如何用PowerShell获取进程信息 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/276/2021_2022__E5_A6_82_E4_BD_95_E7_94_A8P_c67_276491.htm 在脚本学校(Scripting School)专栏的前面内容里，我们讨论了如何收集用户输入,为其分配变量，并将变量记录到帮助文档里。这次我们将要解释如何检索电脑中进程的基本信息，如何使用Windows PowerShell结束你不想要的进程。 检索进程信息 Windows PowerShell中的get-process cmdlet可以帮助你检索电脑中的进程信息。不带任何参数地运行这个命令，你可以获得如下所示的输出：HandlesNPM(K)PM(K)WS(K)VM(M)CPU(s)ID ProcessName--210184208450363 51.84496 1XConfig103511563560320.082308 alg6926042336192.521176 ati2evxx6625722216191.581772 ati2evxx6688338475926325.981512 csrss10859403756350.952220 ctfmon 如果你不确定NPM、WS、VM这些缩写分别代表什么，可以借助下面的表格。资源名称缩写描述Handles无进程的智能指针编号，对内存的存储区域开放。当句柄(handles)关闭时，内存被释放。Non-paged pool (in kilobytes)NPM(non-paged memory)非分页池是从不分页到硬盘的存储器，因此访问速度更快。Paged pool (in kilobytes)PM(paged memory)如果有空间需求，分页池有可能发送给磁盘。这使得分页池比非分页池更大(因为存储器空间仅受磁盘上的页面文件限制)一些内存读取操作可能耗时更长，因为需要的的数据存储在硬盘上。Working set (in kilobytes)WS工作集是指一个进程占用物理内存的页面集。只

有存储在物理内存(当前没有分页到磁盘)的数据才在工作集中。Virtual memory (in megabytes)VM只用于进程的虚拟内存数量。CPU time (in seconds)CPU (s)进程占用的处理器时间(包括所有可用的处理器)。Process ID无给定进程的唯一标识符。即使在一台共享式电脑上，每个进程都只有一个唯一的进程ID。Process name无进程的易记标识，但不同于进程ID，它不一定是唯一的。 注意：你还会接触到很多其它进程属性。要想查看它们的属性名称，键入get-process | get-member即可。基本列表对我们今天的目的来说已经足够了，但是如果你要操作这些进程属性，就需要查看完整的列表。 如何检索最高负载的进程 你不一定需要所有进程的列表，但你有必要大致了解哪些进程占用了大部分的资源。举例来说，一个进程的工作集(如上面的表格所描述)可以很好地指示其系统内存压力的情况。为了找出工作集大于10MB的所有进程，输入下面的命令： get-process | where-object {$_.WorkingSet -gt 10000000} 记住，美元符号代表变量。现在我们来看这些进程的名称、工作集属性及其工作集是否是大于(上面命令中的gt)给定值的。 这个命令会找到每个进程，并把结果发送给where-object cmdlet做评价。然后你就会收到跟完全列表格式一模一样的一个列表，但这个列表要短得多。 结束不必要的进程 如果你管理自己的电脑，很容易获取一些无用进程。比如，有一天你在机场想联机，最后可能在电脑里留下Boingo客户端进程。你下载过某一个系统审核软件的试用版本吗?即使你有几个月都没有使用过它，进程列表仍可能包含系统审核代理。 当然，任务管理器也可以为你显示进程。但get-process更容易查看数据，比如你可以不使用滚动条查看

一个完整列表。你需要应付这些垃圾进程，但同时你也可以结束它们。(在终止一个进程前你应该确定知道自己在干什么，如果你并不确定哪个进程是干什么用的，不要贸然结束它)要结束一个进程，先从整个列表或最消耗资源的前十个进程中检索出它们的识别信息。然后，运行stop-process命令。如果不带任何参数运行该命令，它会提示你输入进程ID号(仅仅输入进程名称是无法结束进程的)。你可以根据自己意愿结束多个进程。完成后，按Enter键就会退出cmdlet。 你也可以使用name parameter，stop-process name processname等命令通过名称来停止进程。然而，我并不推荐这样做。你应该养成用进程ID结束进程的习惯。尽管记住进程ID比记住进程名称困难，但这对防止结束共享电脑上其他人的进程有帮助。