

# 第3章 Windows Server 2008 的账户管理

# 技能目标

- n 理解本地用户账户和域用户账户的区别，熟悉内置本地用户账户及其功能。
- n 掌握本地用户账户命名规则、密码要求，使用服务器管理器、计算机管理器或**net user**命令创建本地用户账户。
- n 掌握**本地用户**账户的属性设置及管理任务。
- n 熟悉**内置本地组**账户及其功能，掌握本地组账户的创建与管理方法。

# 第3章 Windows Server 2008的账户管理

- n § 1 工作场景导入
- n § 2 用户账户
- n § 3 本地用户账户管理
- n § 4 本地组账户管理
- n § 5 回到工作场景
- n § 6 工作实训营、训练实例
- n § 7 习题

# § 1 工作场景导入

## n 工作场景

- n 控制员工对该服务器的访问，需要对各员工进行身份验证
  - n (1) 设计部有经理、副经理各1名，有5个设计小组，每个设计小组有设计人员5~6人，每个小组设主管1名，另外还有归档员、打印员等辅助性人员。
  - n (2) 设计人员访问服务器的权限基本相同；经理、副经理及各组主管对服务器访问权限较大；各个设计小组都有各自的文档，仅供本组使用。

## n 引导问题

- n (1) **Windows Server 2008**有哪些用户账户类型，它们有什么区别？有哪些内置本地用户账户，它们分别有什么功能？
- n (2) 本地用户账户命名有何规则？对密码有什么要求？如何创建本地用户账户？本地用户账户有哪些属性，如何设置？如何批量创建用户账户？
- n (3) 组账户有什么功能？**Windows Server 2008**有哪些内置的组账户？如何创建与管理本地组账户？

## § 2 用户账户

- n § 2.1 用户账户简介
- n § 2.2 默认本地用户账户

## § 2.1 用户账户简介

### n 用户账户机制

- n 维护计算机操作系统安全的基本而重要的技术手段
- n 操作系统通过用户账户来辨别用户身份，让具有一定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计算机的共享资源
- n 系统管理员根据不同用户的具体工作情景，指派不同用户、不同的权限，让用户执行并完成不同功能的管理任务

### n 用户标识符

- n 唯一的
- n 启动运行之初或登录系统已运行的过程中，都将要求用户输入指定的用户名和密码
- n 比较用户输入的账户标识符和密码与本地安全数据库中的用户相关信息是否一致

## § 2.1 用户账户简介

- n 两种用户账户
  - n 本地账户
    - n 本地安全目录数据库中建立的账户
    - n 只能登录到建立该账户的计算机上，并访问该计算机上的系统资源
    - n 用户信息保存在安全数据库(SAM)中
    - n 位于%Systemroot%\system32\config文件夹下
  - n 域账户
    - n 建立在域控制器的活动目录数据库中的账户
    - n 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

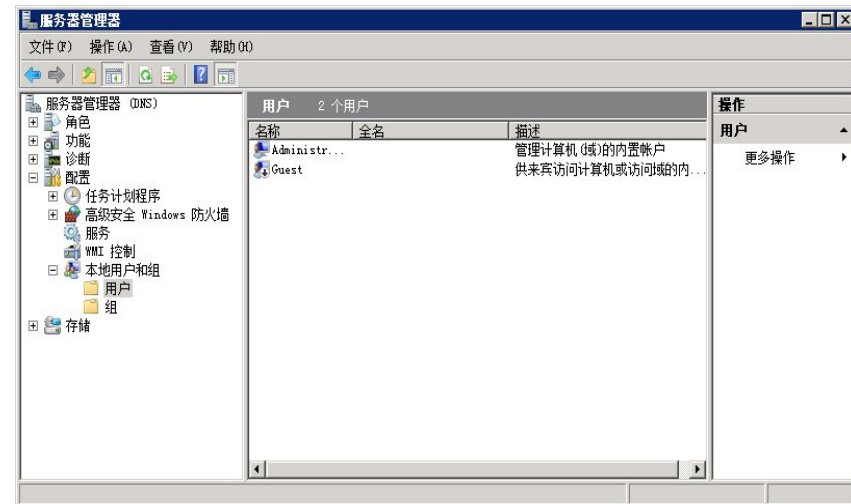
## § 2.2 默认本地用户账户

### n (1)Administrator

- n 系统管理员
- n 拥有最高的使用资源权限
- n 为了安全起见，用户可以根据需要改变其名称或禁用该账户
- n 无法删除

### n (2) Guest

- n 临时访问计算机的用户而提供的账户
- n 自动添加的，不能删除
- n 在默认情况下，**Guest**账户是禁用的
- n 只拥有很少的权限，可以改变其使用系统的权限





## § 3 本地用户账户管理

- n § 3.1 创建本地用户账户
- n § 3.2 管理本地用户账户属性
- n § 3.3 本地用户账户的其他管理任务

## § 3.1 创建本地用户账户

### n 1. 规划本地用户账户

#### 1) 用户账户命名规划

##### (1) 注意事项

- ① 账户名必须唯一
- ② 账户名不能包含以下字符：?、+、\*、/、\、  
[、]、=、<、>、【，等等。
- ③ 账户名称识别字符：只识别前**20** 个字符
- ④ 用户名不区分大小写。

##### (2) 推荐策略

- ① 用户全名：使用真实姓名
- ② 用户登录名：方便记忆和具有安全性，一般采用姓的拼音加名的首字母

## § 3.1 创建本地用户账户

### n 2) 用户账户密码的规划

(1) 最短密码：至少**6**个字符

(2) 尽量采用长密码：最长可以**127** 个字符

(3) 采用大小写、数字和特殊字符组合密码

① 不包含用户的账户名，不包含用户账户名中超过两个连续字符的部分

② 至少包含以下**4**类字符中的**3**类字符：

n 英文大写字母(A~Z)

n 英文小写字母(a~z)

