第 2 章　本地用户和组的管理

每个用户都需要有一个账户名和密码才能访问计算机上的资源。用户的账户类型有域账户、本地账户和内置账户。域账户用来访问域内资源（将在后面章节介绍），本地账户用来本地登录，不能访问域内的资源，内置账户用来对计算机进行管理。

组是权限相同账户的集合，管理员通常通过组来对用户的权限进行设置，从而简化了管理。本章将详细介绍用户和组的管理。

1. 了解本地账户的类型与命名规则
2. 为企业用户创建和管理本地账户
3. 了解本地组的概念
4. 为企业各部门创建和管理本地组

2.1　本地账户

2.1.1　账户的类型

Windows Server 2008 作为独立服务器或域中的成员服务器时，在计算机操作系统中有两种本地账户：系统管理员创建的本地账户和内置本地账户。

1．本地账户

本地账户可以建立在 Windows Server 2008 独立服务器、成员服务器以及 Windows Vista 等系统中。本地账户只能在本地计算机上登录，无法访问其他计算机资源。

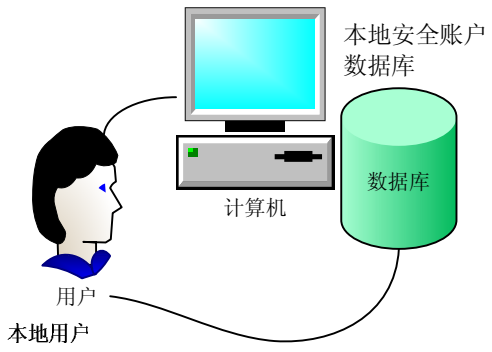

图 2-1　本地账户登录验证

本地计算机上有一个管理账户数据的数据库，称为 SAM（Security Accounts Managers，安全账户管理器），SAM 数据库文件路径为“\Windows\system32\config\SAM”。在 SAM 中，每个账户被赋予唯一的 SID（Security Identifier，安全识别号）。

Windows 内部进程识别账户是用 SID，而不是用账户名。用户要访问本地计算机，都需要经过该机 SAM 中的 SID 验证。如图 2-1 所示。

2．内置本地账户

Windows Server 2008 中还有一种账户类型叫内置账户。当系统安装完毕后，系统会在服务器上自动创建它们。在独立服务器上或是成员服务器上，内置本地账户有：Administrator 和 Guest，创建在 SAM 中。

Administrator（系统管理员）：它拥有最高的权限，管理着 Windows Server 2008 系统。可以将 Administrator 的名字进行更改，但不能删除该账户。该账户无法被禁止，永远不会到期，不受登录时间限制。

Guest（来宾）：是为临时访问计算机的用户提供的。该账户自动生成，且没有密码，不能被删除，可以更改名字。Guest 只有很少的权限，默认情况下，该账户被禁止使用。例如当我们希望局域网中的用户都可以登录到自己的电脑，但又不愿意为每一个用户建立一个账户，就可以启用 Guest。

2.1.2 账户名与密码的命名规则

账户名的命名规则如下：

- 账户名必须唯一，且不分大小写。
- 用户名最多可包含 256 个字符。
- 在账户名中不能使用的字符有：‘、/、\、[、]、:、;、|、=、,、+、*、？、<、>。
- 用户名可以是字符和数字的组合。
- 用户名不能与组名相同。

账户密码规则如下：

- 必须为 Administrator 账户分配密码，防止未经授权就使用。
- 系统默认用户的密码至少 6 个字符，还要至少包含 A～Z、a～z、0～9、非字母数字（例如!、#、$、%）等四组字符中的三种。
- 密码的长度在 8～128 之间。
- 密码不包含全部和部分的用户账户名。
- 密码中不能使用以下字符：‘、/、\、|、;、:、=、,、+、[、]。

2.1.3 创建本地账户

本地账户是工作在本地机的，只有 Administrators 组的成员例如 Administrator 才能创建本地用户。下面我们举例说明如何创建本地用户。例如：在 Windows Server 2008 独立服务器或成员服务器上创建本地账户 Emily，设置密码，并用该账户登录系统。操作如下：

