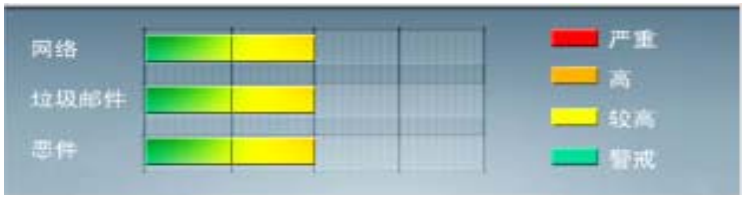
安全威胁每周警讯

2010/10/23～2010/10/30

本周威胁指数



TrendMicro 中国区网络安全监控中心

前十大病毒警讯

排名	病毒名称	威胁类型	风险等级	趋势	病毒行为描述
1	TROJ_DOWNAD.INF	木马	★★★	→	DOWNAD 蠕虫关联木马
2	TROJ_IFRAME.CP	木马病毒	★★★	→	GIF、jpg 和 SWF 文件中被插入一个恶意的 iframe 标记时，趋势科技会将其判断为 TROJ_IFRAME.CP 病毒。 当这些文件被执行时，会重定向到这些 URL，并下载恶意程序
3	WORM_DOWNAD.AD	蠕虫	★★★★	→	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
4	Cryp_Xed-12	木马	★★★	↑	疑似病毒
5	WORM_DOWNAD	蠕虫	★★★★	↓	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
6	JS_EXPLOIT.SMD	网页病毒	★★★	↑	该 JavaScript（JS）的恶意软件可能被托管在一个网站，当用户访问网站时运行并感染。同时，它可能是其他恶意软件的组成部分。通常它检查的 Adobe Flash Player 的系统中安装的版本。然后，它尝试下载一个 SWF 文件根据的 Flash Player 的版本安装。
7	PAK_Generic.001	加壳程序	★★	↑	对加壳文件的通用检测。病毒通常会使用加壳手法来达到不被杀毒软件检测的目的
8	CRCK_KEYGEN	破解程序	★★	↓	非法破解程序
9	WORM_ECODE.E-CN	蠕虫	★★★★	↓	E 语言病毒,产生与当前文件夹同名 exe 文件
10	Gray_Gen	灰色软件	★★★	→	灰色软件的通用检测名。在用户不知情的情况下，在其电脑上安装后门、收集用户信息的软件

系统漏洞信息

MS10-083:Windows Shell 和写字板中的 COM 验证漏洞可能允许远程执行代码

受影响的软件:

Windows XP

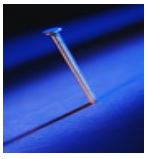
Windows Server 2003

Windows Vista

Windows 7

Windows Server 2008

描述: 请见http://www.microsoft.com/china/technet/security/bulletin/MS10-083.mspx



系统安全技巧

摘要：根据经验，只要服务器管理员善于使用下面四把利剑，那么能够在很大程度上提升 Windows 服务器的稳定性。这四把利剑分别是热插拔、自修复、并行会话与虚拟化。

很多服务器管理员认为 Windows 服务器操作系统在稳定性上不如 Linux 等操作系统，其实这 是一个误解。虽然 Windows2003 以前的版本在稳定性与安全性上是稍有不足，但是在 2008 版本中，在稳定性方面有了很大的改善。从某种程度上来 说，其稳定性已经与 Unix 等服务器操作系统相当。在某些方面甚至是有过之而不及。根据经验，只要服务器管理员善于使用下面四把利剑，那么能够在很大程度 上提升 Windows 服务器的稳定性。这四把利剑分别是热插拔、自修复、并行会话与虚拟化。

一、热插拔让服务器在不当机的情况下完成硬件的升级。

硬件的更新换代速度是很快的。企业可能服务器刚购买一年，就出来了速度更快的 CPU。或者由于企 业数据量的增多，需要增加一块 CPU 以提高服务器数据处理的能力。如果换成其他的服务器操作系统或者说 2008 以前的 Windows 操作系统，需要将服务 器关掉之后，才能够换上新的 CPU 或者内存等硬件。然后再进行重新启动。显然如此操作的话，服务器就会当机。用户会有一段时间将无法访问服务器。对于需要 全天运行的服务器来说，这个时间虽然短暂，但是可能就是很致命的。

Windows2008 服务器操作系统具有支持热插拔核心硬件的能力。简单的说，如果服务器管理 员需要增加 CPU 或者增加内存的话，不需要关掉服务器。而只需要像插 U 盘一样，直接插上去就可以使用。这就可以避免服务器在一定时间内当机的情况，以提高 服务器的稳定性。所以热插拔组件这个利刃，能够在 IT 应用环境中实现零停机。即使服务器某个核心硬件(如 CPU 或者内存)出现故障需要更换或者进行升级 时，也不需要关闭系统。故在服务器上实现了热插拔技术，那么就能够帮助企业最小化系统停机的时间。

这里需要提醒的一点是，虽然在 Windows2003 操作系统上已经有部分零件可以实现热插拔。 不过这基本上是零件供应商的行为。也就是说，像 PCI 适配器等等，硬件供应商已经实现了热插拔的技术。而在 2008 操作系统中，则是 Windows 操作系统自己自带了热插拔的技术。不仅在稳定性上有所提升，而且在硬件的范围上也有了很大的扩展。两者并不能够相提并论。

