

第 2 章 本地用户和组的管理

[单元概述]

本地用户和组的管理是 Windows 系统管理中最基础的管理。本章通过配置与管理本地用户账户与组的项目,使学习者了解 Windows Server 2003 的本地用户和组的命名规则、密码策略等特点,掌握本地用户和组的管理操作方法。

[知识要点及掌握程度]

- 用户和组的特点(理解)
- 本地用户的管理(运用)
- 本地组的管理(运用)

[单元重点与难点]

重点:本地用户和组的管理。

难点:赋予特殊本地组权限。

东软电子出版社

2.1 项目概述

2.1.1 项目背景

创想科技发展有限公司成立后,公司员工随意设置用户账户,且不为账户设置密码,造成公司重要资料外泄,影响了公司业务发展。公司规划用一台服务器来存储业务资料,并要严格设置用户权限,加强管理。系统管理员首先需要统一规划各部门员工账户,划分不同部门组,为分配资源访问权限做好准备。

2.1.2 项目环境和条件

- (1)网络环境;
- (2)安装 Windows XP Professional 或 Windows Vista、Windows 7 的计算机作为客户机;
- (3)安装 Windows Server 2003 计算机作为服务器。

2.1.3 项目目标

- (1)根据企业需求,规划并设置本地用户账户。
- (2)根据企业需求,规划并设置用户所属本地组。

2.1.4 项目需求

公司有多个部门,员工若干,根据员工所属部门分组管理,并统一员工账户设置规则。为了安全,员工首次登录时须更改默认密码,并设置密码策略,密码位数 8 位以上,且密码不能过于简单。密码错误输入最多 3 次,超过 3 次将被计算机锁住 5 分钟。如果用户忘记密码,希望可以进行密码重设。员工或部门有变化时,需相应调整用户和组的设置,原则上离职员工的账户需要删除。技术部门的个别用户拥有服务器关机权限。

2.2 配置与管理本地用户账户与组

2.2.1 项目构思与设计

1. 项目构思

分析企业需求,了解到该项目需求涉及到多项技术知识:

- (1)创建用户和组;
- (2)规划账户设置规则,配置账户锁定策略;

- (3) 密码重设机制；
- (4) 员工部门变化时要调整相应用户和组的设置；
- (5) 设置特殊组，赋予服务器关机权限，将特殊用户加入该组。

2. 项目设计

根据项目构思，分解相关技术知识点，分步骤完成总体项目，项目设计内容如下：

(1) 统一规划用户账户命名规则，用户姓全拼+名首字母组合。创建组，一个部门为一组，并将各部门用户归入各部门组中；

(2) 创建新用户设置密码要求，应用密码策略（启用密码复杂性要求、最短密码长度为 8）。配置账户锁定策略（锁定阈值为 3 次，锁定时间为 5 分钟），增加安全性；

- (3) 设置密码重设盘，方便恢复更改登录密码；
- (4) 管理用户和组，修改所属组和删除离职用户等；
- (5) 设置特殊组 specials，赋予服务器关机权限，将技术部门特殊用户 tom 加入该组。

2.2.2 创建用户账户与组

1. 创建用户账户

为满足公司每位员工都需要访问服务器的需求，系统管理员首先需要为每位员工创建用户账户。用户账户是用户登录到某台计算机访问该机上的资源或登录到域访问网络资源的标识，包括账户名和密码。账户名的命名规则如下。

- (1) 账户名必须唯一，而且不区分大小写；
 - (2) 最多可以包含 20 个大小写字符和数字，但不能包含下列字符：`" / \ [] : ; | = , + * ? < > ;`；
 - (3) 不能只由句点（.）和空格组成；
 - (4) 不能与组名相同。
- 在设置用户账户密码时，需要遵循以下原则。

- (1) Administrator 账户必须设置密码以防止使用空白密码的该账户被非法使用；
- (2) 在密码属性中可以设置用户账户首次登录时自行更改密码；
- (3) 尽量使用难以猜测的密码组合；
- (4) 尽量使用大小写字母、数字和合法的非数字字母组合的强密码，增加破译难度。

Windows Server 2003 的用户账户有以下三种类型。

- (1) 本地账户。

本地账户建立在本地，且只能在本地计算机上登录。所有本地用户账户信息都存储在本地计算机上管理本地账户的数据库中，该数据库称为 SAM (Security Accounts Managers, 安全账户管理器)，其路径为 `%systemroot%\system32\config\SAM`。每个用户账户被创建完成后，系统都会自动产生一个唯一的 SID (Security Identifier, 安全标识符)。系统验证用户访问、指派权利以及授权资源访问权限等都需要使用 SID。在命令提示符下使用“`whoami /logonid`”命

