

windows server 系统用户与用户组管理

1、本地用户的含义

用户分为本地用户和全局用户。所谓“本地”用户指平时直接使用的计算机，本地用户对应着对等网工作组模式，用户验证都在各自的本地计算机上进行。全局用户对应着客户机/服务器工作模式，用户验证都在域控制器上进行。

本地用户只能建立在 **Windows 2003** 独立服务器、**Windows 2003** 成员服务器或基于 **Windows 2003 Professional** 的计算机中，这种用户的作用范围仅限于在创建该用户的计算机上，以控制用户对该计算机上资源的访问。也就是说，如果一个用户需要访问多台计算机上的资源，而这些计算机不属于某个域，则用户要在每一台需要访问的计算机上拥有相应的本地用户帐号，并在登录某台计算机时由该计算机验证。

2、系统内建用户

系统内建用户是 **Windows 2003** 操作系统自带的，在安装好 **Windows 2003** 之后这些用户就已存在，并已经赋予了相应的权限。**Windows 2003** 利用这此用户完成某些特定的工作。

Windows2003 中常见的内置用户包括系统管理员用户 **Administrator** 和来宾用户 **guest**（默认禁用）。系统内建用户和组都不允许被删除，并且 **Administrator** 帐号也不允许被禁用，但内建用户帐号允许更名。

没有能过系统验证的用户，都将自动转为 **guest** 用户访问系统。所以，从安全性角度考虑，**guest** 用户不要轻易启用。

3、组的相关知识

组是 **Windows 2003** 网络环境中的一个非常重要的概念,是用户帐号的集合,当用户较多的时候,就通常将具有相同身份和属性的用户组合到一个逻辑的集合中,并且一次赋予该集合访问资源的权限而不再单独给用户赋予权限,从而简化了管理。

一个用户帐号可属于多个组。用户登录后,如果又修改了权力权限,要再次登录才能生效。

本地组中有两种主要的组类型:用户创建的本地组和系统内置组。

a) Administrators 组的特点

1. 它是所有的 **Windows 2003** 上都有的惟一的一个被赋予了所有内建权力的组
2. 它可以给自己赋予所有自己没有的权力
3. 它可添加系统组件,升级系统
4. 它可配置系统重要参数,如注册表的修改
5. 它可配置安全信息

b) Power Users 组

1. 它存在于非域控制器上
2. 它可进行基本的系统管理工作
3. 它不能修改 **Administrators** 组和 **Backup Operators** 组
4. 它不能备份/恢复文件
5. 它不能修改注册表

c) Backup Operators 组

1. 它是所有的 **Windows 2003** 上都有的
2. 它可以忽略文件系统的权限进行备份和恢复
3. 它可以登录系统和关闭系统
4. 它对加密文件也可以做备份

d) Users 组

1. 它是一般用户所在的组，对系统可使用基本的权力。
2. 它可运行程序，使用网络
3. 它可以关闭 **Windows 2003Professional**，但不能关闭 **Windows 2003Sever**
4. 它不能创建共享目录和本地打印机

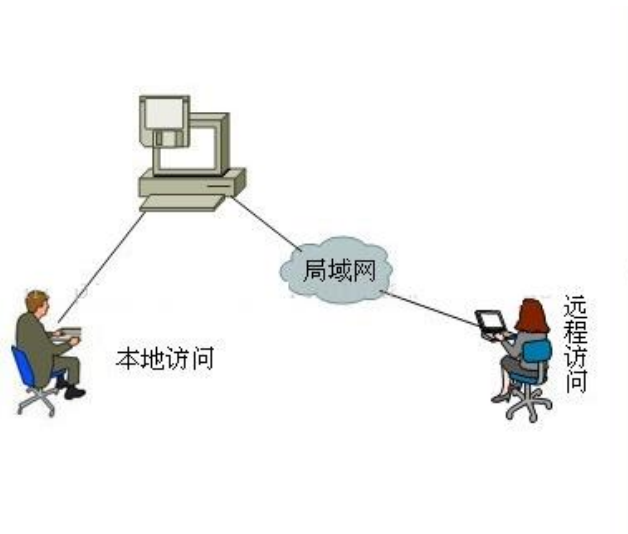
e) 系统内建的特殊组

1. Everyone 组：它包括所有的用户，包括 **guest**
2. Authenticated Users 组：它包含所有被身份验证成功的用户，但不包括 **guest** 组的成员，在 **Windows 2003Sever** 中是 Users 组的成员
3. Interactive 组：包含所有交互式登录的用户

