**如何编写windows服务程序**

这两天想学习关于如何编写windows服务程序的知识，就上网查了些资料。看了一篇文章《用C 语言编写Windows 服务程序的五个步骤》。但可能由于译者的疏忽，忘记了将关键代码放入该文档，导致初学者可能会看不懂。所以又查阅了相关资料。自己完成了《用C 语言编写Windows 服务程序的五个步骤》中的样例程序。

在本文中我希望能给初学者一些帮助，大致讲一下编写windows服务程序需要的知识。

首先Microsoft Windows 服务（即，以前的 NT 服务）使您能够创建在它们自己的 Windows 会话中可长时间运行的可执行应用程序。这些服务可以在计算机启动时自动启动，可以暂停和重新启动而且不显示任何用户界面。这使服务非常适合在服务器上使用，或任何时候，为了不影响在同一台计算机上工作的其他用户，需要长时间运行功能时使用。还可以在不同于登录用户的特定用户帐户或默认计算机帐户的安全上下文中运行服务。

服务是有状态的，当我们使用windows自带的服务管理程序sc.exe查看服务状态时可以显示服务的当前状态，这个状态是由我们在程序代码中进行控制的。你最好在服务初始化的时候将服务设置为SERVICE\_START\_PENDING，当初始化完毕时设为SERVICE\_RUNNING，这些状态是系统自定义的状态，可通过msdn查看其他状态。这个状态信息你会在sc.exe中看到。

在编写windows服务程序过程中你需要关注的函数有：

1.首先是main函数，由于windows服务不需要界面，所以大部分程序为win32控制台应用程序，所以程序主函数为main 而不是WinMain()。在主函数要做的主要工作就是初始化一个SERVICE\_TABLE\_ENTRY 分派表结构体，然后调用StartServiceCtrlDispatcher();这将把调用进程的主线程转换为控制分派器。该分派器启动一个新线程，该线程运行分派表中对应于你的服务的ServiceMain（）函数。ServiceMain（）函数将在下面提到。

此过程示例代码如下：

SERVICE\_TABLE\_ENTRY entrytable[2];

    entrytable[0].lpServiceName="testservice";

    entrytable[0].lpServiceProc=(LPSERVICE\_MAIN\_FUNCTION)ServiceMain;

    entrytable[1].lpServiceName=NULL;

    entrytable[1].lpServiceProc=NULL;

StartServiceCtrlDispatcher(entrytable);

在这之后系统将自动创建一个线程去执行ServiceMain函数的内容，你应该将你要执行的任务在ServiceMain中循环，这样服务就开始运行了。

2．ServiceMain函数为void WINAPI ServiceMain（int argc, char\*\* argv）格式的函数，函数名字可以任意定义。它的作用就是：将你需要执行的任务放到该函数中循环执行即可。这就是服务程序的工作函数。在ServiceMain执行你的任务前，需要给SERVICE\_TABLE\_ENTRY 分派表结构体进行赋值，注意由于此时服务还没有开始执行你的任务所以我们将服务的状态设置为SERVICE\_START\_PENDING，即正在初始化。我们进行如下赋值：

servicestatus.dwServiceType = SERVICE\_WIN32;

    servicestatus.dwCurrentState = SERVICE\_START\_PENDING;

servicestatus.dwControlsAccepted=SERVICE\_ACCEPT\_SHUTDOWN|SERVICE\_ACCEPT\_STOP;

//在本例中只接受系统关机和停止服务两种控制命令

    servicestatus.dwWin32ExitCode = 0;

    servicestatus.dwServiceSpecificExitCode = 0;

    servicestatus.dwCheckPoint = 0;

    servicestatus.dwWaitHint = 0;

hstatus = ::RegisterServiceCtrlHandler("testservice", CtrlHandler);

CtrlHandler为void WINAPI CtrlHandler(DWORD request)型的函数，函数名字可以任意设定。将在下一点讲到。

Hstatus为SERVICE\_STATUS\_HANDLE类型的全局变量。当需要改变服务状态时SetServiceStatus（）函数需要它做为参数来标识一个服务。

3. void WINAPI CtrlHandler(DWORD request)，函数的主要功能是，接收系统传递的控制命令，比如当你通过sc.exe关闭服务时，该函数会收到SERVICE\_CONTROL\_STOP消息，你就可以对服务进行必要的管理。在本例子程序中就只接收SERVICE\_ACCEPT\_SHUTDOWN和SERVICE\_ACCEPT\_STOP消息，这是通过前面给servicestatus赋值设定的。

这样一个基本的服务程序就完成了。

如何安装服务：

运行命令提示符 cmd.exe

输入 sc create testservicename binpath= D:\test.exe

输入 sc start testservicename 启动服务

输入sc query 会在最底部显示你的服务当前的状态

输入 sc stop testservicename 停止服务

输入 sc delete testservicename删除服务，该服务将在下次重启后删除，在重启之前将不能注册同一个名字的服务。