第 2 章　本地用户和组的管理

教学重点

- 本地用户账户管理
- 本地组账户管理
- 本地用户相关安全管理的操作

您是否了解并经历过由一台计算机服务器为成百上千（或是成千上万）名用户同时提供信息共享的系统维护环境？如果该计算机的所有物理系统资源为实现共享而提供了一定的系统硬件基础，那么由于其上运行了不合适（或是缺乏用户安全管理功能）的操作系统软件，结果将是无法统筹管理系统资源而造成用户的低效甚至无法正常使用。Windows Server 2012 提供的用户账户管理功能机制可以安全解决该问题。作为多用户、多任务的操作系统，Windows Server 2012 拥有一个完备的系统账户和安全、稳定的工作环境，系统所提供的账户类型主要包括用户账户和组账户。用户只有首先登录到系统中，才能够使用系统所提供的资源。系统管理员根据不同用户的具体使用情况，设立不同的用户账户，指派不同的权限。用户只有通过某个账户才能登录到计算机，并且只能拥有管理员分配该账户资源的使用权。

2.1　管理本地用户账户

用户账户是用来登录到计算机或通过网络访问计算机及网络资源的凭证，它是用户在 Windows Server 2012 操作系统中的唯一标志。如果用户要登录到 Windows Server 2012 的计算机系统或者 Windows Server 2012 所支持的网络资源环境，那么必须拥有一个合法的用户账户。Windows Server 2012 通过创建账户（包括用户账户和组账户），并赋予账户合适的权限来保证使用网络和计算机资源的合法性，以确保数据访问、存储的安全需要。

2.1.1　用户账户管理原理

用户账户是计算机操作系统实现其安全机制的一种重要技术手段，操作系统通过用户账户来辨别用户身份，让具有一定有使用权限的人登录计算机，访问本地计算机资源或从网络访问这台计算机的共享资源。系统管理员根据不同用户的具体工作情景，指派不同用户的不同权限，从而使用户执行并完成不同的管理任务。因此，运行 Windows Server 2012 系统的计算机，都需要有用户账户才能登录计算机，用户账户是 Windows Server 2012 系统环境中用户唯一的标志符。在 Windows Server 2012 启动运行或登录已

运行系统的过程中，都要求用户输入指定的用户账户名和密码，只有用户输入的账户标志符和密码与本地数据库中的一致，才允许用户登录到本地计算机或从网络上获取对资源的访问权限。

用户登录系统时，本地系统验证用户账户的有效性的基本原理：如果用户提供正确的用户名和密码，则本地系统分配给用户一个访问令牌（Access Token），该令牌定义了用户在本地计算机系统的访问权限，资源所在的计算机系统负责对该令牌进行鉴别，以保证用户只能在管理员定义的权限范围内使用本地计算机上的资源。对访问令牌的分配和鉴别是由本地计算机的安全权限功能负责的。

Windows Server 2012 支持两种用户账户：本地用户账户和域用户账户。

本地用户账户是指安装了 Windows Server 2012 的计算机在本地安全目录数据库中建立的账户。使用本地账户只能登录到建立该账户的计算机，并访问该计算机的系统资源。此类账户通常在工作组网络中使用，其显著特点是基于本机的。

域用户账户是建立在域控制器的活动目录数据库中的账户。此类账户具有全局性，可以登录到域网络环境模式中的任何一台计算机，并获得访问该网络的权限。这需要系统管理员在域控制器中，为每个登录到域的用户创建一个用户账户。本章主要介绍本地用户和组的管理。

另外，Windows Server 2012 还提供内置用户账户（即系统用户账户），用于执行特定的管理任务或使用户能够访问网络资源。Windows Server 2012 系统最常用的两个内置账户是 Administrator 和 Guest。

Administrator 即系统管理员，拥有最高的资源使用权限，可以对该计算机或域配置进行管理，如创建修改用户账户和组、管理安全策略、创建打印机、分配允许用户访问资源的权限等。Administrator 账户是在安装 Windows Server 2012 过程中创建的，系统默认的名称是 Administrator，用户无法删除它。

Guest 即为临时访问计算机的用户而提供的账户。Guest 账户也是在系统安装中自动添加的，并且不能删除。在默认情况下，为了保证系统的安全，Guest 账户是禁用的，但在安全性要求不高的网络环境中，可以使用该账户。Guest 账户只拥有很少的权限，系统管理员可以改变使用系统的权限。

2.1.2 创建用户账户

1. 用户账户创建前的规划

在系统中操作创建之前，先制定一个创建账户所遵循的规则或约定，这样可以方便、统一账户的管理，提供高效、稳定的系统应用环境。

（1）用户账户命名规则

①用户账户命名注意事项。一个良好的用户账户命名策略有助于系统账户的管理，首先要注意以下的账户命名。

- 账户名必须唯一：本地账户名称必须在本地计算机系统中唯一。
- 账户名不能包含的字符：“？”、“+”、“*”、“∧”、“[ ]”、“=”、“<”、“>”等符号。
- 账户名称最长只能包含 20 个字符。用户可以输入超过 20 个字符，但系统只识

