

直观感受Win7防毒技巧的改进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_ti2020/623/2021_2022__E7_9B_B4_E8_A7_82_E6_84_9F_E5_c100_623916.htm

当微软开始大刀阔斧的开展Windows 7计划时，外界对于这个新操作系统早已争论不一。毕竟Vista问世不久，而新操作系统真的会为用户带来更好的体验吗？对于长久以来关注Windows操作系统的用户来说，安全性能否提升则更值得关注。虽然苹果放出话来说“Windows 7不过是Vista加几款补丁而已”，但所有人都有理由相信微软，相信这次新版本的变革绝不会这么简单。一

、UAC变身事实上，在Vista出现UAC功能时外界就争论不休，这种方式在安全性提高的同时却降低了用户体验。由此在Windows 7中，微软开始让用户选择UAC的通知等级，另外还改进了用户界面以提升体验。Windows 7中UAC最大的改进就是在控制面板中提供了更多的控制选项，用户能根据自己需要选择适当的UAC级别。在开始菜单搜索框中输入

“Secpol.msc”后回车，打开本地安全策略编辑器，选择“本地策略” “安全选项”，然后在右侧列表中找到“用户帐户控制：管理员批准模式中管理员的提升提示行为属性”，用户可以看到“本地安全设置”中的下拉列表中共有六种选择，分别是：不提示，直接提升.在安全桌面上提示凭据.在安全桌面上同意提示.提示凭据.同意提示.非Windows二进制文件的同意提示。这里有必要提一下“非Windows二进制文件的同意提示”，该选项可以很好的将Windows系统性文件过滤掉而直接对应用程序使用UAC功能，这是Windows 7的亮点所在。另外一种直观的修改方法为进入控制面板的用户账户更

改界面，点击“更改用户账户控制设置”，Windows 7下的UAC设置提供了一个滑块允许用户设置通知的等级，可以选择4种方式，但显然没有上面的方法灵活。

二、行为中心

Windows 7去掉了最初随Windows XP SP2推出的安全中心(Security Center)，改用行为中心(Action Center)。这里面包含安全中心.问题、报告与解决方.Windows Defender.Windows Update.Diagnostics.网络访问保护.备份与恢复(BackupandRestore).复原(Recovery).以及上面提到的UAC。

在进入行为中心后，Windows 7支持用Windows Defender快速扫描本地电脑。我们在联想T61笔记本中扫描系统盘，耗时仅33秒，扫描资源达34931个，虽然不好界定Windows Defender对于系统本身安全性保障有多高，但作为系统内置与系统契合度很高的软件来说，如此的扫描速度已经非常不错了。其实，Windows Defender在设置中心里的功能还可以让其表现的更加完美。实时保护功能可以对下载以及运行的程序进行扫描。对于特定的文件类型和路径也可以过滤，并且支持邮件以及移动存储的扫描等等。在安全设置中，用户可以非常清晰的看到当前系统各项服务的启用情况，维护区域中也可以显示诸如检测问题报告或者备份方面的信息。

三、全新防火墙功能

Windows 7下的防火墙最大特点就是内外兼防，通过Home or work networks和Public networks来对内外网进行防护。高级设置项目也更加全面，通过入站与出站规则可以清晰勾勒出当前网络流通的情况，并且针对配置文件的操作和策略的导入都有较大的提升。相信以后的更新升级中，Windows 7防火墙将有更大的用武之地。

四、安全部署细节问题&总结

和XP、Vista一样，Windows 7的安全部署也

需要借鉴Windows系列的安全流程。这种近乎通用的方式可以为Windows 7的安全性提供更好的保证。

1.账户问题 绝大多数的黑客入侵，取得root权限后都将如入无人之境。账户的安全问题也就成为重中之重。大家都知道，Administrator级别账户可以有足够高的权限掌控Windows。所以为Administrator起一个不被注意的名字就显得十分必要，但请不要使用Admin之类的名字，二百五博客(<http://www.im250.com.cn>)提醒您因为很多黑客工具的字典里，Admin的猜解频繁度丝毫不比Administrator低。另外在用户管理中把Guest账户停掉，任何时候都不允许其登录系统。当然这种方式对于个人PC比较适用，如果经常遇到多用户登录或者受限登录，最好为账户设置一个通用密码，以屏蔽外界网络的入侵。

2.共享问题 在CMD下输入“net share”查看共享资源。这里有IPC通道、文档以及打印机的共享，当然默认的系统可能还会包含硬盘的共享等。禁止方法如下：
net share c\$ /0delete(删除C盘共享，其它盘符类似)
net share ipc\$ /0delete(删除IPC共享)

3.端口问题 系统中有一些端口是非常危险的，黑客们可以通过这些端口控制我们的计算机，比如3389端口，在关闭之前需要了解一下计算机中开放的端口，在CMD下输入“netstat -an”，看到开放了135、139等端口，需要将其禁止。这种方式最好通过专用防火墙来监听或者直接关闭，在管理上比系统过滤的方式更为方便快捷。很明显，“Windows 7不过是Vista加几款补丁而已”的说法稍显偏颇，但Windows也绝非是无懈可击的。我们可以理解外界以及竞争对手对微软的一些抱怨和质疑，但毋庸置疑的是：Windows 7在安全方面的确有更好的表现。UAC漏洞也不过是被舆论放大的一个事件。面对如

此庞大的代码阵营，众多计算机专家搭建起来的Windows 7势必还会存在瑕疵，就像Windows 2000面对Windows 98，Windows XP面对Windows 2000，Windows Vista面对Windows XP一样，即便是仍有瑕疵，Windows 7也注定成为操作系统发展史上的推动机。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