

4

第4章 本地账户与组账户的管理

每一位用户要使用计算机前都必须登录该计算机，而登录时必须输入有效的用户账户与密码；另外，若我们能够有效利用组来管理用户权限，则必定能够减轻许多网络管理的负担。

- ▼ 内置的本地账户
- ▼ 本地用户账户的管理
- ▼ 密码的更改、备份与还原
- ▼ 本地组账户的管理



4.1 内置的本地账户

我们在第1章介绍过，每一台Windows计算机都有一个**本地安全账户数据库（SAM）**，用户在使用计算机前都必须登录该计算机，也就是要提供有效的用户账户与密码，而这个用户账户就是建立在**本地安全账户数据库**内，这个账户被称为**本地用户账户**，而建立在此数据库内的组被称为**本地组账户**。

4.1.1 内置的本地用户账户

Windows Server 2016内置了两个可供使用的用户账户：

- **Administrator（系统管理员）**：它拥有最高的权限，您可以利用它来管理计算机，例如建立/更改/删除用户账户与组账户、设置安全策略、建立打印机、设置用户权限等。无法删除此账户，不过为了安全起见，建议对其改名。
- **Guest（来宾）**：它是供没有账户的用户来临时使用的，它只有很少的权限。可以更改名称，但无法将其删除。此账户默认是被停用的。

4.1.2 内置的本地组账户

系统内置了许多本地组，它们本身都已经被赋予了一定的权限（rights），以便让它们具备管理本地计算机或访问本机资源的能力。只要用户账户被加入到本地组中，此用户就会具备该组所拥有的权限。下面列出一些常用的本地组：

- **Administrators**：此组内的用户具备系统管理员的权限，他们拥有对这台计算机最大的控制权，可以执行整台计算机的管理工作。内置的系统管理员Administrator就是隶属于此组，而且无法将它从此组内删除。
- **Backup Operators**：此组内的用户可以通过Windows Server Backup工具来备份与还原计算机内的文件，不论他们是否有权限访问这些文件。
- **Guests**：此组内的用户无法永久改变桌面的工作环境，当他们登录时，系统会为他们建立一个临时的用户配置文件（参见第10章的说明），而注销时此配置文件就会被删除。此组默认成员为用户账户Guest。
- **Network Configuration Operators**：此组内的用户可以执行常规的网络配置工作，例如更改IP地址，但是不可安装、删除驱动程序与服务，也不能执行与网络服务器配置有关的工作，例如DNS服务器与DHCP服务器的设置。
- **Performance Monitor Users**：此组内的用户可监视本地计算机的运行性能。
- **Power Users**：为了简化组，这个在旧版Windows系统就已经存在的组就要被淘汰



了，Windows Server 2008（含）之后的系统虽然还留着这个组（以便维持与旧版Windows系统的兼容性），不过并没有像旧版系统一样被赋予较多的特殊权限，也就是它的权限并没有比普通用户多。

- ✎ **Remote Desktop Users:** 此组内的用户可以从远程计算机利用远程桌面服务登录。
- ✎ **Users:** 此组内的用户只拥有一些基本权限，例如运行应用程序、使用本地与网络打印机、锁定计算机等，但是他们不能将文件夹共享给网络上其他的用户、不能将计算机关机。所有新建的本地用户账户都会自动隶属于此组。

4.1.3 特殊组账户

除了前面所介绍的组之外，Windows Server 2016内还有一些特殊组，而且无法更改这些组的成员。下面列出几个常见的特殊组：

- ✎ **Everyone:** 所有用户都属于这个组。若Guest账户被启用的话，则在分配权限给Everyone时要小心，因为如果一位在计算机内没有账户的用户通过网络登录计算机时，他会被自动允许利用Guest账户来连接，此时因为Guest也是隶属于Everyone组，所以他将具备Everyone所拥有的权限。
- ✎ **Authenticated Users:** 凡是利用有效用户账户来登录此计算机的用户，都隶属于此组。
- ✎ **Interactive:** 凡是在本地登录（通过按Ctrl + Alt + Del方式登录）的用户，都隶属于此组。
- ✎ **Network:** 凡是通过网络来登录此计算机的用户，都隶属于此组。
- ✎ **Anonymous Logon:** 凡是未利用有效的普通用户账户登录的用户（匿名用户），都隶属于此组。Anonymous Logon默认并不隶属于Everyone组。
- ✎ **Dialup:** 凡是利用拨号方式连接的用户，都隶属于此组。

