



服务器的硬件维护与软件维护

◎ 袁恩野

摘要: 计算机已经成为现代办公生活中不可缺少的工具之一,极大的提高了人们工作生活的便捷性。但是计算机的迅猛发展却对服务器管理提出了更高的要求。黑客以及病毒等外部入侵对服务器的安全造成了严重的威胁,因此只有做好服务器的维护工作,才能保障服务器的安全运行。本文将从硬件和软件两个方面对服务器的维护工作进行探索研究。

关键词: 服务器; 硬件维护; 软件维护

随着现代化信息技术的发展,互联网在人们的生活中得到了广泛的普及,基本上融入到了人们工作生活的方方面面。但是人们在享受互联网带来便利的同时,同样面临着来自外部的威胁。相对较为开放的网络服务器很容易在病毒和黑客的侵袭下出现安全漏洞,因此探究服务器的维护工作具有十分重要的意义。

1 服务器硬件维护的有效措施

1.1 对服务器储存设备进行扩充

服务器内存和硬盘的扩充是日常工作的一部分,但若是在扩充的过程中出现操作失误或是不规范的现象,则可能会对服务器带来一定的损伤,影响到服务器功能的发挥,严重的甚至会引发服务器死机的现象^[1]。基于此,在进行服务器扩充时,必须要对服务器原有内存和扩充内存之前的匹配性进行检查。同样的,在进行硬盘扩充前,也要实施一定的检查工作,检查的对象是硬盘的剩余空间、支架以及电源接口等,避免出现扩充用硬盘不兼容的现象。

1.2 对服务器硬件设备进行卸载或是更换

在对服务器进行维护的过程中,硬件设备卸载和更新是十分常见的一个环节,在具体操作的过程中同样需要严格按照相应的规范,以避免对服务器本身造成损害。在进行硬件设备卸载和更换前,要对服务器的重要程度进行明确,针对不同的机箱采取不同的工具,并详细了解掌握服务器修理的注意事项。同时,在卸载或是维修服务器时,要认真检查设备的连接线情况,全面了解设备的组成结构。此外,做好电源的检查,服务器硬件设备的卸载和更换必须在电源切断的状态下开展,同时还需检查服务器接地状况,避免静电对服务器硬件设备造成损害。

1.3 做好服务器硬件设备的除尘工作

服务器在长期运行的过程中,其机箱内部的设备表面通常都会积聚大量的灰尘,若是不及时处理,将会对服务器的散热效果造成影响,进而造成服务器的损伤。在进行服务器除尘工作时,为了避免灰尘进入到设备内部,必须使用专业的工具,如螺丝刀、镊子、吹风机等,在除尘作业时,工作人员必须做到小心谨慎,避免产生静电现象,对服务器和人员造成伤害^[2]。

2 服务器软件维护的有效措施

服务器软件维护主要针对的是软件开发或是实际运行中存在的错误,维护的目的是对这些错误进行修正,保障软件的正常运行。具体操作如下:

2.1 为服务器软件安装“补丁”程序

为了服务器产生漏洞,要定期对其进行升级,及时消除或是修改服务器产生的漏洞。这需要工作人员对服务器操作系统管网动态进行跟踪,若是发现系统系统升级或是补丁升级的动态,要及时下载并安装管网提供的更新包,对软件进行升级或是安装新版软件,如此才能为服务器的安装运行奠定坚实的基础。

2.2 做好服务器账号和密码的保护,对服务器系统日志进行定期监测

服务器账号和密码是进入服务器操作系统的重要工具,因此服务器

在遭受外部攻击时,首当其冲的就是其账号和密码。因此为了保障服务器的安全性,在设置账号和密码时,一定要尽可能的提升其复杂性,同时定期对密码进行修改,这样就可以最大程度的降低密码被盗的风险。一般情况下,密码应该采用数字、字母以及特殊符号混合的形式,且长度最好超过8个字符^[3]。此外,服务器维护管理人员还要对服务器系统日志进行定期监测分析,这样可以全面的掌握服务器的密码登录情况,便于异常情况的及时发现和控制。

2.3 及时关闭不必要的服务和端口

对于一些不再需要服务器的服务和端口,要及时进行关闭,这样可以空出大量的系统空间,提升系统的储存能力,降低安全隐患发生的风险。

2.4 在服务器系统中安装杀毒软件和防火墙

安装杀毒软件和防火墙可以有效地防止来自外部网络的攻击,将一些对互联网有伤害的病毒和恶意文件机械与计算机网络进行隔离,以此保障网络安全。在防火墙软件安装完成后,服务器管理人员要对防火墙的工作状态进行动态极监测,减少不必要的对外开放。即使是在对外开放的情况,可以要尽可能做到仅开放一个IP地址。同时,还要保障服务器的杀毒软件和特征码是最新的。为了避免新型病毒的入侵,管理人员应该将杀毒软件的病毒库设置为默认定期更新状态。同时,管理人员也可以通过手动操作向病毒库中添加新病毒类型,保障病毒库始终处于最新状态。一旦发现服务器的软件防火墙出现漏洞,要及时完成更新。

2.5 加强服务器数据库的服务维护

对于服务器数据库中储存的数据,管理人员要定期对数据库上的参数进行修改,使其运行始终处于优化状态下。同时,做好服务器数据库中数据的备份工作,这样即使因系统故障导致数据库中数据损坏或是丢失,也可以及时进行恢复。

2.6 加强操作系统和网络服务的安全维护

为了有效地防止网络黑客的入侵,服务器软件管理人员要对操作系统进行及时更新升级,及时通过不定填补漏洞。同时,管理人员可以通过系统日志查看是否存在异常记录,以便作出针对性调整。此外,互联网上存在多种服务,一旦服务器上网络出现混乱,必然会影响到服务器的安全运行,因此必须加强针对操作系统和网络服务的安全防护力度。

3 结语

综上所述,为了保障服务器的安全运行,应该从硬件维护和软件维护两个方面入手,分别采用合理有效地措施,保障服务器软件和硬件的安全,如此才能提高服务器安全管理水平,减少安全隐患的发生,为企业事业单位正常工作创造良好的条件。

(作者单位:大庆油田信息技术公司)

作者简介: 袁恩野(1982~),男,大学,技术员,研究方向为服务器硬件维护、服务器系统维护。

参考文献

- [1] 王晓东,牛霜霞,李赞,王云鹤,赵振恒.服务器的管理与维护[J].河南电力,2012(4):33-36.
- [2] 李晨.服务器的硬件维护与软件维护[J].硅谷,2012(23):175-176.
- [3] 韦杰.浅析服务器的管理与维护[J].广西轻工业,2011,27(6):64-66.