步骤 1：从“开始”→“管理工具”→“计算机管理”→“本地用户和组”菜单，打开“本地用户和组”窗口，在窗口中右击“用户”，选择“新用户”菜单。

步骤 2：打开“新用户”窗口，输入如图 2-2 所示内容。

- 用户名：系统本地登录时使用的名称。
- 全名：用户的全称。
- 描述：关于该用户的说明文字。

图 2-2　创建本地新账户

- 密码：用户登录时使用的密码。
- 确认密码：为防止密码输入错误，需再输入一遍。
- 用户下次登录时须更改密码：用户首次登录时，使用管理员分配的密码，当用户再次登录时，强制用户更改密码，用户更改后的密码就只有自己知道，保证了安全使用。我们这里是管理员统一创建账户，应该选择此项。
- 用户不能更改密码：通常用于公共账户，防止有人更改密码。
- 密码永不过期：密码默认的有限期为 42 天，超过 42 天系统会提示用户更改密码。选择此项表示系统永远不会提示用户改密码。
- 账户已禁用：选择该项表示任何人都无法使用这个账户登录，适用于某员工休假时，防止他人冒用该账户登录。

步骤 3：注销当前账户，用新账户测试是否可以正常登录。

步骤 4：重复以上步骤为企业内全部员工创建账户。

2.1.4　更改账户

如果要对已经建立的账户更改登录名，则在“计算机管理”→“本地用户和组”→“用户”列表中选择，右击该账户，选择“重命名”，输入新名字，如图 2-3 所示。

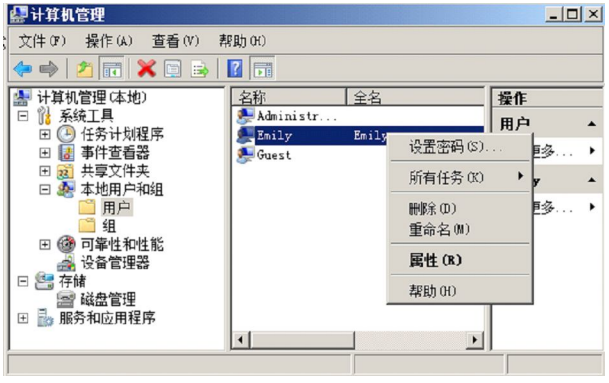

图 2-3　更改账户

2.1.5 删除账户

如果某用户离开公司，为防止其他用户使用该用户账户登录，就要删除该用户的账户。在“计算机管理”→“本地用户和组”→“用户”列表中选择，右击该账户，选择“删除”→“是”，如图 2-3 所示。

2.1.6 更改账户密码

重设密码可能会造成不可逆的信息丢失。出于安全的原因，要更改用户的密码分以下几种情况：

如果用户在知道密码的情况下想更改密码，他在登录后按 Ctrl+Alt+Delete 组合键，如图 2-4 所示，输入正确的旧密码，然后输入新密码。

图 2-4 更改密码

如果用户忘记了登录密码，并且事先已经创建了“密码重设盘”，则使用密码重设盘来进行密码重设，密码重设只能在本地机中设置。创建密码重设盘的步骤如下：

步骤 1：用户登录后按 Ctrl+Alt+Delete 组合键，单击“创建密码重设盘”（见图 2-4），打开“忘记密码向导”窗口，如图 2-5 所示，选择“下一步”按钮。