别前 20 个字符。

- 用户名不区分大小写。

②用户账户命名推荐策略。为加强用户管理，在企业应用环境中通常采用下列命名规范。

- 用户全名：建议用户全名以企业员工的真实姓名命名，便于管理员查找、管理用户账户。比如张玉婷，管理员创建用户账户将其姓指定为“张”，名指定为“玉婷”，则用户在打开“活动目录用户和计算机”时可以方便地查找到该用户账户。
- 用户登录名：用户登录名一般要符合方便记忆和具有安全性的特点。用户登录名一般采用姓的拼音加名的首字母，如将张玉婷登录名命名为 Zhangyt。

（2）用户账户密码的规则

①用户密码设置注意事项。

- Administrator 账户必须指定一个密码，并且除系统管理员外的用户不能随便使用该账户。
- 系统管理员在创建用户账户时，可给每个用户账户指定一个唯一的密码，要防止其他用户对其进行更改，最好使该用户在第一次登录时修改自己的密码。

②用户密码设置推荐策略。

- 采用长密码：Windows Server 2012 用户账户密码最长可以包含 127 个字符，理论上来说，用户账号密码越长，安全性就越高。
- 采用大小写、数字和特殊字符组合密码：Windows Server 2012 用户账户密码严格区分大小写，采用大小写、数字和特殊字符组合密码将使用户密码更加安全。

2. 创建本地用户账户

创建本地用户账户的操作用户必须拥有管理员权限，才可以执行。可以通过使用“计算机管理”中的“本地用户和组”管理单元来创建本地用户账户，创建的步骤如下。

步骤 1：在“开始”桌面选择“管理工具”图标，然后选择“计算机管理”功能，打开如图 2-1 所示的“计算机管理”窗口。

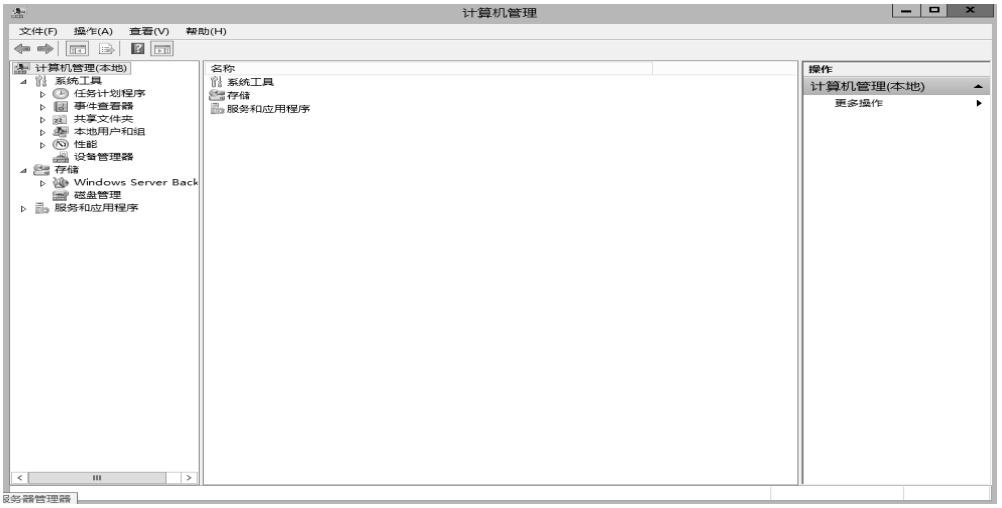

图 2-1 “计算机管理”窗口

步骤 2：在“计算机管理”窗口中，展开“本地用户和组”结点，在“用户”文件夹上右击。选择“新用户”命令，打开如图 2-2 所示的“新用户”对话框。

图 2-2　“新用户”对话框

步骤 3：打开“新用户”对话框后，输入用户名、全名、描述和密码。然后指定用户密码选项，单击“创建”按钮新增用户账户。创建完用户后，单击“关闭”按钮返回到“计算机管理”控制台。

表 2-1 详细说明了各个用户密码选项的作用。

表 2-1　用户账户密码选项说明

选　项	说　明
用户下次登录时须更改密码	选择该项，用户第一次登录系统会弹出修改密码的对话框，要求用户更改密码
用户不能更改密码	选择该项，系统不允许用户修改密码，只有管理员能够修改用户密码。通常用于多个用户共用一个用户账户，如 Guest 等
密码永不过期	默认情况下，Windows Server 2012 操作系统用户账户密码最长可以使用 42 天，选择该项用户密码可以突破限制继续使用。通常用于 Windows Server 2012 的服务账户或应用程序所使用的用户账户
账户已禁用	禁用用户账户，使用户账户不能再登录，用户账户要登录必须清楚对该项的选择