4.2 本地用户账户的管理

系统默认只有Administrators组内的用户才有权限来管理用户账户与组账户，所以此时请利用隶属于该组的Administrator登录系统来执行以下操作。

4.2.1 新建本地用户账户

我们可以利用本地用户和组来建立本地用户账户：【单击左下角的开始图标☛Windows系统管理工具☛计算机管理☛系统工具☛本地用户和组☛如图4-2-1中背景图所示，选中用户后右击☛新用户☛在前景图中输入用户的相关数据☛单击创建按钮】。

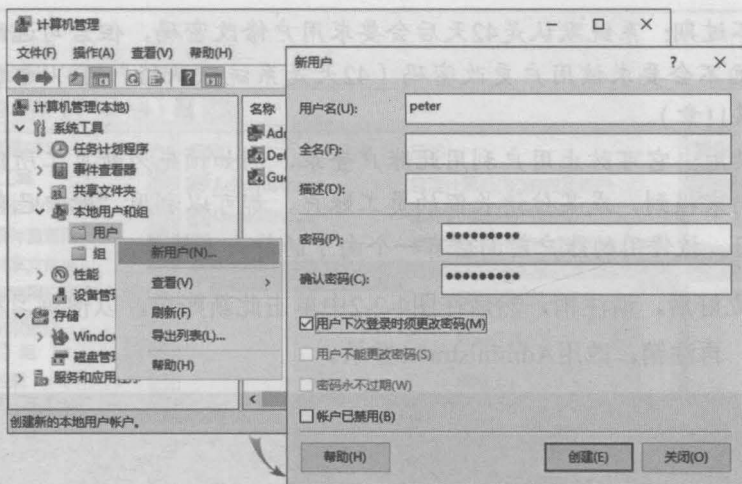


图 4-2-1

附注

也可以通过【开始☞控制面板☞用户账户】来管理用户账户。

- 用户名：它是用户登录时需要输入的账户名称。
- 全名、描述：用户的完整名称，用来描述此用户账户的说明文字。
- 密码、确认密码：设置用户账户的密码。所输入的密码会以黑点来显示，以免被其他人看到，必须再一次输入密码来确认所输入的密码是正确的。

注意

1. 密码中英文字母大小写被视为不同的字符，例如abc12#与ABC12#是不同密码，还有如果密码为空白，则系统默认是此用户账户只能够本地登录，无法通过网络登录（无法从其他计算机利用此账户来连接）。
2. 如果设置密码，则默认要求用户的密码必须至少6个字符，且不可包含用户账户名称或全名，还有至少要包含A - Z、a - z、0 - 9、非字母字符（例如!、\$、#、%）等4组字符中的3组，例如12abAB是一个有效的密码，而123456是无效的密码。

- 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，这个操作可以确保只有该用户知道自己所设置的密码。

注意

若该用户是通过网络来登录的话，请勿勾选此选项，否则用户将无法登录，因为用户通过网络登录时无法更改密码。

- 用户不能更改密码：它可防止用户更改密码。如果没有勾选此选项的话，用户可以在登录完成后，通过【按Ctrl + Alt + Del ☞更改密码】的方法来更改自己的密码。



- 密码永不过期：系统默认是42天后会要求用户修改密码，但若勾选此选项的话，则系统永远不会要求该用户更改密码（42天是系统默认值，可以通过账户策略来更改，见第11章）。
- 账户已禁用：它可防止用户利用此账户登录，例如预先为新员工所建立的账户，但该员工尚未报到，或某位请长假的员工账户，都可以利用“账户已禁用”暂时将该账户停用。被停用的账户前面会有一个向下的箭头↓符号。

