

深入挖掘用好Windows7网络潜能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__E6_B7_B1_E5_85_A5_E6_8C_96_E6_c100_644234.htm 尽管Windows Vista系统已经比较完美了，可是对于那些喜欢标新立异、追逐个性的朋友来说，他们或许并不会满足于此，因为即使十全十美的东西整天与之接触他们也会感到厌烦的。为此，当微软全新操作系统Windows 7正式登场的时候，这些追新一族自然会立即行动起来，将Windows 7系统“请”到自己的计算机中。为了能在新系统下提升网络管理效率，本文下面就

对Windows 7系统的网络潜能进行深入挖掘，希望大家能从中获取裨益! 1、用好智能过滤，远离页面病毒攻击 无论上网用户如何小心，遭遇网络病毒攻击的可能性几乎不能避免。事实上，很多网络病毒都潜藏在网站页面背后，稍微不留神来自网站页面背后的病毒就会袭击到我们。为此，Windows 7系统为上网用户提供了智能过滤功能，巧妙用好该功能

，Windows 7系统会强制要求其自带的IE浏览器首先链接到微软的网站数据库，来检查当前要访问的站点是否能够通过安全审查，只有那些通过安全审查的站点页面才能被正常显示出来，如此一来本地系统遭遇网络病毒攻击的可能性就会大大下降。使用智能过滤功能其实很简单，我们只要先打开Windows 7系统内置的浏览器窗口，从该窗口的菜单栏中依次点选“工具”/“SmartScreen筛选器”/“打开SmartScreen筛选器”选项，在其后弹出的设置窗口中选中“打开SmartScreen筛选器”项目，同时单击“确定”按钮结束设置操作，如此一来Windows 7系统的智能过滤功能就能帮助上

网用户远离页面病毒攻击了。日后，我们一旦怀疑陌生的网站存在安全威胁时，可以依次单击IE浏览器窗口菜单栏中的“工具”/“SmartScreen筛选器”/“检查此网站”命令，随后智能过滤功能就会自动检查当前网站，并把检查结果显示在界面中。如果智能过滤功能提示当前网站存在安全威胁时，我们可以继续执行“工具”/“SmartScreen筛选器”/“报告不安全网站”命令，将当前网站报告给微软公司。

2、用好强制注销，确保远程连接顺畅

为了提升系统管理效率，很多人都喜欢通过远程连接方式来对Windows 7系统进行管理，不过在缺省状态下Windows 7系统对同时建立的远程连接数量是有限制的，一旦超过这个规定，那么后来发起连接的用户就无法成功远程连接到Windows 7系统上，这样一来远程管理的效率就会受到影响。为了保障远程连接顺畅，我们可以巧妙利用Windows 7系统的强制注销功能，来及时将那些处于闲置状态同时已经超过登录时间的远程连接关闭，那样一来后续用户发起连接时就不会受到Windows 7系统的限制了，下面就是具体的实施步骤：

首先依次单击Windows 7系统桌面上的“开始”/“所有程序”/“附件”/“运行”命令，在弹出的系统运行文本框中输入字符串命令“gpedit.msc”，单击“确定”按钮后，打开对应系统的组策略编辑界面。其次在该编辑界面左侧子窗格中，选中“计算机配置”分支，并从目标分支下面逐一点选“Windows设置”/“安全设置”/“本地策略”/“安全选项”，从“安全选项”子项下面找到目标组策略选项“网络安全：在超过登录后强制注销”，同时用鼠标双击该选项，打开选项设置窗口，检查该窗口中的“已启用”选项是否处于选中状态，要是发现它还没有被选中时，

我们必须将它重新选中，最后单击“确定”按钮完成设置操作，如此一来我们日后远程连接 Windows 7系统时就会顺畅很多了。

3、用好任务附加，监控非法网络登录

无论处于Internet环境还是局域网环境中，常常会有一些非法分子偷偷登录Windows 7系统，来实施一些恶意的破坏活动.为了及时发现这种非法破坏活动，我们可以利用Windows 7系统的任务附加功能，来对网络偷偷登录行为进行自动监控，一旦Windows 7系统遭遇非法网络登录行为时，系统屏幕上会自动弹出提示来告诉我们当前有用户偷偷登陆本地系统，下面就是具体的实施步骤：首先依次单击Windows 7系统桌面上的“开始”/“所有程序”/“附件”/“运行”命令，在弹出的系统运行文本框中输入“gpedit.msc”字符串命令，单击“确定”按钮后，进入组策略编辑界面.依次展开该界面左侧子窗格中的“计算机配置”/“Windows设置”/“安全设置”/“本地策略”/“审核策略”分支选项，再用鼠标双击目标分支下面的组策略选项“审核登录事件”，选中其后界面中的“成功”和“失败”选项，最后点击“确定”按钮保存好上述设置操作，如此一来Windows 7系统日后就能对一切登录行为进行跟踪、记录了，包括成功的登录操作、失败的登录操作等，这些记录同时会被保存到系统的日志文件中.其次为了让Windows 7系统自动把登录行为的监控结果通知给我们，我们需要先人工创建一个系统登录事件，日后才能把监控报警的任务附加到该事件上，这样一来系统一发现登录操作，就会自动运行报警任务，那样就能实现自动监控的目的了。人工创建系统登录事件很简单，我们只要注销系统，随意用一个账号登录系统，Windows 7系统就能自动生成系统登录事件

