

第六章、用户与组管理

author：杨哥团队-史密斯

一、服务器系统版本介绍

windows服务器系统：win2000 win2003 win2008 win2012

linux服务器系统：Redhat Centos

二、用户管理

1.1 用户概述

- 每一个用户登录系统后，拥有不同的操作权限。
- 每个账户有自己唯一的SID（安全标识符）
- 用户SID：S-1-5-21-426206823-2579496042-14852678-500

系统SID：S-1-5-21-426206823-2579496042-14852678

- 用户UID：500
- windows系统管理员administrator的UID是500
- 普通用户的UID是1000开始

不同的账户拥有不同的权限，为不同的账户赋权限，也就是为不同账户的SID赋权限！

查看sid值：whoami /user

- 账户密码存储位置：c:\windows\system32\config\SAM #暴力破解/撞库
- windows系统上，默认密码最长有效期42天

1.2 内置账户

- 给人使用的账户：
 - administrator #管理员账户
 - guest #来宾账户
- 计算机服务组件相关的系统账号
 - system #系统账户 == 权限至高无上
 - local services #本地服务账户 == 权限等于普通用户
 - network services #网络服务账户 == 权限等于普通用户

1.3 配置文件

每个用户都有自己的配置文件（家目录），在用户第一次登录时自动产生，路径是：

win7/win2008 c:\用户\

xp/win2003 c:\Documents and Settings\

1.4 用户管理命令

```
net user                #查看用户列表
net user 用户名 密码    #改密码
net user 用户名 密码 /add #创建一个新用户
net user 用户名 /del    #删除一个用户
net user 用户名 /active:yes/no #激活或禁用账户
```

练习：

- 1、练习图形及命令行中，进行用户管理（包括创建、修改密码、删除用户、登录并验证家目录产生、及权限）
- 2、制作一个批处理脚本，可以实现自动创建用户！

三、组管理

3.1 组概述

组的作用：简化权限的赋予。

赋权限方式：

- 1) 用户---组---赋权限
- 2) 用户---赋权限

3.2 内置组

内置组的权限默认已经被系统赋予。

```
1) administrators    # 管理员组
2) guests             # 来宾组
3) users              # 普通用户组，默认新建用户都属于该组
4) network            # 网络配置组
5) print              # 打印机组
6) Remote Desktop    # 远程桌面组
```

3.3 组管理命令

```
net localgroup          # 查看组列表
net localgroup 组名      # 查看该组的成员
net localgroup 组名 /add  # 创建一个新的组
net localgroup 组名 用户名 /add # 添加用户到组
net localgroup 组名 用户名 /del # 从组中踢出用户
net localgroup 组名 /del  # 删除组
```

练习：

- 1、练习图形及命令行中，进行组管理（创建组、组成员添加、查看组成员、成员脱离组、删除组）
- 2、创建1个普通用户lisi，并将lisi提升为管理员，并验证lisi是否成功取得管理员权限！

四、服务管理

开始 -- 运行 -- services.msc