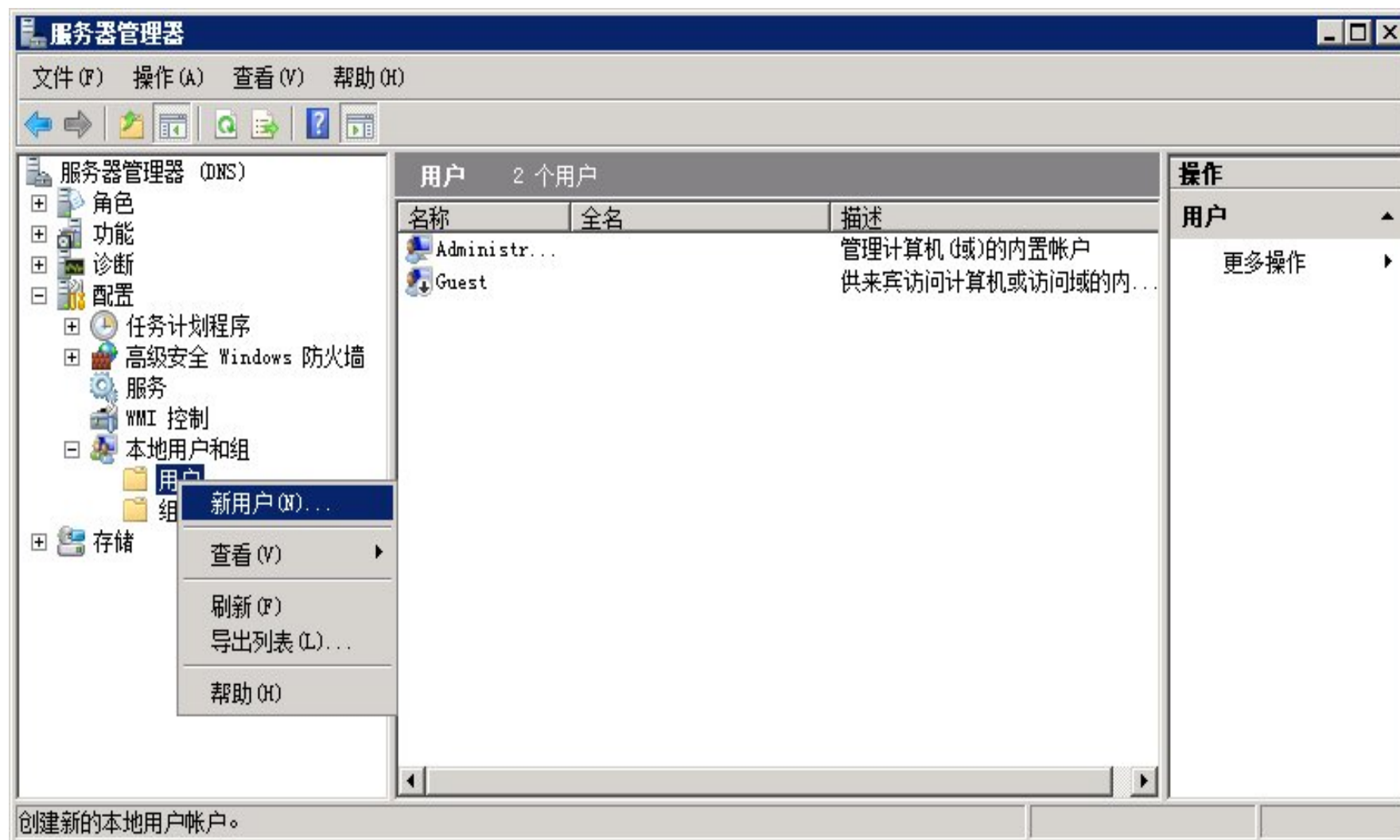
n 10个阿拉伯数字(0~9)。

n 非字母字符(例如：!、@、#、\$、? 、...)

## n 2. 创建用户账户

n 谁能创建用户：拥有管理员权限

n 创建工具：服务器管理器



## n 创建步骤

- n (1) 右击【用户】节点，选择【新用户】命令
- n (2) 在【新用户】对话框中，输入用户名、全名和用户描述信息和用户密码，指定用户密码选项

新用户

用户名 (U): zhangwr

全名 (F): 张伍荣

描述 (D): 网管中心

密码 (P): ●●●●●●●●●●●●

确认密码 (C): ●●●●●●●●●●●●

☒ 用户下次登录时须更改密码 (M)

☐ 用户不能更改密码 (S)

☐ 密码永不过期 (W)

☐ 帐户已禁用 (B)

帮助 (H) 创建 (E) 关闭 (O)

## § 3.1 创建本地用户账户

表 3-1 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	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	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 <b>Guest</b>
密码永不过期	默认情况下， <b>Windows Server 2008</b> 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该限制继续使用。通常用于 <b>Windows Server 2008</b> 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取消对该项的选择

## § 3.1 创建本地用户账户

- n 安全标志符
  - n **Security Identifier, SID**
  - n 识别每个用户账户
  - n 唯一的
  - n 由系统自动产生
  - n 指派权利、授权资源访问权限都需要使用**SID**
  - n 通过**whoami /logonid**命令查询



```
管理员: 命令提示符

C:\Users\Administrator>whoami /logonid
S-1-5-5-0-140471

C:\Users\Administrator>
```

- n 一个用户帐号包含了用户的名称、密码、所属组、等信息，在添加一个用户帐号后，它被自动分配一个安全标识 SID，这个标识是唯一的，
- n 即使帐号被删除，它的 SID 仍然保留，
- n 如果在计算机中再添加一个相同名称的帐号，它将被分配一个新的 SID。



## § 3.1 创建本地用户账户

- n § 使用net user创建用户账户
  - n 创建一个用户：
    - n net user student01 /add
  - n 创建用户名设置用户没有密码、用户不能更改密码
    - n net user student02 /add /passwordchg:no /passwordreq:no

```
C:\Users\Administrator>net user student01 /add  
命令成功完成。
```

```
C:\Users\Administrator>net user student02 /add /passwordchg:no /passwordreq:no  
命令成功完成。
```

## § 3.1 创建本地用户账户

- n 创建大批量账户
  - n 使用记事本写入创建用户的命令
  - n 另存为以**.bat**为扩展名的批处理文件
    - net user student03 /add**
    - net user student04 /add**
    - net user student05 /add**
  - n 运行批处理文件

```
C:\Users\Administrator>createusers.bat
```

```
C:\Users\Administrator>net user student03 /add  
命令成功完成。
```

```
C:\Users\Administrator>net user student04 /add  
命令成功完成。
```

```
C:\Users\Administrator>net user student05 /add  
命令成功完成。
```