注意：密码选项中的“用户下次登录时须更改密码”、“用户不能更改密码”和“密码永不过期”互相排斥，不能同时选择。

本地用户账户仅允许用户登录并访问创建该账户的计算机。当创建本地用户账户时 Windows Server 2012 操作使用的数据库是位于“%Systemroot%\system32\config”文件夹下的安全数据库（SAM）。

Windows Server 2012 创建的用户账户不允许相同，且系统内部通过安全标志符（Security Identifier，SID）来识别每个用户账户。每个用户账户都对应一个唯一的安全标志符，它在用户创建时由系统自动产生。系统指派权利、授权资源访问权限等都需要使用这个安全标志符。

注意：当删除一个用户账户后，重新创建名称相同的账户并不能获得先前账户的权利。

用户登录后，可以在命令提示符状态下输入“whoami/logonid”命令查询当前用户账户的安全标志符，如图 2-3 所示。

图 2-3　查询当前账户的 SID

2.1.3　设置用户账户属性

为了管理和使用的方便，一个用户账户不仅包括用户名和密码，还包括一些属性，如用户隶属的用户组、用户配置文件、用户的拨入权限、终端用户设置等。可以根据需要对账户的属性进行设置。在“本地用户和组”窗口的右侧栏中，双击一个用户，将显示该用户的“用户属性”对话框。图 2-4 所示的是 Administrator 用户的属性设置对话框。

图 2-4　Administrator 用户的属性设置对话框

1. “常规”选项卡

在“常规”选项卡中，设置与账户有关的一些描述信息，包括全名、描述、账户及密码选项等。管理员可以设置密码选项、禁用账户，如果账户已经被系统锁定，管理员可以解除锁定。

2. “隶属于”选项卡

在“隶属于”选项卡中，设置该账户和组之间的隶属关系，把账户加入到合适的本地组中，或者将用户从组中删除，如图 2-5 所示。

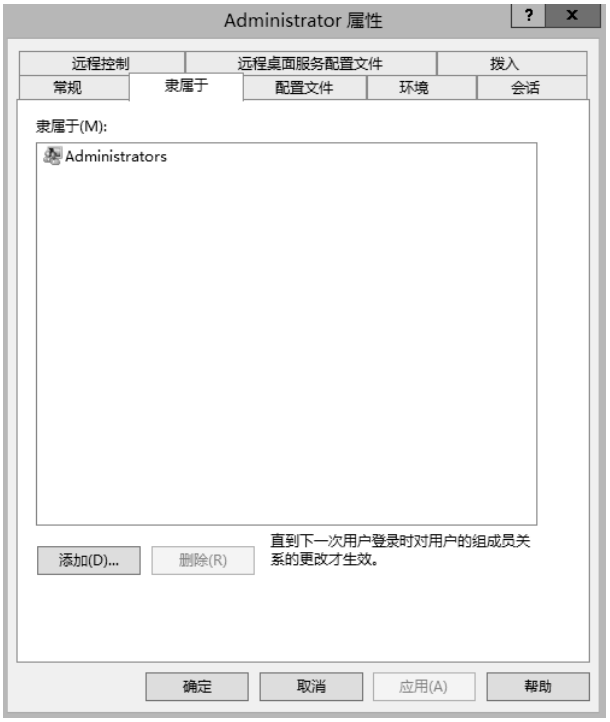

图 2-5　“隶属于”选项卡

为了管理的方便，通常把用户加入到组中，通过设置组的权限统一管理用户的权限。根据需要对用户组进行权限的分配与设置，用户属于哪个组，则就具有该组的权限。新增的用户账户默认的是加入到 Users 组中，Users 组的用户通常不具备一些特殊权限（如安装应用程序、修改系统设置等）。因此当要分配用户某些特殊权限时，可以将该用户账户加入到拥有这些权限的组中。如果需要将用户从一个或几个组中删除，则单击“删除”按钮。

下面以将本地用户账户“userA”添加到管理员组为例，介绍添加用户到组的操作步骤。

步骤 1：在“隶属于”选项卡中，单击图 2-5 中的“添加”按钮。

步骤 2：在图 2-6 所示的“选择组”对话框中输入需要加入组的名称，如输入管理员组的名称“Administrators”。单击“检查名称”按钮，检查该名称是否正确，如果输入了错误的组名称，系统将提示找不到该名称。如果没有错误，则该名称会改变为本地计算

机名称\组名称。这里单击“检查名称”按钮后，名称会改变“ABC\Administrator”。

图 2-6　“选择组”对话框

也可以找出可用的组的列表，从中选择需要的组，这样可以不再手动输入组名称。单击图 2-6 中“高级”按钮，在弹出的对话框中单击“立即查找”按钮，出现可用的组列表，如图 2-7 所示，从列表中选择需要的组即可。