4、实验过程及主要步骤

该实验中具体就是在计算机上建立实验文件夹，对本地访问的用户分配不同的权限，测试用户具有何种操作权限，然后将该文件夹发布于局域网中，再对远程访问用户给与不同的权限，测试远程用户的操作权限。下面具体的对用户和组的权限设置与管理进行详细介绍。

在该实验中用到的网络拓扑图如下：



4.1、创建帐号

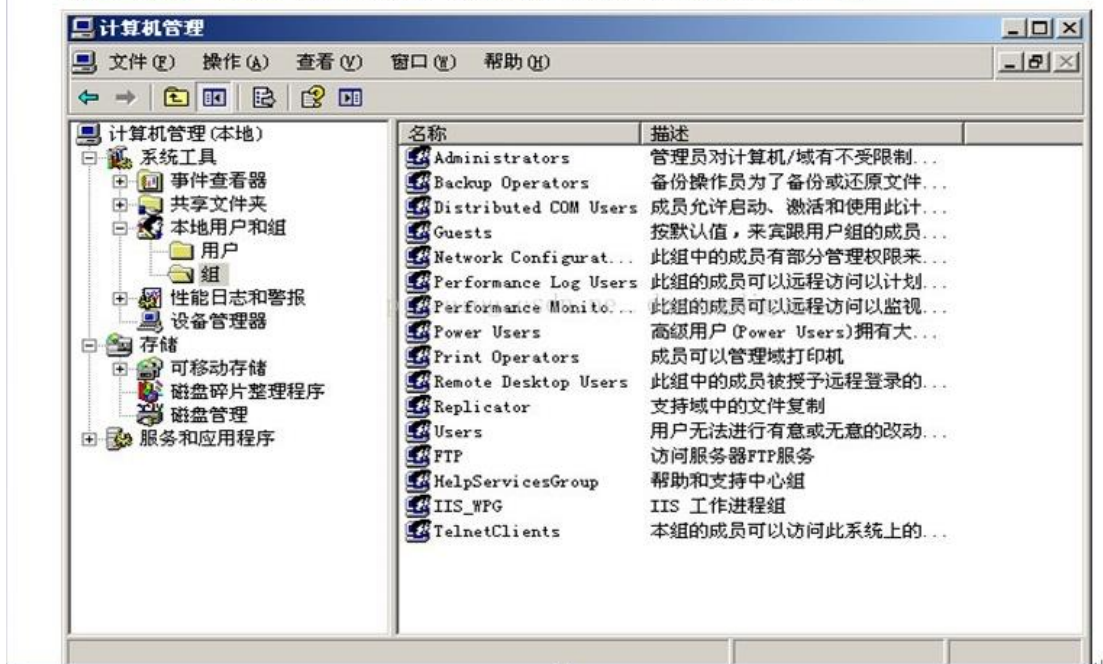
1. 启动 **Windows 2003 Server**，以管理员 (**Administrator**) 身份登录系统，右键点击“我的电脑”，选择管理菜单，就进入到“计算机管理”界面
2. 单击“本地用户和组”前面的加号，展开出现“用户”图标。在“用户”图标上右击，在弹出的快捷菜单中单击“新用户”
3. 打开“新用户”对话框后，在“用户名”文本框中输入用户帐号的登录名称，如输入“bdfw001”；在“全名”文本框中输入用户的全名，在“描述”文本框中输入帐号的简单描述，以方便日后的管理工作；在“密码”和“确认密码”文本框中输入相同的密码。

4.单击“创建”按钮后，该用户帐号会被创建，但新用户对话框不会消失，可以接着创建下一个用户帐号，如 bdfw002, bdfw003。最后，单击“关闭”按钮，结束新用户的创建。

