rundll32.exe命令使用大法 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/140/2021_2022_rundll32e_c100_140428.htm Rundll32.exe是什么？ 顾名思意，“ 执行32位的DLL文件 ”。它的作用是执行DLL文件中的内部函数，这样在进程当中，只会有Rundll32.exe，而不会有DLL后门的进程，这样，就实现了进程上的隐藏。如果看到系统中有多个Rundll32.exe，不必惊慌，这证明用Rundll32.exe启动了多少个的DLL文件。当然，这些Rundll32.exe执行的DLL文件是什么，我们都可以从系统自动加载的地方找到。 现在，我来介绍一下Rundll32.exe这个文件，意思上边已经说过，功能就是以命令行的方式调用动态链接程序库。系统中还有一个Rundll.exe文件，他的意思是“ 执行16位的DLL文件 ”，这里要注意一下。在来看看Rundll32.exe使用的函数原型： Void CALLBACK FunctionName ( HWND hwnd, HINSTANCE hinst, LPTSTR lpCmdLine, Int nCmdShow ). 其命令行下的使用方法为：Rundll32.exe DLLname,Functionname [Arguments] DLLname为需要执行的DLL文件名；Functionname为前边需要执行的DLL文件的具体引出函数；[Arguments]为引出函数的具体参数。 略谈Rundll32.exe的作用 常用Windows9x的朋友一定对Rundll32.exe和Rundll.exe这两个档案不会陌生吧，不过,由於这两个程式的功能原先只限於在微软内部使用，因而真正知道如何使用它们的朋友想必不多。那么好，如果你还不清楚的话，那么就让我来告诉你吧。 首先，请你做个小实验（请事先保存好你正在执行的程式的结果，否则...）：点击“ 开始－程式－Ms－Dos方式 ”，进入Dos视窗，然後键

入rundll32.exe user.exe,restartwindows，再按下回车键，这时你将看到，机器被重启了！怎么样，是不是很有趣？ 当然，Rundll的功能绝不仅仅是重启你的机器。其实，Rundll者，顾名思义，执行Dll也，它的功能就是以命令列的方式呼叫Windows的动态链结库，Rundll32.exe与Rundll.exe的区别就在於前者是呼叫32位的链结库，而後者是运用於16位的链结库，它们的命令格式是： RUNDLL.EXE，， 这里要注意三点：1.Dll档案名中不能含有空格，比如该档案位於c:\ProgramFiles\目录，你要把这个路径改成c:\Progra～1\；2.Dll档案名与Dll入口点间的逗号不能少，否则程式将出错并且不会给出任何资讯！3.这是最重要的一点：Rundll不能用来呼叫含返回值参数的Dll，例如Win32API中的GetUserName(),GetTextFace()等。在Visual Basic中，提供了一条执行外部程式的指令Shell,格式为： Shell “ 命令列 ” 如果能配合Rundll32.exe用好Shell指令，会使您的VB程式拥有用其他方法难以甚至无法实现的效果：仍以重启为例，传统的方法需要你在VB工程中先建立一个模组，然後写入WinAPI的声明，最後才能在程式中呼叫。而现在只需一句: Shell “ rundll32.exe user.exe,restartwindows ” 就搞定了！是不是方便多了？ 实际上，Rundll32.exe在呼叫各种Windows控制面板和系统选项方面有著独特的优势。下面，我就将本人在因特网上收集的有关Rundll的指令列举如下（很有用的，能省去你很多呼叫Windows API的时间！！），供大家在程式设计中引用： 命令列: rundll32.exe shell32.dll,Control_RunDLL 功能: 显示控制面板 命令列: rundll32.exe shell32.dll,Control_RunDLL access.cpl,,1 功能: 显示 “ 控制面板－辅助选项－键盘 ” 选项视

窗 命令列: rundll32.exe shell32.dll,Control_RunDLL access.cpl,,2 功能: 显示“ 控制面板－辅助选项－声音 ”选项视窗 命令列: rundll32.exe shell32.dll,Control_RunDLL access.cpl,,3 功能: 显示“ 控制面板－辅助选项－显示 ”选项视窗 命令列: rundll32.exe shell32.dll,Control_RunDLL access.cpl,,4 功能: 显示“ 控制面板－辅助选项－滑鼠 ”选项视窗 命令列: rundll32.exe shell32.dll,Control_RunDLL access.cpl,,5 功能: 显示“ 控制面板－辅助选项－传统 ”选项视窗 命令列: rundll32.exe shell32.dll,Control_RunDLL sysdm.cpl @1 功能: 执行“ 控制面板－添加新硬体 ”向导。 命令列: rundll32.exe shell32.dll,SHHelpShortcuts_RunDLL AddPrinter 功能: 执行“ 控制面板－添加新印表机 ”向导。 命令列: rundll32.exe shell32.dll,Control_RunDLL appwiz.cpl,,1 功能: 显示“ 控制面板－添加/删除程式－安装/卸载 ”面板。 命令列: rundll32.exe shell32.dll,Control_RunDLL appwiz.cpl,,2 功能: 显示“ 控制面板－添加/删除程式－安装Windows ”面板。 命令列: rundll32.exe shell32.dll,Control_RunDLL appwiz.cpl,,3 功能: 显示“ 控制面板－添加/删除程式－启动盘 ”面板。 命令列: rundll32.exe syncui.dll,Briefcase_Create 功能: 在桌面上建立一个新的“ 我的公文包 ”。 命令列: rundll32.exe diskcopy.dll,DiskCopyRunDll 功能: 显示复制软碟视窗 命令列: rundll32.exe apwiz.cpl,NewLinkHere %1 功能: 显示“ 建立快捷方式 ”的对话框，所建立的快捷方式的位置由%1参数决定。 命令列: rundll32.exe shell32.dll,Control_RunDLL timedate.cpl,,0 功能: 显示“ 日期与时间 ”选项视窗。 命令列: rundll32.exe shell32.dll,Control_RunDLL timedate.cpl,,1 功能: 显示“ 时区 ”

选项视窗。 命令列: rundll32.exe rnaui.dll,RnaDial [某个拨号连接的名称] 功能: 显示某个拨号连接的拨号视窗。如果已经拨号连接，则显示目前的连接状态的视窗。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com