详述WindowsServer2008安全部署的六个方面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_ti2020/566/2021_2022__E8_AF_A6_E8_BF_B0Wind_c100_566922.htm 出于安全性以及新的应用需求，现在越来越多的企业开始部署基于Windows Server 2008平台的服务器，甚至有些个人用户也在使用该系统。就笔者了解，面对一个相对陌生的Server系统，管理员们最关心的是实现系统平台的平滑过度以及如何进行安全部署。下面笔者结合自己的经验，从六个方面谈谈Windows Server 2008的安全部署。 1、安全部署从安装开始 要创建一个强大并且安全的服务器，必须从一开始安装的时候就注重每一个细节的安全性，当然Windows Server 2008的部署也不例外。新的服务器应该安装在一个孤立的网络中，杜绝一切可能造成攻击的渠道，直到操作系统的防御工作完成为止。在开始安装的最初的一些步骤中，我们将会被要求在FAT(文件分配表)和NTFS(新技术文件系统)之间做出选择。这时，大家务必为所有的磁盘驱动器选择NTFS格式。FAT是为早期的操作系统没计的比较原始的文件系统。NTFS是随着NT的出现而出现的，它能够提供了FAT不具备的安全功能，包括存取控制清单(Access Control Lists、ACL)和文件系统日志(File SystemJoumaling)，文件系统日志记录对于文件系统的任何改变。接下来，我们需要安装最新的Service Pack(SP2)和任何可用的热门补丁程序。虽然Service Pack中的许多补丁程序相当老了，但是它们能够修复若干已知的能够造成威胁的漏洞，比如拒绝服务攻击、远程代码执行和跨站点脚本。 2、通过SCW配置安全策略 安装完系统之后，我们就可以坐下来做一些更细致的安全工作

。提高Windows Server 2008免疫力最简单的方式就是利用服务器配置向导(Server Configuration Wizard即SCW)进行安全部署。它可以指导我们根据网络上服务器的角色创建一个安全的策略。 (1).SCW的安装 需要说明的是，SCW与配置服务向导(Configure Your Server wizafd)是不同的。SCW不安装服务器组件，但监测端口和服务，并配置注册和审计设置。SCW并不是默认安装的，所以我们必须通过“ 控制面板 ”的“ 添加/删除程序 ”窗口来添加它。选择“ 添加/删除Windows组件 ”按钮并选择“ 安全配置向导 ”，安装过程就自动开始了。一旦安装完毕，SCW就可以从“ 管理工具 ”中访问。 (2). 用SCW配置安全策略 通过SCW创建的安全策略是XML文件格式的，可用于配置服务、网络安全、特定的注册表值、审计策略，甚至如果可能的话，还能配置IIS。通过配置界面，可以创建新的安全策略，或者编辑现有策略，并将它们应用于网络上的其它服务器上。如果某个操作创建的策略造成了冲突或不稳定，那么我们可以回滚该操作。 可以说，SCW涵盖了Windows Server 2008安全性的所有基本要素。运行该向导，首先出现的是安全配置数据库(security Configuration Database)，其中包含所有的角色、客户端功能、管理选项、服务和端f1等等信息。SCW还包含广泛的应用知识知识库。这意味着当一个选定的服务器角色需要某个应用时客户端功能比如自动更新或管理应用比如备份Windows防火墙就会自动打开所需要的端口。当应用程序关闭时，该端口就会自动被阻塞。网络安全设置、注册表协议以及服务器消息块(ServerMessage Block、SMB)签名安全增加了关键服务器功能的安令性。对外身份验证(Outbound Authentication)设置决