## § 3.2 管理本地用户账户属性

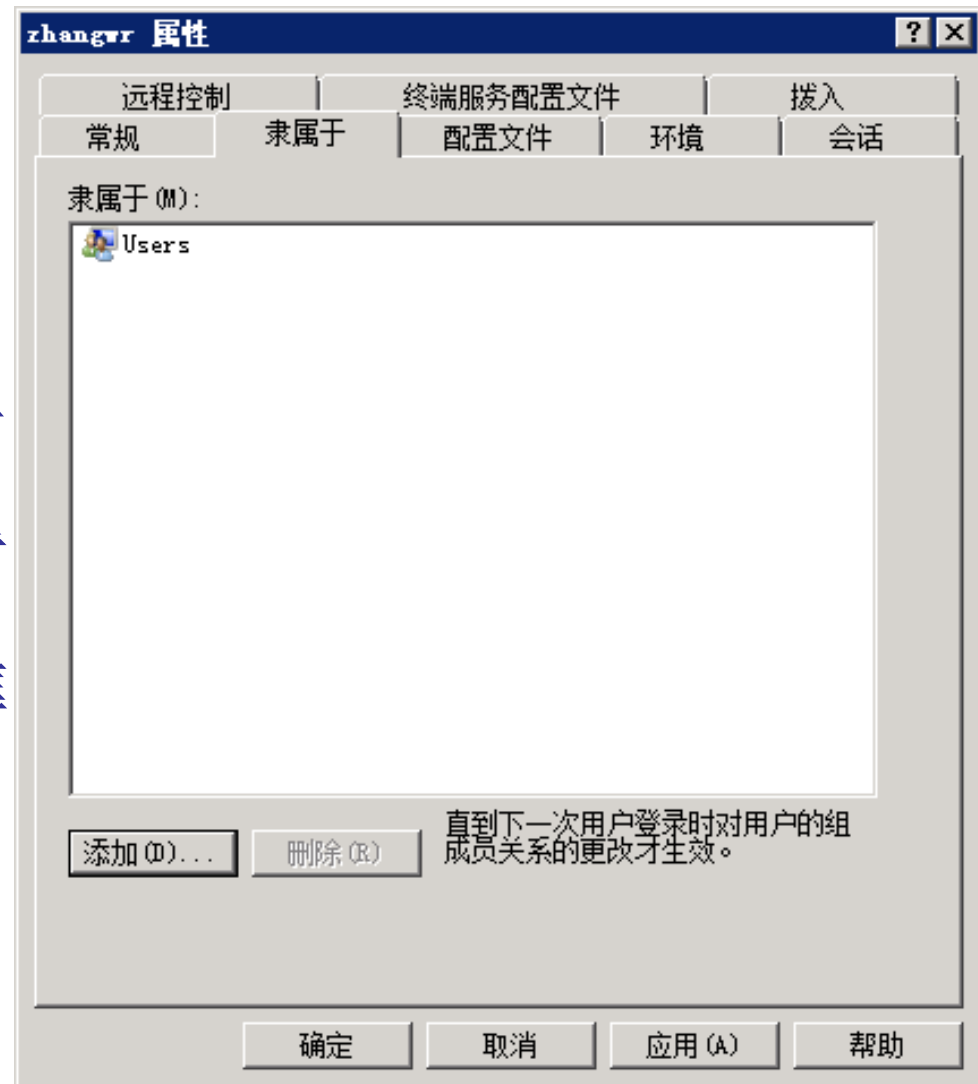
- n 1. 【常规】选项卡
  - n 账户描述信息
    - n 全名
    - n 描述
  - n 密码选项



## § 3.2 管理本地用户账户属性

### n 2. 【隶属于】选项卡

- n 设置将该账户和组之间的隶属关系
- n 将用户添加到管理员组的操作步骤：
  - n (1) 在【隶属于】选项卡中，单击【添加】按钮
  - n (2) 在【选择组】对话框中，输入需要加入的组的名称



## § 3.2 管理本地用户账户属性

**选择组** [?] [X]

选择此对象类型 (S):

组 [对象类型 (O)...]

查找位置 (F):

DNS [查找范围 (L)...]

输入对象名称来选择 (示例) (E):

[ ] [检查名称 (C)]

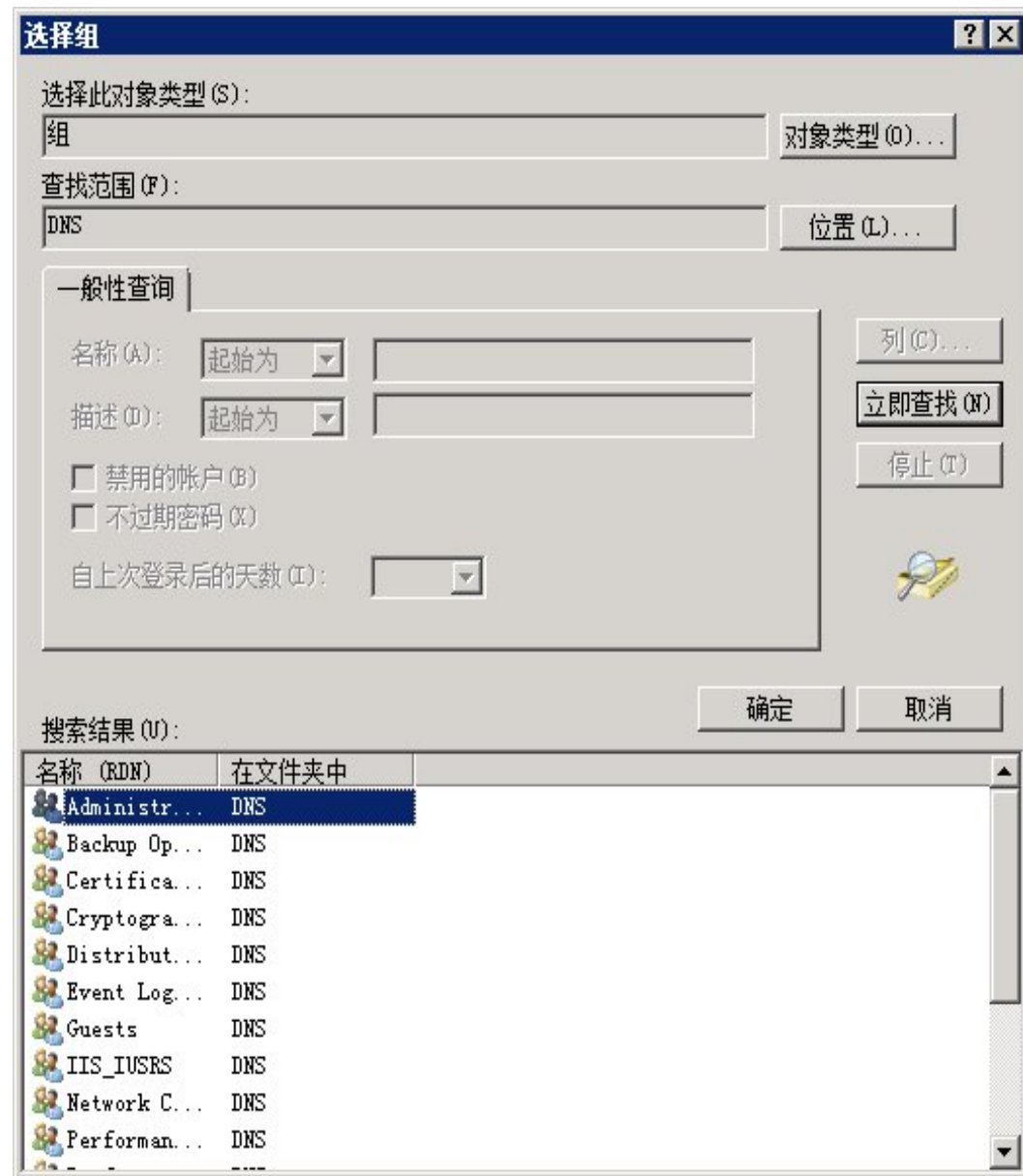
[高级 (A)...] [确定] [取消]