二、文件或者目录的自动修复。

在服务器维护时，不少服务器管理员会抱怨服务器上的文件或者目录会莫名其妙的损坏。确实，在突然 断电重启或者病毒等原因，会造成服务器上的文件或者目录发生损坏。如果问题严重的话(如恰巧损坏的是系统文件)，则有可能导致服务器瘫痪。轻一点的话，就 是导致用户无法访问某个文件。虽然病毒的泛滥与服务器上的应用程序越来越复杂，文件以及目录的损坏已经严重影响到服务器的稳定性。此时服务器管理员可能需 要重新启动服务器，并使用 chkdsk 等工具来清理文件和目录损坏等错误。

为了避免这种情况下，比较好的方法是要求服务器能够对损坏的文件或者目录进行自动修复。就好像人 感冒一样，能够自动生成白细胞来查杀细菌，帮助人体恢复健康。在 Windows2008 服务器操作系统中，有一个 NTFS 自修复功能，可以实现这一点。自 动修复 NTFS 技术，使操作系统中一个在后台不间断运行的辅助线程。这个线程会自动监测系统中是否有损坏的文件或者目录。如果发现有的话，则会进行自动修 复。总之这个 NTFS 自动修复功能能够用于保持操作系统的可靠运行并且具有更少的系统问题。

不过需要提醒的是，这个功能前面带有 NTFS 这个定语。也就是说，这个功能只针对 Windows 操作系统的 NTFS 分区有效。如果采用的是 FAT32 分区的话，就无法享受这一功能带来的优势。为此建议客户，在使用 Windows 服务器操作系统的话，NTFS 文件系统是一个优先选择的文件系统。

三、并行会话让作业不在排队。

在一条车道的马路上，如果车辆比较多，那么就只能够排队通过。而如果车道一多的话，车辆就可以并 排通过，而不用排队等候。在 Windows 操作系统中，也有这方面的限制。在早期的服务器操作系统或者其他类型的操作系统中，往往只有单个 Smss.exe 实例。我们通过任务管理器可以看到这个进程。这个实例又叫作会话管理子系统，主要用来初始化每个会话，直到服务器中含有的处理器数量为 止。由于只有一个 Smss 实例，为此当有多个请求时，服务器必须按顺序来处理系统的请求。如果服务器上部署有多个应用程序，如 Oracle 数据库服务器、 邮件系统等等，这就可能会导致彼此之间相互干扰、冲突。不仅会降低应用程序的性能，而且也会影响其稳定性。

而如果实现并行会话技术的话，这种情况就有很大的改变。如在一个具有四个核心处理器的服务器上，可以运行 3 个客户会话同时登录服务器并以处理器所支持的速率运行应用程序。这也就是说，即使在这台服务器上同时部署有三个不同的应用程序，也不用担心严重的排队问题等等。

并行会话技术是 Windows2008 以及以后的服务器操作系统中自带的一种技术，不需要服务器 管理员进行额外的配置。其并行会话的数量是根据核心处理器的数量增减而变化的。通常情况下，其并性会话的数量为核心服务器的数量减去一。在一个服务器上部 署多个应用程序，或者说终端服务等应用，会从中受益。如果企业具有这种情况，那么建议大家赶快将服务器升级到 Windows2008，以提升应用程序的性 能，并提高服务器的稳定性。

四、Hyper-v 提升服务器虚拟化的能力与性能。

服务器的虚拟化越来越被管理员所重视。因为服务器的虚拟化能够提升服务器对不同应用程序的兼容性。而且当服务器上的应用程序比较多时，还可以通过虚拟化技术为不同的应用程序虚拟多个独立的环境，以避免相互之间的干扰，以提高服务器的稳定性。

虽然很早的时候就能够实现服务器的虚拟化，但是早期的虚拟化软件是一个独立于网络操作系统之外的应用软件，其在性能上和稳定性上都不是很理想。为此很少有服务器管理员会采用。

Hyper- v 在这方面有了比较大的改善。Hyper-v 在系统的硬件抽象层和操作系统之间提供了一个中间层。通过这个中间层可以在虚拟化环境中提供客户会话，以便直 接与系统的硬件层通信。由于这个技术不会受到主机操作系统的限制，客户绘画的执行速度就要比在以前的虚拟化环境中执行的速度快的多。简单的说，就是消除了 主机操作系统的瓶颈，从而提高更高的稳定性与性能。

通常情况下，当需要对服务器进行升级或者进行某个应用程序的测试时，可以先在服务器上搭建一个虚 拟化环境，来进行测试与评估。等到评估的结果比较理想时，再在服务器进行正式的部署。由于虚拟化环境与服务器本身的应用环境相对对立，为此测试评估对系统 原有的应用影响就非常的小。这么操作的话，就可以提高服务器的稳定性。

建议如果需要在 Windows 操作系统上实现虚拟化环境的话，那么管理员需要首选 Hyper-V。而不要采用其他的第三方虚拟化操作软件。两者在性能与稳定性上不可相提并论。

来源： IT 专家网