计算机一级辅导:善用组策略确保Vista系统安全计算机等级考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/582/2021_2022__E8_AE_A1_E7_AE_97_E6_9C_BA_E4_c98_582002.htm Vista系统的细节美是此前的Windows系统所不具备的，但是这些细节往往为用户所忽略或者不知。我们进行系统的管理和维护，就应该挖掘这些细节提升系统使用体验，同时也不应忽视系统中的任何一个安全角落。 一、病毒隔离区，被遗忘的角落 Vista系统虽说安全性有了很大的提高，但为其部署杀毒软件还是非常必要的。当下主流的杀毒软件都有一个叫做“ 隔离区 ”的组件，其实它就是个病毒、木马的收容所，也是一个被大家遗忘的角落，它是否是杀毒软件的“ 鸡肋 ”呢?下面我们一起来挖挖其中的技巧。 (1).隔离区大小，由我定 以瑞星为例设置步骤是：依次定位到“ 开始→所有程序→瑞星杀毒软件 ”然后点击运行“ 病毒隔离系统 ”，在其窗口中依次执行“ 工具→设置空间 ”然后就可以根据需要进行设置。默认情况下隔离区大小为500MB，我们只需点击“ 修改 ”按钮然后输入相应的数值即可。 瑞星在默认情况下是开启“ 将染毒文件备份到病毒隔离系统 ”功能的，因此当隔离区空间不足的时候会弹出“ 备份失败 ”对话框造成杀毒的中断。对此我们可以在空间“ 设置 ”窗口中点选“ 空间自动增长 ”选项即可。 提示：瑞星的病毒隔离区即C:\RavBin文件夹，当瑞星对该文件夹没有操作权限时也会弹出“ 备份失败 ”的对话框。这有可能被病毒、木马利用而中断杀毒，希望引起大家的注意。 (2).删除隔离区，还我磁盘空间 隔离区中的病毒就像装在瓶子里的魔鬼总是让人感觉不舒服，并且会占用一定的磁盘空间。

其实，在大多数情况下我们完全可以删除病毒隔离文件夹。比如瑞星的病毒隔离区文件夹为C:\RavBin，将其删除即可。当然最彻底的解决办法是关闭病毒隔离功能，打开瑞星主程序定位到“ 设置→详细设置 ”，点击左侧的“ 其它设置 ”，取消右侧的对“ 将染毒文件备份到病毒隔离系统 ”的勾选即可。 (3).救命稻草，误杀不再可怕 因为种种原因，杀毒软件误杀频频。无论第三方工具还是系统组件，被杀毒软件误杀这都是我们不能原谅的。通过病毒隔离区，我们可以恢复被杀毒软件误杀的文件。以瑞星为例，操作步骤是：运行“ 瑞星病毒隔离系统 ”，右键单击要恢复的文件选择“ 恢复 ”即可。 文件被恢复后，我们为了防止再次被误杀首先要升级杀毒软件的病毒库。如果病毒库没有修补误杀错误，我们需要将该文件添加到杀毒软件的“ 信任区域 ”(卡巴斯基)。以瑞星为例，打开瑞星主程序定位到“ 设置→详细设置 ”，在“ 其它设置 ”分支下点击“ 查杀是排除指定的目录 ”右侧的“ 设置 ”按钮将该文件所在的目录添加进来即可。 (4).亲自出马，手刃病毒 有的时候杀毒软件并不能除恶务尽，而是将病毒、木马丢进隔离区了事。这时，我们可以通过“ 病毒隔离系统 ”工具将病毒文件另存到其它地方，然后进行病毒分析根据其特征手工清除它。另外，如果你是一个安全爱好者，可以在此抓病毒、木马进行研究。 二、在Vista组策略中“ 淘宝 ” Vista的组策略较XP有了较大的改进，其功能更为强大是一座名副其实的“ 宝藏 ”。下面我们一道出发，在组策略中“ 淘宝 ”。 (1).我的密码你别猜 如果Vista的密码不够“ 强壮 ”时，恶意用户很容易通过多次重试“ 猜 ”出来。要避免这一情况，在组策略设置帐户锁定策略即可完美解决。此时，