了.下面用鼠标右击Windows 7系统桌面上的“计算机”图标，从弹出的右键菜单中点选“管理”命令，打开对应系统的计算机管理窗口，依次点选该窗口左侧列表中的“系统工具”/“事件查看器”/“Windows日志”/“系统”节点选项，再选中目标节点下面刚刚生成的系统登录事件，同时用鼠标右键单击该事件，点选右键菜单中的“将任务附加到此事件”选项，弹出任务附加向导窗口.之后在向导设置窗口中输入附加任务的名称，再设置一个合适的监控报警方式，假设我们在这里选用“显示消息”这种报警方式，接下来编辑好报警的标题以及内容，比方说我们将自动报警内容输入为“小心!有人非法网络登录!”，最后点击“完成”按钮。完成上面的设置操作后，当有非法用户偷偷通过网络登录Windows 7系统时，对应系统的主人就能从屏幕上看到“小心!有人非法网络登录!”这样的自动监控信息了，如此一来我们就能及时采取措施来删除恶意登录账号，保护Windows 7系统安全了。

4、用好兼容模式，正常访问网络内容 很多时候，利用Windows 7系统自带的浏览器访问网络内容时，都会遇到页面内容显示不全，或者遇到显示乱码故障，这些故障往往并不是目标站点自身引起的，也不是由于网络病毒引起的，多数情况下是由于Windows 7系统的兼容性设置不当引起的。此时，我们可以按照下面的设置来用好兼容模式功能，确保用户能够正常访问网络内容：首先打开Windows 7系统自带的IE浏览器，单击该窗口菜单栏中的“工具”选项，从下拉菜单中点选“兼容性视图设置”命令，打开设置窗口，在这里将发生乱码现象的站点地址添加进来.当然，如果频繁遇到站点内容显示错乱现象时，我们可以直接选中界面中的“在兼容

性视图中显示所有网站”选项，再单击“关闭”按钮退出设置窗口，那样一来Windows 7系统的兼容模式功能在浏览任何网站内容时都能发挥作用。

5、用好电脑守卫，谨防网络参数被改 在公共场合下，很多人往往会共用一台计算机上网，在这种情况下一些不自觉的用户可能会随意修改本地系统的上网参数，造成他人无法正常上网访问。有鉴于此，Windows 7系统为上网用户新增加了电脑守卫功能，善于使用该功能，我们可以不用担心任何人胡乱修改自己系统的上网参数，因为当恶意用户从系统注销的时候，该用户所进行的所有设置都会恢复到正常，这当然也包含网络设置了。下面就是使用电脑守卫功能，保护网络参数的具体操作步骤：首先以系统管理员权限登录进入Windows 7系统，依次单击该系统桌面上的“开始”/“控制面板”命令，在弹出的系统控制面板窗口中，依次选中“用户账户和家庭安全”/“用户帐户”选项，之后为普通用户创建一个合适的账号名称，同时设置启用“PC Safeguard”功能(并不是所有版本都有该功能)，最后单击“确定”按钮结束设置操作，那样一来电脑守卫功能就能限制普通用户随意更改上网参数了。

6、用好限制下载，禁止木马不请自来 一些网络木马程序往往会不经过系统的允许，就能直接下载保存到本地硬盘，从而给本地系统的运行安全带来威胁。为了禁止网络中的木马程序不请自来，我们可以利用Windows 7系统的限制下载功能，来拒绝木马程序自动下载保存到本地硬盘中，下面就是具体的实现步骤：来源：考试大的美女编辑们 首先依次单击Windows 7系统桌面上的“开始”/“所有程序”/“附件”/“运行”命令，在弹出的系统运行文本框中输入“gpedit.msc”字符串命令，单击“确

定”按钮后，进入组策略编辑界面。其次依次展开该界面中的“用户配置”、“管理模板”、“Windows组件”、“Internet Explorer”、“安全功能”、“限制文件下载”分支选项，用鼠标双击该分支下面的目标组策略选项“Internet Explorer进程”，打开Internet Explorer进程设置对话框，选中“已启用”选项，再单击“确定”按钮保存好设置操作，这样一来Windows 7系统就能禁止类似木马这样的恶意程序自动下载保存到本地硬盘中了。微软Windows Server 2008认证体系介绍 MCSE认证考试全程心得 联想与微软首推Windows 7联想“EE”认证 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