令,可以查询当前用户账户的 SID,如图 2-1 所示。



图 2-1 查询当前用户账户的 SID

(2) 域账户。

域账户建立在域控制器上,用户可以利用域账户登录到域来访问域内资源。

注意:域账户将在第 7 章介绍,本章主要介绍本地用户账户。

(3) 内置账户。

Windows Server 2003 安装完毕后,系统会在服务器上自动创建一些内置账户。常用的内置账户有 Administrator 和 Guest。Administrator(系统管理员)具有最高权限,可以更改其名字,不能被删除,但可以被禁用。Guest(来宾)是为临时访问计算机的用户提供的。该账户默认情况下是被禁用的,只具有很少的权限,可以更改其名字,但不能被删除。

下面介绍创建本地用户账户的具体操作过程。

步骤 1:选择“开始→管理工具→计算机管理→本地用户和组”选项,在弹出的“计算机管理”窗口中,右击“用户”,在出现的菜单中选择“新用户”命令,如图 2-2 所示。

步骤 2:在弹出的“新用户”对话框中,输入用户名、全名、描述、密码等信息,并选择“用户下次登录时须更改密码”,如图 2-3 所示。

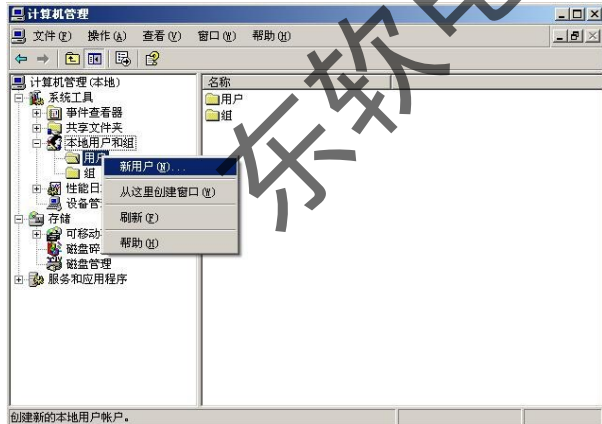


图 2-2 “计算机管理”窗口



图 2-3 “新用户”对话框

说明:“新用户”对话框中各密码选项介绍。

用户下次登录时须更改密码:用户在下次登录时,系统会强制用户更改密码。更改后的密码只有用户自己知道,可以保证安全使用。

用户不能更改密码:不允许用户自行更改密码,比较适用于多个用户共用一个用户账户。

密码永不过期:密码永久有效,系统不会要求该用户更改密码。

账户已禁用:无法使用该账户进行登录。

步骤 3:单击“创建”按钮,完成用户账户创建工作。

步骤 4:重复步骤 2 和步骤 3,为企业每个员工创建用户账户。

新建的用户 zhangm 在第一次登录时,系统提示要求更改用户密码。

2. 创建组

系统管理员为每位员工创建了本地用户账户后,还需要为每一个部门创建一个组,以便根据员工所属部门进行分组管理。组是具有相同权限的用户账户的集合,通过组可以管理用户和计算机对共享资源的访问。如果赋予某个组访问某个资源的权限,那么属于该组的用户账户就具有相同的权限。组的命名规则如下。

(1)本地组名不能与被管理的本地计算机上任何其他组名或用户名相同。

(2)组名最多可以包含 256 个大小写字符,但不能包含下列字符:" / \ [] : ; | = , + * ? < >。

(3)组名不能只由句点(.)和空格组成。

Windows Server 2003 的组有以下三种类型。

(1)本地组。

本地组建立在本地,且只能在本地计算机上使用。本地组的信息也被存储在 SAM 内。只有 Administrators 组或 Account Operators 组的成员才能创建本地组。

(2)域组。

域组建立在域控制器上,能够被使用在整个域的计算机上。

注意:域组将在第 7 章介绍,本章主要介绍本地组。

(3)内置组。

Windows Server 2003 安装时会自动创建一些组,这种组叫内置组。常用的内置本地组列表及说明如表 2-1 所示。

表 2-1

常见内置本地组列表及说明

组名	描述信息
Administrators	该组的成员具有对服务器的完全控制权限,并且可以为其他用户分配用户权利和访问控制权限。管理员账户 Administrator 就是这个组的默认成员
Backup Operators	该组的成员可以备份和还原服务器上的所有文件
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
Power Users	该组的成员具有创建用户账户和组账户的权利,可以在 Power Users 组、Users 组和 Guests 组中添加或删除用户,但是不能管理 Administrators 组成员。可以创建和管理共享资源
Print Operators	该组的成员可以管理打印机
Users	该组的成员可以执行一些常见任务,例如运行应用程序、使用本地和网络打印机以及锁定服务器。用户不能共享目录或创建本地打印机

