**→如图4-6-4所示选中已启用→单击**显示**按钮→输入此设备的GUID后单击**确定**按钮】，注意GUID前后需要附加大括号{}。



图 4-6-4

## ❏ 软盘驱动器：拒绝读取权限、拒绝写入权限

拒绝用户读取或写入属于软盘驱动器类型的设备（包含通过USB连接的设备）。

#### ➤ 可移动磁盘：拒绝读取权限、拒绝写入权限

拒绝用户读取或写入属于可移动磁盘类型的设备，例如U盘或外接式USB硬盘。

#### ➤ 所有可移动存储类：拒绝所有权限

拒绝用户访问所有的可移动存储设备，此策略设置的优先权高于其他策略，因此如果启用此策略的话，则不论其他策略设置如何，都会拒绝用户读取与写入到可移动存储设备。如果禁用或未配置此策略的话，则用户是否可以读取或写入到可移动存储设备，需要根据其他策略的设置而定。

#### ➤ 磁带驱动器：拒绝读取权限、拒绝写入权限

拒绝用户读取或写入隶属于磁带驱动器类型的设备（包含通过USB连接的设备）。

#### ➤ WPD设备：拒绝读取权限、拒绝写入权限

拒绝用户读取或写入隶属于WPD（Windows Portable Device）的设备，例如移动电话、媒体播放器、Windows、CE等设备。

## 4.7 WMI筛选器

我们知道如果将GPO链接到组织单位后，该GPO的设置值默认会被应用到此组织单位内的所有用户与计算机，如果要改变这个默认值的话，可以有以下两种选择：

- 通过前面介绍的**筛选组策略设置**中的**委派**选项卡来选择欲应用此GPO的用户或计算机。
- 通过本节所介绍的**WMI筛选器**来设置。

举例来说，假设已经在组织单位**业务部**内建立**测试用GPO**，并通过它来让此组织单位内的计算机自动安装所指定的软件（后面章节会介绍），不过却只想让64位的Windows 10计算机安装此软件，其他操作系统的计算机并不需要安装，此时可以通过以下的**WMI筛选器**设置来达到目的。

**STEP 1** 如图4-7-1所示【选中**WMI筛选器**并右击**新建**】。



图 4-7-1



**STEP 2** 在图4-7-2中的名称与描述字段分别输入适当的文字说明后单击**添加**按钮。图中将名称设置为**Windows 10（64位）专用的筛选器**。



图 4-7-2

**STEP 3** 在图4-7-3中的命名空间处选用默认的**root/CIMv2**，然后在**查询**处输入以下的查询命令（后述）后单击**确定**按钮：

```
Select * from Win32_OperatingSystem where Version like "10.0%" and ProductType = "1"
```

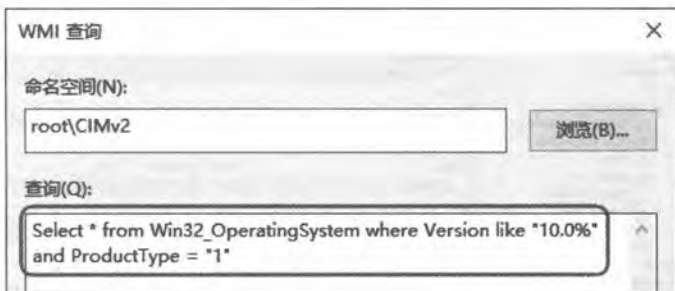


图 4-7-3

**STEP 4** 重复在前面的图4-7-2单击**添加**按钮，然后如图4-7-4所示在**查询**处输入以下的查询命令（后述）后单击两次**确定**按钮，此命令用来选择64位的系统：

```
Select * from Win32_Processor where AddressWidth="64"
```