图 2-7　查找选择可用的组

3. “配置文件”选项卡

在“配置文件”选项卡中，可以设置用户账户的配置文件路径、登录脚本和主文件夹路径。用户配置文件是存储当前桌面环境、应用程序设置以及个人数据的文件夹和数据的集合，还包括所有登录到计算机上所建立的网络连接信息。由于用户配置文件提供

的桌面环境与用户最近一次登录到该计算机上所用的桌面相同，因此就保持了用户桌面环境及其他设置的一致性。当用户第一次登录到计算机时，Windows Server 2012 自动创建一个用户配置文件并将其保存。本地用户账户的配置文件都是保存在本地磁盘“%userprofile%”文件夹中。

“配置文件”选项卡如图 2-8 所示。下面分别介绍用户配置文件、登录脚本和用户主文件夹的相关知识。

图 2-8 “配置文件”选项卡

（1）用户配置文件类型。

① 默认用户配置文件。默认用户配置文件是所有用户配置文件的基础。当用户第一次登录 Windows Server 2012 时，Windows Server 2012 会将本地默认用户配置文件夹复制到“%Systemdrive%\Documents and Settings\%Username%”中，以作为初始的本地用户配置文件。

② 本地用户配置文件。本地用户配置文件保存在本地计算机上的“%Systemdrive%Documents and Settings\Username%”文件夹中，所有对桌面设置的改动都可以修改用户配置文件。

③ 强制用户配置文件。强制配置文件是一个只读的用户配置文件。当用户注销时，Windows Server 2012 不保存用户在会话期内所做的任何改变。

可以为需要同样桌面环境的多个用户定义一份强制配置文件。配置文件中，隐藏文件 Ntuser.at 包含应用单个用户账户的 Windows Server 2012 的部分系统设置和用户环境设置，管理员可以通过将其改名为 Nmset.man，从而把该文件变成只读型，即创建强制用户配置文件。

④ 漫游用户配置文件。通过设置漫游用户配置文件，可以支持在多台计算机上工

作的用户。漫游用户配置文件只能由系统管理员创建，可以保存在某个网络服务器上，用户无论从哪台计算机登录，均可获得这一配置文件。用户登录时，Windows Server 2012 会将该漫游用户配置文件从网络服务器复制到该用户当前所用的 Windows Server 2012 机器上。因此，用户总是能得到自己的桌面环境设置和网络连接设置。漫游用户配置文件只能在域环境下实现。

在第一次登录时，Windows Server 2012 将所有的文件都复制到本地计算机上。此后，当用户再次登录时，Windows Server 2012 只需比较本地储存的用户配置文件和漫游用户配置文件。这时，系统只复制用户最后一次登录并使用这台计算机时被修改的文件，因此缩短了登录时间。当用户注销时，Windows Server 2012 会把对漫游用户配置文件本地备份所做的修改复制到该漫游配置文件的服务器上。

（2）登录脚本。登录脚本是希望用户登录计算机时自动运行的脚本文件，脚本文件的扩展名可以是 .VBS、.BAT 或.CMD。

（3）用户主文件夹。用户主文件夹是 Windows Server 2012 为用户提供的用于存放个人文档的主文件夹。主文件夹可以保存在客户机上，也可以保存在一个文件服务器的共享文件夹中。用户可以将所有的用户主文件夹都定位在某个网络服务器的中心位置，因为主文件夹不属于漫游配置文件的一部分，所以它的大小并不影响登录时网络的通信量。管理员在为用户实现主文件夹时，应考虑以下因素：

在实现对用户文件的集中备份和管理时，基于安全性考虑，应将用户主文件夹存放在 NTFS 卷中，利用 NTFS 的权限来保护用户文件（放在 FAT 卷中只能通过共享文件夹权限来限制用户对主目录的访问）。用户可以通过网络中任意一台联网的计算机访问其主文件夹。

2.1.4 删除本地用户账户

对于不再需要的账户可以将其删除，但在执行删除操作之前应确认其必要性，因为删除用户账户会导致与该账户有关的所有信息丢失。从前面的学习中我们知道，每个用户都有一个名称之外的唯一的标志符 SID 号，SID 号在新增账户时由系统自动产生，不同账户的 SID 不会相同。由于系统在设置用户的权限、访问控制列表中的资源等信息时，内部都使用 SID 号，所以一旦用户账户被删除，这些信息也就跟着消失了。即使重新创建一个名称相同的用户账户，也不能获得原先用户账户的权限。系统内置账户如 Administrator、Guest 等是无法删除的。