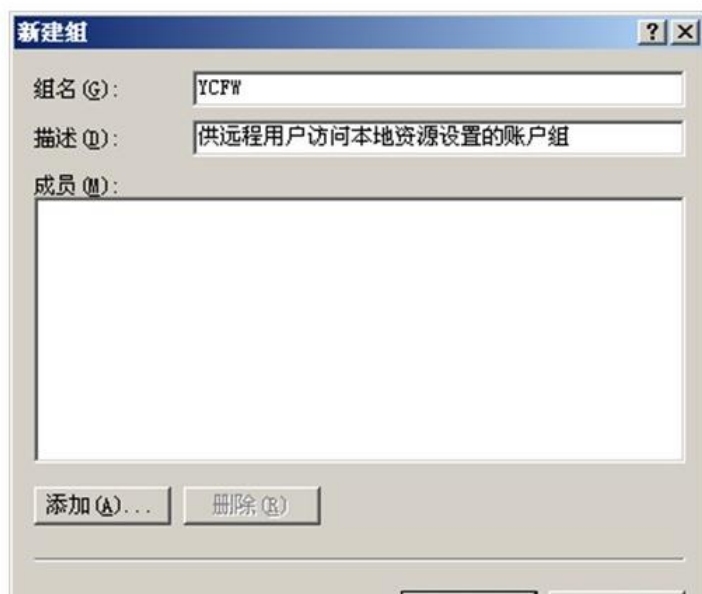
4.2、创建本地组

创建本地组的操作要由本地计算机的 **Administrators** 组或 **Account Operators** 组的成员进行，方法与创建本地用户类似，操作步骤如下：

1. 以系统管理员 **Administrator** 的身份登录。同样打开“计算机管理”窗口，在左窗口展开“本地用户和组”菜单，并且选择组，就可以看到本地组的情况。如图 1-4



2. 在打开的“新建组”对话框的“组名”文本框中输入该组的名称，如 ycfw，在“描述”文本框中可以简单的输入该组的用途。可以通过单击“添加”按钮，在“成员”列表框中加入组的成员，如图 1-6 所示。



单击“创建”按钮，再单击“关闭”按钮，返回到“计算机管理”窗口中。这时在右侧的子窗口中可以看到新建的组。

4.3、本地用户权限分配

1.按照上述方法，建立用于本地访问资源的用户组“bdfw”，并建立用户“bdfw001”让它只隶属于组“bdfw”，不属于组“User”

然后在建立用于远程访问资源的用户组“ycfw”，并建立用户“ycwf001”让它只隶属于组“ycfw”.不属于组“User”.

在 D 盘新建一个文件夹，取名“试验 1”，再建几个子文件夹，放少许文件再里面，打开文件“试验 1”属性对话框，切换到“安全”标签。

点击添加按钮，把组“bdfw”加上，然后对它的权限进行分配，注意此时给权限的时候应该一项一项的加入，不要一次全给，这样方便看用户有何种操作权限。这里首先给“读取、禁止写入”权限。

2.然后把现在的用户“Administrator”注销掉，用“bdfw001”这个用户登陆，看该用户对文件夹有何种操作权限。大家还可以尝试多建几个用户，分别赋予其他的权限，操作方法一致。需要注意的是每给一个权限以后都必须看一下用户具有何种操作！

4.4、远程用户权限分配

方法和上面类似，首先应将现在的账户“administrator”密码进行修改，不能为“123456”，然后建立一个文件夹“试验 1-1”，将该文件共享，并且给“Administrator”组读取权限，给“ycfw”组完全控制权限。

然后在其他电脑上访问你刚才共享的文件，打开我的电脑，在地址栏输入**共享电脑 IP** 分别用账户“Administrator”用户和“ycfw001”进行访问，看两个用户之间的操作权限区别。如图 1-11 注意：当用一个用户登陆以后，系统将记住该

用户,在一定时间内在访问的话就不用输入用户名和密码了,为了换用户登陆可以进行一下操作,打开命令提示符,输入 **net use \\共享电脑 IP /del** 即可。