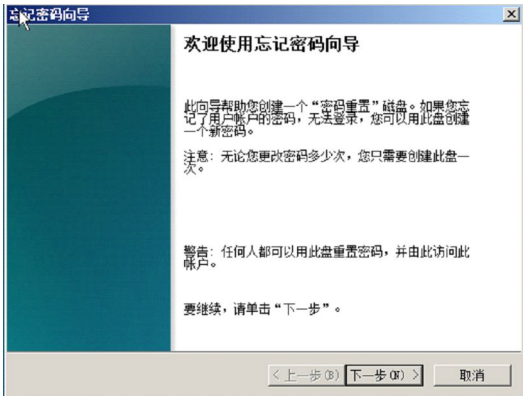

图 2-5 进入向导

步骤 2：如图 2-6 所示，按照提示，选择优盘作为密码重置盘，单击“下一步”按钮。

步骤 3：如图 2-7 所示，输入当前的密码。单击“下一步”按钮。

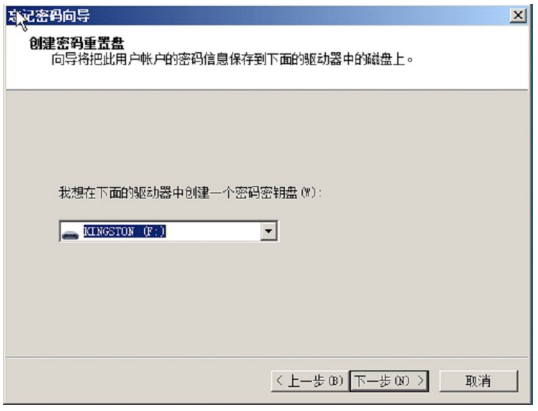

图 2-6　用优盘作为密码重置盘

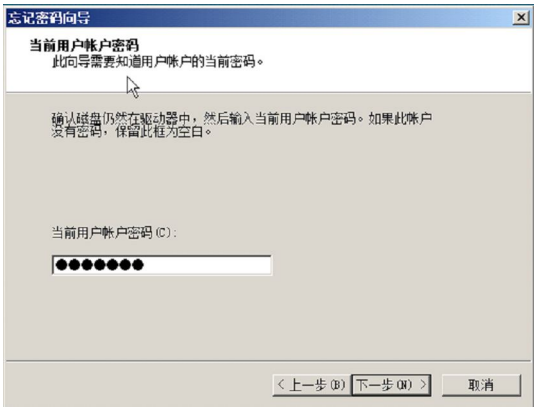

图 2-7　输入密码

步骤 4：如图 2-8 所示，系统开始创建密码重置盘，单击“下一步”按钮完成密码重置盘的创建。

用户忘记密码后，可以利用密码重置盘设置新密码。步骤如下：

步骤 1：在用户登录输入密码有错时，会出现如图 2-9 所示窗口，单击“重设密码”。

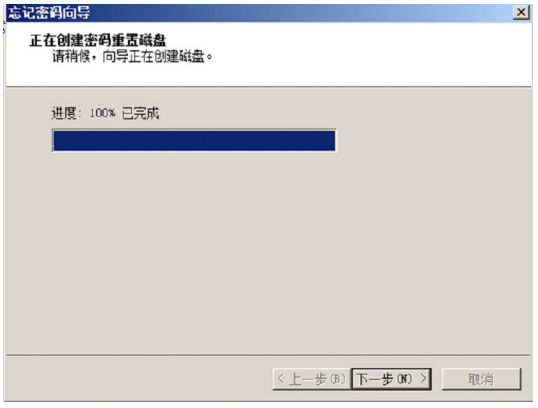

图 2-8　创建密码重置盘

图 2-9　登录失败

步骤 2：打开“重置密码向导”窗口，如图 2-10 所示，选择密码重置盘所在的驱动器，单击“下一步”按钮。

步骤 3：如图 2-11 所示，输入新的密码和密码提示，单击“下一步”按钮，完成密码重置工作。用户 Emily 就可用新密码登录了。

如果用户 Emily 既忘了自己密码又没有密码重置盘，可以让 Administrator 为其更改密码。更改账户密码的步骤为：以 Administrator 账户登录，在“计算机管理”→“本地用户和组”→“用户”列表中选择，右击 Emily 账户，选择“设置密码”菜单项，如图 2-12 所示，输入新密码即可。

