Windows7中提高系统文件的稳定性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_ti2020/590/2021_2022_Windows7_E4_B8_c100_590055.htm 众所周知，微软操作系统文件是经常被木马、病毒等程序所关注的对象。有时候用户也不会在不经意的情况下破坏系统文件。系统不稳定大部分情况下都是由于系统文件遭受到破坏所引起的。在Windows7中这个系统文件的稳定性有了不少的改善。 在谈这个话题之前，首先系统管理员需要明白一点，就是微软操作系统中的系统文件不管是操作系统安装时的必需文件，而且还包括一些驱动程序。微软操作系统对硬件的支持力度要比Linux等开源操作系统强的多。在Windows7操作系统中，一进攻可以检测大多数的硬件，并且在安装过程中会自动查找并安装相应的驱动程序。这主要是因为微软在一个新版本操作系统出来之前，都会对当前主流的硬件设备进行测试。如果测试通过的话会将这个硬件的驱动程序加入到操作系统中。所以在Windows7系统安装成果后不用手工安装驱动程序就可以识别大部分的硬件。而这些驱动程序也就构成了微软操作系统中的系统文件。以下对于系统文件稳定性的一些保护措施，对于这些驱动程序文件同样有效。 一、利用文件签名来验证系统文件是否被修改。 在Windows7操作系统中，所有的系统文件(包括微软认可的驱动程序文件)都会带有微软的签名。在这个签名信息中包含了系统文件名、存储路径、文件创建的日期以及版本号等信息。如果系统管理员在Windows7系统部署完毕后，收集相关的信息。然后当操作系统出现不稳定的情况，系统管理员怀疑是系统文件遭受破坏所引起的，就可以将系统文件的

签名与原始签名进行对比，就可以判断系统文件是否在管理员不知情的情况下被更改了。从而可以采取相关的措施来修复系统文件来恢复操作系统的稳定性。 在微软操作系统中，现在不需要手工来收集这些信息。在系统中提供了一个图形化文件签名工具，可以帮助系统管理员来做这项工作。在命令行模式下，输入sigverif命令就会弹出如下的对话框。 这个文件签名工具是微软操作系统提供的一个基于图形化管理的工具。当安装了某个应用程序或者硬件设别时，如果系统管理员怀疑原始的、被保护的、经过数字签名的系统文件或者启动程序被非法修改或者替换，则就可以利用这个工具来检查是否有这种情况的存在。虽然这个工具在以前版本的操作系统中已经存在，但是以前一直被大家所忽视。在Windows7中对这个工具做了不少的改善，特别是在性能上。经过笔者的测试，在Windows7操作系统中，这个工具的运行速度要比以前版本的操作系统快好几倍。另外这个工具在功能上也有所改进。如在以前的操作系统中只检测系统文件，而不会检测驱动程序。而现在的话，这个工具会同时检测系统文件以及驱动程序文件，以确保所有的文件都具有微软的数字签名。当工具检测到没有经过签名或者不准确的文件版本时，就会将相关的信息文件名、修改时间、版本号等内容告诉给管理员。也会在系统相关日志中保留这些信息，以便系统管理员后续查询。 不过笔者使用后觉得还有一个不方便的地方，就是无法将这写信息直接导入到文本文件或者直接进行复制。如现在这个工具查询到某个文件有问题，如tcpip.sys这个文件有问题。现在系统管理员可能需要在互联网上查找这个文件的具体用途，以及以前是否有人也遇到过这种问题。但是

让笔者气馁的是竟然不能够直接复制这个文件名字。现在笔者要向他人请教这个文件的用途时，不得不手工进行输入，而不能够通过复制粘贴来实现。笔者建议微软的设计专家们，在这方面可以更加人性化一点。最后能够把这些信息在这个窗口中直接导出为文本文件或者可以直接进行复制粘贴操作。而不是要打开日志文件来进行这些行为。 另外需要注意的是，这个工具不会对有问题的文件尽心自我修复。所以运行这个工具并不要求有管理员的权限。也就是说，普通用户也可以运行这个程序来检查系统文件是否被受到恶意更改。
二、利用sfc命令自动修复有问题的系统文件。 如果通过以上的这个工具发现有问题的系统文件该如何处理呢?除了通过系统安装盘来修复系统文件或者手工对文件进行修复外，在操作系统中还提供了另外一个有用的工具，即sfc命令。这个命令的功能跟文件签名认证工具的功能类似，会对系统文件以及驱动程序的签名合法性进行验证。不过两个工具还是有很大的差异。 一是外观上的差异。sfc是一个命令行下面的工具，即没有图形化的管理向导。而文件签名验证工具则是一个图形化的管理工具。所以从方便性上来说，文件签名工具可能更容易上手。不过对于系统管理专家来说，图形化界面与文本界面可能没有本质上的差异。另外最重大的一个差异可能就是功能上的差异了。Sfc 命令不仅会检查系统文件与驱动程序签名的合法性，而且还会自动修复检测到有问题的文件。其修复的方式就是将任何被检测到的不正确的文件都被自动替换为微软版本的额外文件。由于在替换的过程中，不会对系统管理员有任何的提示，所以使用这个工具的时候会有一定的风险。为此笔者的建议是，系统管理员最好先利用文

件签名工具来查询一下到底存在哪些有问题的系统文件或者驱动程序文件。如果确认这些文件被微软版本的文件所代替没有问题的情况下，在使用sfc这个命令行工具来自动修复有问题的文件。 如果在操作系统中，系统管理员部署了一些没有经过签名的系统文件。如果系统管理员认为这些文件是必需的，那么最好不要冒然使用这个工具。如可以在使用这个工具之前，先将那些合法的但是没有签名的文件复制出来，然后在使用这个工具修复其他有问题的系统文件或者驱动程序。等到修复完成之后，再将这些合法的没有签名的文件或者驱动程序文件还原过去。另外由于这个运行这个工具风险比较大，为此在Windows7操作系统中做了比较严格的限制，必须作为管理员才能够运行这个程序。注意这个管理员特质系统默认的 administrator帐户。也就是说，如果系统管理员建立了一个新帐户，然后将这个帐户加入到管理员组。此时这个帐户就具有了管理员的身份，但是其仍然不能够运行这个sfc工具。因为他不是系统默认的管理员帐户。微软在这方面的限制，主要是为了防止这个工具被滥用，从而影响其他用户的应用程序。 另外还可以跟组策略结合来使用这个工具。如可以在组策略中配置在操作系统启动的时候，自动运行这个工具。一般来说，如果Windows7操作系统只是作为客户端来使用，那么这是维持其稳定性的一个很好的选择。但是如果其是作为服务器来使用，那么笔者不建议这么做。由于服务器对于企业信息化应用的敏感性(服务器出现故障所有相关应用的客户端都会受到影响)，所以只有在系统文件损坏或者驱动程序出现问题时才使用这个工具。并且在利用这个工具之前最好先使用签名认证工具查询一下可能有问题的文件

。在必要的情况下，还需要先对服务器中的数据进行备份。以防止由于文件恢复故障而导致操作系统无法启动。为此笔者认为sfc虽然是一个维护系统文件稳定的好工具，但是系统管理员还是需要谨慎使用。 