组策略让Win2008在低安全级别下更安全Microsoft认证考试
 尽管Windows Server 2008系统的安全性要领先其他操作系统一大步，不过默认状态下过高的安全级别常常使不少人无法顺利地在Windows Server 2008系统环境下进行各种操作，为此许多用户往往会采用手工方法来降低Windows Server 2008系统的安全访问级别。可是，一旦降低了安全访问级别，Windows Server 2008系统遭遇安全攻击的可能性就非常大了.那么如何在安全访问级别不高的情况下，我们仍然能够让Windows Server 2008系统安全地运行?要做到这一点，我们可以利用Windows Server 2008系统强大的组策略功能，来对相关选项参数进行有效设置! 1、禁止恶意程序“ 不请自来 ”在Windows Server 2008系统环境中使用IE浏览器上网浏览网页内容时，时常会有一些恶意程序不请自来，偷偷下载保存到本地计算机硬盘中，这样不但会白白浪费宝贵的硬盘空间资源，而且也会给本地计算机系统的安全带来不少麻烦。为了让Windows Server 2008系统更加安全，我们往往需要借助专业的软件工具才能禁止应用程序随意下载，很显然这样操作不但麻烦而且比较累人.其实，在Windows Server 2008系统环境中，我们只要简单地设置一下系统组策略参数，就能禁止恶意程序自动下载保存到本地计算机硬盘中了，下面就是具体的设置步骤： 首先以特权帐号进入Windows Server 2008系统环境，依次点选系统桌面中的“ 开始 ”/“ 运行 ”命令，在系统运行框中执行gpedit.msc命令，打开本地计算机的组策略编辑窗口.其次在组策略编辑窗口左

侧区域展开“ 计算机配置 ”分支，再依次选择该分支下面的“ 管理模板 ”/“ Windows组件 ”/“ Internet Explorer ”/“ 安全功能 ”/“ 限制文件下载 ”子项，双击“ 限制文件下载 ”子项下面的“ Internet Explorer进程 ”组策略选项，打开如图1所示的目标组策略属性设置窗口.选中“ 已启用 ”选项，再单击“ 确定 ”按钮退出组策略属性设置窗口，这样一来我们就能成功启用限制Internet Explorer进程下载文件的策略设置，日后Windows Server 2008系统就会自动弹出阻止Internet Explorer进程的非用户初始化的文件下载提示，单击提示对话框中的“ 确定 ”按钮，恶意程序就不会通过IE浏览器窗口随意下载保存到本地计算机硬盘中了。 2、对重要文件夹进行安全审核 Windows Server 2008系统可以使用安全审核的方法来跟踪访问重要文件夹或其他对象的登录尝试、用户账号、系统关闭、重启系统以及其他一些事件。要是我们能够充分利用Windows Server 2008系统文件夹的审核功能，就能有效保证重要文件夹的访问安全性，其他非法攻击者就无法轻易对其进行恶意破坏.在对Windows Server 2008系统中的重要文件夹进行访问审核时，我们可以按照如下步骤来进行： 首先以特权帐号进入Windows Server 2008系统环境，依次点选系统桌面中的“ 开始 ”/“ 运行 ”命令，在系统运行框中执行gpedit.msc命令，打开本地计算机的组策略编辑窗口. 其次在组策略编辑窗口左侧区域展开“ 计算机配置 ”分支，再依次选择该分支下面的“ Windows设置 ”/“ 安全设置 ”/“ 本地策略 ”/“ 审核策略 ”选项，在对应“ 审核策略 ”选项的右侧显示区域中找到“ 审核对象访问 ”目标组策略项目，并用鼠标右键单击该项目，执行右键菜单中的“ 属性 ”命令打开目标组策略项目

的属性设置窗口. 选中该属性设置窗口中的“ 成功 ”和“ 失败 ”复选项，再单击“ 确定 ”按钮，如此一来访问重要文件夹或其他对象的登录尝试、用户账号、系统关闭、重启系统以及其他一些事件无论成功与失败，都会被Windows Server 2008系统自动记录保存到对应的日志文件中，我们只要及时查看服务器系统的相关日志文件，就能知道重要文件夹以及其他一些对象是否遭受过非法访问或攻击了，一旦发现系统存在安全隐患的话，我们只要根据日志文件中的内容及时采取针对性措施进行安全防范就可以了。 3、禁止改变本地安全访问级别 在办公室中，我们有时需要与其他同事共享使用同一台计算机，当我们对本地计算机的IE浏览器安全访问级别设置好，肯定不希望其他同事随意更改它的安全访问级别，毕竟安全级别要是设置得太低的话，会导致潜藏在网络中的各种病毒或木马对本地计算机进行恶意攻击，从而可能造成本地系统运行缓慢或者无法正常运行的故障现象。为了防止其他人随意更改本地计算机的安全访问级别，Windows Server 2008系统允许我们进入如下设置，来保护本地系统的安全：首先以特权帐号进入Windows Server 2008系统环境，依次点选系统桌面中的“ 开始 ”/“ 运行 ”命令，在系统运行框中执行gpedit.msc命令，打开本地计算机的组策略编辑窗口. 其次在组策略编辑窗口左侧区域展开“ 用户配置 ”分支，再依次选择该分支下面的“ 管理模板 ”/“ Windows组件 ”/“ Internet Explorer ”/“ Internet控制模板 ”选项，在对应“ Internet控制模板 ”选项的右侧显示区域中找到“ 禁用安全页 ”目标组策略项目，并用鼠标右键单击该项目，执行右键菜单中的“ 属性 ”命令打开目标组策略项目的属性设置窗口. 选中该属性设

置窗口中的“ 已启用 ”选项，再单击“ 确定 ”按钮结束目标组策略属性设置操作，如此一来Internet Explorer的安全设置页面就会被自动隐藏起来，这样的话其他同事就无法进入该安全标签设置页面来随意更改本地系统的安全访问级别了，那么本地计算机系统的安全性也就能得到有效保证了。 当然，我们也可以通过隐藏Internet Explorer窗口中的“ Internet选项 ”，阻止其他同事随意进入IE浏览器的选项设置界面，来调整本地系统的安全访问级别以及其他上网访问参数。在隐藏Internet Explorer窗口中的“ Internet选项 ”时，我们可以按照前面的操作步骤打开Windows Server 2008系统的组策略编辑窗口，将鼠标定位于“ 用户配置 ”/“ 管理模板 ”/“ Windows组件 ”/“ Internet Explorer ”/“ 浏览器菜单 ”分支选项上，再将该目标分支选项下面的禁用“ Internet选项 ”组策略的属性设置窗口打开，然后选中其中的“ 已启用 ”选项，最后单击“ 确定 ”按钮就能使设置生效了。 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