第3章 Windows Server 2008 系统管理

本章目标

- 了解 MMC、本地帐户和组帐户、NTFS 文件系统、文件夹共享、磁盘管理、安全策略以及防火墙、数据备份与恢复、性能监视和日志，以及群集管理的基本概念与原理。
- 掌握不同类型服务的管理方法。

MMC 提供了一个管理工具的方便途径，效率极高；本地用户和组帐户权利与权限规则，并与 NTFS 权限加以区别；文件夹共享可方便不同计算机之间进行交流；磁盘管理方法得当，可以使系统的瓶颈段——硬盘的使用效能提高许多；安全策略指在某个安全区域内用于所有与安全相关活动的一套规则，本地安全策略与 Windows 防火墙可使系统处于安全可靠的状态；性能监视和日志可以及时发现系统出现的故障；群集就是一组协同工作以提高服务和应用程序可用性的独立计算机，可以使系统整体性能大幅提高。

3.1 使用基本管理工具

3.1.1 操作实例：使用 MMC

MMC（Microsoft 管理控制台，Microsoft Manage Console）提供了一个管理工具的途径。MMC 允许用户创建、保存并打开管理工具，这些管理工具用来管理基于 Windows 的硬件，软件和网络部件，包含了控件、向导、任务、文件和来自微软或其他软件厂商或用户自定义的嵌入式管理单元。为了创建一个控制台，管理员运行 MMC 可执行文件来打开一个空的控制台，并在安装在系统上的工具（例如证书服务器管理器、设备管理器、域名服务器（DNS）管理器）中进行选择。MMC 本身并不执行管理功能，它只是集成管理工具而已。因为控制台以文件形式存在，管理员可以创建它们并以 E-mail 附件发给负责特殊任务的开发者。

单击“开始”按钮，在“开始搜索”文本框中，输入 MMC，然后按 Enter 键即可打开控制台，如图 3.1 所示。

可以添加到控制台中的主要工具类型称为管理单元，如图 3.2 所示，管理单元是 MMC 控制台的基本组件，它总是在 MMC 中运行，而不能在 MMC 之外运行。MMC 支持两种类型的管理单元：独立管理单元和扩展管理单元。可以独立添加到控制台树中，而无须首先添加其他项目的这种管理单元称为独立管理单元；反之需要先添加其他项目才可以被添加的管理单元称为扩展管理单元。

在“文件”菜单中选择“保存”或者“另存为”命令可以把控制台进行保存，下次直接双击

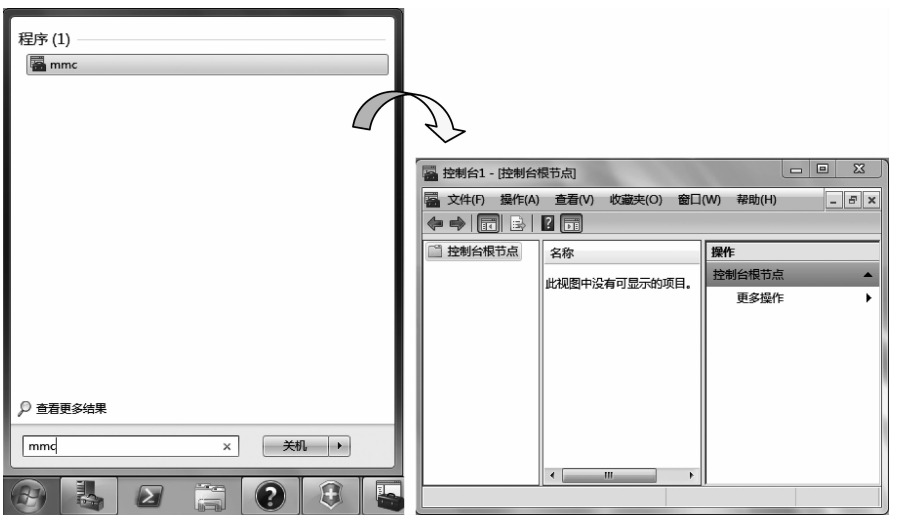

图 3.1　打开 Microsoft 管理控制台

图 3.2　添加/删除管理单元

控制文件打开控制台，原先添加的管理单元仍旧存在，可以用来进行计算机的管理工作。

3.1.2　MMC 模式和功能

有时用户想创建一个控制台给一个普通用户使用，但不想给予它在控制台中添加或者删除管理单元的权利。在“文件”菜单中选择“选项”命令，如图 3.3 所示进入模式选择界面。

