Linux系统服务器安全防护设置部署托管

产品名称	Linux系统服务器安全防护设置部署托管
公司名称	河南刘贵商务服务有限公司
价格	.00/件
规格参数	品牌:融河矩媒 服务项目:技术支持 发票:提供
公司地址	河南省南阳市卧龙区卧龙岗街道卧龙路经纬国际1号楼810（注册地址）
联系电话	13323693821 13140513661

产品详情

我们没有办法彻底解决网络安全问题，但可以不断加强防护，提高服务器的抵御能力。那么，我们要如何提升服务器的安全性呢?IT运维专家为大家提供了七个维护服务器安全的技巧。

IT技术可以说是一把双刃剑，为我们带来便捷的同时，也带来了威胁，网络安全问题就是其中之一。如今，随着黑客技术的发展，服务器被攻击的事件屡见不鲜，如何保障服务器安全是运维界广泛关注的问题。

我们没有办法彻底解决网络安全问题，但可以不断加强防护，提高服务器的抵御能力。那么，我们要如何提升服务器的安全性呢? IT运维专家为大家提供了七个维护服务器安全的技巧。

1. 从基本做起，及时安装系统补丁

不论是Windows还是Linux，任何操作系统都有漏洞，及时的打上补丁避免漏洞被蓄意攻击利用，是服务器安全比较重要的保证之一。

2. 安装和设置防火墙

现在有许多基于硬件或软件的防火墙，很多安全厂商也都推出了相关的产品。对服务器安全而言，安装防火墙非常必要。防火墙对于非法访问具有很好的预防作用，但是安装了防火墙并不等于服务器安全了。在安装防火墙之后，你需要根据自身的网络环境，对防火墙进行适当的配置以达到较好的防护效果。

3. 安装网络杀毒软件

现在网络上的病毒非常猖獗，这就需要在网络服务器上安装网络版的杀毒软件来控制病毒传播，同时，在网络杀毒软件的使用中，必须要定期或及时升级杀毒软件，并且每天自动更新病毒库。

4. 关闭不需要的服务和端口

服务器操作系统在安装时，会启动一些不需要的服务，这样会占用系统的资源，而且也会增加系统的安全隐患。对于一段时间内完全不会用到的服务器，可以完全关闭;对于期间要使用的服务器，也应该关闭不需要的服务，如Telnet等。另外，还要关掉没有必要开的TCP端口。

5. 定期对服务器进行备份

为防止不能预料的系统故障或用户不小心的非法操作，必须对系统进行安全备份。除了对全系统进行每月一次的备份外，还应对修改过的数据进行每周一次的备份。同时，应该将修改过的重要系统文件存放在不同服务器上，以便出现系统崩溃时(通常是硬盘出错)，可以及时地将系统恢复到正常状态。

6. 设置账号和密码保护

账号和密码保护可以说是服务器系统的第1道防线，目前网上大部分对服务器系统的攻击都是从截获或猜测密码开始。一旦黑客进入了系统，那么前面的防卫措施几乎就失去了作用，所以对服务器系统管理员的账号和密码进行管理是保证系统安全非常重要的措施。

7. 监测系统日志

通过运行系统日志程序，系统会记录下所有用户使用系统的情形，包括近来登录时间、使用的账号、进行的活动等。日志程序会定期生成报表，通过对报表进行分析，你可以知道是否有异常现象。

服务器安全问题是一个大问题，如果你不希望重要的数据被病毒或是黑客破坏，甚至被可能用这些数据来对付你的人窃取，那么本文介绍的安全小技巧可能会对你有所帮助。