

第 3 章

CHAPTER

Windows Server 2003 账户
和组的管理

本章知识要点:

- 本地账户管理;
- 本地组的管理;
- 域账户的管理;
- 域模式中组的管理;
- 用户配置文件的创建和使用。

3.1 本地账户管理

本地用户账户是指在本机计算机中建立的账户。

3.1.1 本地账户的创建

在 Windows Server 2003 中,管理员可以使用“本地用户和组”管理工具创建用户账户并为其设置访问权限。下面介绍本地用户账户的创建步骤。

(1) 在桌面上右击“我的电脑”图标,在弹出的快捷菜单中选择“管理”命令,打开“计算机管理”窗口,如图 3-1 所示。

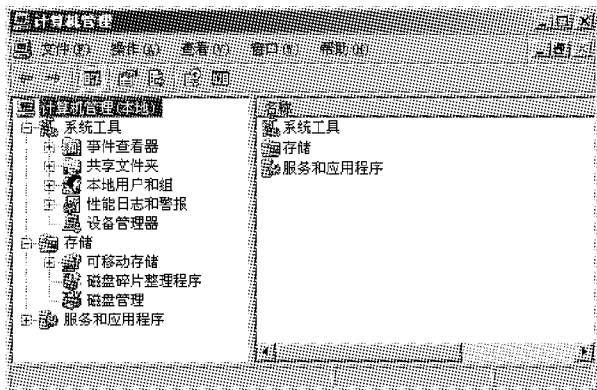


图 3-1 “计算机管理”窗口

(2) 在树形目录中双击展开“本地用户和组”，选择“用户”，在右边的窗格中显示系统中已有用户账户的列表，如图 3-2 所示。

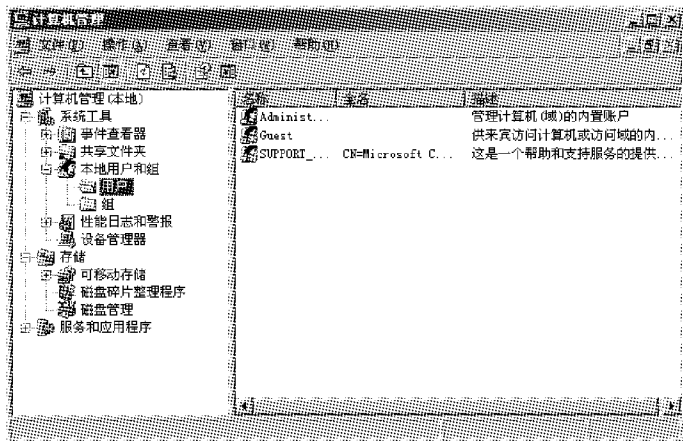


图 3-2 用户账户列表

(3) 右击“用户”或在右边窗格的空白处右击，在弹出的快捷菜单中选择“新用户”命令，如图 3-3 所示。

(4) 弹出“新用户”对话框，设置“用户名”和“密码”等参数，如图 3-4 所示。



图 3-3 选择“新用户”



图 3-4 “新用户”对话框

在如图 3-4 所示的“新用户”对话框中，对以下选项作简要说明。

① “用户名”文本框：最好使用英文或拼音，在“全名”和“描述”中可以输入一些说明信息，有助于快速识别该账户。

② “用户下次登录时须更改密码”复选框：如果选中此复选框，则要求用户在下次登录时必须设置一个新的密码。

③ “用户不能更改密码”复选框：选中此复选框，则用户不能更改密码，通常用于设置一些公共账户。

④ “密码永不过期”复选框：默认情况下，用户密码的使用期限是 42 天，如果不希望定期更改密码，可以选中此复选框。

⑤ “账户已禁用”复选框：如果一个用户暂时(或永久)不使用这台计算机,可以将其账户暂时禁用。尽量不要删除账户,因为在创建用户账户时,系统会为每个用户账户分配一个 SID,这个 SID 称为“安全的标识符”,用于唯一标识一个对象。系统创建的每一个 SID 都不能重复。当删除了一个账户后,即使再重新建立一个同名的账户,因为 SID 不一样,系统也会认为这两个账户是不同的账户,这使新的用户账户不能正常访问原来的账户可以访问的资源。所以,对于不用的账户,尽可能选择禁用(停用)账户而不是删除账户。