注意:内置组分为内置本地组和内置域组。内置域组将在第 7 章介绍,本章主要介绍内置本地组。

下面介绍创建本地组的具体操作过程。

步骤 1:选择“开始→管理工具→计算机管理→本地用户和组”选项,在弹出的“计算机管理”窗口中右击“组”,在出现的菜单栏中选择“新建组”,如图 2-4 所示。

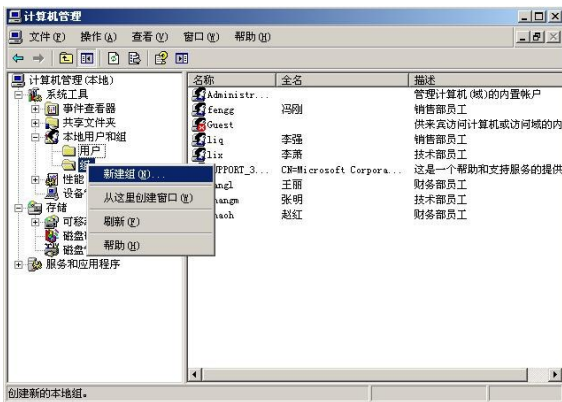


图 2-4 创建本地组



图 2-5 “新建组”对话框

步骤 2:在弹出的“新建组”对话框中,输入组名、描述,并单击“添加”按钮将本部门员工账户添加到本部门组中,如图 2-5 所示。

说明:多个用户账户访问相同资源时,推荐使用 ALP 规则。ALP(Accounts Localgroup Permission)是用户账户、本地组和权限的英文简称。ALP 规则就是将具有相同属性的用户账户加入到同一个本地组中,再针对某些资源赋予这个本地组相应的访问权限。

步骤 3:单击“创建”按钮,完成组的创建工作。

步骤 4:重复步骤 2 和步骤 3,为其他部门创建相应组。

2.2.3 配置密码与账户锁定策略

1. 配置密码策略

用户密码的安全是计算机系统安全的基础,如果用户账户特别是系统管理员账户没有设置密码或密码设置过于简单,那么该计算机就很容易被非法登录,进而被访问资源或更改系统设置。因此,设置合适的密码并配置密码策略对保证系统的安全是很重要的。

系统管理员根据企业各部门及其员工信息创建了用户账户和组之后,就需要配置密码策略。下面介绍配置密码策略的具体操作过程。

步骤 1:点击“开始→管理工具→本地安全策略”,在弹出的“本地安全设置”窗口中选择“账户策略→密码策略”,如图 2-6 所示。

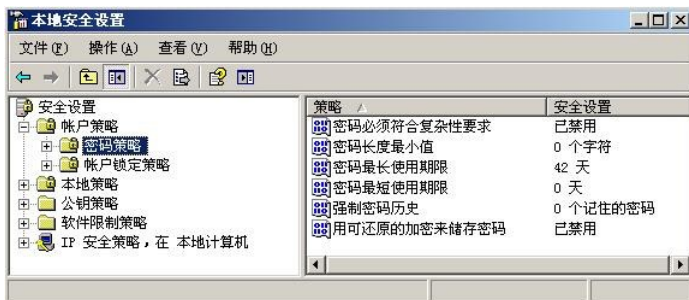


图 2-6 “本地安全设置”窗口

步骤 2: 双击“本地安全设置”窗口右侧策略列表中的“密码必须符合复杂性要求”，在弹出的对话框中选择“已启用”，如图 2-7 所示，然后单击“确定”按钮使配置更改生效。

步骤 3: 双击“本地安全设置”窗口右侧策略列表中的“密码长度最小值”，在弹出的对话框中将密码长度最小值设为“8”，如图 2-8 所示，然后单击“确定”按钮使配置更改生效。

