**psexec.exe命令详解**

实用工具（如 Telnet）和远程控制程序（如 Symantec 的 PC Anywhere）使您可以在远程系统上执行程序，但安装它们非常困难，并且需要您在想要访问的远程系统上安装客户端软件。PsExec 是一个轻型的 telnet 替代工具，它使您无需手动安装客户端软件即可执行其他系统上的进程，并且可以获得与控制台应用程序相当的完全交互性。PsExec 最强大的功能之一是在远程系统和远程支持工具（如 IpConfig）中启动交互式命令提示窗口，以便显示无法通过其他方式显示的有关远程系统的信息。

注意：某些反病毒扫描程序会报告其中的一个或多个工具感染了"远程管理"病毒。这些 PsTools 都不带病毒，但是如果病毒使用了这些工具，则它们可能触发病毒通知。

安装

只需将 PsExec 复制到可执行路径。键入"psexec"可显示其使用语法。

PsExec 可在 Windows Vista、NT 4.0、Win2K、Windows XP 和 Server 2003（包括 64 位版本的 Windows）上运行。

用法

有关介绍了 PsExec 的高级用法的 Mark 的文章，请参阅《Windows IT Pro 杂志》2004 年 7 月刊。

用法：psexec [\\computer[,computer2[,...] | @file][-u user [-p psswd]][-n s][-l][-s|-e][-x][-i [session]][-c [-f|-v]][-w directory][-d][-<priority>][-a n,n,...] cmd [arguments]

computer

指示 PsExec 在指定的一台或多台计算机上运行应用程序。如果省略计算机名称，则 PsExec 将在本地系统上运行应用程序；如果输入计算机名称"\\\*"，则 PsExec 将在当前域中的所有计算机上运行应用程序。

@file

指示 PsExec 在指定的文本文件中列出的每台计算机上运行命令。

-a

用逗号分隔可以运行应用程序的处理器，CPU 编号最小为 1。例如，要在 CPU 2 和 CPU 4 上运行应用程序，请输入："-a 2,4"

-c

将指定的程序复制到远程系统以便执行。如果省略此选项，则应用程序必须位于远程系统上的系统路径中。

-d

不等待应用程序终止。请只对非交互式应用程序使用此选项。

-e

不加载指定帐户的配置文件。

-f

将指定的程序复制到远程系统，即使远程系统中已存在该文件。

-i

运行程序，以便它与远程系统中指定会话的桌面进行交互。如果未指定会话，则进程将在控制台会话中运行。

-l

以受限用户身份（去除 Administrators 组的权限，并且只允许使用分配给 Users 组的权限）运行进程。在 Windows Vista 上，此进程将以"低完整性"运行。

-n

指定与远程计算机连接的超时（秒）。

-p

指定用户名的密码（可选）。如果省略此选项，系统将提示您输入隐藏密码。

-s

在系统帐户中运行远程进程。

-u

指定用于登录远程计算机的可选用户名。

-v

仅在指定文件具有更高版本号或该文件比远程系统上的文件新时复制该文件。

-w

设置进程的工作目录（相对于远程计算机）。

-x

在 Winlogon 桌面上显示 UI（仅限于本地系统）。

-priority

指定 -low、-belownormal、-abovenormal、-high 或 -realtime 按不同优先级运行进程。

program

要执行的程序的名称。

arguments

要传递的参数（请注意，文件路径必须是目标系统中的绝对路径）

对于其名称中含有空格的应用程序，可以在其两侧加引号，例如，psexec \\marklap "c:\long name\app.exe"。按下 Enter 键时，仅将输入内容传递到远程系统。键入 Ctrl-C 可终止远程进程。

如果省略用户名，则远程进程将以执行 PsExec 时所使用的相同帐户运行，但由于远程进程以模仿方式运行，因此它无权访问远程系统上的网络资源。指定用户名时，远程进程将以指定的帐户执行，并可访问该帐户有权访问的任何网络资源。请注意，密码是以明文形式传递到远程系统的。

当目标系统是本地系统时，由于 PsExec 不需要您具有管理员权限，因此您可以使用当前版本的 PsExec 来取代 Runas。

示例

我写的这篇文章对 PsExec 的工作原理进行了描述，并给出了一些有关如何使用它的提示：

http://www.winnetmag.com/Windows/Issues/IssueID/714/Index.html

以下命令可在 \\marklap 上启动交互式命令提示窗口：

psexec \\marklap cmd

此命令通过 /all 开关在远程系统上执行 IpConfig，并在本地显示输出结果：

psexec \\marklap ipconfig /all

此命令将程序 test.exe 复制到远程系统，并以交互方式执行此程序：

psexec \\marklap -c test.exe

如果远程系统中已经安装的程序不在系统路径中，请指定该程序的完整路径：

psexec \\marklap c:\bin\test.exe

在系统帐户中以交互方式运行 Regedit，以便查看 SAM 和 SECURITY 注册表项的内容：

psexec -i -d -s c:\windows\regedit.exe

要以受限用户权限运行 Internet Explorer，请使用此命令：

psexec -l -d "c:\program files\internet explorer\iexplore.exe