(1) 作者模式：使用者即可以往控制台中添加、删除管理单元，也可以在控制台中创建新的窗口、改变视图等。

(2) 用户模式，可以进一步分为：

- 完全访问——使用者不能添加、删除管理单元或者控制台的属性，但是可以访问所有的窗口管理命令以及所有提供的控制台树的全部权限。
- 受限访问、多窗口——仅允许用户访问在保存控制台时可见的控制台树的区域，可以创建新的窗口，但是不能关闭已有的窗口。
- 受限访问、单窗口——仅允许用户访问在保存控制台时可见的控制台树的区域，可以创建新的窗口，阻止用户打开新的窗口。

图 3.3　MMC 模式

(3) MMC 主要功能：只需 MMC 就能完成大部分管理任务；集中化管理；利用大部分管理单元进行远程管理；可建立任意个自定义的主控制台。

3.1.3　操作实例：创建定制 MMC

在本次实验中，将创建一个可用来管理活动目录域和信任关系以及 WMI 服务的定制 MMC。

(1) 在桌面上，单击“开始”→“运行”命令，在文本框中输入 MMC，然后单击“确定”按钮。

(2) 在“控制台 1”窗口，单击菜单上的“文件”→“添加/删除管理单元”命令。

(3) 在“添加/删除管理单元”对话框中，单击“添加”按钮。

(4) 在“添加独立管理单元”对话框中，单击“Active Directory 用户和计算机”选项，然后单击“添加”按钮，如图 3.4 所示。

图 3.4　定制 MMC

(5) 在“添加独立管理单元”对话框中，单击“Exchange 系统”选项，然后单击“添加”按钮。

(6) 在“更改域控制器”对话框中，单击“确定”按钮，然后在“添加独立管理单元”对话框中单击“关闭”按钮，如图 3.4 所示。

(7) 在“添加/删除管理单元”对话框中,验证“Active Directory 用户和计算机”以及 WMI 控件已经列出,然后单击“确定”按钮,如图 3.5 所示。

图 3.5 定制 MMC

(8) 在控制台根节点,验证“Active Directory 用户和计算机”以及 WMI 服务已经列出。

(9) 在“控制台”中,单击“文件”→“另存为”命令。

(10) 在“另存为”对话框中,在快捷方式菜单工具栏内,单击“桌面”图标,在“文件名”文本框内,输入“My MMC. msc”然后单击“保存”按钮。

(11) 关闭 My MMC 界面,然后验证 My MMC 已在桌面上存在。

3.2 本地用户和组帐户管理

3.2.1 本地用户和组帐户概述

1. 基本概念

用户帐户:本地用户帐户就相当于钥匙,有了钥匙才能开锁。本地帐户存储在本地计算机上的 SAM 中:%systemroot%\system32\config\SAM。Windows Server 2008 默认用户帐户有两种:Administrator 帐户和 Guest 帐户。

- Administrator:内置管理员帐户,此帐户对当前计算机拥有最大的权限。该帐户必须仅用于需要管理凭据的任务,强烈建议将此帐户设置为使用强密码(至少含 8 个字符,包括字母、数字和符号的组合)。
- Guest:用于临时访问的帐户,默认的权限很少,而且默认状态下,该帐户是被禁用的。

注意:本地用户只能登录到本地计算机,后继会学到的域帐户可以登录到域中的其他计算机上。

组帐户:各个用户归属的组。例如 administrator 组,还有 power user 组等,各个组的权限是不一样的。组帐户是用户帐户的集合,通常将组帐户命名为复数形式。在设置用户权限时,如果用户数量比较多,并且权限设置经常变动,管理员就会做大量重复性工作,此时就可以考虑使用组来完成权限的分配,并且一个用户帐户可以同时加入到多个组,如图 3.6 所示。

