**windows SC命令详解**

2009-11-26 17:04:27

标签：[命令](http://blog.51cto.com/tag-%E5%91%BD%E4%BB%A4.html) [windows](http://blog.51cto.com/tag-windows.html) [休闲](http://blog.51cto.com/tag-%E4%BC%91%E9%97%B2.html) [详解](http://blog.51cto.com/tag-%E8%AF%A6%E8%A7%A3.html) [职场](http://blog.51cto.com/tag-%E8%81%8C%E5%9C%BA.html)

原创作品，允许转载，转载时请务必以超链接形式标明文章 [原始出处](http://hukunlin.blog.51cto.com/545402/235229) 、作者信息和本声明。否则将追究法律责任。<http://hukunlin.blog.51cto.com/545402/235229>

SC命令详解(一个很有用的command)

作为一个命令行工具，SC.exe可以用来测试你自己的系统，你可以设置一个批处理文件来使用不同的参数调用 SC.exe来控制服务。

**一.SC使用这样的语法：**

1. SC [Servername] command Servicename [Optionname= Optionvalues]   
2. SC [command]   
这里使用第一种语法使用SC，使用第二种语法显示帮助。   
下面介绍各种参数。   
Servername   
可选择：可以使用双斜线，如[\\myserver](file:///\\myserver\)，也可以是[\\192.168.1.223](file:///\\192.168.1.223\)来操作远程计算机。如果在本地计算机上操作   
就不用添加任何参数。   
Command   
下面列出SC可以使用的命令。   
config----改变一个服务的配置。（长久的）   
continue--对一个服务送出一个继续控制的要求。   
control----对一个服务送出一个控制。   
create----创建一个服务。（增加到注册表中）   
delete----删除一个服务。（从注册表中删除）   
EnumDepend--列举服务的从属关系。   
GetDisplayName--获得一个服务的显示名称。   
GetKeyName--获得一个服务的服务键名。   
interrogate--对一个服务送出一个询问控制要求。   
pause----对一个服务送出一个暂停控制要求。   
qc----询问一个服务的配置。   
query----询问一个服务的状态，也可以列举服务的状态类型。   
start----启动一个服务。   
stop----对一个服务送出一个停止的要求。

Servicename   
在注册表中为service key制定的名称。注意这个名称是不同于显示名称的（这个名称可以用net start和服务控   
制面板看到），而SC是使用服务键名来鉴别服务的。   
Optionname

这个optionname和optionvalues参数允许你指定操作命令参数的名称和数值。注意，这一点很重要在操作名称和等   
号之间是没有空格的。一开始我不知道，结果………………，比如，start= optionvalues，这个很重要。   
optionvalues可以是0，1，或者是更多的操作参数名称和数值对。   
如果你想要看每个命令的可以用的optionvalues，你可以使用sc command这样的格式。这会为你提供详细的帮助。

Optionvalues   
为optionname的参数的名称指定它的数值。有效数值范围常常限制于哪一个参数的optionname。如果要列表请用   
sc command来询问每个命令。

Comments   
很多的命令需要管理员权限，所以我想说，在你操作这些东西的时候最好是管理员。呵呵！   
当你键入SC而不带任何参数时，SC.exe会显示帮助信息和可用的命令。当你键入SC紧跟着命令名称时，你可以得   
到一个有关这个命令的详细列表。比如，键入sc create可以得到和create有关的列表。   
但是除了一个命令，sc query，这会导出该系统中当前正在运行的所有服务和驱动程序的状态。   
当你使用start命令时，你可以传递一些参数（arguments）给服务的主函数，但是不是给服务进程的主函数。

**二.SC create**

这个命令可以在注册表和服务控制管理数据库建立一个入口。   
语法1   
sc [servername] create Servicename [Optionname= Optionvalues]   
这里的servername，servicename，optionname，optionvalues和上面的一样，这里就不多说了。这里我们详细说   
明一下optionname和optionvalues。   
Optionname--Optionvalues   
描述   
type=----own, share, interact, kernel, filesys   
关于建立服务的类型，选项值包括驱动程序使用的类型，默认是share。   
start=----boot, sys tem, auto, demand, disabled   
关于启动服务的类型，选项值包括驱动程序使用的类型，默认是demand（手动）。   
error=----normal, severe, critical, ignore   
当服务在导入失败错误的严重性，默认是normal。   
binPath=--(string)   
服务二进制文件的路径名，这里没有默认值，这个字符串是必须设置的。   
group=----(string)   
这个服务属于的组，这个组的列表保存在注册表中的ServiceGroupOrder下。默认是nothing。   
tag=----(string)   
如果这个字符串被设置为yes，sc可以从CreateService call中得到一个tagId。然而，SC并不显示这个标签，所   
以使用这个没有多少意义。默认是nothing   
depend=----(space separated string)有空格的字符串。   
在这个服务启动前必须启动的服务的名称或者是组。   
obj=----(string)   
账号运行使用的名称，也可以说是登陆身份。默认是localsys tem   
Displayname=--(string)   
一个为在用户界面程序中鉴别各个服务使用的字符串。   
password=--(string)   
一个密码，如果一个不同于localsystem的账号使用时需要使用这个。   
Optionvalues   
Optionname参数名称的数值列表。参考optionname。当我们输入一个字符串时，如果输入一个空的引用这意味着   
一个空的字符串将被导入。   
Comments   
The SC CREATE command perFORMs the operations of the CreateService API function.   
这个sc create命令执行CreateService API函数的操作。详细请见CreateService。