定了连接外部资源时所需要的验证级别。 SCW的最后一步与审计策略有关。默认情况下，WindowsServer 2008只审计成功的活动，但是对于一个加强版的系统来说，成功和失败的活动都应该被审计并记入日志。一旦向导执行 完成后，所创建的安伞策略就保存在一个XML中，并且立刻就能被服务器所使用，或者供日后使用，甚至还能被其它服务器使用。在服务器安装过程中没有进行第一步强化过程的服务器也能安装SCW。 3、数据存取权限的控制 (1).设置服务器的开机顺序 可以说，从我们按下服务器的电源按钮那一刻开始，直到操作启动并且所有服务都活跃之前，威胁系统的恶意行为依然有机会破坏系统。除了操作系统以外，一台健康的服务器开始启动时应该具备密码保护的BIOS/固件。此外，就BIOS而言，服务器的开机顺序应当被正确设定，以防从未经授权的其它介质启动。 在启动后，进入BIOS设置页面。我们可以使用组合键在BIOS的各个设置标签上来回移动。在启动顺序(Boot Order)标签页上，设置服务器启动首选项为内部硬盘(Internal HDD)。在系统安全(Boot Order)标签页上，硬盘密码有三种选项可供选择：Primary、Administratortive和Hard。 (2).管理好自动运行 自动运行外部介质的功能包括光碟、DVD和USB驱动器，应该被禁用。在注册表，进入路径HKEY_LOCAL_MACHINE\SYSTEM \CurrentControl\Set\Services\Cdrom(或其他设备名称)下，将Automn的值设置为0。自动运行功能有可能自动启动便携式介质携带的恶意应用程序。这是安装特洛伊木马(Trojan)、后门程序(Backdoor)、键盘记录程序(KeyLogger)、窃听器(Listener)等恶意软件的一种简单的方法。 (3).选择用户登录方

式 下一道防线是有关用户如何登录到系统。虽然身份验证的替代技术。比如生物特征识别、令牌、智能卡和一次性密码，都是可以用于Windows Server 2008用来保护系统，但是很多系统管理员，无论是本地的还是远程的，都使用用户名和密码的组合作为登陆服务器的验证码。不过很多时候，他们都是使用缺省密码。这显然是自找麻烦。 上面这些注意点都是很显然的。但是，如果我们非要使用密码的话，那么最好采用一个强壮的密码策略：密码至少8个字符那么长。包括英文大写字母、数字和非字母数字字符：此外，我们最好定期改变密码并在特定的时期内不使用相同的密码。一个强壮的密码策略加上多重验证(Multifactor Authentication)，这也仅仅只是一个开始。多亏了NTFS提供的ACL功能，使得一个服务器的各个方面，每个用户都可以被指派不同级别的访问权限。文件访问控制打印共享权限的设置应当基于组(Group)而不是“ 每个人(Everyone) ”。这在服务器上是可以做到的，或者通过 Active Directory。确保只有一个经过合法身份验证的用户能访问和编辑注册表，这也很重要。这样做的目的是限制访问这些关键服务和应用的用户人数。 4、基于账户、端口、服务等限制 (1).账户安全控制 在安装过程中，三个本地用户帐户被自动创建管理员(Administrator)、来宾(Guest)、远程协助账户(Help Assistant，随着远程协助会话一起安装的)。管理员帐户拥有访问系统的最高权限。它能指定用户权限和访问控制。虽然这个主帐户不能被删除，但是我们应该禁用或给它重新命名，以防被轻易就被黑客盗用而侵入系统。正确的做法是，我们应该为某个用户或一个组对象指派管理员权限。这就使得黑客更难判断究竟哪个用户拥有管理员权限。这

对于审计过程也是至关蓖要的。想象一下，如果一个部门的每一个人都可以使用同一个管理员账户和密码登录并访问服务器，这是一个多么重大的安全隐患啊。因此，笔者建议最好不要使用管理员帐户。同样地，来宾账户和远程协助账户为那些攻击Windows Server 2008的黑客提供了一个更为简单的目标。进入”控制面板”→”管理工具”→”计算机管理”，右键单击我们想要改变的用户帐户，选择”属性”，这样我们就可以禁用这些账户。务必确保这些账户在网络和本地都是禁用的。 (2).关闭危险的端口 开放的端口是最大的潜在威胁，Windows Server 2008有65535个可用的端口，而我们的服务器并不需要所有这些端口。SPl中包含的防火墙允许管理员禁用不必要的TCP和UDP端口。所有的端口被划分为三个不同的范围：众所周知的端口(0～1023)、注册端口(1024～49151)、动态，私有端口(49152～65535)。众所周知的端口都被操作系统功能所占用.而注册端u则被某些服务或应用占用。动态/私有端门则是没有任何约束的。 如果能获得一个端口和所关联的服务和应用的映射清单，那么管理员就可以决定哪些端口是核心系统功能所需要的。举例来说，为了阻止任何 Telnet或FTP传输路径，我们就可以禁用与这两个应用相关的通讯端口。同样地，知名软件和恶意软件使用那些端口都是大家所熟知的，这些端口可以被禁用以创造一个更加安全的服务器环境。最好的做法是关闭所有未用的端口。要找到服务器上的那些端口是开启状态、监听状态还是禁用状态，使用Nmap工具是一个比较简单高效的方式，默认情况下，SCW关闭所有的端口，当设定安装策略的时候再打开它们。 (3).管理好各种服务 增强服务器免疫力最有效的方法是不