删除本地用户账户在“计算机管理”控制台中进行，选择要删除的用户账户，执行删除功能，出现如图 2-9 所示对话框，进一步确认即可。

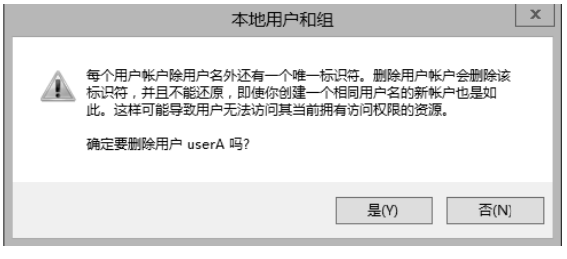

图 2-9 “删除用户账户”对话框

2.2　管理组账户

2.2.1　组账户概述

组是多个用户、计算机账号、联系人和其他组的集合，也是操作系统实现其安全管理机制的重要技术手段。属于特定组的用户或计算机称为组的成员。使用组可以同时为多个用户账户或计算机账户指派一组公共的资源访问权限和系统管理权限，而不必单独为每个账户指派权限，从而简化管理，提高效率。

需要注意的是组账户并不用于登录计算机操作系统，用户在登录到系统时均使用用户账户，同一个用户账户可以同时为多个组的成员，这样该用户的权限就是所有组权限的合并。

根据创建方式的不同，组可以分为内置组和用户自定义组。内置组是 Windows Server 2012 操作系统自动创建的一些组，拥有系统事先定义好的执行系统管理任务的权利。

关于内置组的相关描述，可以参看系统内容。具体操作：打开“计算机管理”控制台，在“本地用户和组”结点中的“组”文件夹里，查看本地内置的所有组账户，如图 2-10 所示。

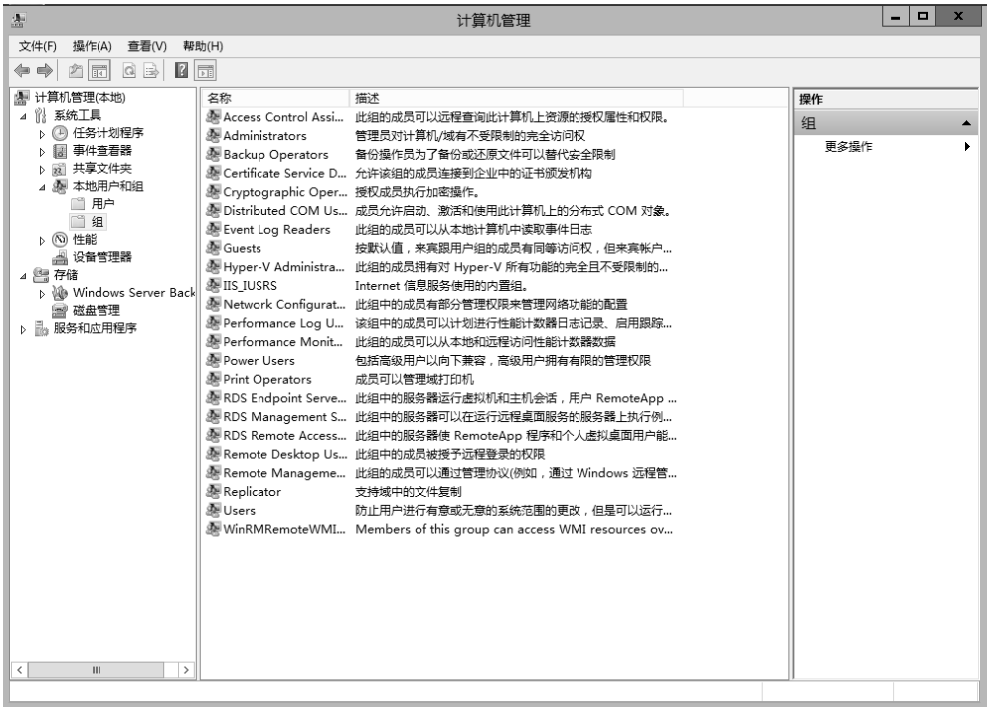

图 2-10　查看内置组账户

管理员不但可以根据自己的需要向内置组添加成员或删除内置组成员，而且可以重命名内置组，但不能删除内置组。

2.2.2 创建本地用户组的操作

仅使用系统内置组可能无法满足安全性和灵活性的需要。因为通常系统默认的用户组能够满足某些方面的系统管理需要，但是不能满足系统管理的特殊需要，所以管理员必须根据情况新增一些组，即用户自定义组。这些组创建之后，就可以像管理系统内置组一样，赋予其权限和进行组成员的增加。只有本地计算机上的 Administrators 组和 Power Users 组成员有权创建本地用户组。在本地计算机上创建本地组的步骤如下。

步骤 1：在 Windows Server 2012“桌面”界面，选择“管理工具”及“计算机管理”。

步骤 2：从“计算机管理”控制台中展开“本地用户和组”，在“组”文件夹上右击，选择“新建组”命令，打开如图 2-11 所示对话框。

图 2-11 “新建组”对话框

步骤 3：在“新建组”对话框中输入组名和描述，然后单击“创建”按钮即可完成创建。

可以在创建用户组的同时向组中添加用户。在图 2-11 所示对话框中，单击“添加”按钮，显示“选择用户”对话框，如图 2-12 所示。在“选择此对象类型”选项中输入成员名称，或者使用“高级”按钮查找用户，然后单击“确定”按钮。