## § 3.2 管理本地用户账户属性

### n 2. 【隶属于】选项卡

n (3) 在展开后的【选择组】对话框中，单击【立即查找】按钮，从【搜索结果】列表框中选择一个或多个用户组

n (4) 切换到【隶属于】选项卡后，单击【确认】按钮



## § 3.2 管理本地用户账户属性



## § 3.2 管理本地用户账户属性

- n § 【配置文件】选项卡
  - n 用户配置文件
    - n 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
    - n 保持了用户桌面环境及其他设置的一致性
    - n 本地用户账户的配置文件保存在本地磁盘%userprofile%文件夹中
  - n 配置的主要内容
    - n 配置文件路径
    - n 登录脚本
    - n 主文件夹路径



Administrator 属性

远程控制 终端服务配置文件 拨入

常规 隶属于 配置文件 环境 会话

用户配置文件

配置文件路径 (P):

登录脚本 (L):

主文件夹

☒ 本地路径 (O):

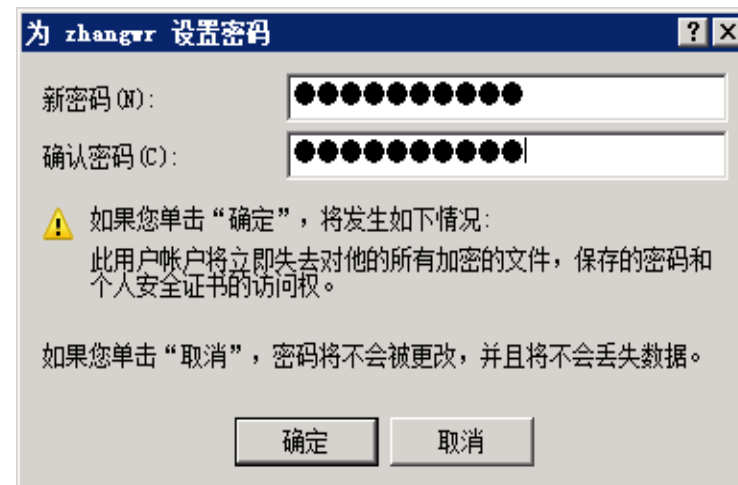
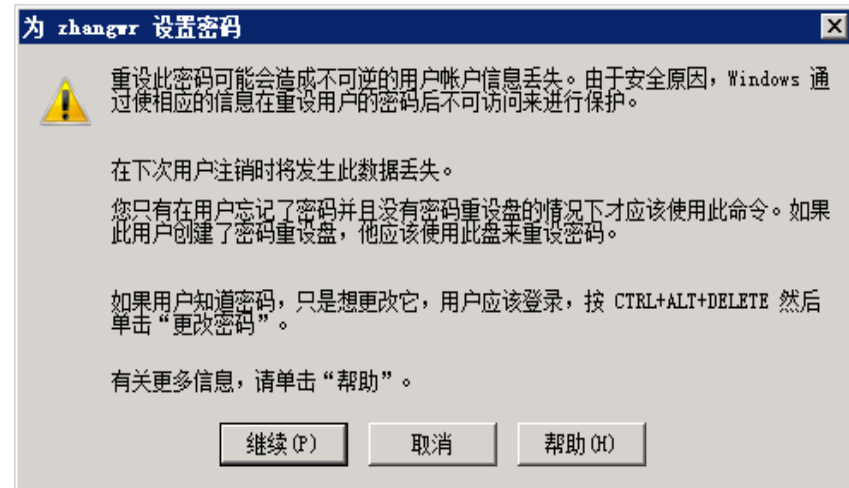
☐ 连接 (C): Z: 到 (T):

确定 取消 应用 (A) 帮助

## § 3.3 本地用户账户的其他管理任务

### n 1. 重设本地用户账户密码

- n (1) 右击用户账户，选择【设置密码】命令
- n (2) 提示对话框中，建议管理员不要重新设置密码
- n (3) 在设置密码对话框中，输入用户的新密码并确认



