Windows7随时监控电脑上运行的程序Microsoft认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022_Windows7_E9_9A_c100_644207.htm 每次启动系统后，在任务管理器中会看到系统加载很多进程，其中包括随机启动的程序、加载各项服务等，这些进程是不是都是我们用的呢？哪个进行占用的资源大呢？每个程序运行后启动了多少个关联的程序呢？哪个程序是木马程序加载的呢？在以前的Windows系统中我们只能靠三方软件来参看，现在好了，Windows7中增强了任务管理器功能，这样我们非常方便的对系统中的各项程序的进程了如指掌了，就算是病毒入侵，我们也能轻松掌控。 1.查看UAC虚拟化进程 在Windows7中，系统增强了用户帐户控制(UAC)虚拟化功能，通过这个功能我们可以防止系统文件、文件夹和注册表因为误操作而损坏。通过UAC可以将系统中的应用程序重新定向其它位置，但是用户还能正常使用，但是这些应用程序写入的数据不会被发送至系统位置，以帮助维护整个操作系统的稳定性。有了这种虚拟化功能，也意味着现在多个用户可以运行同一台计算机上的应用程序了，因为他们各自的数据会写入各自的位置中。起到了系统安全的效果。 使用UAC功能，我们需要在“ 组策略 ”中将其开启，在运行中键入“ GPEDIT.MSC ”命令，打开组策略编辑器，随后在左侧依次展开“ 本地计算机→Windows设置→安全设置→本地策略→安全选项 ”分支，在此将该分支下的“ 将文件及注册表写入失败虚拟化到每用户位置 ”设置为启用即可。 用户帐户控制虚拟化启用后，我们就可以在任务管理器查看UAC进程了。查看时，和以前的系统一样，使用“ Ctrl

Alt Del ”组合热键打开“ 任务管理器 ”，切换到“ 进程 ”项下，在此单击菜单中的“ 查看 ”→“ 选择列 ”，打开“ 选择进程列 ”对话框，在此勾选“ 用户帐户控制(UAC)虚拟化 ”复选框。随后单击“ 确定 ”按钮，随后在“ 进程 ”窗口中勾选“ 显示所有的用户进程 ”，这样我们就可以了解到系统中所有进程的虚拟化信息了。当我们有发现系统已经对某个进程停用了虚拟化功能，如果想启用虚拟化进程时，在该进程的名称上单击右键，弹出右键菜单，随后勾选“ UAC虚拟化 ”，这样即可启用该进程的UAC虚拟化功能。2. 为进程选择CPU 现在用户配置的电脑一般都是双核以上，这样运算速度更快，但是一些程序由于编写问题，不支持双CPU，这样往往因为资源占用太多而导致系统不稳定。此外，还有一进程，根据一些需要我们还有选择某个CPU还执行这些进程。设置时，在任务管理器中进入到进程列表，选中某个需要设置的进程后，单击“ 右键 ”，在弹出的邮件菜单中选择“ 设置相关性 ”，打开“ 处理器相关性 ”对话框，在此我们可以根据需要为该经常选择处理器。3. 查出隐藏在进程中的木马在任务管理器中我们可以方便的对系统的各项资源、进程进行了解。有时候我们发现自己的电脑运行起来非常慢，这可能是由于一些木马程序进入占用大量的系统资源造成的。一些木马程序进入我们系统后，在后台运行它都会伪装起来，这样我们会很难发现他的行踪。我们除了能方便的查看各个任务的进程来查看是否中了木马等病毒程序外，我们还可以通过windows7提供的“ 资源监视 ”功能，这样我们可以在查看进程的同时还能了解系统资源的各种状态，揪出系统背后木马程序。首先在“ 性能 ”界面中单击“ 资源监视器 ”按钮

，打开“ 资源监视器 ”界面，windows7“ 资源监视器 ”功能，比以前的版本要强大很多，在此我们可以方便的查看各项资源情况。在此我们非常方便的查看系统中运行的程序对CPU、内存、网络监视器等使用情况，下面我们就以查看哪个程序CPU使用率高 为例来了解一下查看方法。 一般木马程序在后运行时都要不同复制系统中的文件信息，这样该程序会占用大量的CPU和内存资源。首先我们先查看某个程序占用CPU资源情况时，在“ 资源监视器 ”界面切换到CPU项下，在此显示出所有正在运行的程序的CPU使用情况。如果你发现某个进程CPU使用率较高，在“ 进程 ”列表中勾选某个需要查看的进程后，在“ 服务 ”项中我们可以看到与该进程相关联的所有服务项目，在下面的“ 关联句柄 ”项目中我们可以看到和该程序关联的所有进程信息。来源：www.examda.com 如果我们想了解该进程的更多信息，在该进程上单击右键，在弹出的右键菜单中选择“ 分析进程 ”后，我们可以看到该程序的PID和线程数。如果我们想了解某个进程的详细信息，我们可以选择“ 联机搜索 ”功能，这样系统会自动打开IE浏览器，使用默认的搜索引擎进行进程的相关搜索，这样我们可以对程序使用的各个进行进行进一步了解。以预防了病毒的伪装。如果觉得这个进程可疑，或者断定是木马程序，我们可以通过右键菜单中的结束进程或结束进程树命令将该进程以及关联的服务停止即可。随后打开该进程所在的文件夹将该进程文件删除。Windows7增强后的“ 任务管理器 ”，给我们资源监控提供了方便，这样我们也非常清楚的了解当前系统中各项进程了。 编辑特别推荐: 右键菜单快速整理Windows7磁盘碎片 Windows安全性饱受质疑