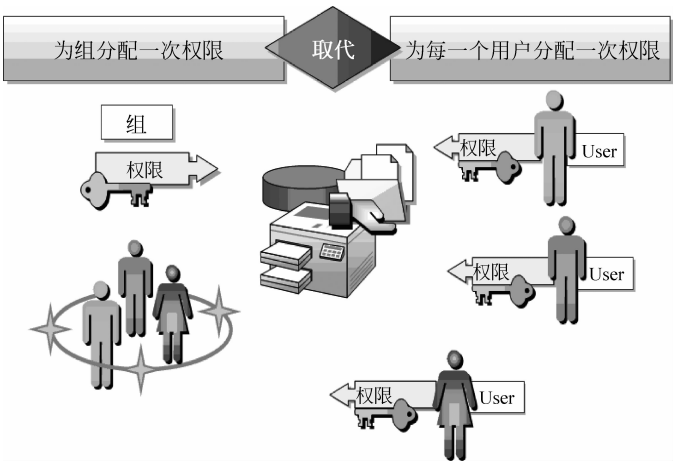

图 3.6　组帐户意义

计算机帐户：也可以说是计算机名称，在局域网中用来识别计算机组策（即定义系统管理员需要管理的用户桌面环境的多种组件）。

2. 基本功能

本地用户和组位于计算机管理中，用户可以使用这一组管理工具来管理单台本地或远程计算机。可以使用本地用户和组保护并管理存储在本地计算机上的用户帐户和组。可以在特定计算机上（只能是这台计算机）分配本地用户帐户或组帐户的权限和权利。通过本地用户和组，可以为用户和组分配权利和权限，从而限制用户和组执行某些操作的能力。权利可授权用户在计算机上执行某些操作，如备份文件和文件夹或者关机。权限是与对象（通常是文件、文件夹或打印机）相关联的一种规则，它规定哪些用户可以访问该对象以及以何种方式访问。

3. 打开本地用户和组

右击本地计算机，依次选择“管理”→“配置”→“本地用户和组”命令，即可打开本地用户和组管理界面，如图 3.7 所示。

图 3.7　本地用户和组管理界面

3.2.2 本地用户和组帐户管理

1. 本地用户帐户管理

在左边列表中选择用户，可以在中间列表中看到已存在的用户，选中一个用户，可以在操作列表中单击进行相应操作，如图 3.8 所示。

图 3.8 本地用户帐户管理

选择“新用户”命令，得到“新用户”对话框，可以在其中对新用户的属性进行设置；如果选择已存在用户，则在右键快捷菜单中选择“属性”命令，可以对此用户进行属性配置，如图 3.9 所示。

图 3.9 创建新用户

2. 本地组帐户管理

在左边列表中选择组，可以在中间列表中看到已存在的组，选中一个组，可以在操作列表中单击左键进行相应操作，如图 3.10 所示。注意：新建的用户默认属于 Users 组。

图 3.10　本地组帐户管理

选择“新建组”命令，得到“新建组”对话框，可以对新建组的属性进行设置；如果选择已存在的组，则在右键快捷菜单中选择“属性”命令，可以对此组进行属性配置，如图 3.11 所示。

图 3.11　新建本地组帐户

3.2.3　本地用户和组帐户权利与权限规则

当一个用户属于多个组时，其权利和权限遵循以下规则。

(1) 多个组的权利和权限是累加的。

例 1：如果组 A 可以对文件夹 A 完全控制，组 B 可以对文件夹 B 完全控制，则同时属于两个组的用户帐户可以对两个文件夹完全控制。

例 2：如果一个用户既属于 Power Users 组，又属于 Backup Operators 组，那么用户可以完成两个组的所有工作：即可以完成 Power Users 组的高级用户拥有的管理权限(向后兼容)工作，以及 Backup Operators 组的登录和关闭计算机、备份和还原计算机上的所有文件的工作。

(2) 文件权限覆盖文件夹权限。

例：如果组 A 可以对文件夹 A 完全控制，文件夹 A 中的文件 a 权限是只读，则同时属

于两个组的用户帐户可以对文件夹 A 中除文件 a 以外所有文件进行完全控制，对文件 a 的权限是只读。

(3) 拒绝权限覆盖其他所有权限。

例：如果组 A 可以对文件夹 A 完全控制，文件夹 A 中的文件 a 权限是拒绝所有访问，则同时属于两个组的用户帐户可以对文件夹 A 中除文件 a 以外所有文件进行完全控制。

注意：如果想要知道一个用户对某项资源的最终的权利或权限，可以右击该资源，在弹出的快捷菜单中依次选择“属性”→“安全”→“高级”→“有效权限”→“选择”命令，将用户名输入或查找，找到该用户，即可得到最终有效权限(参考 3.3.3 节)。