## § 3.3 本地用户账户的其他管理任务

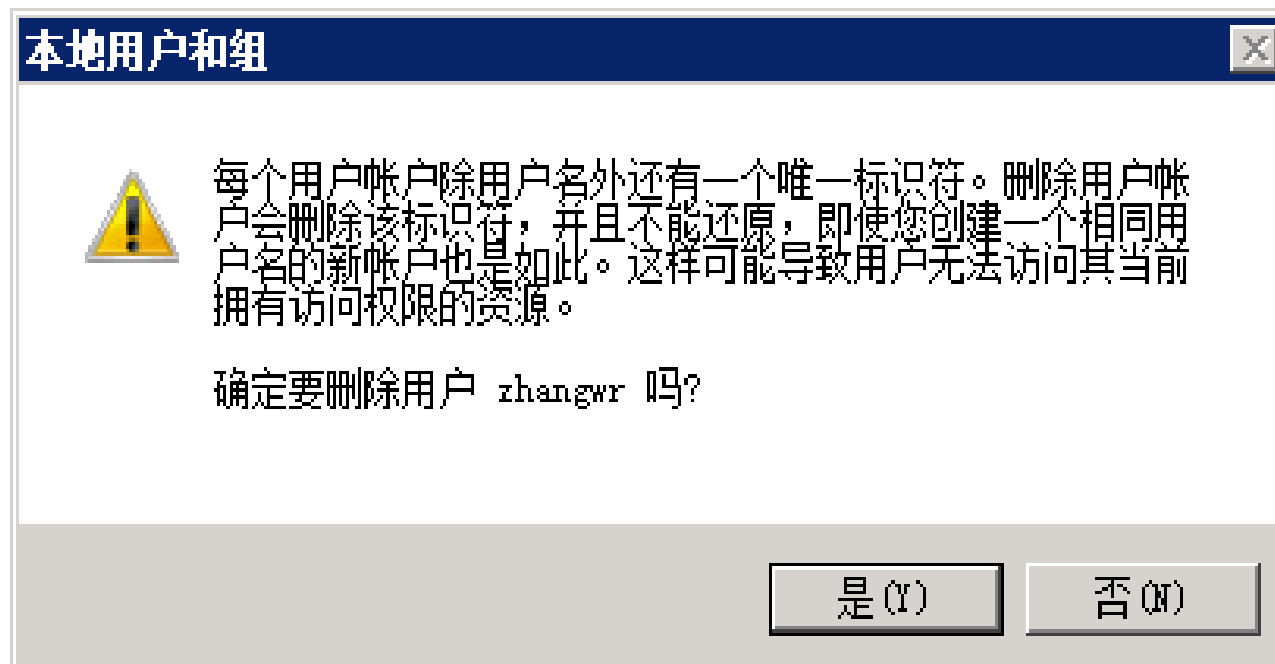
### n 2. 删除本地用户账户

n 系统内置账户如**Administrator**、**Guest** 等无法删除

n 操作步骤:

n (1) 右击需要删除的用户账户，选择【删除】命令

n (2) 在删除用户账户对话框中，单击【确定】按钮进行确认



## § 3.3 本地用户账户的其他管理任务

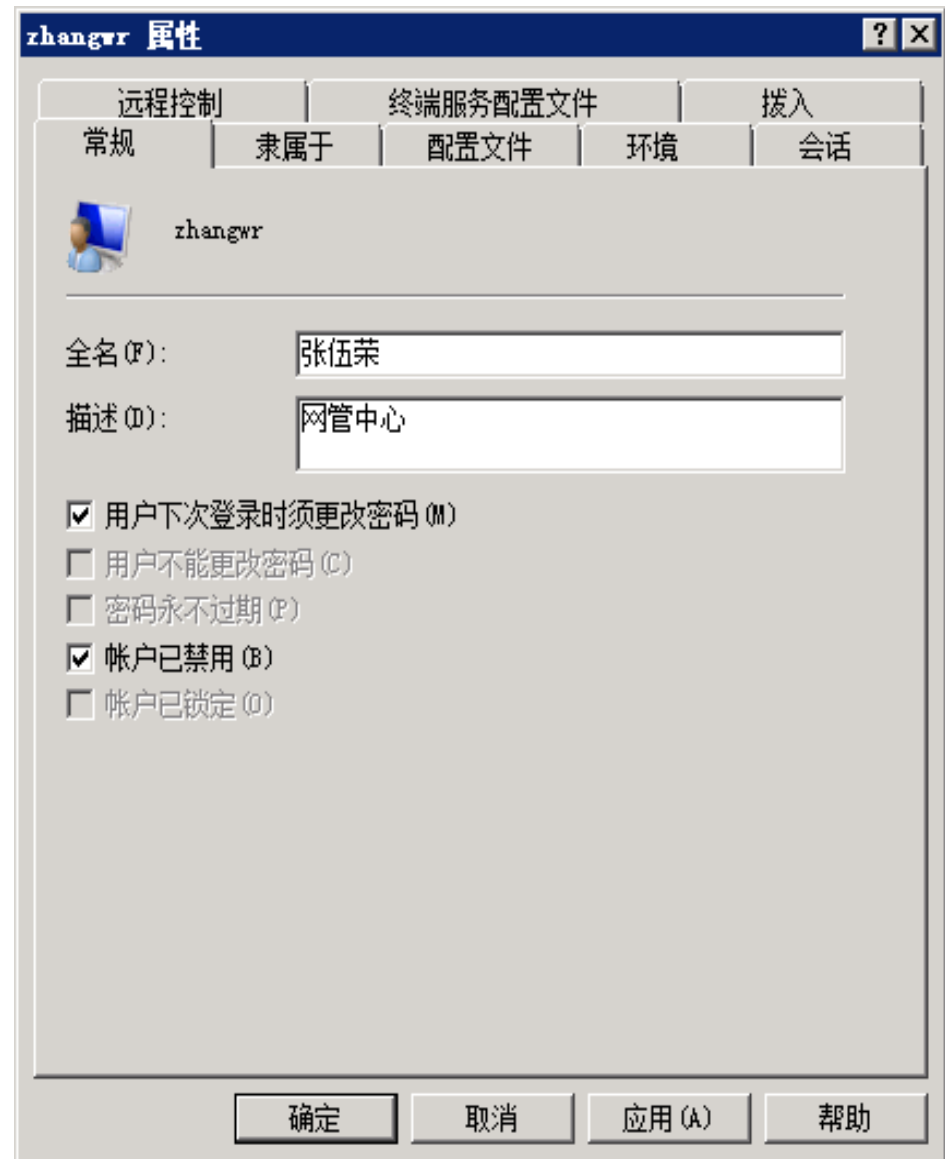
### n § 禁用或激活账户

#### n 作用

- n 临时停而不删除
- n 可重新激活

#### n 操作步骤:

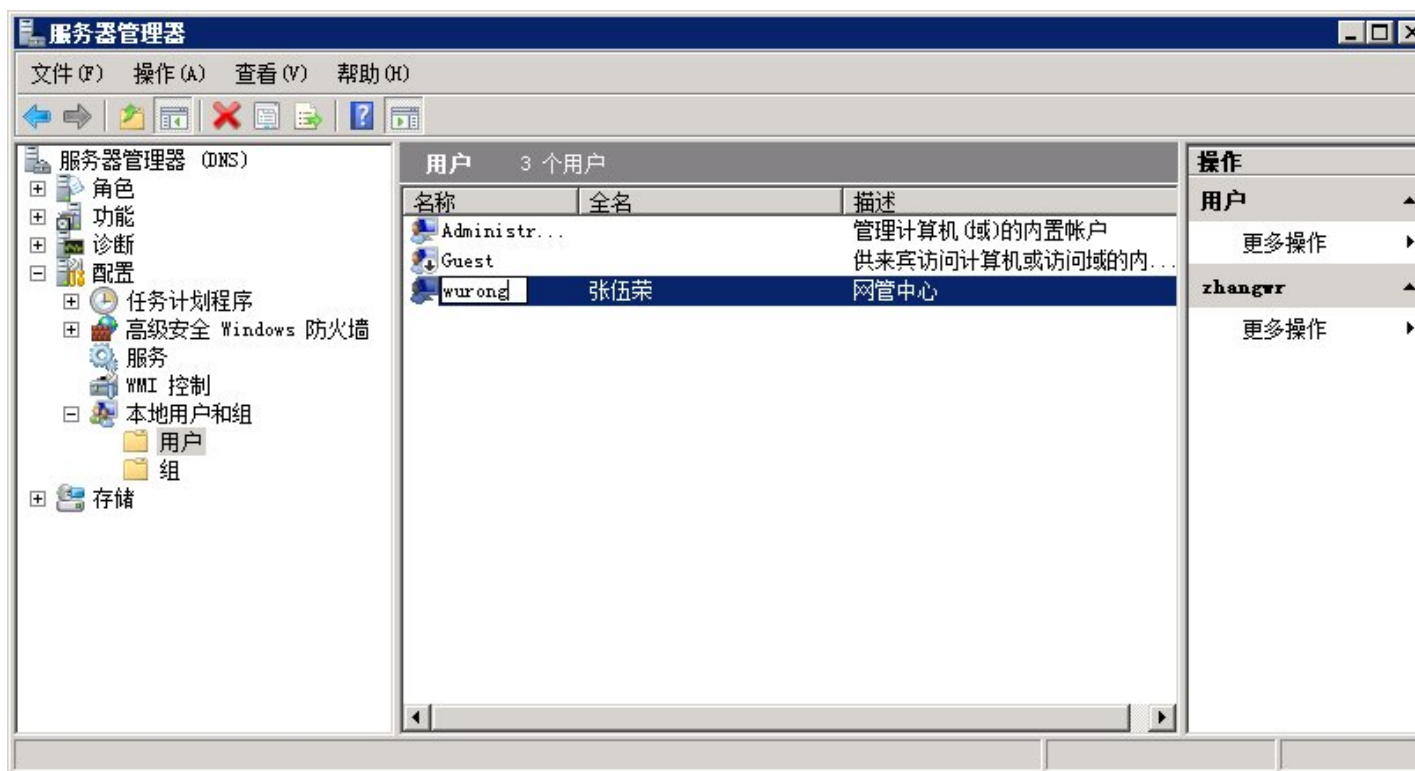
- n (1) 右击用户账户，选择【属性】命令
- n (2) 在【常规】选项卡
  - n 禁用：选中【账户已禁用】复选框
  - n 激活：取消选中【账户已禁用】复选框



## § 3.3 本地用户账户的其他管理任务

### n 4. 重命名

- n 用户名不符合命名规范
- n 重命名只是修改登录时系统的标识，用户账号的**SID**号并没有发生改变




## 其他启动用户管理方式

- n 控制面板->用户帐户
- n **control userpasswords**
- n **control userpasswords2**
- n **rundll32 netplwiz.dll,UsersRunDll**


用户帐户

用户 | 高级

 用下列表授予或拒绝用户访问您的计算机，还可以更改其密码和其他设置。


☒ 要使用本机，用户必须输入用户名和密码(E)

本机用户(U):

用户名	组
 Administrator	Administrators

添加(D)...    删除(R)    属性(O)

Administrator 的密码

 要更改您的密码，请按 Ctrl-Alt-Del 并选择“更改密码”。

重置密码(P)...

确定    取消    应用(A)