安装任何与业务不相关的应用程序，并且关闭不需要的服务。虽然在服务器上安装一个电子邮件客户端或管理工具可能会使管理员更方便，但是， 如果不直接涉及到服务器的功能，那么我们最好不要安装它们。在Windows Server2008上，有100多个服务可以被禁用。举例来说，最基础的安装包含DHCP服务。不过，如果我们不打算利用该系统作为一个DHCP服务器，禁用tcpsvcs.exe将阻止该服务的初始化和运行。希望大家记住，并非所有的服务都是可以禁用的。举例来说，虽然远端过程调用(Remote Procedure Call、RPC)服务可以被Blaster蠕虫所利用，进行系统攻击。不过它却不能被禁用，因为RPC允许其它系统过程在内部或在整个网络进行通讯。为了关闭不必要的服务，我们可以通过“ 控制面板 ”的“ 管理工具 ”打开“ 服务 ”管理工具进行管理。双击对于的服务，打开“ 属性 ”对话框，在“ 启动类型框 ”中选择“ 禁用 ”即可。 5、创建健壮的审计和日志策略 阻止服务器执行有害的或者无意识的操作，是强化服务器的首要的目标。为了确保所执行的操作是都是正确的并且合法的。那么就得创建全面的事件日志和健壮的审计策略。通过一致性的约束，强大的审计策略应该是健壮的Windows Server 2008服务器的一个重要组成部分。成功和失败的帐户登录和管理尝试，连同特权使用和策略变化应该被审核的记录。 在Windows Server2008中。创建的日志类型有：应用日志、安全日志、目录服务日志、文件复制服务(File Replication Service)日志和DNS服务器日志。这些日志都可以通过事件查看器(Event Viewer)临测。同时事件查看器还提供广泛的有关硬件、软件和系统问题的信息。在每个日志条目里，事件查看器显示五

种类型的事件：错误、警告、信息、成功审计和失败审计。 6、其他安全部署措施 (1).未雨绸缪，进行基线备份 在我们花费了大量时间和精力强化你的Windows Server 2008服务器时，大家所要做的最后一步是创建一个0/full级别的机器和系统状态备份。一定要对系统定期进行基线备份，这样当有安全事故发生时，我们就能根据基线备份对服务器进行恢复。可以说，基线备份就是服务器的 ” 还魂丹 ” 。在对Windows Server 2008服务器的主要软件和操作系统进行升级后，务必要对系统进行基线备份。 (2).密切关注用户帐户 为了确保服务器的安全性，还需要密切注意用户帐户的状态。不过，管理帐户是一个持续的过程。用户帐户应该被定期检查，并且任何非活跃的、进行复制、共享的一般或测试账户都应该被删除。 (3).确保及时打上最新的系统补丁 强化服务器补丁是一个持续的过程，并不会因为安装了Windows Server 2008 SP2而结束。为了第一时间安装服务期升级/补丁软件，我们可以通过 “ 系统菜单 ” 中的 “ 控制面板 ” 启用 “ 自动更新功能 ” 。在 “ 自动更新 ” 选项卡上，选择 “ 自动下载更新 ” 。因为关键的更新通常要求服务器重新启动，大家可以给服务器设定一个安装这些软件的计划任务，从而尽可能小地影响服务器的正常运行。 总结：以上六个方面是笔者在Windows Server 2008学习以及实战部署中总结的一些经验，希望能够帮助到你们。 