Windows组策略之软件限制策略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_Windows_E7_BB_84_c100_644188.htm 对于Windows的组策略，也许大家使用的更多的只是 管理模板 里的各项功能。对于 软件限制策略 相信用过的筒子们不是很多：）。软件限制策略 如果用的好的话，相信可以和某些HIPS类软件相类比了。如果再结合NTFS权限和注册表权限，完全可以实现系统的全方位的安全配置，同时由于这是系统内置的功能，与系统无缝结合，不会占用额外的CPU及内存资源，更不会有不兼容的现象，由于其位于系统的最底层，其拦截能力也是其它软件所无法比拟的，不足之处则是其设置不够灵活和智能，不会询问用户。下面我们就来全面的了解一下 软件限制策略。 1、概述 使用 软件限制策略，通过标识并指定允许哪些应用程序运行，可以保护您的计算机环境免受不可信任的代码的侵扰。通过散列规则、证书规则、路径规则和Internet 区域规则，就用程序可以在策略中得到标识。默认情况下，软件可以运行在两个级别上：“ 不受限制的 ”与“ 不允许的 ”。在本文中我们主要用到的是路径规则和散列规则，而路径规则呢则是这些规则中使用最为灵活的，所以后文中如果没有特别说明，所有规则指的都是路径规则。 2、附加规则和安全级别 附加规则 在使用 软件限制策略 时，使用以下规则来对软件进行标识： 证书规则 软件限制策略可以通过其签名证书来标识文件。证书规则不能应用到带有 .exe 或 .dll 扩展名的文件。它们可以应用到脚本和Windows 安装程序包。可以创建标识软件的证书，然后根据安全级别的设置，决定是否允许软件运行。

路径规则 路径规则通过程序的文件路径对其进行标识。由于此规则按路径指定，所以程序发生移动后路径规则将失效。路径规则中可以使用诸如 %programfiles% 或 %systemroot% 之类环境变量。路径规则也支持通配符，所支持的通配符为 * 和 ?。 散列规则 散列是唯一标识程序或文件的一系列定长字节。散列按散列算法算出来。软件限制策略可以用 SHA-1（安全散列算法）和 MD5 散列算法根据文件的散列对其进行标识。重命名的文件或移动到其他文件夹的文件将产生同样的散列。 例如，可以创建散列规则并将安全级别设为“ 不允许的 ”以防止用户运行某些文件。文件可以被重命名或移到其他位置并且仍然产生相同的散列。但是，对文件的任何篡改都将更改其散列值并允许其绕过限制。软件限制策略将只识别那些已用软件限制策略计算过的散列。 Internet区域规则 区域规则只适用于 Windows 安装程序包。区域规则可以标识那些来自 Internet Explorer 指定区域的软件。这些区域是 Internet、本地计算机、本地 Intranet、受限站点和可信站点。 以上规则所影响的文件类型只有“ 指派的文件类型 ”中列出的那些类型。系统存在一个由所有规则共享的指定文件类型的列表。默认情况下列表中的文件类型包括：ADE ADP BAS BAT CHM CMD COM CPL CRT EXE HLP HTA INF INS ISP LNK MDB MDE MSC MSI MSP MST OCX PCD PIF REG SCR SHS URL VB WSC，所以对于正常的非可执行的文件，例如TXT JPG GIF这些是不受影响的，如果你认为还有哪些扩展的文件有威胁，也可以将其扩展加入这里，或者你认为哪些扩展无威胁，也可以将其删除。 安全级别 对于软件限制策略，默认情况下，系统为我们提供了两个安全级别：“ 不受限的 ”和

“ 不允许的 ” 注：“ 不允许的 ” 级别不包含任何文件保护操作。你可以对一个设定成 “ 不允许的 ” 文件进行读取、复制、粘贴、修改、删除等操作，组策略不会阻止，前提当然是你的用户级别拥有修改该文件的权限 “ 不受限的 ” 级别不等于完全不受限制，只是不受软件限制策略的附加限制。事实上，“ 不受限的 ” 程序在启动时，系统将赋予该程序的父进程的权限，该程序所获得的访问令牌决定于其父进程，所以任何程序的权限将不会超过它的父进程。 但实际上，还有三个级别在默认情况是隐藏掉的，我们可以通过手动修改注册表来开启其它的三个级别，打开注册表编辑器，展开至：HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\ Safer\CodeIdentifiers 新建一个DOWRD，命名为Levels，其值为 0x4131000(十六十制的4131000) 创建完毕后重新打开gpedit.msc，我们会看到另外三个级别此时已经开启了。 不受限的 最高权限，但其也并不是完全的不受限，而是 “ 软件访问权由用户的访问权来决定 ”，即继承父进程的权限。 基本用户 基本用户仅享有 “ 跳过遍历检查 ” 的特权，并拒绝享有管理员的权限。 受限的 比基本用户限制更多，但也享有 “ 跳过遍历检查 ” 的特权。 不信任的 不允许对系统资源、用户资源进行访问，直接的结果就是程序将无法运行。 不允许的 无条件地阻止程序执行或文件被打开 根据权限大小可以排序为：不受限的 