用户账户建立好后，请注销，然后在图4-2-2中单击此新账户，以便练习利用此账户来登录。完成练习后，再注销，改用Administrator登录。

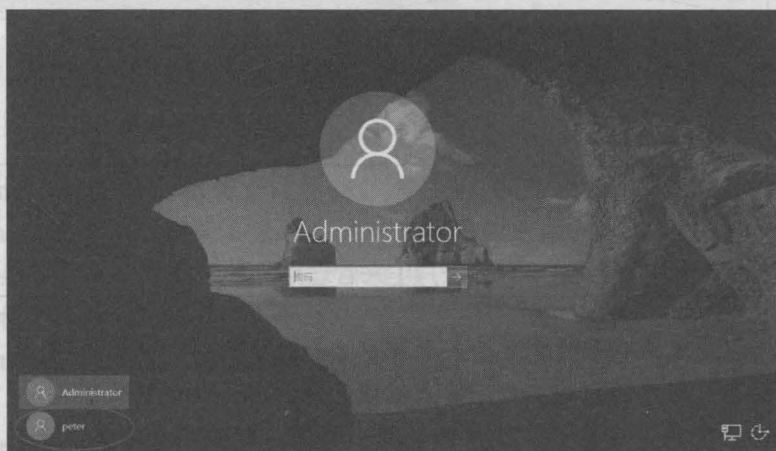


图 4-2-2

4.2.2 修改本地用户账户

如图4-2-3所示，选中用户账户，右击，然后通过界面中的选项来设置：

- 设置密码：用来更改用户的密码（请参阅下一节的说明）。
- 删除、重命名：您可以删除不需要的账户，也可以更改用户的账户名称，不过请注意以下说明。

系统会为每一个用户账户建立一个唯一的安全标识符（security identifier, SID，它是一串字母数字的组合），在系统内部是利用SID来代表该用户的，例如文件权限列表中是通过SID来记录该用户具备何种权限的，而不是通过用户账户名称来记录的，不过为了便于查看这些列表，当通过文件资源管理器来查看这些列表时，系统所显示的是用户账户名称。

当将账户删除后，即使再新建一个名称相同的账户，此时因为系统会为这个新账户分配一个新SID，它与原账户的SID不同，所以这个新账户不会拥有原账户的权限。

若是重命名账户的话，由于SID不会改变，因此用户原来所拥有的权限与权利都不会受到影响。例如，当某员工离职时，您可以暂时先将其用户账户停用，等到新员工接替他的工作时，再将此账户改为新员工的名称并重新设置密码与相关的个人资料。