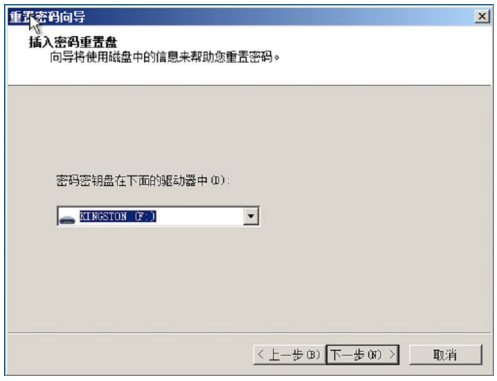

图 2-10　使用密码重置盘

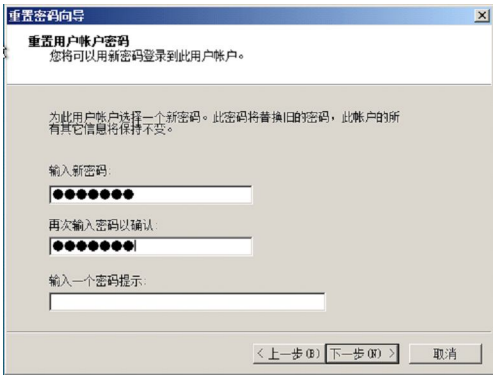

图 2-11　输入新密码

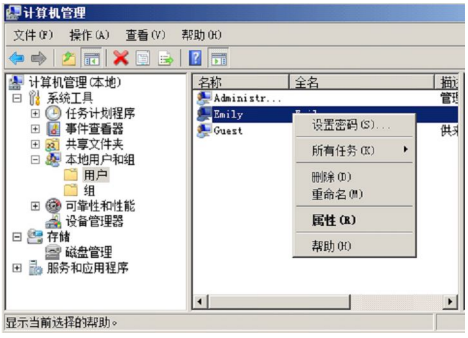

图 2-12　用 Administrator 重设账户密码

2.1.7　禁用与激活本地账户

当某个用户长期休假，就要禁用该用户的账户，不允许该账户登录。该账户信息会在计算机管理窗口中显示为“×”。禁用 Emily 账户的步骤如下：

右击 Emily 账户，选择“属性”，打开如图 2-13 所示的窗口，选择“账户已禁用”。如果要重新启用某账户，只要取消“账户已禁用”复选框即可。

图 2-13　禁用本地账户

【提示】为了安全起见，可以使用以上步骤把内置账户 Guest 禁用。

2.1.8 账户属性

账户的属性如图 2-14 所示，包括常规、隶属于、配置文件、环境、会话、拨入、终端服务配置文件和远程控制等项目。

图 2-14 账户属性

- “常规”选项卡主要设置用户名描述和密码期限的问题，见 2.1.7 节。
- “隶属于”选项卡设置用户所属组，通过“添加”按钮，将用户添加到合适的用户组中去。
- “配置文件”选项卡说明了用户每次登录系统时都使用的配置文件设置的桌面、控制面板设置、可用的菜单选项以及应用程序等。
- “拨入”选项卡和远程访问 VPN 的设置有关。
- “环境”、“会话”、“远程控制”和“终端服务配置文件”选项卡都和终端服务有关。具体配置见有关终端服务器配置的内容。

2.2 本地组

2.2.1 组的概念

组是账户、联系、计算机和其他组的集合。组用于以下目的：管理用户和计算机的访问，其访问范围包括网络对象、本地对象、共享、打印机队列和设备等；创建分配表；筛选组策略等。

Windows Server 2008 也使用唯一安全标识符 SID 来跟踪组。权限的设置都是通过 SID 设置的，不是利用组名。

2.2.2 组的类型

在 Windows Server 2008 独立服务器或成员服务器上的工作组称为本地组。该组的成员是本地账户，这些组账户的信息被存储在本地安全账户数据库（SAM）内。本地组有两种类型：用户组和系统内置的组。

2.2.3 创建本地组

创建本地组的用户必须是 Administrators 组、Account Operators 组的成员。例如在 Windows Server 2008 上建立本地组 wl 并将本地账户 Emily 添加到该组中，步骤如下：