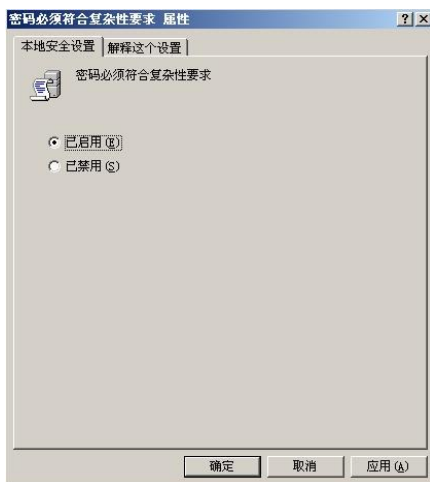


图 2-7 启用密码复杂策略

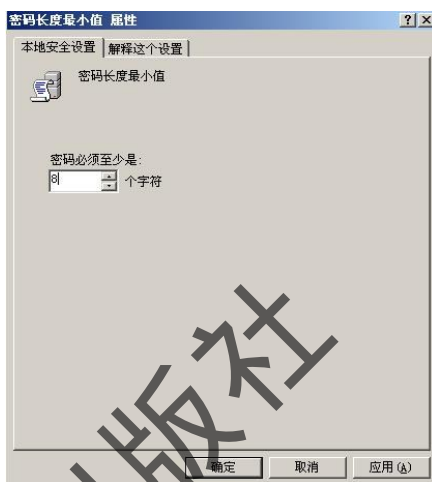


图 2-8 设置密码长度最小值

2. 密码策略的应用

启用了密码复杂度策略后，密码必须符合下列最低要求：

- (1) 不能包含用户的账户名，不能包含用户姓名中超过两个连续字符的部分；
- (2) 至少有 6 个字符长；
- (3) 包含以下四类字符中的三类字符：
 - ① 英文大写字母(A 到 Z)
 - ② 英文小写字母(a 到 z)
 - ③ 10 个基本数字(0 到 9)
 - ④ 非字母字符(例如 !, \$, #, % 等)
- (4) 在更改或创建密码时执行复杂性要求。

如此，企业所有员工配置的用户账户密码不符合以上要求时系统会提示错误，从而保证了系统安全性。

3. 配置账户锁定策略

在默认情况下，Windows Server 2003 没有对账户锁定策略进行设定。这样通过自动登录工具和密码猜解字典等方式很容易对系统进行攻击。为了保证系统的安全，最好设置账户锁定策略。

系统管理员在“本地安全设置”窗口中设置完密码策略后，接着就可以设置账户锁定策略。下面将介绍账户锁定策略的具体操作过程。

步骤 1: 在“本地安全设置”窗口中选择“账户锁定策略”，如图 2-9 所示，然后双击窗口右侧策略列表中的“账户锁定阈值”，在弹出的对话框中将账户锁定阈值设为“3”，如图 2-10 所示，然后单击“确定”按钮使配置更改生效。

步骤 2: 双击“本地安全设置”窗口右侧策略列表中的“账户锁定时间”，在弹出的对话框中

将账户锁定时间设为“5”分钟,如图 2-11 所示,然后单击“确定”按钮使配置更改生效。



图 2-9 账户锁定策略



图 2-10 设置账户锁定阈值



图 2-11 设置账户锁定时间

4. 账户锁定策略的应用

启用了此账户锁定策略后,如果用户 3 次登录失败,系统将自动锁定这个账户 5 分钟以避免有人使用列举密码方法尝试登录系统,保证了系统安全。

2.2.4 设置密码重设盘

1. 制作密码重设盘

系统管理员为了保证系统安全性已经启用了密码策略,因此所有企业用户的用户账户密码难免会比较复杂。这就很容易出现忘记密码而无法进入系统的情况。如果由系统管理员重设密码可能会造成不可逆的信息丢失,因此员工在平常使用时就应该自行制作密码重设盘以备忘记登录密码时使用。下面介绍密码重设盘的具体制作过程。

步骤 1: 用户登录后按【Ctrl+Alt+Delete】,然后单击“更改密码→备份”,弹出“密码忘记向导”对话框,如图 2-12 所示,单击“下一步”按钮继续。

步骤 2: 根据提示插入一张空白并格式化的软盘,单击“下一步”按钮。

步骤 3: 输入当前用户账户密码,如图 2-13 所示,单击“下一步”按钮以创建密码重置磁盘。

步骤 4: 单击“下一步”按钮,再单击“完成”按钮,当前用户的密码重设盘创建完成。

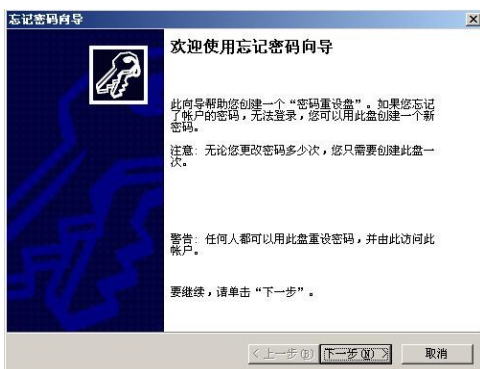


图 2-12 “忘记密码向导”对话框



图 2-13 输入当前用户账户密码

2. 应用密码重设盘

市场部员工李强忘记了其用户账户密码,他可以应用之前制作的密码重设盘来重新设置密码。下面将介绍如何应用密码重设盘来重新设置密码。

步骤 1: 李强用其用户账户登录时输入错误密码,系统将显示“登录失败”窗口。单击“重设”按钮,如图 2-14 所示,弹出“重设密码向导”对话框,单击“下一步”按钮继续。