图 2-12 “选择用户”对话框

2.2.3　删除、重命名本地组及修改本地组成员

对于系统不再需要的本地组，系统管理员可以将其删除。但是管理员只能删除自己创建的组，而不能删除系统提供的内置组。当管理员删除系统内置组时，将被系统拒绝。

删除本地组的方法：在“计算机管理”控制台中选择要删除的组账户，然后右击该组，再选择“删除”，弹出如图 2-13 所示的对话框，单击“是”按钮即可。

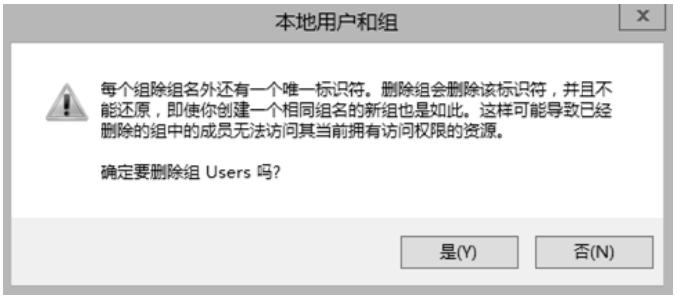

图 2-13　“本地用户和组”对话框

每个组都拥有一个唯一的安全标志符（SID），所以一旦删除了用户组，就不能重新恢复，即使新建一个与被删除组有相同名字和成员的组，也不会与被删除组有相同的特性和特权。

重命名组的操作与删除组的操作类似，只须在弹出的菜单中选择“重命名”，输入相应的名称即可。

修改本地组成员通常包括向组中添加成员或从组中删除已有的成员。如果要添加成员，则选择相应的组，单击“添加”按钮后选择相应用户即可。如果要删除某组的成员，则双击该组的名称，选择相应要删除的成员，然后单击“删除”按钮。

2.3　与本地用户相关的安全管理操作

在 Windows Server 2012 中，除了创建账户、设置账户的基本属性、删除账户等管理外，为确保计算机系统的安全，系统管理员需要应用与账户相关的一些操作对本地安全进行设置，从而达到提高系统安全性的目的。Windows Server 2012 对登录到本地计算机的用户都定义了一些安全设置。所谓本地计算机是指用户登录执行 Windows Server 2012 的计算机，在没有活动目录集中管理的情况下，本地管理员必须为计算机进行设置以确保其安全。例如，限制用户如何设置密码、通过账户策略设置账户安全性、通过锁定账户策略避免他人登录计算机、指派用户权限等。将这些安全设置分组管理，组成了 Windows Server 2012 的本地安全策略。

Windows Server 2012 的安全设置在“管理工具”提供的“本地安全策略”单元控制台中进行，此控制台可以集中管理本地计算机的安全设置原则。使用管理员账户登录到本地计算机，即可打开“本地安全策略”控制台，如图 2-14 所示。