(5) 单击“创建”按钮,在计算机管理控制台中将能够看到新创建的用户账户,如图 3-5 所示。

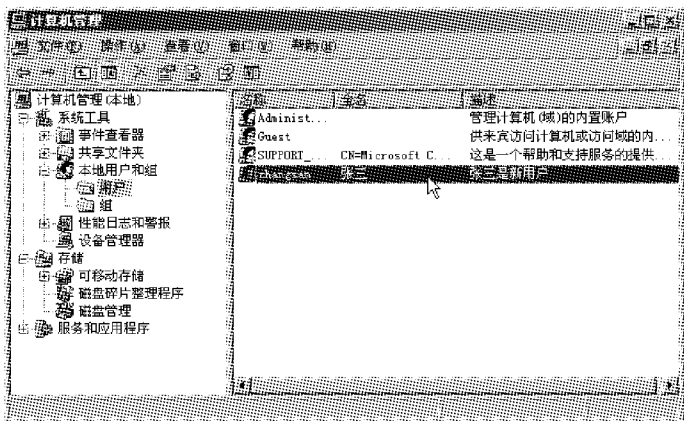


图 3-5 成功创建一个用户账户

3.1.2 本地账户属性设置

创建完本地账户后,下面介绍如何设置本地账户属性。

(1) 在计算机管理控制台的一个用户账户上右击,弹出如图 3-6 所示的快捷菜单。

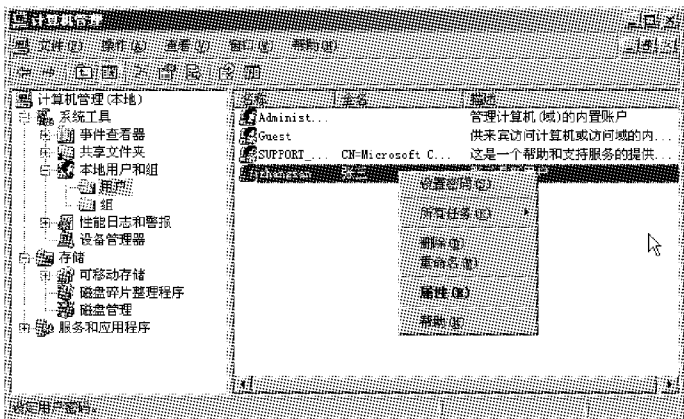


图 3-6 右击用户账户

(2) 在快捷菜单中选择“设置密码”命令,可以更改当前用户账户的密码;选择“删除”或“重命名”命令可以删除当前用户账户或更改当前用户账户的名称;选择“属性”命令,将会弹出该账户的属性对话框,如图 3-7 所示。

