Windows系统和用户管理常用命令

1.1、系统操作命令

```
1、 start：启动一个单独的窗口来运行指定的程序或命令。
格式：start [选项] [程序 [参数]]
常用选项：
/d：设置应用程序的启动目录。
/b：在后台启动应用程序，不会显示新窗口。
示例：start /d "C:\Program Files\Internet Explorer" iexplore.exe
示例说明：在 "C:\Program Files\Internet Explorer" 目录下启动 iexplore.exe。

2、 tasklist：显示系统中正在运行的所有任务。
格式：tasklist [选项]
常用选项：
/S：指定远程系统。
/U：指定用户名。
/P：指定密码。
/M：显示加载的DLL模块。
示例：tasklist /S remotePC /U username /P password
示例说明：显示远程计算机 remotePC 上的任务列表，使用 username 和 password 作为登录凭据。

3、 taskkill：根据进程ID或进程名称终止任务。
格式：taskkill [选项] [/PID processID | /IM imageName]
常用选项：
/F：强制终止进程。
/T：终止指定进程及其子进程。
/PID：指定要终止的进程的 PID
/IM：通过映象名称终止进程
示例：taskkill /F /IM notepad.exe
示例说明：强制终止名为 notepad.exe 的进程。

4、 shutdown：关闭、重启或注销计算机。
格式：shutdown [选项]
常用选项：
/s：关闭计算机。
/r：重启计算机。
/a：终止系统关闭
/t：设置延迟时间（以秒为单位）。
/f：强制关闭应用程序。
/c：设置一个注释
示例：shutdown /r /t 60
示例说明：在 60 秒后重启计算机。

5、 systeminfo：显示计算机的详细系统信息。
格式：systeminfo [选项]
常用选项：
/S：指定远程系统。
/U：指定用户名。
/P：指定密码。
示例：systeminfo /S remotePC /U username /P password
```

```
示例说明：显示远程计算机 remotePC 的系统信息，使用 username 和 password 作为登录凭据。

6. 命令：reg
作用：对注册表进行相关操作
/v  表示选项之下要添加的值名
/t  注册表项数据类型
/d  要分配给添加的注册表值的数据
/f  不提示，强行改写现有注册表项
    reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v test /t
REG_SZ /d "c:\windows\system32\cmd.exe" /f  # 强制添加一条开机启动cmd的注册表项
    reg delete "hklm\software\microsoft\windows\currentversion\run" /v test /f #
强制删除值名为test的注册表项
    reg add
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters" /v
DefaultTTL /t REG_DWORD /d 64 /f  # 强制修改默认TTL值

7. 命令：netsh advfirewall
作用：设置防火墙
例：netsh advfirewall set allprofiles state off  # 关闭所有类型网络的防火墙
例：netsh advfirewall set allprofiles state on   # 开启所有类型网络的防火墙
例：netsh advfirewall firewall add rule name=TCP-In-8888 protocol=TCP
localport=8888 dir=in action=allow   #添加名为TCP-In-8888入站规则：允许TCP端口8888

例：netsh advfirewall firewall add rule name=TCP-In-8888 protocol=TCP
localport=8888 dir=in action=block   #添加名为TCP-In-8888入站规则：阻止TCP端口8888

例：netsh advfirewall firewall add rule name=TCP-out-8888 protocol=TCP
localport=8888 dir=out action=allow  #添加名为TCP-out-8888出站规则：允许TCP端口8888

例：netsh advfirewall firewall add rule name=TCP-out-8888 protocol=TCP
localport=8888 dir=out action=block  #添加名为TCP-out-8888出站规则：阻止TCP端口8888

例：netsh advfirewall firewall add rule name=允许ping protocol=icmpv4 dir=in
action=allow # 添加允许ping的规则

例：netsh advfirewall firewall delete rule name=xxx # 删除名为xxx的防火墙规则，如果
name=all 表示删除所有规则
```