例子1   
下面这个例子在计算机上建立叫“mirror”的服务建立的一个注册表登记,是自动运行服务,从属于TDI组和NetBios服务。   
C:\WINDOWS\system32&gt;sc create mirror binPath= "D:\Ftp\新建文件夹\mirror.exe" type= own start= auto   
[SC] CreateService SUCCESS   
重启后生效

例子2 删除Mirror服务   
C:\WINDOWS\system32&gt;sc delete mirror binPath= "D:\Ftp\新建文件夹\mirror.exe" type= own start= auto   
[SC] DeleteService SUCCESS

**三. SC QC**

这个SC QC“询问配置”命令可以列出一个服务的配置信息和QUERY\_SERVICE\_CONFIG结构。   
语法1   
sc [Servername] qc Servicename [Buffersize]   
Parameters   
servername和servicename前面已经介绍过了，这里不再多说。   
Buffersize，可选择的，列出缓冲区的尺寸。   
Comments   
SC QC命令显示了QUERY\_SERVICE\_CONFIG结构的内容。   
以下是QUERY\_SERVICE\_CONFIG相应的区域。   
TYPE------dwServiceType   
START\_TYPE----dwStartType   
ERROR\_CONTROL----dwErrorControl   
BINARY\_PATH\_NAME--lpBinaryPathName   
LOAD\_ORDER\_GROUP--lpLoadOrderGroup   
TAG------dwTagId   
DISPLAY\_NAME----lpDisplayName   
DEPENDENCIES----lpDependencies   
SERVICE\_START\_NAME--lpServiceStartName

例1   
下面这个例子询问了在上面例子中建立的“mirror”服务的配置：   
sc [qc   
sc显示下面的信息：   
SERVICE\_NAME: mirror   
        TYPE               : 10 WIN32\_OWN\_PROCESS   
        START\_TYPE         : 2   AUTO\_START   
        ERROR\_CONTROL      : 1   NORMAL   
        BINARY\_PATH\_NAME   : D:\Ftp\   
        LOAD\_ORDER\_GROUP   :   
        TAG                : 0   
        DISPLAY\_NAME       : mirror   
        DEPENDENCIES       :   
        SERVICE\_START\_NAME : LocalSystem   
mirror有能力和其他的服务共享一个进程。这个服务 不依靠与其它的的服务，而且运行在lcoalsystem的安全上下关系中。这些都是调用QueryServiceStatus基本的返回，如果还需要更多的细节届时，可以看看API函数文件。](file:///\\qc\)mirror

**四.SC QUERY**   
SC QUERY命令可以获得服务的信息。   
语法：   
sc [Servername] query { Servicename | ptionname= Optionvalues... }   
参数：   
servername, servicename, optionname, optionvalues不在解释。只谈一下这个命令提供的数值。   
Optionname--Optionvalues   
Description   
type=----driver, service, all   
列举服务的类型，默认是service   
state=----active, inactive, all   
列举服务的状态，默认是active   
bufsize=--(numeric values)   
列举缓冲区的尺寸，默认是1024 bytes   
ri=----(numeric values)   
但开始列举时，恢复指针的数字，默认是0   
Optionvalues   
同上。   
Comments

SC QUERY命令可以显示SERVICE\_STATUS结构的内容。   
下面是SERVICE\_STATUS结构相应的信息：   
TYPE------dwServiceType   
STATE------dwCurrentState, dwControlsAccepted   
WIN32\_EXIT\_CODE----dwWin32ExitCode   
SERVICE\_EXIT\_CODE--dwServiceSpecificExitCode   
CHECKPOINT----dwCheckPoint   
WAIT\_HINT----dwWaitHint

在启动计算机后，使用SC QUERY命令会告诉你是否，或者不是一个启动服务的尝试。如果这个服务成功启动，WIN32\_EXIT\_CODE区间会将会包含一个0，当尝试不成功时，当它意识到这个服务不能够启动时，这个区间也会提供一个退出码给服务。   
例子   
查询“mirror'服务状态，键入：   
sc query mirror   
显示一下信息：

SERVICE\_NAME: mirror   
        TYPE               : 10 WIN32\_OWN\_PROCESS   
        STATE              : 1 STOPPED   
                                (NOT\_STOPPABLE,NOT\_PAUSABLE,IGNORES\_SHUTDOWN   
        WIN32\_EXIT\_CODE    : 0 (0x0)   
        SERVICE\_EXIT\_CODE : 0 (0x0)   
        CHECKPOINT         : 0x0   
        WAIT\_HINT          : 0x0   
注意，这里存在一个给这个服务的退出码，即使这个服务部不在运行，键入net helpmsg 1077，将会得到对1077错误信息的说明：   
上次启动之后，仍未尝试引导服务。   
所以，这里我想说一句，希望大家可以活用net helpmsg，这会对你的学习有很大的帮助。   
下面在对SC query的命令在说明一下：   
列举活动服务和驱动程序状态，使用以下命令：   
sc query   
显示messenger服务，使用以下命令：   
sc query messenger   
只列举活动的驱动程序，使用以下命令：   
sc query type= driver   
列举Win32服务，使用以下命令：   
sc query type= service   
列举所有的服务和驱动程序，使用以下命令：   
sc query state= all   
用50 byte的缓冲区来进行列举，使用以下命令：   
sc query bufsize= 50   
在恢复列举时使用index=14，使用以下命令：   
sc query ri=14   
列举所有的交互式服务，使用以下命令：   
sc query type= service type= interact

**五、sc命令启动已经禁用的服务,例如：启动telnet服务**

sc  config  tlntsvr  start= auto

net start tlntsvr

本文出自 “[成功不仅是个人荣誉，..](http://hukunlin.blog.51cto.com/)” 博客，请务必保留此出处<http://hukunlin.blog.51cto.com/545402/235229>