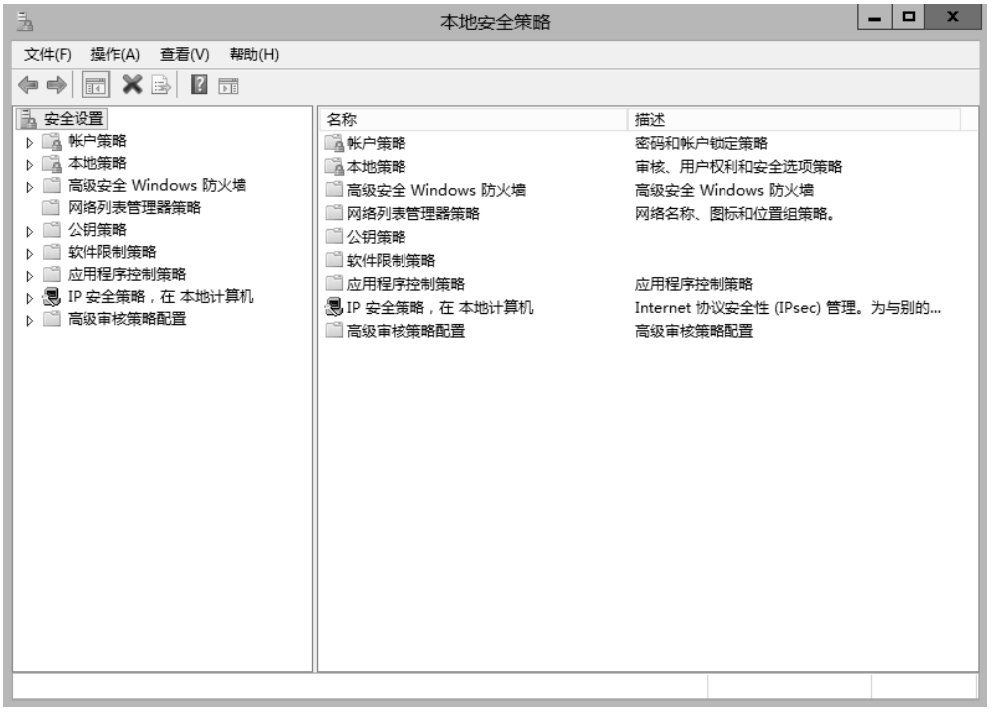

图 2-14 “本地安全策略”控制台

1. 密码安全设置

用户账户密码是保证计算机安全的重要基础手段。如果用户账户（特别是管理员账户）没有设置密码，或者设置的密码非常简单，那么计算机系统将很容易被非授权用户登录侵入，进而访问计算机资源或更改系统配置。目前互联网上的攻击很多都是因为密码设置过于简单或根本没设置密码造成的，因此应该设置合适的密码，从而保证系统的安全。Windows Server 2012 的密码强度原则主要包括以下 4 项：密码必须符合复杂性要求、密码长度最小值、密码使用期限和强制密码历史等。下面分别介绍这些项的含义和设置方法。

（1）密码必须符合复杂性要求。要使本地计算机启用密码复杂性要求，只要在“本地策略”中选择“账户策略|密码策略”，双击右边子窗口的“密码必须符合复杂性要求”，选择“已启用”，单击“确定”按钮即可，如图 2-15 所示。配置其他策略时，在右边选择相应的选项即可。配置“密码必须符合复杂性要求”选项，确定密码是否符合复杂性要求，启用该策略，则密码必须符合以下最低要求：

① 不包含全部或部分的用户账户名。

② 长度至少为 6 个字符。

③ 包含来自以下 4 个类别中 3 种的字符：英文大写字母（A～Z）；英文小写字母（a～z）；10 个基本数字（0～9）；非字母字符（如!、#、$、%）。

对于工作组环境的 Windows 系统，默认密码没有设置复杂性要求，用户可以使用空密码或简单密码，如“12345”、“password”等，这样黑客很容易通过一些扫描工具得到系统管理员的密码。对于网络环境的 Windows Server 2012，默认启用了密码复杂性要求。

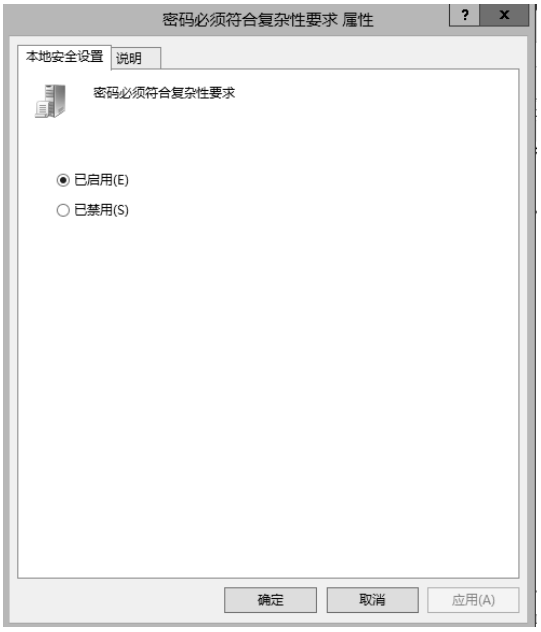

图 2-15　密码必须符合复杂性属性的管理

（2）密码长度最小值。该安全设置确定用户账户的密码可以包含的最少字符个数。可以设置为 1～14 个字符之间的某个值，或者通过将字符数设置为 0，可设置不需要密码。在工作组环境的服务器上，默认值是 0，对于域环境的系统，默认值是 7。为了系统的安全，最好设置最小密码长度为 6 或更长的字符，如图 2-16 所示设置的密码最小长度为 8 个字符。

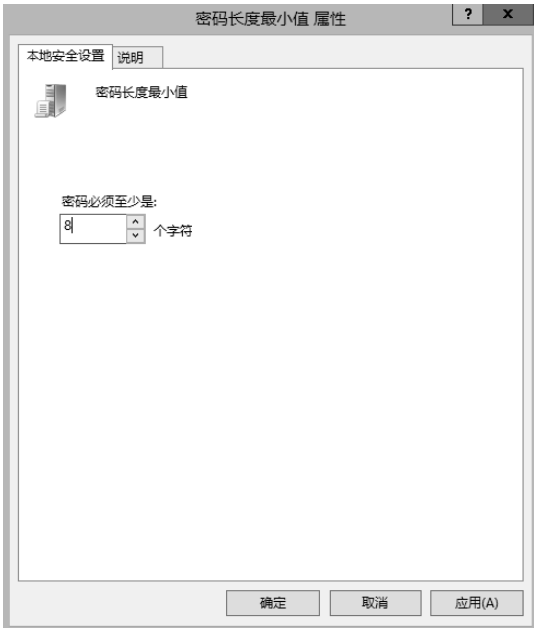

图 2-16　密码长度最小值属性的管理

（3）密码使用期限。密码使用期限包括密码最长使用期限和密码最短使用期限。密码最长使用期限确定系统要求用户更改密码之前可以使用该密码的时间（单位为天）。密码最短使用期限确定用户可以更改密码之前必须使用该密码的时间（单位为天），可设置 1～998 之间的某个值。如果设置为 0，则表明允许立即修改密码。密码最短使用期限设置的值必须小于密码最长使用期限设置的值。如果密码最短使用期限设置为 0，则密码最长使用期限可以是 1～998 之间的任何值。默认密码最长有效期设置为 42 天，默认密码最短有效期为 0 天。