3.3 NTFS 文件系统管理

3.3.1 NTFS 安全权限简介

权限是在对象的安全描述符中定义的。权限与特定的用户和组相关联，或者是指派到特定的用户和组。用户或组的每个权限的分配都在系统中作为访问控制项 (Access Control Entry，ACE) 显示。安全描述符中的整个权限项集称作权限集或访问控制列表 (Access Control List，ACL)。

与 FAT32 比，NTFS 具有如下优点：安全性和稳定性极其出色，在使用中不易产生产生文件碎片，NTFS 分区对用户权限做出了非常严格的限制，每个用户都只能按着系统赋予的权限进行操作，任何试图越权的操作都将被系统禁止，同时它还提供了容错结构日志，可以将用户的操作全部记录下来，从而保护了系统的安全。NTFS 安全权限结构如图 3.12 所示。

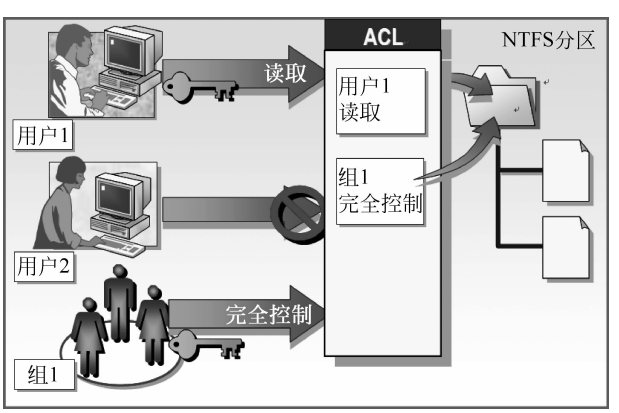

图 3.12 NTFS 安全权限

3.3.2 NTFS 权限的应用规则

1. NTFS 文件夹权限与 NTFS 文件权限设置

对某个文件夹右击，在弹出的快捷菜单中依次选择“属性”→“安全”→“编辑”命令，即可打开文件夹权限对话框，如图 3.13 所示。

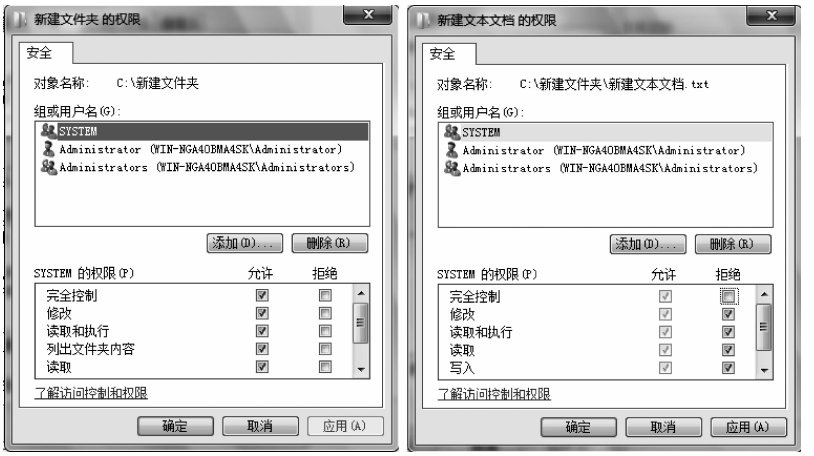

图 3.13　NTFS 安全权限设置

2. NTFS 权限应用规则

1）权限的组合

用户对资源的有效权限(参考 3.3.3 节)：分配给用户帐户的权限和用户所属各个组的累加权限。

例：如图 3.14 所示，user 属于组 group1 和 group2，user 有读取权限，group1 有写入权限，user 的有效权限是读取和写入(累加)。

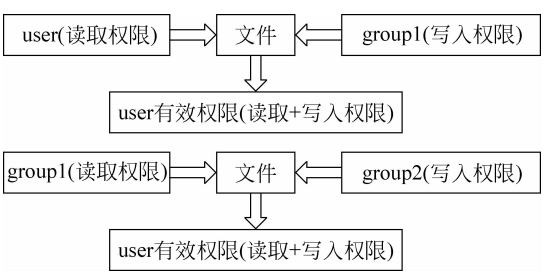

图 3.14　NTFS 安全权限设置

2）权限的拒绝

规则：拒绝权限可以覆盖所有其他权限；可以设置拒绝用户帐户，也可以拒绝组。

使用场合：某文件并没有给某些用户设置访问权限，但由于用户自动累加了其所属的多个组的权限，而能够访问文件，如何解决？这就需要设置拒绝权限。

例 1：如图 3.15 所示，用户 1 同时属于组 A 和组 B，此时用户 1 同时拥有两个组的权限，但是组 A 对文件 2 的权限是“拒绝写入”，根据规则，用户 1 无法对文件 2 进行修改。