步骤 1：以 Administrator 身份登录。

步骤 2：单击“开始”→“管理工具”→“计算机管理”→“本地用户和组”→“组”，右击“组”，选择“新建组”，如图 2-15 所示，打开“新建组”窗口。

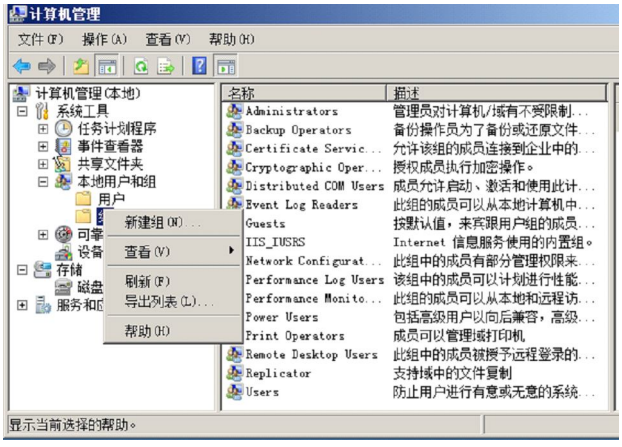

图 2-15　新建本地组

步骤 3：如图 2-16 所示，在“新建组”窗口中，输入组名、组的描述。

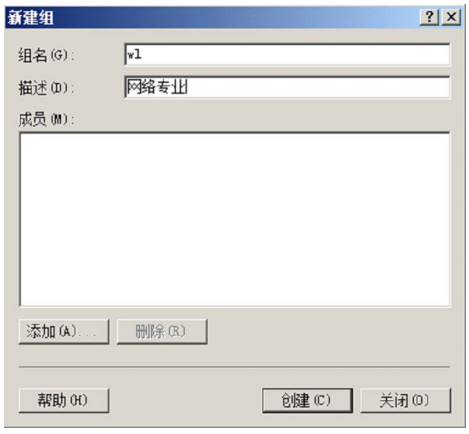

图 2-16　输入组名

步骤 4：如图 2-16 所示，单击“添加”按钮打开如图 2-17 所示的窗口，手工输入用户

名或者通过查找选择用户名，单击“确定”按钮。

步骤 5：回到如图 2-18 所示的窗口，单击“创建”按钮完成创建工作，本地组是用背景为计算机的两个人头像来表示。

图 2-17　选择用户

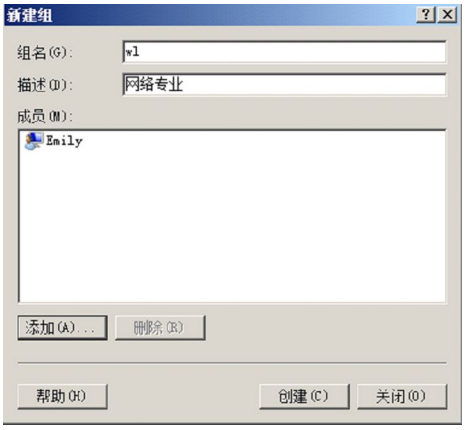

图 2-18　创建完毕

步骤 6：重复以上步骤，根据第 1 章 1.1.2 节的规划，为企业各部门创建组，并把各部门的账户加入到组中。

2.2.4　管理本地组

在“计算机管理”窗口右边的组列表中，用鼠标右击选定的组，如图 2-19 所示，选择菜单中的相应选项可以删除组、更改组名等。

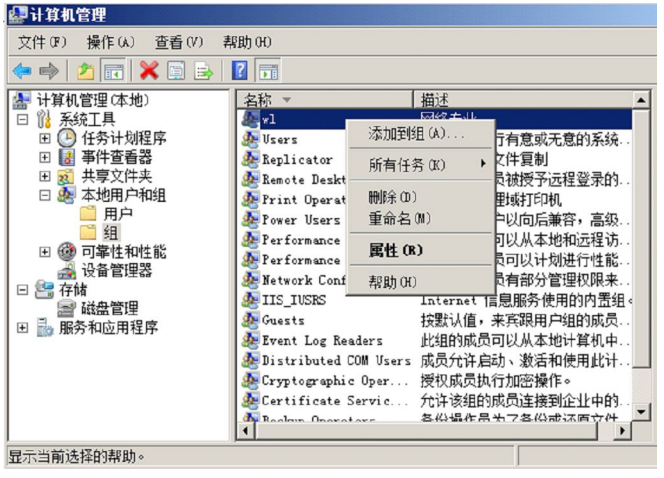

图 2-19　管理本地组

2.2.5　内置组

Windows Server 2008 在安装时会自动创建一些组，这种组叫内置组，如图 2-20 所示。内置组创建在 Windows Server 2008、Windows Server 2003/Windows 2000 Server/Windows NT

独立服务器或成员服务器、Windows Vista、Windows NT Workstation 等非域控制器的本地安全账户数据库中。这些组在建立的同时就已被赋予一些权力，以便管理计算机。