（4）强制密码历史。重新使用旧密码之前，该安全设置确定某个用户账户所使用的新密码不能与该账户最近所使用的旧密码一致。例如，将强制密码历史设置为 4，即系统会记住最后 4 个用户设置过的密码，当用户修改密码时，如果为最后 4 个密码之一，系统将拒绝用户的要求。该值必须为 0～24 之间的一个数。该策略通过确保旧密码不能在某段时间内重复使用，使用户账户更安全。强制密码历史设置如图 2-17 所示，默认强制密码历史为 0 个。

图 2-17 “强制密码历史属性”对话框

2. 账户锁定策略管理

账户锁定策略指用户设置什么时候及多长时间内账户将在系统中被锁定不能使用。Windows Sever 2012 在默认情况下，没有对账户锁定进行设定，为了保证系统的安全，最好设置账户锁定策略。账户锁定原则包括如下设置：账户锁定时间、账户锁定阈值和复位账户锁定计数器。

账户锁定时间设置，确定锁定的账户在自动解锁前保持锁定状态的分钟数。有效范围是 0～99999。如果将账户锁定时间设置为 0，那么在管理员明确将其解锁前，该账户

将被锁定。如果定义了账户锁定阈值，则账户锁定时间必须大于或等于重置时间。默认值为无。因为只有指定了账户锁定阈值，该策略设置才有意义。

账户锁定阈值设置，确定造成用户账户被锁定的登录失败尝试的次数。登录尝试失败的范围为 0～999。如果将此值设为 0，则将无法锁定账户。对于使用 Ctrl+Alt+Delete 组合键或带有密码的屏幕保护程序锁定的工作站或成员服务器，失败的密码尝试将计入失败的登录尝试次数中，默认值为 0。可以设置为 5 次或更多的次数以确保系统安全，如图 2-18 所示。

图 2-18　账户锁定阈值修改

复位账户锁定计数器设置，确定在登录尝试失败计数器被复位为 0（即 0 次失败登录尝试）之前，尝试登录失败之后所需的分钟数，其有效范围为 1～99999。如果定义了账户锁定阈值，则该复位时间必须小于或等于账户锁定时间，默认值为无，因为只有指定了“账户锁定阈值”，该策略设置才有意义。

实训 2

1. 实训目的

熟练掌握 Windows Server 2012 本地用户账户、组账户的创建与管理，以及常用的账户安全管理设置方法。

2. 实训环境

安装了 Windows Server 2012 操作系统的计算机。

3. 实训内容

（1）通过“计算机管理”控制台添加本地账户 MyUser1、MyUser2、MyUser3，在创建时分别为三个用户选择不同的用户账户密码选项。

（2）用不同的用户账户登录系统。

（3）删除用户账户 MyUser3。

（4）创建组 MyGroup1 和 MyGroup2。

（5）将（1）中创建的用户账户 MyUser1 加入到组 MyGroup1 和 MyGroup2 中，MyUser2 加入到 Administrators 组中。

（6）将 MyGroup2 重命名为 MyGroup3，将 MyUser1 从中移除。

（7）删除组账户 MyGroup3。

（8）从开始“管理工具”功能提供的“本地安全策略”打开控制台。

（9）对 MyUser1 进行密码安全设置，对 MyUser2 进行账户锁定安全设置，体会各种设置，尤其是设置为特殊值的效果。

习题 2

1. 填空题

（1）用户要登录到 Windows Server 2012 的计算机，必须拥有一个合法的_____。

（2）Windows Server 2012 系统的最常用的两个内置账户是_____和_____。

（3）使用_____可以同时为多个用户账户指派一组公共的权限。

（4）用户必须拥有_____权限，才可以创建用户账户。

（5）用户登录后，可以在命令提示符状态下输入_____命令查询当前用户账户的安全标志符。

（6）_____是存储当前桌面环境、应用程序设置以及个人数据的文件夹和数据的集合。

2. 简答题

（1）Windows Server 2012 的用户账户有哪几种类型？其含义是什么？

（2）简述使用组技术管理用户账户的原因。

（3）用户配置文件哪几种类型？各有什么作用？

（4）Windows Server 2012 关于用户账户管理的本地安全策略主要有哪些？