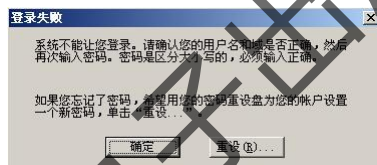


图 2-14 “登录失败”窗口

步骤 2: 根据提示插入密码重设盘,如图 2-15 所示,然后单击“下一步”按钮继续。

步骤 3: 如图 2-16 所示,输入新密码及密码提示,然后单击“下一步”按钮继续。

步骤 4: 单击“完成”按钮,密码重设向导完成。李强可以使用刚刚重设的密码进行登录了。

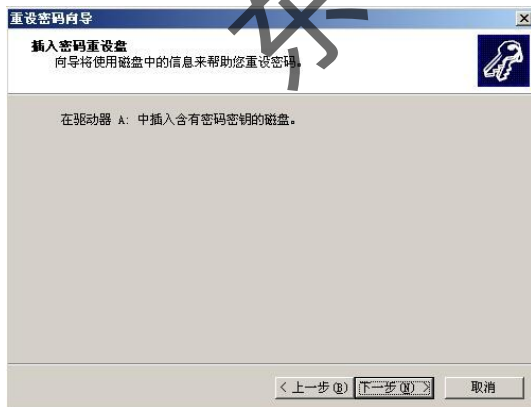


图 2-15 插入密码重设盘



图 2-16 重设用户账户密码

2.2.5 管理操作

1. 修改用户账户所属组

由于工作需要,技术部员工李萧要调到市场部,那么就需要修改其账户所属组。具体操作过程如下。

步骤 1:选择“开始→管理工具→计算机管理→本地用户和组”选项,在弹出的“计算机管理”窗口中,右击要修改的账户名 lix,选择“属性”,如图 2-17 所示。

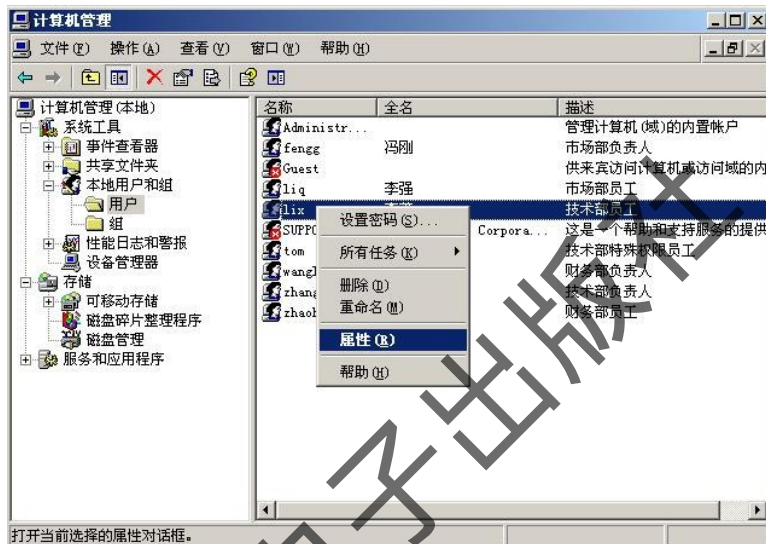


图 2-17 修改用户账户属性

步骤 2:在“lix 属性”对话框的“常规”选项卡中修改员工描述信息,如图 2-18 所示。

步骤 3:在“lix 属性”对话框的“隶属于”选项卡中,选中原所属部门组 jishubu,然后单击“删除”,再单击“添加”按钮添加调入部门组 shichangbu,如图 2-19 所示,然后单击“确定”按钮使配置更改生效。



图 2-18 修改用户账户描述信息



图 2-19 修改用户账户所属组

2. 添加用户账户到组

技术部来了一个新员工刘明,系统管理员为其创建了用户账户后,需要将其用户账户添加到相应所在技术部门组 jishubu。具体操作过程如下。

步骤 1:选择“开始→管理工具→计算机管理→本地用户和组”选项,在弹出的“计算机管理”窗口中,右击要加入的部门组 jishubu,然后单击“添加到组”,如图 2-20 所示。

步骤 2:在弹出的“jishubu 属性”对话框中,单击“添加”按钮将新员工账户 lium 添加到 jishubu 组成员列表中,如图 2-21 所示。

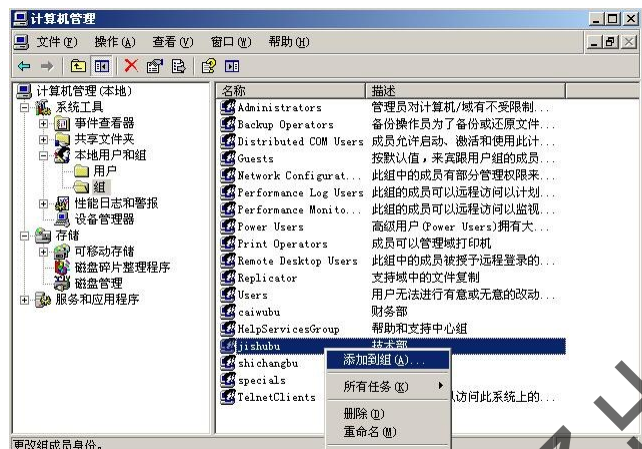


图 2-20 添加到组



图 2-21 添加用户账户

3. 删除用户账户

财务部员工赵红离职了,系统管理员需要将其用户账户删除。下面简要介绍删除用户账户的操作过程。

选择“开始→管理工具→计算机管理→本地用户和组”选项,在弹出的“计算机管理”窗口中,右击要删除的用户账户 zhaoh,然后单击“删除”按钮,如图 2-22 所示。单击“是”按钮,确认删除操作。