## § 4 本地组账户管理

- n § 4.1 组账户简介
- n § 4.2 默认本地组账户
- n § 4.3 创建本地组账户
- n § 4.4 本地组账户的其他管理任务

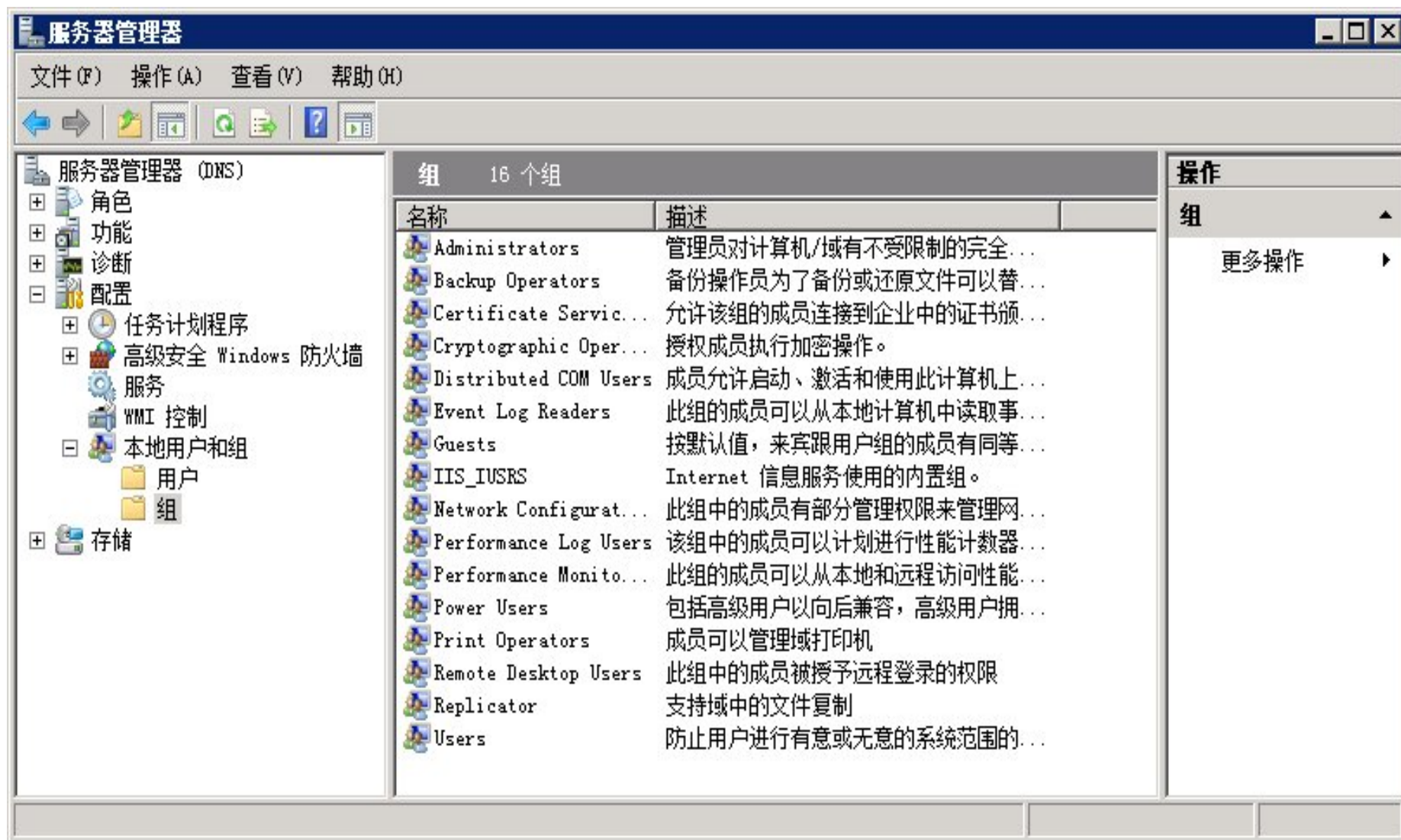


## § 4.1组账户简介

- n 多个用户、计算机账户、联系人和其他组的集合
- n 操作系统实现其安全管理机制的重要技术手段
- n 属于特定组的用户或计算机称为组的成员
- n 简化管理，提高效率
- n 组账户不能用于登录计算机操作系统
- n 同一个用户账户可以同时为多个组的成员，权限就是所有组权限的并集

## § 4.2默认本地组账户

- n 根据创建方式的不同，组可以分
  - n 用户自定义组
  - n 默认组
    - n 自动创建
    - n 查看本地默认组



## § 4.2默认本地组账户

表 3-2 默认组及描述

默 认 组	描 述
Administrators	此组的成员具有对计算机的完全控制权限，并且他们可以根据需要向用户分配用户权利和访问控制权限。 <b>Administrator</b> 账户是此组的默认成员。当计算机加入域中时， <b>Domain Admins</b> 组会自动添加到此组中。因为此组可以完全控制计算机，所以向其中添加用户时要特别谨慎。
Backup Operators	此组的成员可以备份和还原计算机上的文件，而无须理会保护这些文件的权限。这是因为执行备份任务的权利要高于所有文件权限。此组的成员无法更改安全设置。
Cryptographic Operators	已授权此组的成员执行加密操作。
Distributed COM Users	允许此组的成员在计算机上启动、激活和使用 <b>DCOM</b> 对象。
Guests	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，此配置文件将被删除。 <b>Guests</b> 账户(默认情况下已禁用)也是该组的默认成员。

## § 4.2默认本地组账户

续表

默 认 组	描 述
IIS_IUSRS	这是 <b>Internet</b> 信息服务(IIS)使用的默认组。
Network Configuration Operators	该组的成员可以更改 <b>TCP/IP</b> 设置, 并且可以更新和发布 <b>TCP/IP</b> 地址。该组中没有默认的成员。
Performance Log Users	该组的成员可以从本地计算机和远程客户端管理性能计数器、日志和警报。
Performance Monitor Users	该组的成员可以从本地计算机和远程客户端监视性能计数器。
Power Users	默认情况下, 该组的成员拥有不高于标准用户账户的用户权利或权限。在早期版本的 <b>Windows</b> 中, <b>Power Users</b> 组专门为用户提供特定的管理员权利和权限以执行常见的系统任务。在此版本 <b>Windows</b> 中, 标准用户账户具有执行最常见配置任务的能力, 例如更改时区。对于需要与早期版本的 <b>Windows</b> 相同的 <b>Power User</b> 权利和权限的旧应用程序, 管理员可以应用一个安全模板, 此模板可以启用 <b>Power Users</b> 组, 以假设具有与早期版本的 <b>Windows</b> 相同的权利和权限。

## § 4.2默认本地组账户

Remote Desktop Users	该组的成员可以远程登录计算机。
Replicator	该组支持复制功能。 <b>Replicator</b> 组的唯一成员应该是域用户账户，用于登录域控制器的复制器服务。不能将实际用户的用户账户添加到该组中。
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计算机。该组的成员无法共享目录或创建本地打印机。默认情况下， <b>Domain Users</b> 、 <b>Authenticated Users</b> 以及 <b>Interactive</b> 组是该组的成员。因此，在域中创建的任何用户账户都将成为该组的成员。

- n 管理员可以根据自己的需要向默认组添加成员或删除默认组成员，也可以重命名默认组，但不能删除默认组

## § 4.3创建本地组账户

### n 1. 规划本地组账户

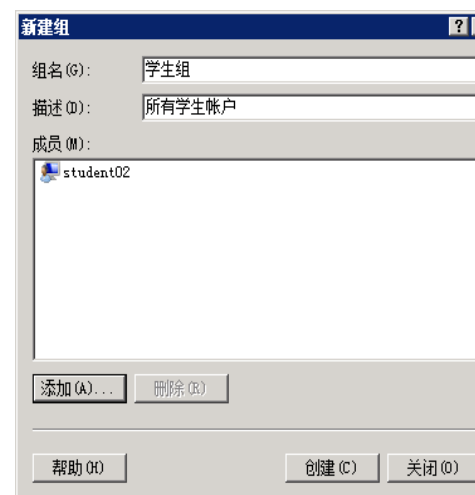
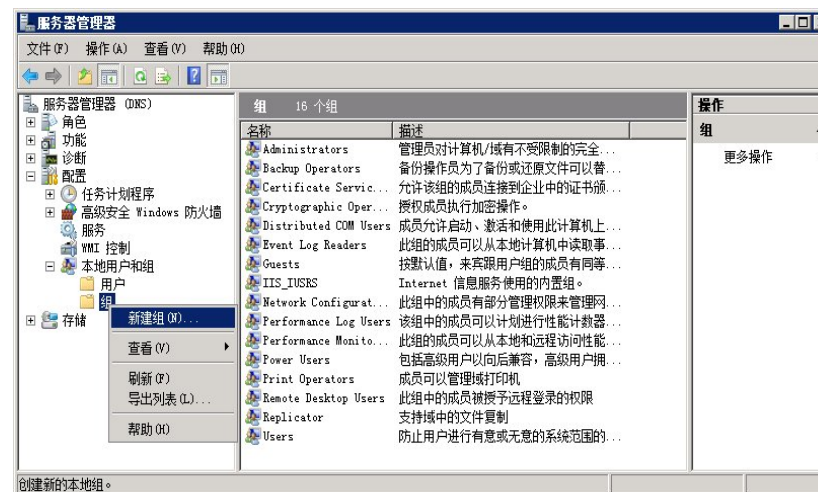
- n 不能与被管理的本地计算机上的任何其他组名或用户名相同
- n 不能用含有“、/、\、[、]、:、;、|、=、,、+、\*、?、<、>、@等字符
- n 不能只由句点 (.)和空格组成