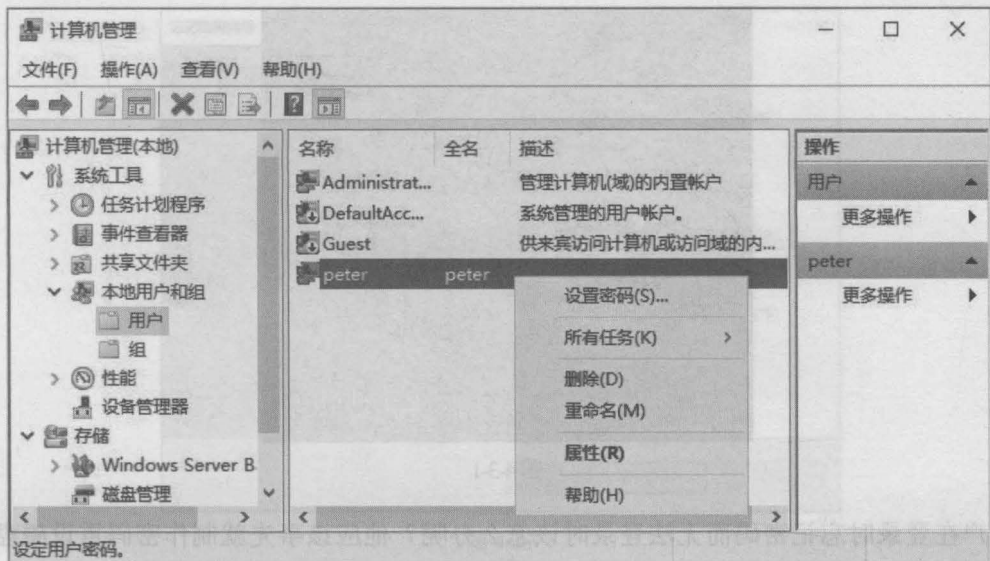


图 4-2-3

若要修改用户账户的其他相关数据，【选中用户账户后右击➤属性】。

4.2.3 控制面板中的用户账户管理工具

也可以通过【开始➤控制面板➤用户账户➤用户账户➤管理其他账户（如图4-2-4所示）】的方法来管理用户账户，它与前面所使用的本地用户和组各有特色。

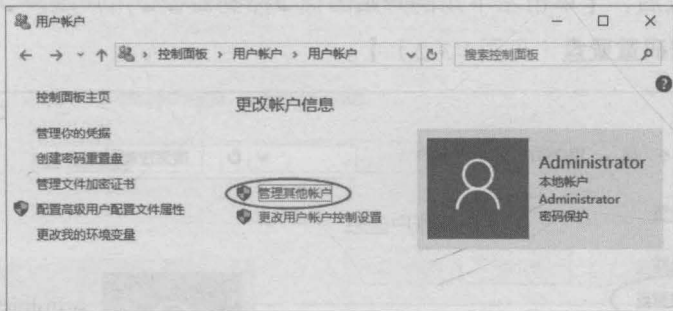


图 4-2-4

4.3 密码的更改、备份与还原

本地用户要更改密码的话，可以在登录完成后按 Ctrl + Alt + Del 键，然后在图4-3-1中单击更改密码。



图 4-3-1

用户在登录时忘记密码而无法登录时该怎么办呢？他应该事先就制作密码重置磁盘，此磁盘在密码忘记时可以派上用场。

4.3.1 创建密码重置盘

可以使用可移动磁盘（以下以U盘为例）来制作密码重置盘。

- STEP 1** 在计算机上插入已经格式化的U盘，若尚未格式化的话，先【打开文件资源管理器 ➡选中U盘，右击 ➡格式化】。
- STEP 2** 登录完成后，【单击左下角的开始图标 ➡控制面板 ➡用户账户 ➡用户账户 ➡单击左侧创建密码重置盘（见图4-3-2）】。