下面对属性对话框的“常规”选项卡中的一些选项作简要说明。

① “全名”文本框:用于输入用户的全名。这里可以为用户设置一个中文名称,以方便识别。

② “描述”文本框:用于输入用户的描述信息,如部门、职位等,可以用中文。

③ “账户已锁定”复选框:当用户输错一定次数的密码时账户会被锁定。用户账户被锁定后,用户将不能登录系统。使用管理员账户登录系统后取消该选项即可解除锁定。

(3) 属性对话框的“隶属于”选项卡如图 3-8 所示。

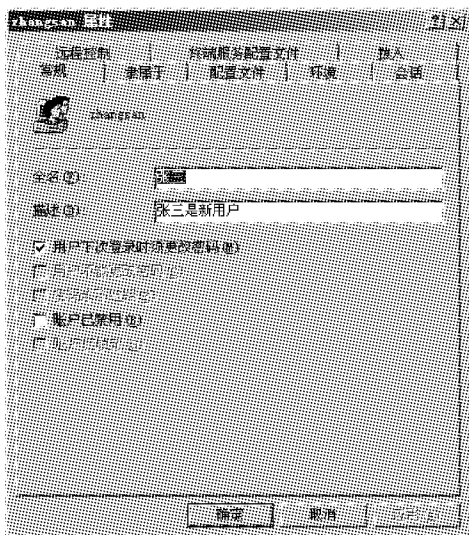


图 3-7 用户账户的属性对话框



图 3-8 “隶属于”选项卡

在“隶属于”选项卡中单击“添加”按钮,弹出“选择组”对话框,如图 3-9 所示。

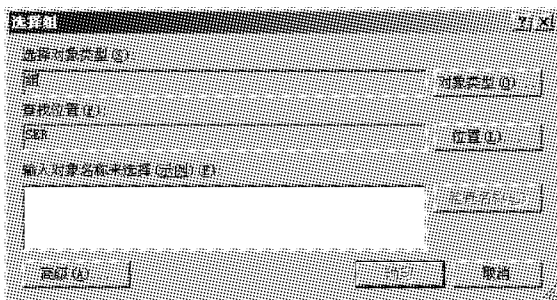


图 3-9 “选择组”对话框

(4) 单击“高级”按钮,然后单击“立即查找”按钮,在“搜索结果”列表框中选择要添加的组,如图 3-10 所示,单击“确定”按钮,则使用户隶属于新添加的组。



图 3-10 选择要添加的组

3.2 本地组的管理

组账户是具有相同权限的用户账户的集合。组账户可以对组内的所有用户赋予相同的权利和权限。在安装 Windows Server 2003 操作系统时会自动创建一些内置的组,即默认本地组。下面介绍 Windows Server 2003 中的默认本地组。

① Administrators 组: 该组的成员对服务器有完全控制权限, 可以为用户指派用户权利和访问控制权限。

② Guests 组: 该组的成员拥有一个在登录时创建的临时配置文件。“来宾”账户(默认为禁用)也是 Guests 组的默认成员。

③ Power Users 组: 该组的成员可以创建本地组并在已创建的本地组中添加或删除用户, 还可以在 Users 组和 Guests 组中添加或删除用户。

④ Users 组: 该组的成员可以运行应用程序、使用本地和网络打印机以及锁定服务器。但该组成员不能共享目录或创建本地打印机。

在 Windows Server 2003 系统中, 管理员可以用以下几步创建组账户。

(1) 在如图 3-2 所示的“计算机管理”窗口, 右击“本地用户和组”中的“组”选项, 在弹出的快捷菜单中选择“新建组”命令。

(2) 在弹出的“新建组”对话框的“组名”文本框中输入组名(最好使用英文字符, 以便管理), 在“描述”文本框中输入一些描述信息以便识别该组(描述信息可以使用中文), 如图 3-11 所示。