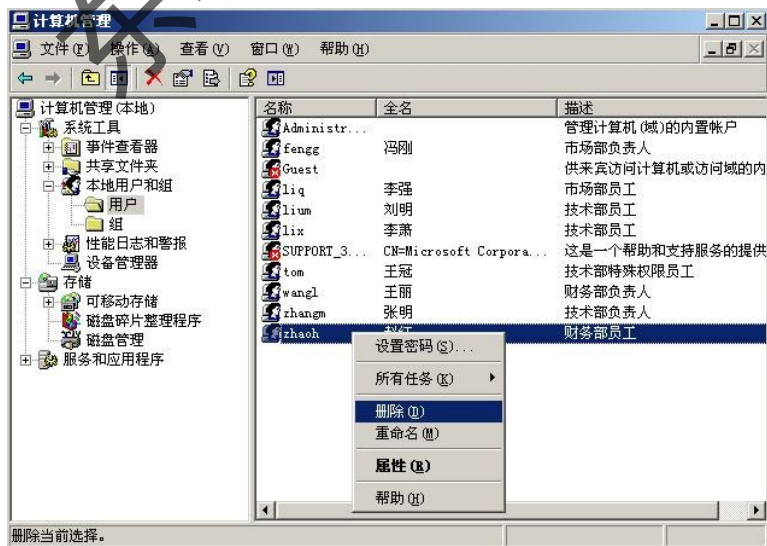


图 2-22 删除用户账户

说明:因为每个用户账户的SID都是唯一的,所以当删除一个用户账户后,即使重新创建名称相同的账户也不能获得之前账户的权利。

4. 重设用户账户密码

市场部员工李萧忘记了其用户账户密码又没有密码重设盘,系统管理员需要为其重设密码。下面介绍重设用户账户密码的具体操作过程。

步骤 1:选择“开始→管理工具→计算机管理→本地用户和组”选项,在弹出的“计算机管理”窗口中,右击要更改密码的用户账户 lix,然后单击“设置密码”,如图 2-23 所示。

步骤 2:在弹出的警告对话框中,单击“继续”按钮继续。

步骤 3:在弹出的“设置密码”对话框中输入新密码,如图 2-24 所示,然后单击“确定”按钮以确认更改。

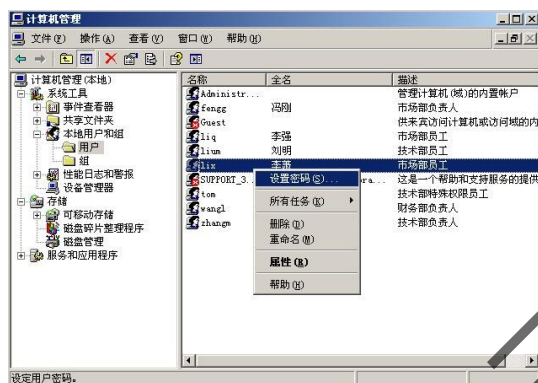


图 2-23 重设密码

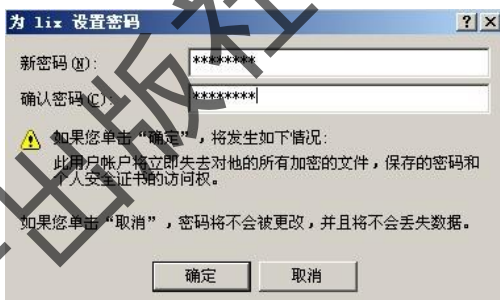


图 2-24 输入新密码

5. 删除组

公司在成立之初设置了一个研发部以专门负责新技术研发工作。刚刚召开了董事会,会上经各股东商议决定原研发部工作合并到技术部,不再单独设置研发部。系统管理员需要先修改用户账户所属组,然后再删除研发部组,下面简要介绍删除组的操作过程。

选择“开始→管理工具→计算机管理→本地用户和组”选项,在弹出的“计算机管理”窗口中,右击要删除的组 yanfa,然后单击“删除”按钮,如图 2-25 所示。单击“是”按钮,确认删除操作。



图 2-25 删除组

说明:与用户账户一样,每个组也都有一个唯一的 SID。当删除一个组后,即使重新创建一个名称相同、成员也相同的组,也不会与之前被删除的组有相同的特性和特权。管理员只能删除新增的组,不能删除系统内置组。