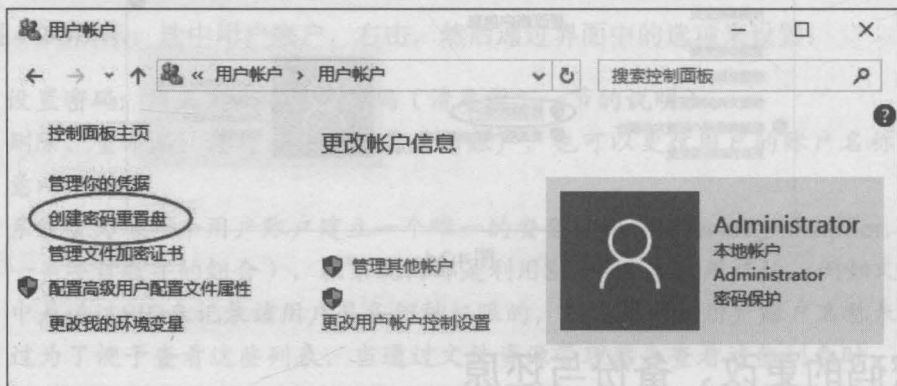


图 4-3-2

- STEP 3** 从图4-3-3中的说明可知密码重置磁盘制作完成之后，无论更改过多少次密码，都不需要再重新制作密码重置磁盘，单击下一步按钮。

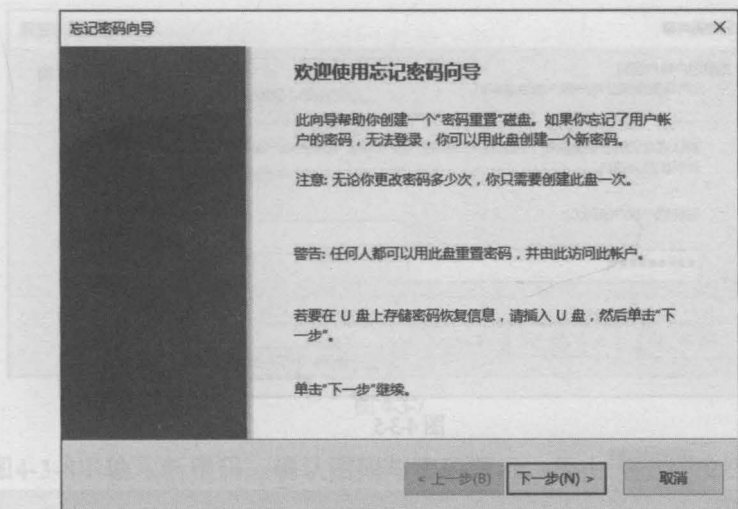


图 4-3-3

注意

请保管好**密码重置磁盘**，因为任何人得到它，就可以重设您的密码，进而访问您的个人数据。

STEP 4 在图4-3-4中选择利用可移动磁盘（U盘）。

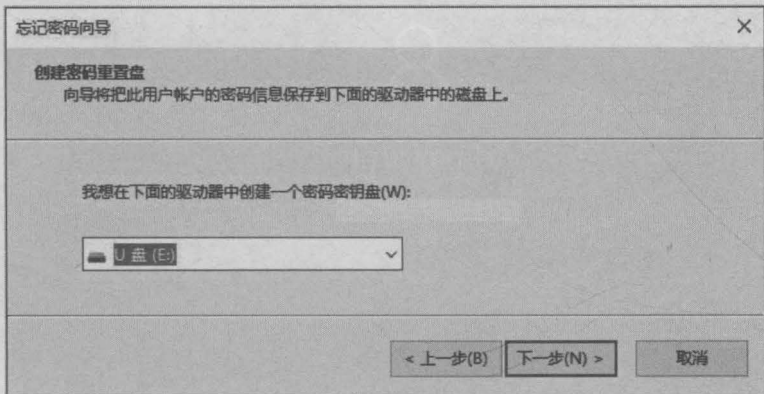


图 4-3-4

STEP 5 在图4-3-5中输入当前用户账户的密码，单击**下一步**按钮，完成后续的步骤。

注意

若您之前已经制作过**密码重置磁盘**，系统会警告之前密码重置磁盘将无法再使用。若所放入的磁盘已经是**密码重置磁盘**，系统会警告该磁盘内现有的密码信息将被覆盖。