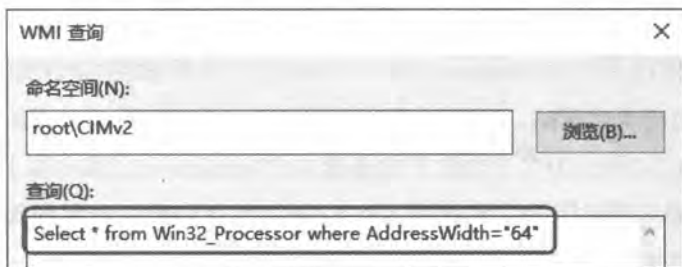


图 4-7-4

**STEP 5** 在图4-7-5中单击**保存**按钮。



图 4-7-5

**STEP 6** 在图4-7-6中测试用的GPO右下方的WMI筛选处选择刚才所建立的Windows 10（64位）专用的筛选器。



图 4-7-6

组织单位**业务部**内所有的Windows 10客户端都会应用**测试用GPO**策略设置，但是其他Windows系统并不会应用此策略。可以到客户端计算机上通过执行**gpresult /r**命令来查看应用了哪些GPO，如图4-7-7所示为在一台位于**业务部**内的Windows 8.1客户端上利用**gpresult /r**命令所看到的结果，因为**测试用的GPO**搭配了**Windows 10（64位）专用的筛选器**，故Windows 8.1计算机并不会应用此策略（被WMI筛选器拒绝）。



图 4-7-7

图4-7-3中的命名空间是一组用来管理环境的类（class）与实例（instance）的集合，系统内包含着各种不同的命名空间，以便于通过其中的类与实例来管控各种不同的环境，例如命名空间CIMv2内所包含的是与Windows环境有关的类与实例。

图4-7-3中的查询字段内需要输入WMI 查询语言（WQL）来执行筛选工作，其中的Version like后面的数字所代表的意义如表4-7-1所示：

表4-7-1

Windows版本	Version
Windows 10与Windows Server 2016	10.0
Windows 8.1与Windows Server 2012 R2	6.3
Windows 8与Windows Server 2012	6.2
Windows 7与Windows Server 2008 R2	6.1
Windows Vista 与Windows Server 2008	6.0
Windows Server 2003	5.2
Windows XP	5.1

而ProductType右侧的数字所代表的意义如表4-7-2所示。

表4-7-2

ProductType	所代表的意义
1	客户端等级的操作系统，例如Windows 10、Windows 8.1
2	服务器等级的操作系统并且是域控制器
3	服务器等级的操作系统，但不是域控制器

综合以上两个表格的说明后，我们在表4-7-3中列举几个WQL范例命令。

表4-7-3

要筛选的系统	可用的WQL命令范例
Windows 10 (64位与32位)	<code>select * from Win32_OperatingSystem where Version like "10.0%" and ProductType="1"</code>
Windows 10 (64位)	<code>select * from Win32_OperatingSystem where Version like "10.0%" and ProductType="1"</code> <code>select * from Win32_Processor where AddressWidth="64"</code>
Windows 10 (32位)	<code>select * from Win32_OperatingSystem where Version like "10.0%" and ProductType="1"</code> <code>select * from Win32_Processor where AddressWidth="32"</code>
Windows 8.1 (64位与32位)	<code>select * from Win32_OperatingSystem where Version like "6.3%" and ProductType="1"</code>
Windows 8.1 (64位)	<code>select * from Win32_OperatingSystem where Version like "6.3%" and ProductType="1"</code> <code>select * from Win32_Processor where AddressWidth="64"</code>
Windows 8.1 (32位)	<code>select * from Win32_OperatingSystem where Version like "6.3%" and ProductType="1"</code> <code>select * from Win32_Processor where AddressWidth="32"</code>
Windows Server 2016域控制器	<code>select * from Win32_OperatingSystem where Version like "10.0%" and ProductType="2"</code>
Windows Server 2016成员服务器	<code>select * from Win32_OperatingSystem where Version like "10.0%" and ProductType="3"</code>
Windows 10与Windows Server 2016	<code>select * from Win32_OperatingSystem where Version like "10.0%"</code>
Windows Server 2012 R2域控制器	<code>select * from Win32_OperatingSystem where Version like "6.3%" and ProductType="2"</code>
Windows Server 2012 R2成员服务器	<code>select * from Win32_OperatingSystem where Version like "6.3%" and ProductType="3"</code>
Windows 8.1与Windows Server 2012 R2	<code>select * from Win32_OperatingSystem where Version like "6.3%"</code>
Windows 8	<code>select * from Win32_OperatingSystem where Version like "6.2%" and ProductType="1"</code>
Windows 7	<code>select * from Win32_OperatingSystem where Version like "6.1%" and ProductType="1"</code>
Windows Vista	<code>select * from Win32_OperatingSystem where Version like "6.0%" and ProductType="1"</code>
Windows Server 2012 R2与 Windows Server 2012成员服务器	<code>select * from Win32_OperatingSystem where (Version like "6.3%" or Version like "6.2%") and ProductType="3"</code>
Windows 8.1、Windows 8、Windows 7、Windows Vista	<code>select * from Win32_OperatingSystem where Version like "6.%" and ProductType="1"</code>
Windows 8.1、Windows Server 2012 R2成员服务器	<code>select * from Win32_OperatingSystem where Version like "6.3%" and ProductType&lt;&gt;"2"</code>
Windows XP	<code>select * from Win32_OperatingSystem where Version like "5.1%"</code>
Windows XP Service Pack 3	<code>select * from Win32_OperatingSystem where Version like "5.1%" and ServicePackMajorVersion=3</code>
Windows XP Service Pack 2 (含) 以上	<code>select * from Win32_OperatingSystem where Version like "5.1%" and ServicePackMajorVersion&gt;=2</code>