一、 用户与组管理

1.1、用户概述

- 每一个用户登陆系统后拥有不同的权限。
- 每个账户有自己唯一的SID（安全标识符）
- 用户SID：S-1-5-21-1487092334-3931679330-1155163103-500
- 系统SID：S-1-5-21-1487092334-3931679330-1155163103
- **SID也就是安全标识符（Security Identifiers），是标识用户、组和计算机帐户的唯一的号码。在第一次创建该帐户时，会给帐户发布一个唯一的 SID。如果创建帐户，再删除帐户，然后使用相同的用户名创建另一个帐户，则新帐户将不具有授权给前一个帐户的权力或权限，原因是该帐户具有不同的 SID 号。**

- windows系统管理员administrator的UID是500
- 普通用户的UID是1000开始
- 查看当前用户的SID：whoami /user
- 查看所有用户的SID：wmic useraccount get name,sid
- Windows Server系统上，默认密码最长有效期42天

1.2、内置账户

- 给用户使用的账户

  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，真正意义上的管理账户

  local services　#本地服务账户，权限略小于普通用户，主要负责系统中的一些本地服务，例如音频服务、DHCP客户端服务等

  network services #网络服务账户，权限与普通用户相同， 主要负责一些网络相关的服务，例如DNS客户端服务

1.3、 账户管理命令

```
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 #激活账户

net user 用户名 /active:no #禁用账户
```

1.4、 组概述

- 组的作用：简化权限的赋予

  组和用户的关系：一个组可以有多个用户、一个用户可以属于多个组

- 常用内置组：内置组的权限默认已经被系统赋予

```
administrators # 管理员组

guests # 来宾组

users # 普通用户组，默认新建用户都属于该组

network # 网络配置组

print # 打印机组

Remote Desktop # 远程桌面组
```

1.5、 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
```

二、 批处理编写

- **批处理作用：自上而下的自动处理每一条命令，直到执行最后一条！**
- **创建批处理：新建一个记事本文件，然后将扩展名改为.bat**

```
案例：新建一个记事本文件，写入下列命令，然后修改扩展名为.bat，然后执行.bat文件查看效果
d:
cd \
del . /s /q
```

2.1、 批处理基本语句

```
命令：@echo off
作用：关闭回显功能，也就是屏蔽过程，建议放置在批处理的首行。

命令：rem
作用：添加注释

命令：pause
作用：暂停批处理运行

命令：title
作用：为批处理脚本设置标题
title 定时关机小程序

命令：mode con cols=50 lines=25
作用：设置批处理窗口大小
mode con cols=50 lines=25 & color 0a

命令：echo.
作用：在执行批处理脚本时，可以空一行。

命令：set
作用：设置变量，常用与在脚本中的互动赋值，也可用于查看系统变量
查看全部系统变量：set
互动赋值：set /p time=请输入时间：
常用系统变量：
    %username%  #显示当前登录用户的名字
    %USERPROFILE%  #显示当前用户的用户数据目录
```

```
    %errorlevel% # 返回使用过的命令的错误代码。通常用非零值表示错误。
```
注：系统变量是操作系统用来指定运行环境的一些参数，系统环境变量对一台电脑的所有用户都是有效的。

命令：%变量名%
作用：取变量的值
```
    set a=10000
    echo %a%
```

命令：if else
作用：进行条件判断，如果条件正确就执行if后面的语句，如果条件不正确就执行else后面的语句
例如：比较两次输入的字符是否相同
```
    @echo off
    set /p var1=请输入第一个比较的字符：
    set /p var2=请输入第二个比软的字符：
    if "%var1%"=="%var2%" (
    echo 输入的两个字符相同
    ) else (
    echo 输入的两个字符不相同
    )
    pause
```

注：if else 配合环境变量%errorlevel%可以实现对上一条命令的执行结果进行判断

：和goto命令
作用：
```
    ：定义标签名
    goto实现跳转
```
当程序运行到 goto时，将自动跳转到：定义的标签部分去执行命令块了，所以：和goto联合起来可以实现在批处理执行时进行跳转功能。