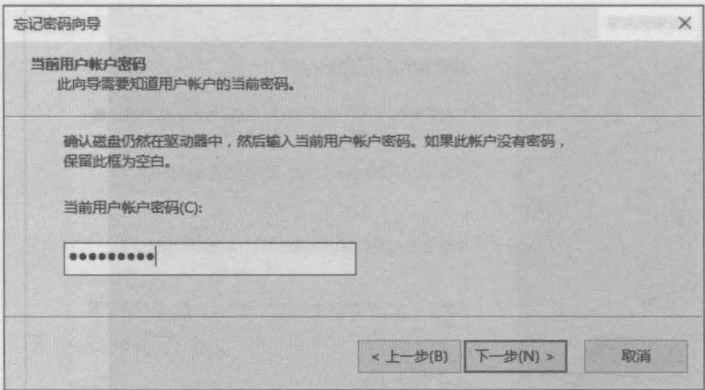


图 4-3-5

4.3.2 重置密码

如果用户在登录时忘记密码，此时就可以利用前面所制作的密码重置磁盘来重新设置一个新密码，其步骤如下所示：

STEP 1 在登录、输入错误的密码后，单击图4-3-6中的**重置密码**。

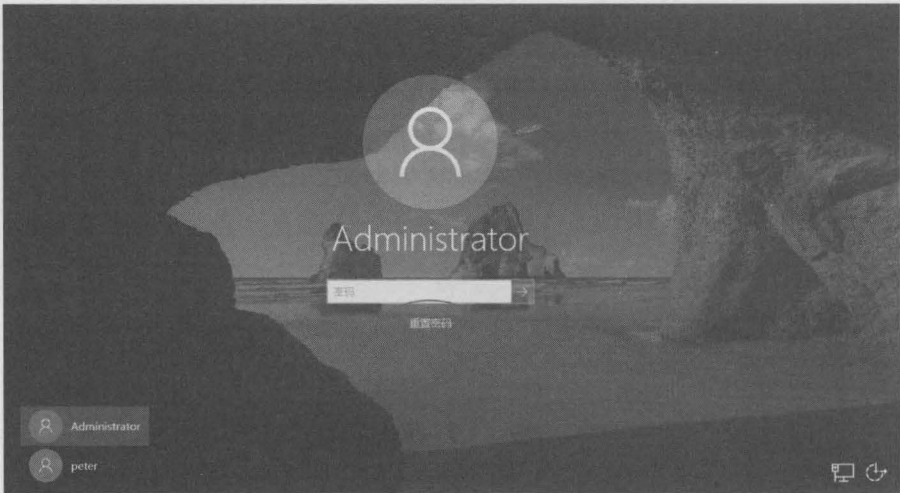


图 4-3-6

STEP 2 出现**欢迎使用密码重置向导**界面时单击**下一步**按钮。

STEP 3 在图4-3-7中选择所插入的U盘后单击**下一步**按钮。



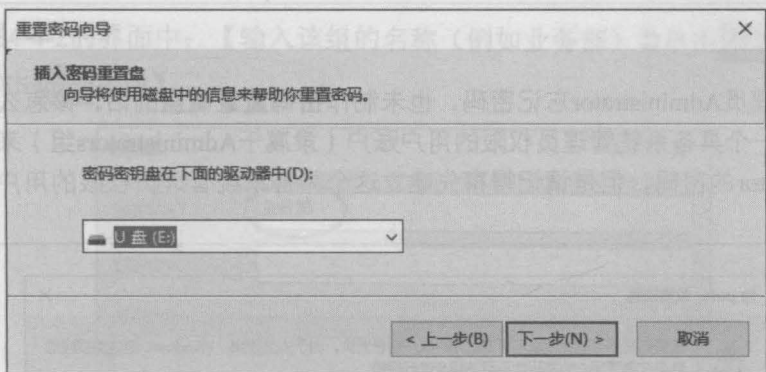


图 4-3-7

STEP 4 在图4-3-8中输入新密码、确认密码与密码提示，单击 **下一步** 按钮。

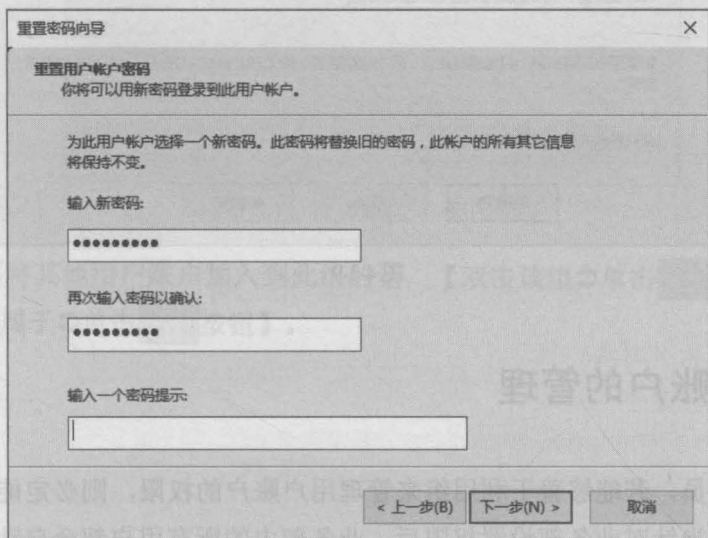









图 4-3-8

STEP 5 继续完成之后的步骤并利用新密码登录。

4.3.3 未制作密码重置磁盘怎么办

若用户忘记了密码，也未事先制作密码重置磁盘，此时则需请系统管理员为用户重置新的密码（无法查出旧密码）：**【单击左下角开始图标  Windows 管理工具  计算机管理  系统工具  本地用户和组  用户  选中用户账户后右击  设置密码】**，之后会出现如图4-3-9所示的警告信息，提示应该在用户未制作密码重置磁盘的情况下才使用这种方法，因为有些受保护的数据在通过此种方法将用户的密码更改后就无法再被用户访问了，例如被用户加密的文件、利用用户的公钥加密过的电子邮件、用户存储在本地计算机内用来连接Internet的密码等。

**注意**

若系统管理员Administrator忘记密码，也未制作**密码重置磁盘**的话，该怎么办？此时请利用另外一个具备系统管理员权限的用户账户（隶属于Administrators组）来登录与更改Administrator的密码，但是请记得事先建立这个具备系统管理员权限的用户账户，以备不时之需。