当恶意用户尝试登录系统，输入错误密码的次数达到一定次数(阈值)时即自动将该帐户锁定，在帐户锁定期满之前，该帐户将不可使用，除非管理员手动解除锁定。其设置方法如下： 在开始菜单的搜索框输入“ Gpedit.msc ”打开组策略对象编辑器，然后依次点击定位到“ 计算机设置→Windows设置→安全设置→帐户策略→帐户锁定策略 ”策略项下。双击右侧的“ 帐户锁定阈值 ”，此项设置触发用户帐户被锁定的登录尝试失败的次数。该值在0到999之间，默认为0表示登录次数不受限制。大家可以根据自己的安全策略进行设置，我们设置为5。 (2).我的电脑你别关 在单位经常有一些好事之徒喜好偷窥别人电脑上的资料，虽然我们可以通过Windows L来锁定计算机以防偷窥，但是在在锁定页面上还有一个“ 关闭计算机 ”选项。如果好事之人点击一下“ 关闭计算机 ”，那么，前期的工作很可能就付之东流了。百考试题提示很有必要给“ 关闭计算机 ”再加一把锁。通过组策略即可轻易完成这样的任务。 点击“ 开始→运行 ”，在弹出的运行对话框中输入“ Gpedit.msc ”，回车后打开组策略编辑器。依次展开如下分支“ 计算机配置→Windows设置→安全设置→本地策略→安全选项 ”，在右侧的窗格中找到“ 关机：允许在未登陆前关机 ”选项，双击，在弹出来的属性对话框中将其属性设置为“ 已禁用 ”，点击“ 确定 ”按钮并关闭组策略编辑器即可。 (3).我的分区你别看 我们的电脑中存储着某些数据资料，这是不必让别人知道的。其实我们不需要第三方软件在Vista中通过对磁盘分区进行隐藏或者限制即可轻易实现对数据的保护的。下面我们以限制C分区为例进行演示，其具体操作步骤如下： 第一步：在开始菜单的“ 运行 ”对话框中

，输入“ Gpedit.msc ”，打开“ 组策略 ”设置窗口，在“ 组策略 ”设置窗口中，依次打开“ 本地计算机策略→用户配置→管理模板→Windows组件→Windows资源管理器 ”选项。 第二步：在右边的设置窗口中，选择“ 防止从‘ 我的电脑 ’访问驱动器 ”项，在这个选项上单击鼠标右键，选择“ 属性 ”，接着出现“ 防止从‘ 我的电脑 ’访问驱动器的属性 ”设置窗口。在其中有三个选项，分别是“ 未配置 ”、“ 已启用 ”、“ 已禁用 ”。 第三步：我们选择“ 已启用 ”后，在下面就会出现选择驱动器的下沉列表，如果希望限制某个驱动器的使用，只要选中该驱动器就可以了。比如，我们要限制C盘的使用，选中“ 仅限制驱动器C ”，就可以了。如果希望关闭所有的驱动器，包括光驱等，可以选中“ 限制所有驱动器 ”。 (4).我的USB你别插 利用U盘等移动设备进行数据窃密已经是屡见不鲜了，如何让系统只能使用指定移动存储设备呢? 利用Vista的组策略就能实现对USB存储设备的有效控制。 第一步：把自己的U盘先插入到Vista 系统中，让系统可以正常使用U盘，接着进入“ 控制面板 ”，双击“ 设备管理器 ”，在里面展开“ 便携设备 ”，可以看见里面有你的U盘。 第二步：在上面点击鼠标右键来选择“ 属性 ”，在弹出的“ 属性 ”窗口中点击“ 详细信息 ”标签，然后在设备“ 属性 ”下拉框中选择“ 硬件ID ”，下面的“ 值 ”中会出现字符串，这个就是你的U盘的硬件ID，把它复制出来保存好。 第三步：还需要复制“ 通用串行总线控制器 ”中“ USB大容量存储设备 ”的硬件ID，在“ 设备管理器 ”中展开“ 通用串行总线控制器 ”列表，找到“ USB大容量存储设备 ”，在它的“ 属性 ”窗口中点击“ 详细信息 ”标签，复制出它的硬件ID也保存一

下。 第四步：找出U盘的硬件ID后就可以通过组策略来实现了。“ 开始→运行 ” 输入 “ Gpedit.msc ” 打开组策略窗口，依次展开 “ 计算机配置→管理模板→系统→设备安装→设备安装限制 ”，双击右侧的 “ 禁止安装未由其他策略设置描述的设备 ”，在弹出的窗口中选择 “ 已启用 ”，再点击 “ 确定 ” 按钮，设置它可以来禁止策略没描述的USB设备。 细节决定成败，做系统是这样，当然维护系统也是此理。Vista中的细节美无处不在，需要大家进一步去探索。 特别推荐： 2009年9月全国计算机等级考试时间及科目预告 2009年上半年全国计算机等级考试参考答案请进入计算机考试论坛 2009年全国计算机等级考试报名信息汇总 2009年NCRE考试有新变化 2009年全国计算机等级考试大纲 2009年上半年全国计算机二级考试试题及答案 2009年上半年全国计算机等级考试试题答案汇总 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