2.2.6 设置特殊权限

1. 创建特殊组

参考 2.2.2 节创建特殊组 specials,并将技术部门特殊用户 tom 加入该组。

2. 赋予特殊权限

为避免普通权限用户误操作,关闭计算机而影响企业关键业务系统的正常运行,系统管理员只为特殊组 specials 分配了关闭服务器的权限。下面介绍分配关机权限的具体操作过程。

步骤 1:点击“开始→管理工具→本地安全策略”,在弹出的“本地安全设置”窗口中选择“本地策略→用户权限分配”,如图 2-26 所示。

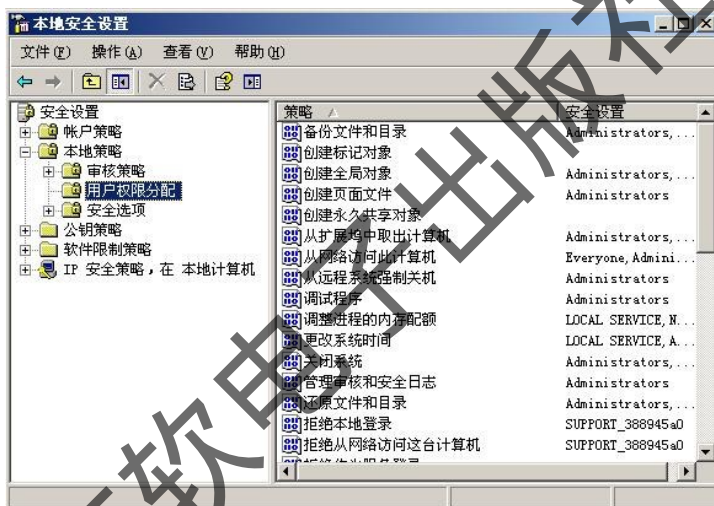


图 2-26 用户权限分配

说明:用户权限是指登录到系统的用户有权在系统上完成的某些操作。Windows Server 2003 为计算机管理的各项任务设定了默认的权限,并且将这些默认的权限分配给了内置组,这些组便有了对应的权限。

系统管理员在新增了用户账户或组之后,如果需要指派管理计算机的某项任务,可以将这些用户账户或组加入内置组,但是这种方式不够灵活。系统管理员可以单独为用户账户或组分配权限,这种方式提供了更好的灵活性。

步骤 2:双击“本地安全设置”窗口右侧策略列表中的“关闭系统”,在弹出的对话框中单击“添加用户或组”按钮将 specials 组加入,如图 2-27 所示,然后单击“确定”按钮使配置更改生效。

说明:在“关闭系统 属性”对话框中可以看到默认情况下哪些内置组具有此权限。

3. 测试用户权限

以用户账户 tom 身份登录服务器时具有关机权限,而其他员工的用户账户则没有此权限,如图 2-28 所示,lix 用户仅有注销权限,不能关闭或重启计算机。



图 2-27 “关闭系统 属性”对话框



图 2-28 “关闭 Windows”对话框

2.3 本章小结

每个用户都需要有一个账户以便登录到域访问网络资源或登录到某台计算机访问该计算机上的资源。具有相同权限用户账户的集合就是组，系统管理员通常通过对组的权限设置来管理用户和计算机的权限。

本章通过分析企业用户账户与组的管理需求，构思了涉及项目的相关技术知识点、设计了项目的实施细节，然后针对此项目涉及到的技术介绍知识点和配置实施步骤，最终实现并运行项目。通过配置与管理本地用户账户与组的项目，创建本地用户账户与组，配置密码与账户锁定策略，设置并应用密码重设盘，掌握管理用户与组的方法，为用户分配特殊权限。

2.4 课外实践环节

根据下面具体项目练习要求，实现用户与组的基本管理及本地安全策略。

- (1) 创建本地用户账户 user1、user2，要求用户首次登录时须更改密码。
- (2) 创建本地组 specialgroup，使其具有关机的本地安全策略，将 user2 加入该组。
- (3) 配置密码策略，要求启用密码复杂度策略，密码最小长度为 8，最长使用期限为 50 天。配置账户锁定策略，账户锁定阈值设为 3，锁定时间设为 20 分钟。
- (4) 为 user1 设置密码重设盘，并应用密码重设盘为 user1 重新设置密码。

2.5 教学效果测评

2.5.1 选择题

1. 有一台系统为 Windows Server 2003 的计算机,管理员希望在该计算机上创建用户账户时密码必须包含大写字母、小写字母、数字和特殊符号这四类字符中的三类,管理员应该启用()密码策略。(选一项)

- A. 密码必须符合复杂性要求
- B. 密码最小长度为 3
- C. 密码最短使用期限为 3
- D. 账户锁定阈值为 3

2. 公司有一台处于工作组中的计算机,操作系统为 Windows Server 2003,出于安全性的考虑,公司的系统管理员希望这台计算机的用户账号在设置密码时最小密码长度为 8,应该采取()措施来实现这一目标。(选一项)