## 4.8 组策略建模与组策略结果

可以通过**组策略建模**（Group Policy Modeling）来针对用户或计算机模拟可能的情况，例如某用户账户当前是位于甲组织单位内，某计算机账户目前是位于乙容器内，而我们想要知道未来如果该用户或计算机账户被移动到其他容器时，该用户到此计算机上登录后，其用户或计算机策略的设置值。另外，在当前现有的环境之下，如果想要知道用户在某台计算机登录之后，其用户与计算机策略设置值的话，可以通过**组策略结果**（Group Policy Result）来提供这些信息。

### 1. 组策略建模

我们将利用图4-8-1的环境来练习**组策略建模**。图中用户账户**陈玛莉**（mary）与计算机账户Win10PC1目前都是位于组织单位**业务部**内，而如果用户账户**陈玛莉**（mary）与计算机账户Win10PC1未来都被移动到组织单位**金融部**，此时如果用户**陈玛莉**（mary）到计算机Win10PC1上登录的话，其用户与计算机策略设置值可以通过**组策略建模**来事先模拟。



图 4-8-1

**STEP 1** 在图4-8-2中【选中**组策略建模**并右击**组策略建模向导**】。

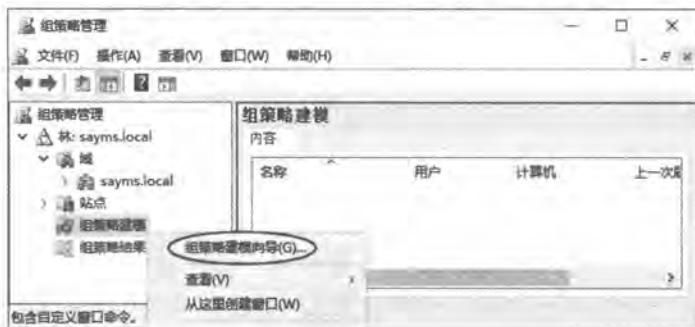


图 4-8-2



**STEP 2** 出现欢迎使用组策略建模向导界面时单击 **下一步** 按钮。

**STEP 3** 由于需要指定一台至少是Windows Server 2003域控制器来执行模拟工作，因此请通过图4-8-3来选择域控制器，图中我们让系统自行挑选。



图 4-8-3

**STEP 4** 在图4-8-4中分别选择要练习的用户账户mary与计算机账户Win10PC1后单击 **下一步** 按钮。



图 4-8-4

**STEP 5** 在图4-8-5中选择慢速连接是否要处理策略、是否要采用环回处理模式等。完成后单击 **下一步** 按钮。

**STEP 6** 由图4-8-6的背景图中可知用户账户（陈玛莉，mary）与计算机账户（Win10PC1）目前都是位于组织单位**业务部**，请通过 **浏览** 按钮来将其模拟到未来的位置，也就是前景图中的组织单位**金融部**。单击 **下一步** 按钮。



