为Windows7系统做有针对性的安全优化Microsoft认证考试
 随着互联网的普及，病毒和木马以及其他恶意程序的传播越来越快。一旦中招，很容易造成系统崩溃或个人隐私泄露，而如果中的是那些以金钱利益为目标的病毒或木马，带来的危害就更是严重，很可能造成财产的损失。这个问题在Windows 7(以下简称Win7)中一样存在。因此，为了保证系统安全，对Windows 7系统进行有针对性的安全优化就显得特别重要。 关闭默认共享 封锁系统后门 同XP、Vista一样，Win7在默认情况下也开启了网络共享(如图1所示)。虽然这可以让局域网共享更加方便，但同时也为病毒传播创造了条件。因此关闭默认共享，可以大大降低系统被病毒感染的概率。 打开魔方，点击“ 系统优化→网络共享 ”，将“ 禁止默认的管理共享及磁盘分区共享 ”选中，点“ 保存设置 ”后重启计算机，此时就无法通过默认共享访问系统了(如图2所示)。如果不希望一次性关闭所有默认共享，魔方还提供了关闭单个默认共享的功能。在刚才的界面中选中“ 默认共享 ”点“ 刷新 ”，可以看到当前系统的默认共享列表，将不需要的默认共享选中后点“ 清除共享 ”，保存设置重启计算机，选中的默认共享就会被关闭。 此外，魔方还提供了“ 限制IPC$的远程默认共享 ”、“ 禁止进程间通讯IPC$的空连接 ”等能够有效提升系统安全性的设置，建议全部启用。 修改组策略 加固系统注册表 和XP、Vista相同，Win7中仍然开放了风险极高的可远程访问注册表的路径。将可远程访问注册表的路径设置为空，可以有效避免黑客利

用扫描器通过远程注册表读取Win7的系统信息及其他信息。打开控制面板，选择“ 管理工具 ”，双击“ 本地安全策略 ”，依次打开“ 本地策略→安全选项 ”，在右侧找到“ 网络访问：可远程访问的注册表路径 ”和“ 网络访问：可远程访问的注册表路径和子路径 ”，双击打开，将窗口中的注册表路径删除(如图3所示)。 锁定重要功能 防止病毒盗用 系统中一些常用的、权限较高的功能，如命令行程序、批处理文件、注册表编辑器等也经常被病毒等恶意软件利用，成为入侵系统的“ 帮凶 ”。而这些程序作为普通用户又不是经常用到，因此，禁用这些功能可以有效地加固系统，保障日常应用安全。 打开魔方，选择“ 安全优化→系统安全设置 ”，建议选中“ 禁用管理控件台(MMC)插件 ”、“ 禁止执行autoexec.bat文件 ”、“ 禁止用注册表编辑 ”、“ 禁止导入.reg注册表文件 ”、“ 禁用命令行程序和批处理文件 ”几项，保存设置后重启计算机，即可完成设定。 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