## § 4.3创建本地组账户

### n 2. 使用服务器管理器创建本地组账户

n (1) 右击【组】节点，选择【新建组】命令

n (2) 在【新建组】对话框中输入组名和描述





## § 4.3创建本地组账户

n § 使用**net localgroup**命令创建本地组账户

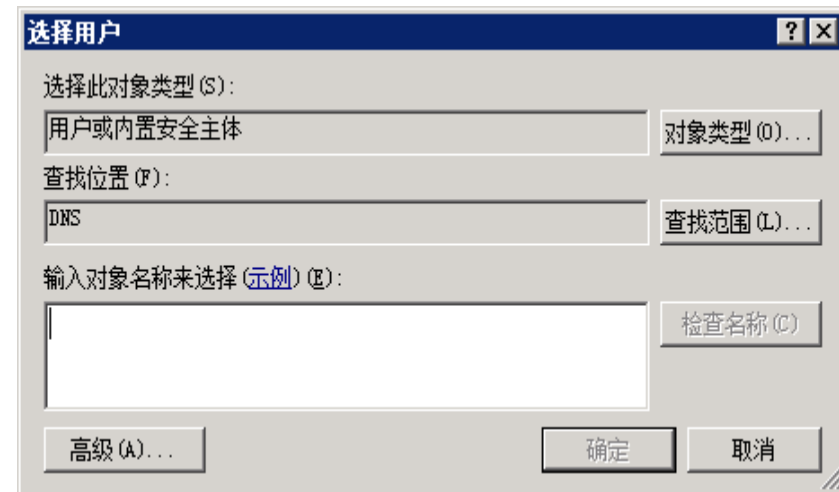
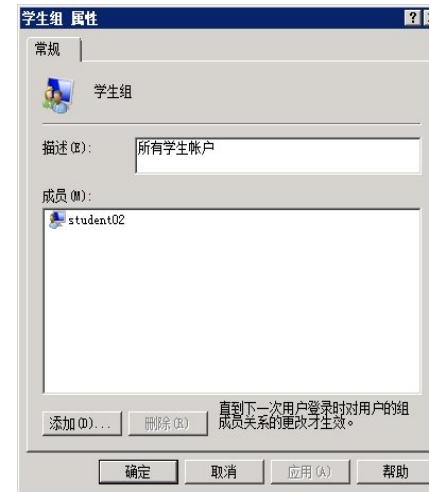
n (1) 打开【命令提示符】窗口

n (2) 执行命令

n **net localgroup 组名 /add**

## § 4.4本地组账户的其他管理任务

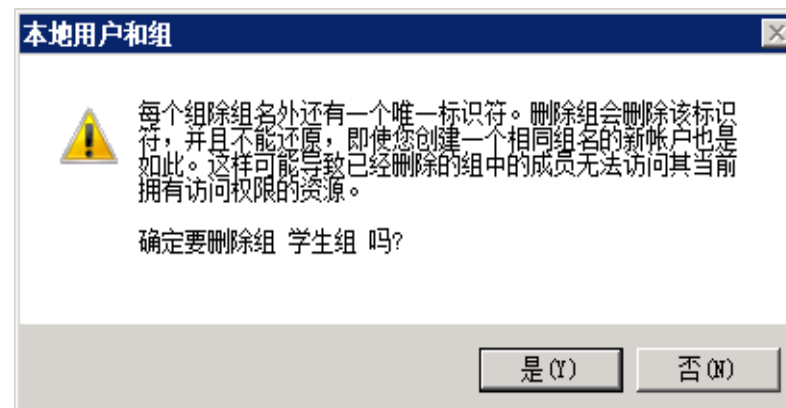
- n 1. 修改本地组成员
  - n (1) 打开用户组【属性】对话框，单击【添加】按钮
  - n (2) 在【选择用户】对话框中，可以在字段中输入成员名称，或者单击【高级】按钮查找用户，然后单击【确定】按钮
  - n (3) 如果要删除某组的成员，则双击该组的名称，选择相应要删除的成员，然后单击【删除】按钮即可



## § 4.4本地组账户的其他管理任务

### n 2. 删除本地组账户

- n (1) 用鼠标右键单击组，选择【删除】命令
- n (2) 在确认对话框中，确认删除
- n 每个组都拥有一个唯一的安全标识符(SID)，一旦删除了用户组，就不能重新恢复



## § 4.4本地组账户的其他管理任务

### n § 重命名本地组账户

n 用鼠标右键单击组，选择【重命名】命令

## § 5 回到工作场景

### n 创建用户

- n 制订本地用户账户命名规则、密码要求
- n 为每个员工创建一个本地用户账户

### n 创建用户组

- n 制订用户组命名规则和所属用户
- n 创建经理及主管、设计人员、设计一组、设计二组、设计三组、设计四组、设计五组等7个本地组账户
- n 修改上述7个本地组账户属性，将相关的员工的本地用户账户，加入到各自所属组中

## § 6 工作实训营

n § 6.1 训练实例

n § 6.2 工作实践常见问题解析

## § 6.1 训练实例

- n 实训环境和条件
  - n (1) VMware Workstation虚拟机软件。
  - n (2) 安装有Windows Server 2008的计算机或虚拟机。
- n 实训目的
  - n 理解本地用户账户和本地组账户的概念
  - n 掌握创建和管理本地用户账户和本地组账户的方法
- n 实训内容
  - n (1) 利用计算机管理控制台创建本地用户账户。
  - n (2) 使用net user命令批量创建本地用户账户。
  - n (3) 利用计算机管理控制台创建本地用户组账户。
- n 【实训过程】
  - n (略)

## § 6.2 工作实践常见问题解析

- n **【问题】**普通用户登录到计算机时，显示用户账户限制而登录失败，如何解决？
  - n **【答】**可能的原因包括不允许空密码，登录时间限制，或强制的策略限制。改用非空密码的账户试试，或者查看目标机上的本地策略，操作方法：在**【运行】**执行**gpedit.msc**命令，在**【计算机配置】\【Windows设置】\【安全设置】\【本地策略】\【安全选项】**下，将默认值**【启用】**改为**【禁用】**。