图 4-8-5



图 4-8-6

**STEP 7** 在图4-8-7中的背景与前景图会分别显示用户与计算机账户当前所属的组，有需要的话，可通过单击**添加**按钮来模拟他们未来会隶属的组。图中两个界面我们都直接单击**下一步**按钮。



图 4-8-7

**STEP 8** 在图4-8-8中的背景与前景图会分别显示用户与计算机账户目前所应用的**WMI筛选器**，有需要的话，可通过单击**添加**按钮来模拟他们未来会应用的**WMI筛选器**。图中两个界面我们都直接单击**下一步**按钮。



图 4-8-8

**STEP 9** 确认选择的摘要界面的设置无误后单击**下一步**按钮。

**STEP 10** 出现正在完成组策略建模向导界面时单击**完成**按钮。

**STEP 11** 完成后，通过图4-8-9右侧3个选项卡来查看模拟运行的结果。



图 4-8-9

2. 组策略结果

我们将利用图4-8-10的环境来练习**组策略结果**。我们想要知道图中用户账户**陈玛莉** (mary) 到计算机Win10PC1登录后的用户与计算机策略的设置值。



图 4-8-10

STEP 1 如果用户陈玛莉 (mary) 还没有到计算机Win10PC1登录的话, 请先登录。

STEP 2 请到域控制器上以系统管理员身份登录、执行组策略管理、如图4-8-11所示【选中组策略结果并右击组策略结果向导】。



图 4-8-11

STEP 3 出现欢迎使用组策略结果向导界面时单击下一步按钮。

STEP 4 在图4-8-12中选择要查看的域成员计算机Win10PC1后单击下一步按钮。



图 4-8-12



**注意**

先将此域成员计算机Win10PC1的**Windows防火墙**关闭，否则无法连接此计算机。

**STEP 5** 在图4-8-13中选择域用户mary（陈玛莉）后单击**下一步**按钮。只有当前登录的用户与曾经登录过的用户账户可以被选择。



图 4-8-13

**STEP 6** 确认选择的摘要界面中的设置无误后单击**下一步**按钮。

**STEP 7** 出现正在完成组策略结果向导界面时单击**完成**按钮。

**STEP 8** 通过图4-8-14右侧3个选项卡来查看结果。

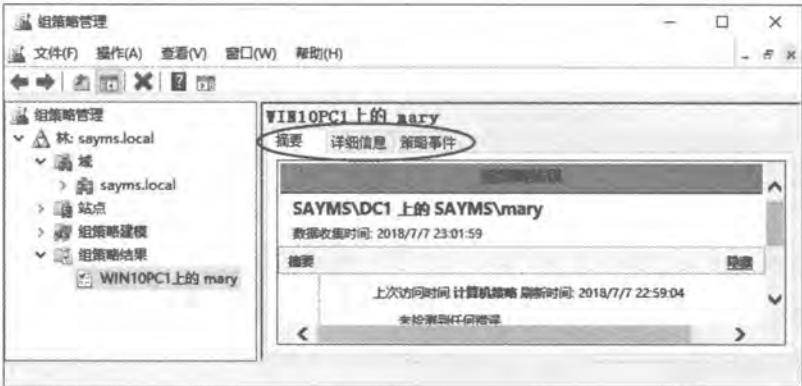


图 4-8-14

## 4.9 组策略的委派管理

可以将GPO的链接、新建与编辑等管理工作，分别委派给不同的用户来负责，以分散与减轻系统管理员的管理负担。



### 4.9.1 站点、域或组织单位的GPO链接委派

可以将连接GPO到站点、域或组织单位的工作委派给不同的用户来执行，以组织单位**业务部**为例，可以如图4-9-1所示单击组织单位**业务部**后，通过**委派**选项卡来将链接GPO到此组织单位的工作委派给用户，由图中可知默认是Administrators、Domain Admins或Enterprise Admins等组内的用户才拥有此权限。还可以通过界面中的**权限**下拉列表来设置**执行组策略建模分析与读取组策略结果数据**这两个权限。



