深入探讨WindowsXP系统文件保护功能 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/454/2021_2022__E6_B7_B1_E5_85_A5_E6_8E_A2_E8_c100_454486.htm 当你安装一个应用程序却不料引起windows崩溃的时候，很有可能是因为应用程序改写了关键的windows系统文件，导致系统崩溃。在文件被修改后，结果往往不可预知。系统可能正常运行，或者出一些错误，或者完全崩溃。幸运的是，windows000, xp, 和server003应用了一个称作windows文件保护(windows file protection， wfp)机制，它可以防止关键的系统文件被改写。在这篇文章中，我将解释何谓wfp和它是如何工作的。我还要告诉你如何修改或忽略wfp的行为。(注释:尽管在windows000, xp，和server003上，wfp的运行没什么区别，但这篇文章中的信息，包括注册表相关条目和sfc语法，是针对xp的。) windows文件保护是如何工作的 wfp被设计用来保护windows文件夹的内容。wfp保护特定的文件类型，比如sys、exe、dll、ocx、fon和ttf，而不是阻止对整个文件夹的任何修改。注册表键值决定wfp保护的文件类型。 当一个应用程序试图替换一个受保护的文件，wfp检查替换文件的数字签名，以确定此文件是否是来自微软和是否是正确的版本。如果这两个条件都符合，则允许替换。正常情况下，允许替换系统文件的文件种类包括windows的服务包，补丁和操作系统升级程序。系统文件还可以由windows更新程序或windows设备管理器/类安装程序替换。 如果这两个条件没有同时满足，受保护文件将被新文件替换，但将很快被正确的文件替换回来。当这种情况发生时，windows会从windows安装cd或者计算机的dllcache

文件夹中复制正确版本的文件。 windows文件保护并不仅仅通过拒绝修改来保护文件，它还可以拒绝删除。来看看wfp的做法，打开/windows/system32文件夹并将calc.exe文件重命名为calc.old。当你这样做时，一个消息将提示你如果改变这个文件的扩展名可能会导致这个文件不可用。点击yes按钮确认这个警告。现在，等几分钟后按f5键以刷新文件系统的视图，完成替换可能要花些时间。当文件最终被替换后，windows会在事件日志中做相应的记录。 关于wfp值得关注的一点是它和windows安装程序结合的很紧密。无论何时，如果windows安装程序需要安装一个受保护的文件，它就把这个文件交给wfp，而不是自己试图去安装这个文件。然后由wfp判断是否允许安装。 系统文件检查 虽然自动文件替换会节省时间，但也存在需要手动干预的情况。例如，你可能不愿意空等着wfp去判断受保护的文件是否已经被替换。幸运的是，你可以用一个名为系统文件检查(sfc)的工具手动控制wfp。 sfc是一个命令行工具，需要在命令提示符窗口下运行。它的语法像这样: sfc [/scannow] [/scanonce] [/scanboot] [/revert] [/purgecache] [/cachesize=x] /scannow选项通知sfc立即扫描所有受保护的系统文件。如果在扫描过程中发现一个错误的文件版本，这个错误的版本将被替换为微软正确的版本。当然，这意味着你可能必须有windows安装cd，最新的服务包或者升级补丁。 /scanonce参数通知wfp在系统下次启动的时候扫描受保护的系统文件。在扫描过程中，任何错误的文件将被正确的版本替换。正如这个参数名的意思，这个扫描只进行一次。之后的系统启动将恢复正常，sfc不再运行。 /scanboot参数和/scanonce选项类似。区别在于scanonce只在windows下次启

动时扫描受保护的文件，而scanboot参数则在windows每次启动时都扫描系统文件。如果需要，这两个参数将替换错误的系统文件，这可能需要你提供正确文件版本的拷贝。 /revert选项用来关闭sfc，例如，假设你使用scanboot选项在每次系统启动的时候扫描所以保护的文件。正如你所能想到的，这确实会增加计算机启动的总时间。最后，你可能厌倦了漫长的启动时间，想关闭sfc。只需要简单的使用sfc /revert，就可以在启动的时候关闭sfc。 对/purgecache选项就需要谨慎些。在这之前，我解释说windows使用一个缓存文件夹来保存各类系统文件正确版本的备份。如果你运行sfc /purgecache命令，那么这个文件缓存将被清空，那些备份文件将被删除。这个命令还会导致windows开始扫描各类受保护文件，并在扫描的同时重建这个文件缓存。当然，这可能意味着你必须向windows提供windows安装cd或系统文件升级的拷贝。 最后一个sfc命令选项是/cachesize=x。对于文件缓存的缺省大小确实存在很多自相矛盾的信息，在写这篇文章的时候，我发现三篇不同的微软知识库文章中指定的文件缓存的缺省大小都不一样。一篇文章中建议文件缓存的大小为50 mb，而另一篇建议的大小却是300 mb。更有甚者，第三篇指出这个大小应该是无限的。其实缺省值的大小并不重要，因为你可以根据你的需要，使用cachesize选项来改变这个文件缓存的大小。 在使用cachesize选项时，你必须键入命令sfc /cachesize=x，这个x是指你想分配给文件缓存的兆字节数。在指定了新的文件缓存大小后，你必须重启系统并运行sfc /purgecache命令。 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