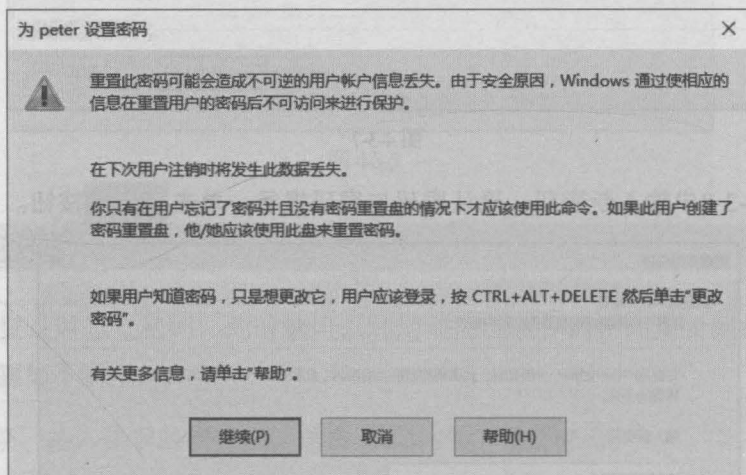







图 4-3-9

4.4 本地组账户的管理

作为系统管理员，若能够善于利用组来管理用户账户的权限，则必定能够减轻许多管理负担。举例来说，当针对业务部设置权限后，业务部内的所有用户都会自动拥有此权限，不需要为每个用户单独设置权限。建立本地组账户的方法为：【单击左下角**开始**图标Windows 管理工具计算机管理如图4-4-1所示选中**组**右击新建组】。

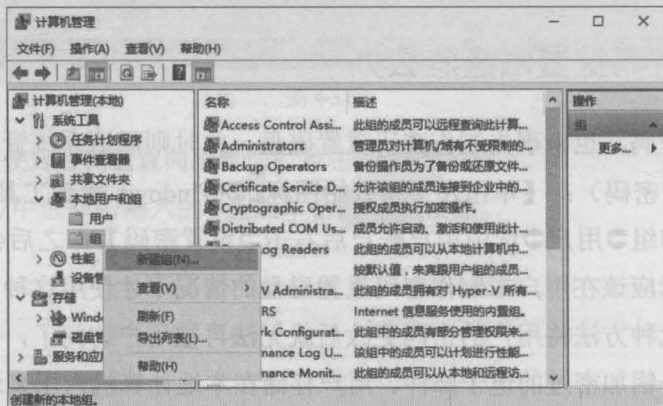


图 4-4-1



接着在图4-4-2的界面中：【输入该组的名称（例如业务部）】单击**添加**按钮来将用户加入到此组单击**创建**按钮】。

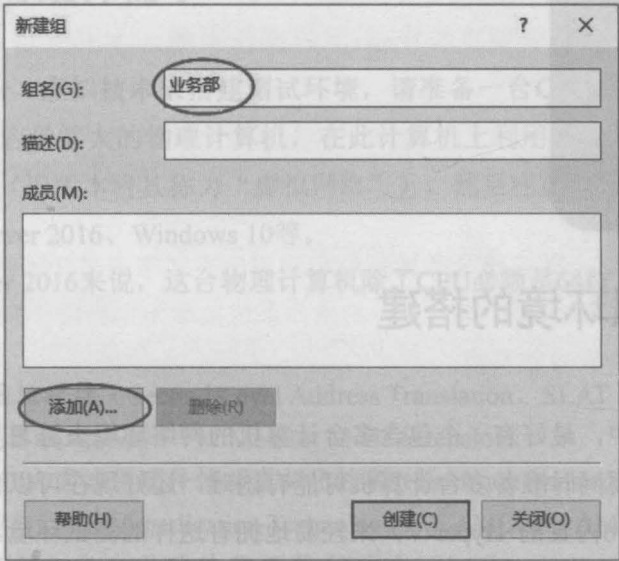


图 442

以后若要再将其他用户账户加入到此组的话，【双击该组】单击**添加**按钮】，或是【双击用户账户】隶属于单击**添加**按钮】。