图 4-9-1

### 4.9.2 编辑GPO的委派

默认是Administrators、Domain Admins或Enterprise Admins组内的用户才有权编辑GPO，如图4-9-2所示为**测试用的GPO**的默认权限列表，可以通过此界面来赋予其他用户权限，这些权限包含**读取、编辑设置与“编辑设置、删除、修改安全性”**3种。



图 4-9-2



## 4.9.3 新建GPO的委派

默认是Domain Admins与Group Policy Creator Owners组内的用户才有权限新建GPO（如图4-9-3所示），也可以通过此界面来将此权限赋予其他用户。



图 4-9-3

Group Policy Creator Owners组内的用户在新建GPO后，他就是这个GPO的所有者，因此他对这个GPO拥有完全控制的权限，所以可以编辑这个GPO的内容，不过他却没有权限编辑其他的GPO。

## WMI 筛选器的委派

系统默认是Domain Admins与Enterprise Admins组内的用户才有权限在域内建立新的WMI筛选器，并且可以修改所有的WMI筛选器，如图4-9-4所示中的完全控制权限。而Administrators与Group Policy Creator Owners组内的用户也可以建立新的WMI筛选器与修改其自行建立的WMI筛选器，不过却不能修改其他用户所建立的WMI筛选器，如图4-9-4所示中的创建者所有者权限。也可以通过此界面将权限赋予其他用户。



图 4-9-4





Group Policy Creator Owners组内的用户，在新建WMI筛选器后，他就是此WMI筛选器的所有者，因此他对此WMI筛选器拥有完全控制的权限，所以可以编辑此WMI筛选器的内容，不过他却没有权限编辑其他的WMI筛选器。

## 4.10 StarterGPO的设置与使用

StarterGPO内仅包含**管理模板**的策略设置，可以将经常会用到的**管理模板**策略设置值创建到**StarterGPO**内，然后在建立常规GPO时，就可以直接将**StarterGPO**内的设置值导入到这个常规GPO内，如此便可以节省建立常规GPO的时间。建立**StarterGPO**的步骤如下所示：

**STEP 1** 如图4-10-1所示【选中**StarterGPO**并右击**新建**】。



图 4-10-1

### 附注

可以不需要单击界面右侧的**创建StarterGPO文件夹**，因为在建立第1个**StarterGPO**时，它也会自动建立此文件夹，此文件夹的名称是**StarterGPOs**，它是位于域控制器的sysvol共享文件夹之下。

**STEP 2** 在图4-10-2中为此**StarterGPO**设置名称与输入注释后单击**确定**按钮。

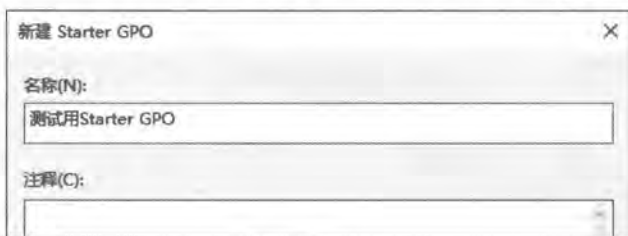


图 4-10-2



STEP 3 在图4-10-3中【选中此StarterGPO并右击 $\Rightarrow$ 编辑】。



图 4-10-3

STEP 4 通过图4-10-4来编辑计算机与用户设置的管理模板策略。



图 4-10-4

完成StarterGPO的建立与编辑后，之后在建立常规GPO时，就可以如图4-10-5所示选择从这个StarterGPO来导入其管理模板的设置值。

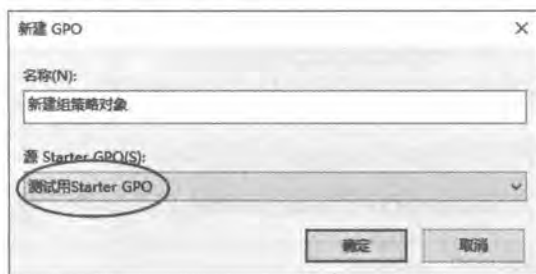


图 4-10-5