例 2：user 属于组 group1 和 group2，其有效权限如图 3.16 所示。

3. NTFS 权限继承

新建的子文件夹和文件会继承上一级目录的权限；根目录下的文件夹或文件继承磁盘分区的权限；下一级目录或文件可以取消继承；上一级目录或文件可以强制继承；对某个文件夹右击，在弹出的快捷菜单中依次选择“属性”→“安全”→“高级”→“更改权限”命令，如图 3.17 所示。

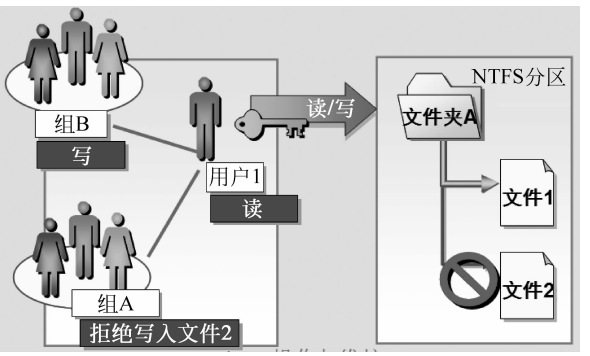

图 3.15　NTFS 拒绝权限

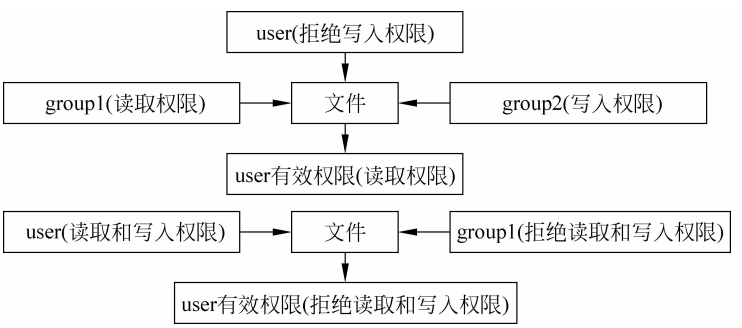

图 3.16　NTFS 有效权限

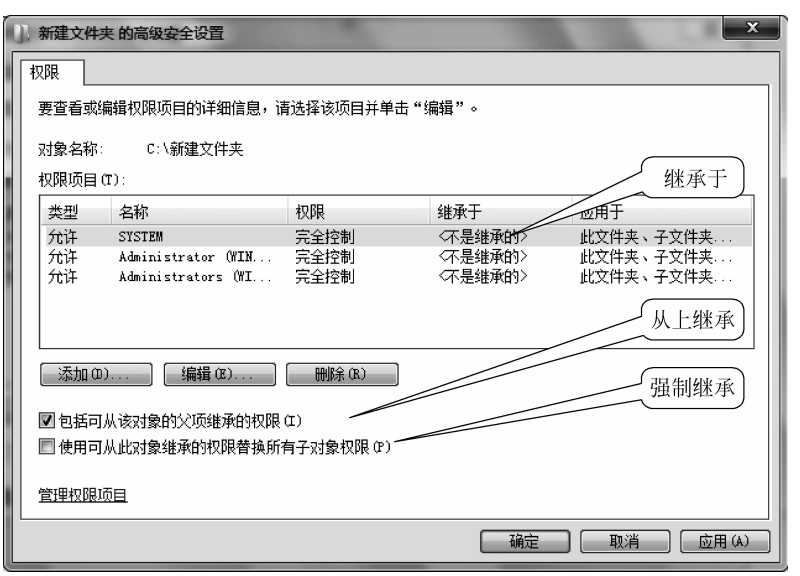

图 3.17　NTFS 权限的继承

4. 移动和复制对 NTFS 权限影响

引入：对文件和文件夹的移动和复制是比较频繁的操作，如此操作后对文件和文件夹的权限有何影响？