(3) 单击“添加”按钮,弹出“选择用户”对话框,如图 3-12 所示。

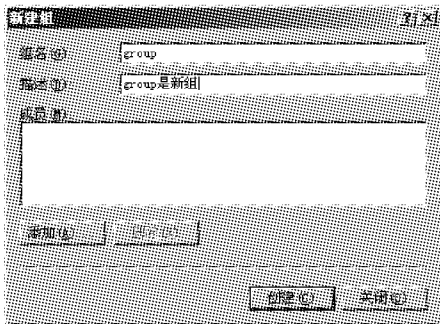


图 3-11 “新建组”对话框

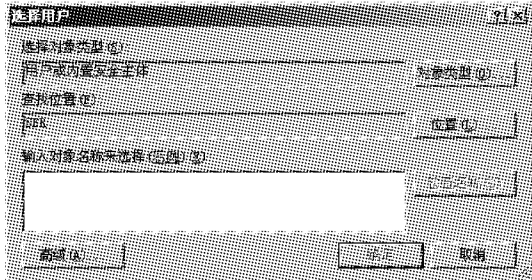


图 3-12 “选择用户”对话框

(4) 单击“高级”按钮,然后单击“立即查找”按钮,在“搜索结果”列表框中选择一个用户账户,如图 3-13 所示。



图 3-13 选择一个用户账户

注意: 按住 Ctrl 键的同时依次单击要选择的用户,可以同时选择多个用户。

(5) 单击“确定”按钮,选中的用户显示在“输入对象名称来选择”列表框中,如图 3-14 所示。

(6) 单击“选择用户”对话框中的“确定”按钮,即可在组中添加选择的用户,如图 3-15 所示。

注意: 可以向本地组添加本地用户账户、域用户账户、计算机账户以及组账户,但不能向域组账户添加本地用户账户和本地组账户。

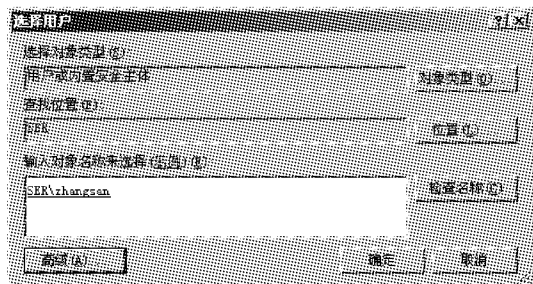


图 3-14 显示选择的用户账户

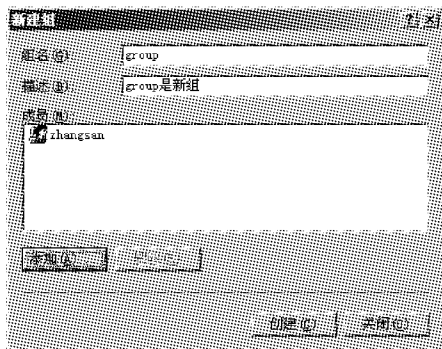


图 3-15 在组中添加选中的用户

3.3 域账户的管理

域用户账户是使用网域用户账户注册的用户。它必须在域控制器上建立,并且作为活动目录的一个对象保存在域的活动目录数据库中。域用户账户信息被复制到其他网域控制器中,因此它可以使用网域上的资源。

域用户账户保存在 Active Directory(活动目录)数据库中,该数据库位于在域控制器上的\%systemroot%\NTDS 文件夹下。为了保证账户在域中的唯一性,每一个账户都被 Windows Server 2003 签订一个唯一的安全识别符(Security Identifier, SID)。SID 将成为一个账户的属性,不随账户的修改、更名而改动,即便重新创建一个一模一样的账户,其 SID 也不会和原有的一样,对于 Windows Server 2003 而言,这就是两个不同的账户。在 Windows Server 2003 中系统实际上是利用 SID 来对应用户权限的,因此只要 SID 不同,新建的账户就不会继承原有账户的权限与组的隶属关系。

3.3.1 创建域用户

创建域用户账户一般是在域控制器中进行的,包括以下几步。

(1) 选择“开始”→“控制面板”→“管理工具”→“Active Directory 用户和计算机”命令,打开“Active Directory 用户和计算机”窗口。在该窗口左边的列表框中展开本机中新创建的 Active Directory(这里是 wjphist.com),右击 User,在弹出的快捷菜单中选择“新建”→User 命令,如图 3-16 所示。

注意: 也可在启动 Windows Server 2003 操作系统时,在弹出的“管理您的服务器”对话框中单击“管理 Active Directory 中的用户和计算机”按钮,打开“Active Directory 用户和计算机”窗口。

(2) 选择“新建”→User 命令后,弹出“新建对象-User”对话框。在该对话框中输入姓名和登录名等相关信息,如图 3-17 所示。

(3) 输入完成后,单击“下一步”按钮,弹出安全设置对话框,在此进行密码设置等,如图 3-18 所示。



图 3-16 “Active Directory 用户和计算机”窗口



图 3-17 “新建对象-User”对话框

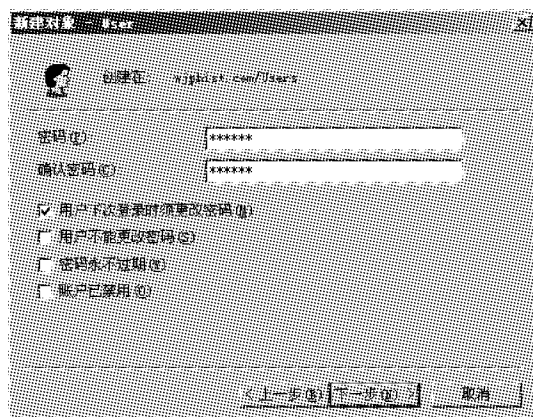


图 3-18 进行安全设置

(4) 需要注意的是,为了域用户账户的安全,在给每个用户设置初始化密码后,最好选中“用户下次登录时须更改密码”复选框,以使用户在第一次登录时更改自己的密码。在服务器提升为域控制器后,Windows Server 2003 对域用户的密码复杂性要求比较高,如果不符合要求,就会提示用户无法创建,如图 3-19 所示。

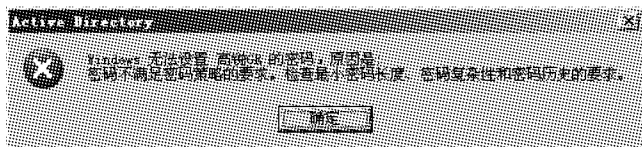


图 3-19 提示密码不符合要求

(5) 符合域控制器安全性密码设置条件设置完成后,单击“下一步”按钮,弹出如图 3-20 所示的对话框。单击“完成”按钮,即完成对域用户的创建。



图 3-20 完成域用户的创建

3.3.2 设置域用户属性

域账户的属性设置相对本地用户的属性来说要复杂得多。下面以前面新创建的账户为例,讲解如何设置域账户属性。

(1) 在“Active Directory 用户和计算机”窗口中,展开 User,在右侧窗格中右击“高锐 GR”,在弹出的快捷菜单中选择“属性”命令,弹出“高锐 GR 属性”对话框,如图 3-21 所示。在“高锐 GR 属性”对话框中,可以看见有“常规”、“地址”、“账户”、“配置文件”、“电话”等多个选项卡。