- A. 制定一个行政规定,要求用户的密码长度最小为 8
- B. 设置计算机本地策略中的审核策略,设置“密码长度最小值”为 8
- C. 设置计算机本地策略中的安全选项,设置“密码长度最小值”为 8
- D. 设置计算机账户策略中的密码策略,设置“密码长度最小值”为 8

3. 有一台系统为 Windows Server 2003 的计算机,管理员在计算机上建立了一个普通用户账户 public 供来宾使用,并为其配置了相应的权限,一段时间后不知道谁更改了该账户的密码,使用以前的密码无法登录,此时()才能使用 public 登录且其他的设置都不变。(选两项)

- A. 删除用户账户 public 后再重新创建同名账户
- B. 使用管理员账户登录,将账户 public 的属性设置为“用户不能更改密码”
- C. 使用管理员账户登录,重新为账户 public 设置密码
- D. 只有账户 public 能更改自己的密码,忘记密码相当于该账户被禁用

4. 安装完 Windows Server 2003 系统之后,在计算机中有自动生成的内置组,其中的 Power Users 组有以下管理功能()。(选两项)

- A. 对计算机有完全控制权限
- B. 可以管理 administrators 组的成员
- C. 具有创建用户账户和组账户的权利
- D. 可以共享计算机上的文件夹

5. 关于禁用账户的描述,正确的是()。(选三项)

- A. Administrator 账户可以被禁用
- B. Administrator 账户不可以被禁用
- C. 普通用户账户可以被禁用
- D. 普通用户账户不可以被禁用

- E. 禁用的目的是暂时禁止该用户登录
6. 办公网络中计算机的逻辑组织形式可以有两种,工作组和域。下列关于工作组的叙述中正确的是()。(选两项)
- A. 工作组中的每台计算机都在本地存储账户
 - B. 本计算机的账户可以登录到其他计算机上
 - C. 工作组中的计算机的数量最好不要超过 10 台
 - D. 工作组中的操作系统必须一样
7. Windows Server 2003 服务器的管理员有禁用账户的权限。当一个用户有一段时间不用账户(可能是休假等原因),管理员可以禁用该账户。下列关于禁用账户叙述正确的是()。(选两项)
- A. Administrator 账户可以禁用自己,所以在禁用自己之前应该先创建至少一个管理员组的账户
 - B. 普通用户可以被禁用
 - C. Administrator 账户不可以被禁用
 - D. 禁用的账户过一段时间会自动启用
8. 下列用户账户名不是合法的用户账户名()。(选一项)
- A. Administrator*
 - B. qing_568
 - C. microsoft software
 - D. appleLiEMC
9. 关于账户删除的描述不正确的是()。(选一项)
- A. Administrator 账户不可以删除
 - B. 普通用户可以删除
 - C. 删除后的用户,可以建立同名账户,并具有原来账户的权限
 - D. 删除用户只能通过系统备份来恢复
10. 一位助理网络管理员在用自己的账户登录到位于工作组中的 Windows Server 2003 服务器后,发现在打开本地网络连接的属性时不能修改该连接的 TCP/IP 配置,但他必须具备相应的特权。为了最快速、简捷和安全地达到这个目的,作为网络管理员的你最佳的选择是()。(选一项)
- A. 修改该计算机的本地组策略,允许该助理管理员账户修改 TCP/IP 的配置
 - B. 将该助理管理员的用户账户加入到 Administrators 组中
 - C. 将该助理管理员的用户账户加入到 Backup Operators 组中
 - D. 将该助理管理员的用户账户加入到 Network Configuration Operators 组中
11. A user has forgotten his or her password and attempts to log on several times with an incorrect password. Eventually, the user receives a logon message indicating that the account is either disabled or locked out. The message suggests that the user contact an administrator. What must you do? (Choose all that apply.)
- A. Delete the user object and re-create it.

- B. Rename the user object.
- C. Enable the user object.
- D. Unlock the user object.
- E. Reset the password for the user object.

12. To configure account lockout so that users must contact the Desk Administrator to unlock their accounts, which policy should be specified?

- A. Account Lockout Duration: 999
- B. Account Lockout Threshold: 999
- C. Account Lockout Duration: 0
- D. Account Lockout Threshold: 0

2.5.2 简答题

1. Windows Server 2003 系统安装自动创建的账户中默认被禁用的是哪个账户? 管理员账户可以被禁用吗?

2. 创建用户账户时,什么情况下需要设置“用户下次登录时须更改密码”? 什么情况下需要设置“用户不能更改密码”?

3. 简述强密码需要至少具备哪些条件?

4. 简述账户锁定策略中“复位账户锁定计数器”“账户锁定时间”“账户锁定阈值”三者之间的关系。

5. 如何查看当前登录用户的 SID?