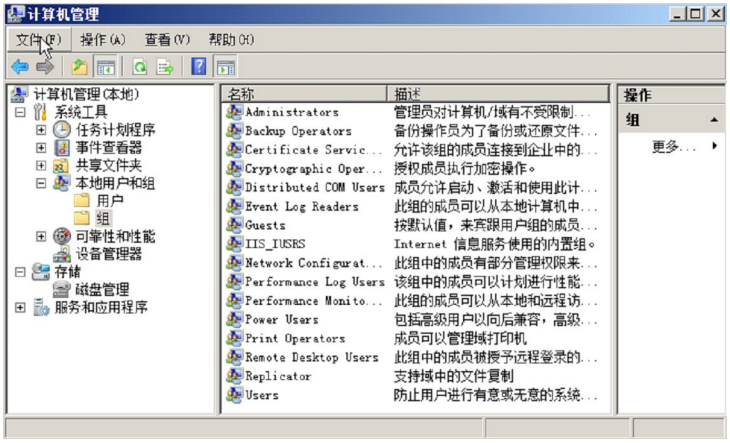

图 2-20　内置组

- Administrators：在系统内有最高权限，可以赋予权限；添加系统组件，升级系统；配置系统参数，如注册表的修改；配置安全信息等权限。内置的系统管理员账户是 Administrators 组的成员。如果这台计算机加入到域中，域管理员自动加入到该组，并且有系统管理员的权限。
- Backup Operators：该组的成员可以备份和还原服务器上的文件，而不管保护这些文件的权限如何。因为执行备份任务的权限高于所有文件权限。但是该组成员不能更改文件安全设置。该组成员的具体权限有通过网络访问此计算机；允许本地登录；备份文件和目录；跳过遍历检查；作为批处理登录；还原文件和目录；关闭系统。
- Cryptographic Operators：已授权此组的成员执行加密操作。
- Distributed COM Users：允许成员启动、激活和使用此计算机上的分布式 COM 对象。
- Guests：内置的 Guest 账户是该组的成员，该组的成员拥有一个在登录时创建的临时配置文件，在注销时，该配置文件被删除。
- IIS_IUSRS：这是 Internet 信息服务（IIS）使用的内置组。
- Network Configuration Operators：该组的成员可以更改 TCP/IP 设置并更新和发布 TCP/IP 地址。
- Performance Monitor Users：该组的成员可以从本地服务器和远程客户端监视性能计数器。
- Performance Log Users：该组的成员可以从本地或远程管理性能计数器、日志和警报。
- Power Users：存在于非域控制器上，可进行基本的系统管理；如共享本地文件夹、管理系统访问和打印机、管理本地普通用户；但是它不能修改 Administrators 组、Backup Operators 组，不能备份/恢复文件，不能修改注册表。
- Remote Desktop Users：该组的成员可以通过网络远程登录。
- Users：是一般用户所在的组，新建的用户都会自动加入该组；对系统有基本的权力，如运行程序，使用网络；不能关闭 Windows Server 2008；不能创建共享目录和

本地打印机。如果这台计算机加入到域，则域的用户自动被加入到该机的 Users 组。

本章首先介绍用户的分类，在 Windows Server 中用户包括本地账户和域账户（后面章节介绍）以及各种内置账户。本地账户对应工作组模式，只能在本地机运行；内置账户是为了方便管理系统而设置的账户。然后又介绍了如何管理不同账户，如：建立账户、删除账户、更改密码等。本章最后介绍了 Windows 组的概念以及对它的管理。组是权限相同的用户的集合，是为了方便管理这些权限相同的用户引入的概念。根据工作模式不同组分为本地组和域组。本章重点介绍本地组的创建和管理。本地组信息被存储在本地安全账户数据库（SAM）内。

一、理论习题

1．Windows Server 2008 本地账户存储在_____中；Windows Server 2008 内置账户中，默认被禁用的是_____。

2．下列哪个账户名不是合法的账户名？_____。

A．abc_123　　B．windows book

C．dictionar*　　D．abdkeofFHEKLLOP

3．本地账户的类型分为_____和_____。

4．用户忘记密码，该采取什么方式处置？

二、上机练习项目

1．项目 1：在独立或成员服务器上建立本地组 Group_test、本地账户 User1，把 User1 加入到 Group_test 组中；设置 User1 用户下次登录时要修改密码。

2．项目 2：用项目 1 建立的账户 User1 登录，修改密码。