(2) 在“常规”选项卡中,可以修改姓、名、显示名称等信息。在如图 3-22 所示的“账户”选项卡中,可以设置登录名、账户策略等信息。在“账户”选项卡中,可以控制用户的登录时间和只能登录哪些服务器或计算机。

(3) 单击“登录时间”按钮,可在如图 3-23 所示的对话框中设置登录时间(图中横轴每个方块代表一小时,纵轴每个方块代表一天,蓝色方块表示允许用户使用的时间,空白方块表示该时间不允许用户使用,默认为在所有时间均允许用户使用)。

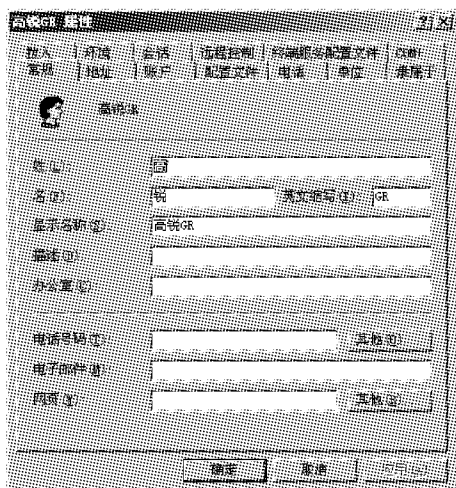


图 3-21 “高锐 GR 属性”对话框

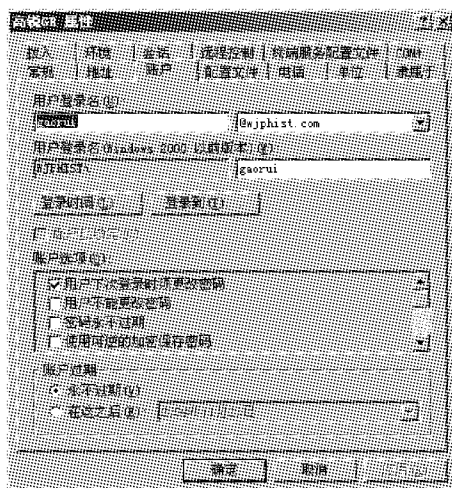


图 3-22 “账户”选项卡

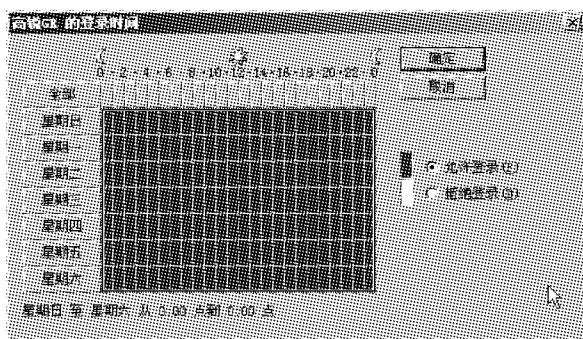


图 3-23 设置登录时间

(4) 在“账户”选项卡中,通过单击“登录到”按钮,可在弹出的对话框中控制用户只能登录哪些服务器或计算机,如图 3-24 所示。

(5) 在如图 3-25 所示的“隶属于”选项卡中,单击“添加”按钮,可以将该用户添加到组。

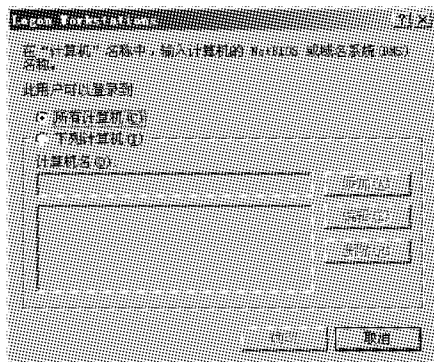


图 3-24 可以登录哪些服务器或计算机



图 3-25 “隶属于”选项卡